Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri

Análisis de Big Data y compliance anticorrupción Cuestiones críticas de la práctica actual y escenarios futuros

Big Data Analytics and Anti-corruption Compliance Critical Issues of Current Practice and Future Scenarios

Emanuele Birritteri
Dottorando di ricerca in Diritto e Impresa presso l'Università LUISS "Guido Carli"
ebirritteri@luiss.it

compliance, e-compliance, corruzione, responsabilità da reato degli enti collettivi, pubblica amministrazione

Privacy, *Ne bis in idem*

compliance, e-compliance, corruption, corporate criminal liability, public administration

Abstracts

L'articolo analizza il tema dell'utilizzo di tecniche di *big data analytics* nelle attività di *compliance* anticorruzione nei settori pubblico e privato, evidenziando come tali nuove prassi possano trasformare le caratteristiche attuali della prevenzione del rischio reato nelle organizzazioni complesse. Vengono evidenziati vantaggi e rischi derivanti dall'adozione di questi strumenti informatici, nonché alcuni ipotetici scenari futuri legati alla possibilità di regolamentare in via legislativa l'utilizzo di simili sistemi di *compliance* anche per fini diversi dalla mera gestione del rischio.

El presente artículo analiza la utilización de técnicas de big data en las actividades de compliance anticorrupción en el sector público y privado, evidenciando cómo tales prácticas pueden transformar las características actuales de la prevención del riesgo de delitos en las organizaciones complejas. Se destacan las ventajas y riesgos derivados de la adopción de estos instrumentos informáticos, así como algunos hipotéticos escenarios futuros ligados a la posibilidad de regular por vía legislativa el uso de estos sistemas de compliance, incluso para fines diversos de la mera gestión del riesgo.

This paper addresses the issue of implementation of big data analytics techniques in public and private anti-corruption compliance, highlighting how this new practice can transform the current features of crime-risk prevention activities. The work is aimed at showing the potential benifit and risks related to the adoption of these digital tools, as well as hypothetical future scenarios, including the perspective of regulating the use of such compliance systems also for purposes other than the risk management.

Sommario

1. Nuove tecnologie e contrasto alla corruzione: verso una metamorfosi della *compliance*.

Al giorno d'oggi sia le pubbliche amministrazioni che le imprese private (specie se di notevoli dimensioni) devono fare i conti con una notevole mole di dati eterogenei e prodotti in tempo reale[1]. Tale tipologia di dati (i c.d. *big data*[2]) proprio per queste caratteristiche non possono essere gestiti attraverso le tradizionali metodologie di archiviazione e analisi, ma necessitano inevitabilmente dell'ausilio delle nuove tecnologie[3].

Ben si comprende, quindi, come ciò possa rappresentare un rilevante problema di *governance* per i soggetti coinvolti.

Tuttavia, 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[4].

Insomma, quello che sta iniziando ad emergere in via embrionale è che la gestione dei dati più che rappresentare un problema può in realtà divenire un'interessante opportunità per i settori pubblico e privato, 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, al di là dell'esistenza di obblighi cogenti[5].

E 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 e esterni all'impresa, in particolare in una triplice direzione : 1) identificare indicatori di anomalia e rischio corruzione, nonché ulteriori segnali d'allarme nelle operazioni aziendali (in particolare azioni anomale rispetto ai modelli di comportamento che il sistema qualifica come ricorrenti/ordinari); 2) monitorare il traffico *mail* interno, allo scopo di individuare conversazioni in cui si utilizzino determinate parole chiave considerate "a rischio"; 3) 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*)[6].

[1] Al riguardo si veda Buttarelli (2017), p. 31 ss.

[2] La letteratura al riguardo è vasta. Per ulteriori approfondimenti sul tema si vedano, senza pretesa di esaustività: Falcone (2017), p. 601 ss.; Zeno-Zencovich (2018), p. 1 ss.; Ponte (2017), p. 31 ss.; Di Porto (2016), p. 5 ss.; Pitruzzella (2016), p. 15 ss.; Ottolia (2017), *passim*; Wachter e Mittelstadt (2019), p. 1 ss.; Levy (2013), p. 73 ss.; Colajanni (2017), p. 79 ss.

[3] Cfr. sul punto il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, *L'intelligenza artificiale al servizio del cittadino,* p. 52, ove si evidenzia che «…pur rappresentando una miniera di informazioni, i dati hanno bisogno di strumenti adeguati per poter essere sfruttati in tutto il loro potenziale. In particolare, servono modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise».

[4] V. anche Hughes Parker (2014), p. 1 ss.

[5] Sul tema specifico della corruzione v.: Severino (2019), p. 1 ss., la quale evidenzia al riguardo che «…una delle sfide già intraprese e che caratterizzeranno gli anni a seguire sarà quella di favorire il più possibile lo scambio di esperienze e buone prassi tra mondo pubblico e privato, dovendosi comprendere come siano esattamente comuni le sfide, le strategie e gli obiettivi da raggiungere per creare un mondo economico veramente competitivo e che sappia affrontare con successo i nuovi rischi della modernità»; Gullo (2017), p. 93 ss.

[6] Va rilevato come il tema al centro della presente analisi, in considerazione della sua novità, non sia ancora stato oggetto di attenzione in letteratura rispetto ai risvolti di carattere penalistico legati all'uso di tali sistemi, avendo piuttosto suscitato l'attenzione dei professionisti operativi della *compliance* rispetto alle potenzialità applicative di questi strumenti. Per una panoramica di tali procedure applicative nella prassi aziendale si vedano, *ex multis*: Olsen *et al.* (2016), p. 1 ss.; Daniels *et al.* (2018), p. 1 ss.
Si veda altresì il rapporto di gennaio 2014 dello *EY Center for Board Matters*, p. 7 ss.: *The bar is raised: anti-corruption compliance now requires big data analytics*. Una ricognizione dei *software* attualmente presenti sul mercato nel settore della c.d. *RegTech*, inoltre, è stata effettuata da *Deloitte*

I *red flag* oggetto di attenzione sono davvero 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'ente[7].

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 – mediante l'incrocio di svariati dati provenienti dalle fonti più disparate (da documenti di polizia a *social network*) – aree territoriali in cui vi è maggiore probabilità di attività delittuose[8] o di aiutare gli inquirenti a selezionare, tra milioni di file, quelli più "promettenti" per l'indagine[9]; 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*[10].

Le straordinarie potenzialità e la versatilità 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[11].

Ben poco però si è, sino ad ora, riflettuto sulla possibilità che lo sviluppo di tali procedure possa portare a una vera e propria metamorfosi del volto attuale della *compliance* pubblica e privata: da un sistema che ruota attorno alle classiche attività umane di analisi e indagini preventive "sul campo", a un sistema (parzialmente o integralmente) 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, ad 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[12].

L'obiettivo del lavoro è quindi quello di indagare le potenzialità (e per converso i rischi) legati alla possibile importazione di tali strumenti di *compliance* anticorruzione nella realtà italiana pubblica e privata, delineando, nella parte conclusiva, alcune linee di futuro sviluppo di questi sistemi.

2. *Big Data Analytics* e prevenzione della corruzione nelle pubbliche amministrazioni: quali prospettive?

Prendendo le mosse dalla possibile adozione di questi sistemi in ambito pubblico, e immaginando, in particolare, una loro applicazione nei piani triennali di prevenzione della corruzione delle amministrazioni (nati, come noto, dalla volontà di innervare anche nella P.A.

ed è consultabile al seguente link: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html#.

[7] Per una panoramica di alcuni di tali *red flags* v.: Berliner e Dupuy (2018), p. 3 ss.; Gee (2015), p. 243 ss.

[8] Sul punto, in particolare, v.: Bonfanti (2018), p. 1 ss.; Kraft (2017), p. 249 ss.

[9] Il riferimento è qui al *software* di intelligenza artificiale denominato RAVN, che ha aiutato il *Serious Fraud Office* britannico a risolvere il noto caso di corruzione c.d. *Rolls-Royce*, strutturando un sistema informatico in grado di indicizzare, sintetizzare e individuare i file più promettenti tra centinaia di migliaia di documenti di rilevanza investigativa, riducendo in modo estremamente significativo il lavoro di analisi degli inquirenti (si veda in particolare un articolo pubblicato al riguardo sul sito del *Financial Times*, www.ft.com, dal titolo: *SFO expected to promote Ravn's crime-solving AI robot*).

[10] Cfr. sul punto, anche per ulteriori approfondimenti: Gialuz (2019), p. 1 ss.; Parodi e Sellaroli (2019), p. 47 ss.

[11] Esistono, peraltro, esempi di applicazione di tali strumenti anche per la prevenzione di illeciti in tema di *market abuse*, nonché in materia ambientale. Per una panoramica al riguardo si vedano: Dombalagian (2016), p. 1 ss.; Glicksman *et al.* (2017), p. 41 ss. Per una compiuta analisi dei legami tra intelligenza artificiale e abusi di mercato v. Consulich (2018), p. 195 ss. Rispetto alle attività della *Securities and Exchange Commission* degli Stati Uniti al riguardo si veda White (2016), p. 1 ss.

[12] V., in particolare, Cariola (2019). Più in generale, per un'analisi delle connessioni tra corruzione, *blockchain* e *bitcoin* v. Kossow *et al.* (2018), p. 1 ss.

l'esperienza dei *compliance program* 231[13]), a nostro avviso un primo problema è quello della qualità e dell'attendibilità dei dati posti al centro dell'analisi informatica[14].

Rispetto a questi modelli, infatti, non esistono *software* dal funzionamento standard, essendo il singolo ente (pubblico o privato) a decidere quali istruzioni dare e quali analisi far svolgere al sistema e, soprattutto, quali dati (interni ed esterni all'ente) far confrontare alla macchina[15].

Un aspetto essenziale delle prassi in esame, infatti, è dato dall'assenza di regolamentazioni pubblicistiche – a livello interno, così come sovranazionale e in seno ad ordinamenti stranieri – sull'utilizzo di queste procedure[16], cosicché ciascuna organizzazione ha assoluta libertà nello strutturare, come meglio crede, siffatti sistemi.

Da qui dunque un primo, delicato, problema che si sta imponendo nei diversi campi di utilizzo dell'AI: la provenienza dei dati da fonti affidabili e sicure. Solo su questo presupposto, infatti, i fattori di rischio che i *big data analytics system* identificano possono essere credibili. È di agevole intuizione, del resto, che usare in questi processi d'analisi l'intera quantità dei dati presenti in Internet rischia di produrre un risultato fuorviante, sicché assicurare una corretta e credibile formazione della base d'indagine appare essenziale (e ciò ovviamente vale anche per le attività private di *compliance*)[17].

Per le amministrazioni pubbliche, peraltro, un simile obiettivo non può dirsi così complesso come all'apparenza potrebbe sembrare. Le nostre amministrazioni, infatti, possiedono uno straordinario patrimonio informativo composto da atti pubblici di varia natura e di intrinseca affidabilità (stante, appunto, la loro natura pubblicistica), nonché diverse banche dati – come, ad esempio, quella degli appalti pubblici – i cui contenuti si rivelano preziosi per individuare possibili *red flag* di interesse per la prevenzione della corruzione[18].

Ciò che spesso manca è appunto la capacità professionale e tecnica di mettere in correlazione tali dati (nonché di stabilire meccanismi di connessione tra le diverse banche dati pubbliche), così pure di processare i loro contenuti; questo è però un problema rispetto al quale tali *software* di *big data analytics* offrono una soluzione[19].

A quel punto, chiaramente, resterebbe il non trascurabile tema di costruire metodologie di indagine informatica il più possibile affidabili, complete e ispirate alle migliori *best practice* nel campo dell'individuazione e della gestione del rischio reato/corruzione[20].

A queste condizioni, ci sembra che l'impiego di tali strumenti nel settore pubblico andrebbe incoraggiato: le pubbliche amministrazioni potrebbero identificare e gestire con maggiore efficienza situazioni di rischio, migliorando i propri piani triennali anticorruzione. Proprio perché, partendo dalla predetta (estremamente affidabile) base di dati, le capacità computazionali del sistema di processare tali informazioni appaiono in grado di identificare il rischio corruzione (in termini di anomalie statistiche e gestionali) in modo estremamente efficace e completo, sottoponendo ad analisi una base di dati e operazioni non analizzabile – per la sua

[13] Sul punto si vedano, per tutti: Severino (2019), p. 1 ss.; Severino (2016a), p. 7, che evidenzia come «…la logica del Piano Nazionale Anticorruzione e poi dei singoli piani anticorruzione delle diverse amministrazioni nonché l'individuazione di un responsabile anticorruzione riflettono da vicino quella dei modelli di organizzazione, gestione e controllo sperimentati nel campo delle persone giuridiche. Si vuole con ciò rafforzare anche nella pubblica amministrazione l'etica della responsabilità e spingere la struttura organizzativa a dotarsi delle cautele e dei presidi necessari a minimizzare il rischio reato. Un percorso nuovo e stimolante che dovrebbe condurre la pubblica amministrazione a essere attrice del processo di prevenzione della corruzione»; Gullo (2018), p. 39, il quale rileva al riguardo che «…la filosofia di fondo è stata quella di coinvolgere i funzionari pubblici in un approccio proattivo alla lotta alla corruzione, costruendo meccanismi di gestione che possano consentire di operare individuando il rischio e predisponendo cautele dirette a minimizzarlo».

[14] Sull'importanza di tali aspetti v., in via generale rispetto ai sistemi giudiziari, anche la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, elaborata dalla *European Commission for the Efficiency of Justice* (CEPEJ), p. 8 ss.

[15] 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, ove si legge che «…*if further must be considered that designers of algorithmic systems have varying levels of discretion when deciding, for instance, what training data to use or how to respond to false positives, and that the power of the operator of the algorithm may lie in his or her knowledge of the structure of the data set, rather than in insight into the exact workings of the algorithms*».

[16] Sul tema dei legami tra *compliance* e nuove tecnologie e sui problemi connessi alla mancanza di una sufficiente regolazione del settore, si veda, per tutti, Laufer (2017), p. 71 ss.

[17] Più in generale, sul punto, v. la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, cit., p. 10.

[18] In argomento, in particolare, v. per approfondimenti Falcone (2017), p. 617 ss.

[19] Sul punto, ancora, Falcone (2018), p. 105, il quale peraltro evidenzia come l'organizzazione ragionata e funzionale dei dati sia fondamentale per prevenire la corruzione e in particolare per farlo utilizzando sistemi di *big data analytics*.

[20] A quest'ultimo riguardo, del resto, un grande ausilio è offerto dai diversi strumenti di standardizzazione e supporto alle imprese esistenti in materia di indagini e strutturazione di *compliance program* anticorruzione. Per una panoramica delle *best practice* di costruzione di tali modelli v., in particolare, Giavazzi *et al.* (2014), p. 125 ss.

impressionante mole – nemmeno da un nutrito *team* di esperti[21].

Ciò anche in considerazione della tendenza ad allargare il perimetro della prevenzione amministrativa della corruzione che, come noto, tende ad avere ad oggetto non soltanto l'identificazione di comportamenti di possibile rilevanza penale, ma anche più semplicemente mere ipotesi di *maladministration*. E allora l'identificazione in via informatica di scostamenti dai prezzi standard di settore, eccessi di spesa, anomalie nelle caratteristiche degli appalti e altri *red flags* può diventare un formidabile strumento per eliminare sprechi e combattere inefficienze anche non necessariamente legati a condotte illecite[22].

Certo incentivare (se non addirittura obbligare) le pubbliche amministrazioni a utilizzare questi strumenti ha un costo notevole e rischia di essere controproducente in alcune realtà medio-piccole che già oggi faticano ad essere *compliant* con la normativa nazionale anticorruzione[23].

Al netto però di questo, si dovrebbe riflettere su una regolamentazione ragionata. A quali condizioni, e attraverso quali soluzioni operative, si avrà modo di chiarire non appena soffermeremo la nostra attenzione sul versante delle organizzazioni di matrice privatistica.

Va detto, del resto, che in Italia, da tempo, l'Autorità Nazionale Anticorruzione sta definendo innovative metodologie volte alla costruzione di indicatori di rischio corruzione[24] e, in questa prospettiva, va segnalata la recente adesione dell'ANAC a un contratto quadro per l'implementazione di modelli informatici per l'analisi di *big data*[25].

3. *Big Data Analytics* e *compliance* anticorruzione nel settore privato: categorizzazione e risvolti dogmatico-applicativi delle attuali prassi operative.

Volgendo adesso lo sguardo al settore della *compliance* anticorruzione privata riteniamo che – al di là del già menzionato profilo relativo all'attendibilità dei dati posti alla base dell'analisi – siano identificabili alcuni temi principali.

Innanzi tutto, come visto, 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[26].

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* (come si anticipava, peraltro, ciò può valere *mutatis mutandis* anche laddove si pensi a una applicazione di tali meccanismi nel settore pubblico)[27].

Queste analisi informatiche dei dati, infatti, potranno essere soltanto strumenti di analisi e valutazione (e *non* anche di gestione) del rischio ove l'ente decida di condurle sulla base di una logica *ex post*, sottoponendo cioè semplicemente a revisione il proprio patrimonio infor-

[21] Su tali aspetti v. anche Trapani (2018), p. 10 ss.

[22] Sul tema della *maladministration* v., per tutti, Cantone (2017), p. 4, che evidenzia sul punto l'esistenza di «…un mutamento di prospettiva per cui diventano rilevanti situazioni nelle quali il rischio è meramente potenziale, il conflitto di interessi "apparente", ma in presenza delle quali è necessario entrino in gioco misure di "allontanamento" dal rischio, con scelte che talvolta prescindono completamente dalle condotte individuali».

[23] Non a caso, con la delibera n. 1074 del 21 novembre 2018 l'Autorità Nazionale Anticorruzione ha individuato ulteriori modalità semplificate di applicazione degli obblighi in materia di pubblicità, trasparenza e prevenzione della corruzione per i piccoli comuni – oltre a quelle già identificate nel Piano Nazionale Anticorruzione del 2016 – in attuazione dell'art. 3, comma 1-ter, del d.lgs. n. 33 del 2013 (introdotto dal d.lgs. n. 97 del 2016) in base al quale l'ANAC, con il PNA, può prevedere misure di semplificazione per i comuni con popolazione inferiore ai 15.000 abitanti.

[24] Si veda, in particolare, lo studio pubblicato nel gennaio del 2018 dall'Autorità Nazionale Anticorruzione dal titolo: *Efficienza dei contratti pubblici e sviluppo di indicatori di rischio corruttivo*. Il lavoro è reperibile sul sito dell'Autorità (www.anticorruzione.it).

[25] Cfr. la Determina a contrarre del 5 giugno 2018, a firma del Segretario Generale dell'Autorità, con cui l'ANAC ha disposto l'adesione al contratto quadro Consip per l'affidamento dei Servizi di interoperabilità dati e cooperazione applicativa, finalizzati, tra l'altro, a sviluppare meccanismi per l'integrazione e la gestione di *Big Data*. Il documento è reperibile sul sito dell'Autorità (www.anticorruzione.it).

[26] Cfr. lo studio del Consiglio d'Europa, dal titolo: *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, cit., p. 6.

[27] Come si rilevava pocanzi, la dottrina non si è ancora occupata di "incasellare" queste prassi nelle categorie generali della disciplina della responsabilità da reato degli enti collettivi. Per una panoramica delle possibilità di utilizzo di questi sistemi, tuttavia, oltre ai contributi pocanzi citati, si veda il rapporto pubblicato dal *Deloitte Center for Regulatory Strategy* (*Americas*) nel 2017, dal titolo: *Compliance modernization is no longer optional. How evolved is your approach?*

mativo (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[28].

In tali casi, invero, l'anomalia documentale verrebbe rilevata in un momento in cui la procedura di formazione della volontà dell'ente si è conclusa. In una fase, quindi, in cui l'eventuale corruzione si è già consumata – con il conseguente radicamento della responsabilità da reato dell'ente.

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 non già su valutazioni di massima o controlli a campione, ma 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[29] (in grado di identificare modelli di comportamento anomali e correlazioni tra informazioni non individuabili sulla base della sola valutazione dell'uomo)[30].

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[31].

Come visto, infatti, in tal caso le esigenze di gestione del rischio non verrebbero rilevate sulla base delle tradizionali attività di indagine empirica gestite da *team* di esperti, ma, al contrario, sulla base di 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 (se non sempre) non identificabili altrimenti[32].

Tali meccanismi, peraltro, consentono di allocare efficacemente i costi della *compliance* verso i settori di attività dell'ente che più necessitano di attenzione in tal senso, evitando lo spreco di risorse[33].

Ma, 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[34], 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

[28] In argomento v. anche Pitaro (2018), p. 1 ss.

[29] Sul tema, in generale, della rilevanza giuridico-penale dell'automazione quale strumento di sostituzione dell'attività dell'uomo v., per tutti, Picotti (2019), p. 43 ss., secondo il quale al riguardo occorre muovere dalla premessa che la specifica qualità tecnica dell'informatica che interesse il penalista è costituita «…dall'*automazione* dei trattamenti o processi di elaborazione dei dati, secondo *programmi* specifici, che consentono di pervenire, con l'esecuzione di appositi ed evoluti algoritmi, a risultati *complessi* e straordinariamente più *precisi*, in tempi infinitamente più *rapidi* rispetto a quelli conseguibili con l'attività dell'uomo in carne ed ossa». Per una visione critica sull'automazione nel settore legale v. Pasquale (2019), p. 1 ss.

[30] In generale, sul tema della costruzione di un *fraud data analytics plan* nell'ambito del contrasto alla corruzione v. Vona (2017), p. 269 ss. (e, con riferimento specifico al settore del *procurement*, p. 247 ss.). In argomento v. anche Zwiebel (2017), p. 1 ss.

[31] Su tale aspetto v., per tutti: Severino (2016b), p. 76, la quale evidenzia al riguardo che «…in assenza di indicazioni vincolanti e specifiche, la valutazione di idoneità del modello è interamente rimessa alla discrezionalità del giudice, alla sua sensibilità e conoscenza dei meccanismi aziendali ed economici, alla corretta applicazione di quel complesso e delicato giudizio (*ex post*) che riguarda la tenuta (*ex ante*) del modello. In tale contesto appare evidente che senza un impegno da parte del legislatore non sembra facile assicurare la necessaria uniformità applicativa in materia e il saldo ancoraggio del modello alla sua vocazione «premiale», al riparo il più possibile dal rischio di sconfinamenti nella logica del «senno di poi» - che vede la verificazione del reato come una spia dell'inidoneità del modello, in particolar modo quando a venire in gioco è l'agire dei soggetti apicali»; Manacorda (2017), p. 71 ss.

[32] Sul tema, in generale, dell'importanza del *risk assessment* nella costruzione dei modelli organizzativi v. Piergallini (2013), p. 843.

[33] Cfr., in particolare, il rapporto pubblicato da *Deloitte* dal titolo: *Compliance modernization is no longer optional. How evolved is your approach?*, cit., p. 5.

[34] Sulla costruzione dei protocolli di gestione v. per tutti, ancora, Piergallini (2013), cit., p. 845 ss.

partner/agente commerciale (specie per affari all'estero rispetto ai quali può esistere un rischio di corruzione internazionale)[35].

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 (alla luce della peculiare diffusione del controllo su ogni dato aziendale e della necessità di aggirare un sistema informatico molto articolato e protetto da sofisticate misure di sicurezza)[36]. 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 predetto 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[37].

Ancora, in termini più generali si è rilevato come l'automazione della *compliance* potrebbe dar luogo ad una modifica della base fattuale (umana e non anche o solo tecnologica) su cui oggi si basa la responsabilità da reato degli enti collettivi, 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'ente si limita ad utilizzare, senza esserne l'autore[38].

L'effettiva messa in atto di alcune di queste pratiche di sorveglianza generalizzata apre poi l'ulteriore profilo – che qui può essere solo accennato – dell'eventuale ammissibilità di simile procedure rispetto alla disciplina dei controlli sui lavoratori[39], 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 *mail* dei dipendenti (pubblici o privati)[40].

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[41],

[35] Uno dei software più diffusi al riguardo sul mercato, in particolare, è il sistema CERICO, oggi offerto da *Dow Jones Risk & Compliance* (www.dowjones.com), che effettua una valutazione su svariati dati, alcuni dei quali offerti direttamente dall'agente di cui deve valutarsi l'affidabilità, assegnando in *real time* un determinato tasso di rischio all'operazione commerciale e consentendo così al *management* di decidere se intraprendere o meno l'affare. Un altro sistema molto diffuso è il software WORLD CHECK della *Thomson-Reuters* (www.risk.thomsonreuters.com/products/world-check), che compara dati – correggendo anche tutti i possibili falsi positivi – provenienti da svariati fonti pubbliche (come giornali e media in generale, tribunali, siti web governativi) al fine di valutare i rischi legali e reputazionali che l'impresa può correre intraprendendo una certa operazione, anche affidandosi a determinati agenti. Si analizzi anche, al riguardo, l'*Enterprise Legal Risk Management Framework*, su cui v. Apollon (2017), p. 486 ss.

[36] Sul tema dell'elusione fraudolenta si veda, per tutti, il lavoro monografico di Tripodi (2013), *passim*.

[37] Cfr., in particolare, Manacorda (2017), cit., p. 68, il quale rileva che, riferendosi al tema dell'efficace attuazione, il legislatore «…ha inteso rimarcare che l'onere di auto-organizzazione in chiave prevenzionistica non deve rimanere meramente cartolare, negando la valenza esimente ad un modello che, per quanto adottato correttamente, non sia ritenuto essere sorretto da impegni, procedure e sforzi adeguati. Si tratta di un'esigenza più che comprensibile, la quale introduce tuttavia un elemento valutativo (ulteriormente) incerto in sede di apprezzamento ad opera del giudicante, e sul quale – non a caso – tendono ad appuntarsi le pronunce giudiziarie».

[38] Così, in particolare, Selvaggi (2019), p. 7 ss. del dattiloscritto, il quale tuttavia rileva che, per evitare un arretramento rispetto agli attuali sviluppi della colpa di organizzazione, difficilmente potrebbe prescindersi «…dalla verifica di un contributo specifico dell'ente diverso da quello o da quelli che abbiano confezionato la tecnologia applicata alla compliance», dovendosi in particolare esaminare «…i comportamenti tenuti da coloro, diversi dall'autore del reato, che abbiano operato lungo le filiere della decisione e del controllo […] dal momento genetico della installazione dei sistemi all'interno della compagine organizzativa e del loro eventuale adattamento al mancato intervento correttivo […] che le circostanze concrete eventualmente richiedano». Sul tema, in generale, della colpa di organizzazione v., per tutti, Paliero, Piergallini (2006), p. 167 ss.

[39] Per approfondimenti al riguardo si vedano, in particolare: Proja (2016), p. 547 ss.; Tebano (2017), p. 3 ss.

[40] In argomento v., *ex multis*: Cass., Sez. V, 31 marzo 2016, con nota di Colucci (2016), p. 32 ss. Cass., Sez. VI, 14 dicembre 1999, con nota di Cuomo (2000), p. 2990 ss.

[41] In alcune ipotesi, infatti, in caso di controllo delle mail dei dipendenti o analisi di determinati documenti di rilievo non solo aziendale, tali procedure potrebbero qualificarsi come pratiche di trattamento dei dati personali, con tutto ciò che ne deriva in termini di ulteriori problematiche e adempimenti di *compliance* normativa per le organizzazioni complesse coinvolte. Per ulteriori approfondimenti v., in particolare, Lynskey (2019), p. 162 ss.

anche in considerazione del fatto che l'art. 22 del Regolamento europeo sulla protezione dei dati personali[42] – nonché l'art. 11 della Direttiva 2016/680/UE sulla protezione dei dati personali nell'attività di prevenzione, indagine, accertamento e perseguimento di reati – 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[43].

Si tratta di una questione per certi versi già sperimentata con riferimento all'utilizzo di algoritmi intelligenti nelle c.d. attività di *sentencing* da parte del giudice, sollevandosi in tal caso il tema dell'assenza di possibilità concrete di difesa da parte del condannato rispetto alla contestazione di una valutazione compiuta interamente da una macchina, senza alcun intervento di mediazione da parte dell'uomo[44].

Una problematica, quest'ultima, che potrebbe a ben vedere verificarsi anche con riferimento all'utilizzo dei predetti sistemi di *data analytics* nell'ambito delle attività di *compliance*.

Infatti, l'*output* prodotto dai *software* in parola non soltanto potrebbe basarsi su un trattamento di dati (a volte, personali) integralmente automatizzato e senza alcun intervento umano di "mediazione valutativa" del risultato dell'analisi, ma potrebbe determinare, con tutto ciò che ovviamente ne consegue, 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.

Non a caso, pertanto, le predette normative eurounitarie prevedono la necessità che il risultato di decisioni – connesse al trattamento di dati – che producono effetti giuridici o incidono significativamente sulla vita dell'interessato non possa basarsi sul solo prodotto del trattamento automatizzato, ma come quest'ultimo debba costituire in sostanza un elemento oggetto di una più ampia considerazione da parte del responsabile del trattamento (con un correlato diritto di pretendere un simile intervento "umano" da parte dell'individuo coinvolto)[45].

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'ente può svolgere le proprie indagini interne[46]. E ciò, chiaramente, impone di individuare il sistema di garanzie da riconoscere ai soggetti coinvolti, specie in considerazione del fatto che – fatte salve le ipotesi in cui tali investigazioni possano qualificarsi come indagini difensive ai sensi degli artt. 391-*bis* ss. del codice di rito – il nostro apparato di regolazione non appare privo di lacune sotto tali profili[47].

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[48].

[42] Cfr. Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

[43] In argomento, di recente, anche per una più ampia disamina del tema della tutela penale dei dati personali, v. D'Agostino (2019), p. 17 ss.

[44] Per approfondimenti sul tema dell'*evidence-based sentencing*, oltre ai contributi pocanzi citati, si veda anche Starr (2014), p. 803 ss.

[45] Sul punto Gialuz (2019), cit., p. 17, il quale rileva peraltro a tale riguardo come «…accanto all'obbligo di un intervento umano andrebbe ritenuta sussistente quella che, nel lessico processualpenalistico, chiameremmo regola di valutazione, in forza della quale l'*output* prodotto dall'IA va considerato come un mero indizio, che va sempre corroborato con altri elementi di prova». Per un approfondimento sugli aspetti di interesse penalistico della direttiva 2016/680/UE v. anche Flor (2019), p. 134 ss.

[46] Sul tema delle *internal investigation* v., in particolare, Mancuso (2016), p. 217 ss.; Bourtin *et al.* (2016), p. 199 ss. Nella lettura internazionale v., per tutti, Nieto (2014), p. 69 ss.

[47] Al riguardo, in particolare, anche per un'analisi delle prospettive *de iure condendo* v. Nicolicchia (2014), p. 805 ss., il quale evidenzia come «…ove non fosse possibile inquadrare le investigazioni interne poste in essere dal soggetto collettivo nei canoni di una indagine difensiva compiuta ai sensi degli artt. 391 *bis* e ss. c.p.p., ci si troverebbe di fronte ad un'attività incidente sui diritti dell'indagato per il reato presupposto e potenzialmente assai pregiudizievole per la sua sorte processuale, la quale risulterebbe però sprovvista di qualsivoglia specifica regolamentazione. L'eventualità segnalata appare tutt'altro che inverosimile, basti pensare, in via di prima approssimazione, al compimento di attività di indagine da parte di soggetti non investiti dell'apposito incarico professionale risultate da atto scritto ai sensi dell'art. 327 *bis* c.p.p., o addirittura sprovvisti della stessa qualifica di avvocato, ipotesi assai verosimile nei processi di *internal audit*, dove diverse specializzazioni e competenze vengono in rilievo».

[48] Sul problema della trasparenza e dell'intellegibilità dei sistemi di *algorithmic decision-making* v., in particolare, Chiao (2019), p. 135. In argomento, però, va segnalato che la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, elaborata dalla *European Commission for the Efficiency of Justice* (CEPEJ), p. 55, evidenzia, per quanto avuto riguardo al contesto specifico del processo penale, che «*..the party concerned should have access to and be able to challenge the scientific validity of an algorithm, the weighting given to its various elements and any erroneous conclusions it comes to whenever a judge suggests that he/she might use it before making his/her decision*». V. al riguardo anche Gialuz (2019), cit., p. 13.

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.

Laddove, 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 gli enti che si avvalgono di innovative metodologie di gestione del rischio[49].

Vediamo adesso di analizzare quali potrebbero essere alcune delle (possibili) strade da percorrere nella direzione di una (ipotetica) regolazione del settore in futuro.

4. (Ipotetici) scenari futuri tra positivizzazione legislativa delle cautele anticorruzione e premialità per gli enti virtuosi: alcuni spunti.

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[50]. 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 gli analizzati 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?

Qui 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[51]. 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 (in particolare con riferimento a uno dei principali problemi emergenti dalle esaminate prassi, ovverosia quello dell'individuazione della base di dati da analizzare, della loro fonte nonché delle tipologie di

[49] Nell'ambito della letteratura internazionale sulla responsabilità da reato degli enti collettivi, per un'analisi di tali problematiche nell'ambito della "*partnership*" pubblico-privato per contrastare i *corporate crimes* – in particolare nel senso di una non corretta distribuzione delle responsabilità di *enforcement* tra regolatore e soggetti regolati – v., per tutti, Laufer (2018), p. 392 ss. Nella dottrina italiana v., invece, Centonze (2017), p. 945 ss.

[50] L'affermazione è stata ripresa di recente da Gialuz (2019), cit., p. 1, il quale ricorda che «…due anni fa, durante un incontro pubblico, venne chiesto al Presidente della Corte suprema degli Stati Uniti, John Roberts, se potesse prevedere il giorno in cui le *smart machines*, guidate da intelligenze artificiali, potranno assistere il giudice nella ricostruzione del fatto o addirittura intervenire nel processo di *decision-making*. La risposta del giudice Roberts è stata più sorprendente della domanda: "*It's a day that's here*" ha detto, "*and it's putting a significant strain on how the judiciary goes about doing things*"».

[51] In tale direzione v., *ex multis*, anche per ulteriori riferimenti bibliografici: Piergallini (2013), cit. p. 860 ss.; Manes, Tripodi (2016), p. 137 ss.; Manacorda (2017), cit., p. 111, il quale peraltro rileva che «…il terreno che ci sembra si presti meglio ad un esercizio di tal fatta è tuttavia quello della corruzione, ove si coagulano una molteplicità di elementi di segno convergente». In argomento si vedano anche i rilievi critici di Mongillo (2011), p. 82. Per un'analisi delle ulteriori posizioni emerse in dottrina sul tema si rinvia, anche per gli opportuni riferimenti bibliografici, a Colacurci (2016), p. 77 ss.

indagini da compiere).

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*[52].

Da qui la proposta, appena richiamata, di positivizzare per settori differenziati le cautele da imporre all'ente, stabilendo una presunzione di idoneità relativa del modello organizzativo conforme alle indicazioni legislative[53].

Nella materia anticorruzione, quindi, l'implementazione di queste procedure di *big data analytics* potrebbe costituire una delle indicazioni da fornire all'ente in merito alle cautele da implementare per costruire il proprio sistema di *compliance*.

Ciò, ovviamente, a patto che il legislatore – è utile ribadirlo – 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.

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, ad 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 (presidiati, peraltro, da rigorose sanzioni penali e civili capaci di estendersi a certe condizioni anche alla *holding* per violazioni commesse nell'ambito di altre *firms* del gruppo) a carico di alcune società emittenti strumenti finanziari negli USA[54].

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[55]. Procedure cui eventualmente collegare benefici di intensità graduabile: dalla riduzione del carico sanzionatorio alla radicale non punibilità per l'ente che si autodenunci[56].

Il legislatore, infatti, potrebbe ritenere che il rischio evidenziato, in relazione a tali procedure, di una strumentalizzazione dell'autodenuncia (in termini di selezione opportunistica dei dati interni da diffondere[57]) 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 gli enti virtuosi, 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 compor-

[52] Su tali aspetti v., per tutti, Severino (2016b), cit., p. 74 ss.

[53] In tale direzione, in particolare, Manes, Tripodi (2016), cit., p. 168.

[54] Si tratta, in particolare, di disposizioni autonome dalle *antibribery provisions* dell'FCPA, e per la mera violazione delle quali l'ente viene sanzionato anche allorquando non si sia verificata alcuna vicenda corruttiva. Per approfondimenti v., *ex multis*: Vuona (2019), p. 979 ss.; Woody (2017), p. 101 ss.; Jordan (2017), p. 1 ss. Un aspetto di ulteriore rilievo, inoltre, è dato dal fatto che l'adozione dell'*anticorruption compliance program* rappresenta un aspetto essenziale del sistema di controllo interno descritto dalle *accounting provisions* dell'FCPA: sul punto, in particolare, si veda Deming (2012), p. 118.

[55] Nella letteratura internazionale sul tema v., per tutti, in particolare rispetto alla valorizzazione del *self-reporting* per l'accesso a procedure negoziate di definizione dei procedimenti a carico dell'ente (in particolare DPAs e NPAs): Arlen (2017), p. 1 ss. Sul tema v. anche Fiorella, Selvaggi (2018), p. 121 ss.

[56] Per una proposta in tale ultima direzione nella dottrina italiana v., in particolare, Centonze (2017), cit., p. 986, il quale in particolare propone l'introduzione, nella trama del d.lgs. n. 231 del 2001, di un nuovo art. 17-*bis* (rubricato: Causa di esclusione della responsabilità), che, si spiega, «…potrebbe dunque suonare così: 1. *Quando il reato è stato commesso dalle persone indicate nell'art. 5, comma 1, l'ente non risponde se prima della notifica dell'informazione di garanzia, in relazione al predetto reato, abbia fornito all'autorità di polizia o all'autorità giudiziaria elementi di prova determinanti per l'esatta ricostruzione del fatto e per l'individuazione degli autori. 2. In ogni caso, l'esclusione della responsabilità è subordinata alla riparazione delle conseguenze dell'illecito ai senti dell'art. 17. 3. È comunque disposta la confisca del profitto che l'ente ha tratto dal reato, anche nella forma per equivalente*».

[57] Per alcuni rilievi critici al riguardo v., in particolare, Mongillo (2018), p. 380 ss.

tamento chiari, osservati i quali l'ente possa nutrire la ragionevole aspettativa di andare esente da responsabilità[58].

Bibliografia

Apollon, Garrick (2017): "FCPA compliance should not cost «an arm and a leg»: assessing the potential for enhanced cost-efficiency and effectiveness for an anti-corruption compliance program with the implementation of an enterprise legal risk management framework", *Penn State Journal of Law & International Affairs*, vol. 5, n. 2, pp. 486-537.

Arlen, Jennifer (2017): "Corporate Criminal Enforcement in the United States: Using Negotiated Settlements to Turn Corporate Criminals Into Corporate Cops", *NYU School of Law Public Law Research Paper n. 17.12*, april 1, 2017.

Berliner, Daniel, Dupuy, Kendra (2018): "The promise and perils of data for anti-corruption efforts in international development work", U4 Brief 2018:7, Michelsen Institute (www.u4.no).

Bonfanti, Angelica (2018): "*Big data* e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali", *La rivista di diritto dei media*, 3, pp. 1-13.

Bourtin, Nicolas, Houle, Amanda (2016): "Investigazioni interne: uno sguardo all'esperienza americana", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 199-215.

Buttarelli, Giovanni (2017): "Le sfide dei Big Data tra evoluzione tecnologica, etica e interessi collettivi", *Gnosis*, 2, pp. 31-39.

Cantone, Raffaele (2017): "Il sistema della prevenzione della corruzione in Italia", *Diritto penale contemporaneo*, 27 novembre 2017.

Cariola, Gianfranco (2019): "Così la blockchain aggiorna i controlli interni", *Quotidiano del Fisco* (il Sole24ore), 16 febbraio 2019.

Centonze, Francesco (2017): "Responsabilità da reato degli enti e *agency problems*", *Rivista italiana di diritto e procedura penale*, III, pp. 945-987.

Chiao, Vincent (2019): "Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice", *International Journal of Law in Context*, 15, pp. 126-139.

Colacurci, Marco (2016): "L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 66-79.

Colajanni, Michele (2017): "Il ruolo del *big data analytics* e *machine learning* nella sicurezza", *Gnosis*, 2, pp. 79-89.

Colucci, Giuseppe (2016): "L'accesso abusivo all'e-mail del dipendente protetta da password", *Guida al Lavoro*, 20, pp. 32-37.

Consulich, Federico (2018): "Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato", *Banca, borsa e titoli di credito*, 2, pp. 195-234.

Cuomo, Luigi (2000): "La tutela penale del domicilio informatico", *Cassazione penale*, 11, pp. 2990-3002.

[58] Sul tema del rafforzamento delle logiche premiali del d.lgs. n. 231 del 2001, v., per tutti, Severino (2018), p. 1101 ss.

D'Agostino, Luca (2019): "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101", *Archivio penale*, 1, pp. 1-58.

Daniels, Donna *et al.* (2018): "Real Risks, Artificial Intelligence: The Next Wave of Anti-Corruption Compliance?", *The Anti-corruption Report* (www.anti-corruption.com), v. 7, n. 4, february 2018.

Deming, Stuart H. (2012): "Internal Controls and Anti-Bribery Compliance", *The Global Business Law Review*, vol. 3:1, pp. 103-141.

Di Porto, Fabiana (2016): "La rivoluzione "big data". Un'introduzione", *Concorrenza e mercato*, 1, pp. 5-14.

Dombalagian, Onnig H. (2016): "Preserving Human Agency in Automated Human Compliance", *Brooklyn Journal of Corporate, Financial & Commercial Law*, WP n. 16-11, pp. 1-40.

Falcone, Matteo (2017): "Big Data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica", *Rivista trimestrale di diritto pubblico*, 3, pp. 601-639.

Falcone, Matteo (2018): "La *big data analytics* per conoscere, misurare e prevenire la corruzione", in Gnaldi Michela, Ponti Benedetto (eds.): "Misurare la corruzione oggi" (Milano, Franco Angeli), pp. 90-110.

Fiorella, Antonio, Selvaggi, Nicola (2018): "Dall'«utile» al «giusto». Il futuro dell'illecito dell'ente nello 'spazio globale'" (Torino, Giappichelli).

Flor, Roberto (2019): "*Cyber-criminality*: le fonti internazionali ed europee", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): "Cybercrime" (Utet, Torino), pp. 35-96.

Gee, Sunder (2015): "Fraud and Fraud Detection: A Data Analytics Approach" (Hoboken, John Wiley & Sons).

Gialuz, Mitja (2019): "Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti ed Europa", *Diritto penale contemporaneo*, 29 maggio 2019.

Giavazzi, Stefania *et al.* (2014): "The ABC Program: An Anti-Bribery Compliance Program Recommended to Corporations Operating in a Multinational Environment", in Manacorda Stefano, Centonze Francesco, Forti Gabrio (eds.): "Preventing Corporate Corruption. The Anti-Bribery Compliance Model" (Londra, Springer), pp. 125-177.

Glicksman, Robert L., Markell, David L., Monteleoni, Claire (2017): "Technological Innovation, Data Analytics and Environmental Enforcement", *Ecology Law Quarterly*, 44:41, pp. 41-88.

Gullo, Antonio (2017): "Il contrasto alla corruzione tra responsabilità della persona fisica e responsabilità dell'ente: brevi note", in Castaldo Andrea R. (editor): "Il Patto per la legalità. Politiche di sicurezza e di integrazione" (Milanofiori Assago, Wolters Kluwer), pp. 89-99.

Gullo, Antonio (2018): "Note minime sul rapporto tra diritto amministrativo e diritto penale", *Luiss Law Review*, 2, pp. 35-41.

Hughes Parker, Rebecca (2014): "Ernst & Young Experts Reveal How Forensic Data Analytics Can Transform Anti-Corruption Compliance", *The Anti-corruption Report* (www.anti-corruption.com), v. 3, n. 9, April 2014.

Jordan, Jon (2017): "BNY Mellon and Qualcom: a recent focus on improper hiring practices in violation of the Foreign Corrupt Practices Act", *Loyola Law Review*, vol. 63, pp. 1-26.

Kossow, Niklas, Dykes Victoria (2018): "Blockchain, bitcoin and corruption. A review of the linkages", *Transparency International Anti-Corruption Helpdesk Answer*, 22 january 2018.

Kraft, Timothy J. (2017): "Big Data Analytics, Rising Crime, and Fourth Amendment Protections", *University of Illinois Journal of Law, Technology & Policy*, pp. 249-273.

Laufer, William S. (2017): "The Missing Account of Progressive Corporate Criminal Law", *New York University Journal of Law & Business*, vol. 14, n. 1, pp. 71-142.

Laufer, William S. (2018): "A Very Special Regulatory Milestone", *University of Pennsylvania Journal of Business Law*, vol. 20.2, pp. 392-428.

Levy, Karen E.C. (2013): "Relational Big Data", *Standford Law Review Online*, 73, pp. 73-79.

Lynskey, Orla (2019): "Criminal justice profiling and EU data protection law: precarious protection from predictive policing", *International Journal of Law in Context*, 15, pp. 162-176.

Manacorda, Stefano (2017): "L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive", *Rivista trimestrale di diritto penale dell'economia*, n. 1-2, pp. 49-113.

Mancuso, Enrico Maria (2016): "Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 217-245.

Manes, Vittorio, Tripodi, Andrea Francesco (2016): "L'idoneità del modello organizzativo", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 137-174.

Mongillo, Vincenzo (2011): "Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione", *La responsabilità amministrativa delle società e degli enti*, III, pp. 69-100.

Mongillo, Vincenzo (2018): "La responsabilità penale tra individuo ed ente collettivo" (Torino, Giappichelli).

Nicolicchia, Fabio (2014): "*Corporate Internal Investigations* e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della «lezione americana»", *Rivista trimestrale di diritto penale dell'economia*, 3-4, pp. 781-809.

Nieto, Adàn Martin (2014): "Internal Investigations, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process", in Manacorda Stefano, Centonze Francesco, Forti Gabrio (eds.): "Preventing Corporate Corruption. The Anti-Bribery Compliance Model" (Londra, Springer), pp. 69-92.

Olsen, William P. *et al.* (2016): "Using Data Analytics to Meet the Government's Anti-Corruption Compliance Expectations", *The Anti-corruption Report* (www.anti-corruption.com), v. 5, n. 9, may 2016.

Ottolia, Andrea (2017): "*Big Data* e innovazione computazionale" (Torino, Giappichelli).

Paliero, Carlo Enrico, Piergallini, Carlo (2006): "La colpa di organizzazione", *La responsabilità amministrativa delle società e degli enti*, III, pp. 167-184.

Parodi, Cesare, Sellaroli, Valentina (2019): "Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco", *Diritto penale contemporaneo*, 6, pp. 47-71.

Pasquale, Frank A. (2019): "A Rule of Persons, Not Machines: The Limits of Legal Automation", *George Washington Law Review*, 1, pp. 1-60.

Picotti, Lorenzo (2019): "Diritto penale e tecnologie informatiche: una visione d'insieme", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (eds.): "Cybercrime" (Utet, Torino), pp. 35-96.

Piergallini, Carlo (2013): "Paradigmatica dell'autocontrollo penale (dalla funzione alla struttura del "modello organizzativo" ex. d.lg. n. 231/2001)", *Cassazione penale*, 2, pp. 842-867.

Pitaro, Vincent (2018): "Using Data Analytics to Boost Compliance Program Effectiveness", *The Anti-corruption Report* (www.anti-corruption.com), v. 7, n. 13, june 2018.

Pitruzzella, Giovanni (2016): "Big data, competition and privacy: a look from the antitrust perspective", *Concorrenza e mercato*, 1, pp. 15-27.

Ponte, Federico (2017): "I "big data" come "common goods"", *Ciberspazio e diritto*, 1, pp. 31-67.

Proja, Giampiero (2016): "Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza", *Rivista italiana di diritto del lavoro*, 4, pp. 547-578.

Selvaggi, Nicola (2019): "Compliance, sicurezza informatica e nuove tecnologie", relazione tenuta al Congresso dell'Associazione Internazionale di Diritto Penale – Gruppo Italiano su "*Nuove tecnologie e giustizia penale. Problemi aperti e future sfide*", Teramo, 22-23 marzo 2019.

Severino, Paola (2016a): "Legalità, prevenzione e repressione nella lotta alla corruzione", *Archivio Penale*, 3, pp. 1-8.

Severino, Paola (2016b): "Il sistema di responsabilità degli enti *ex* d.lgs. n. 231/2001: alcuni problemi aperti", in Centonze Francesco, Mantovani Massimo (eds.): "La responsabilità «penale» degli enti. Dieci proposte di riforma" (Bologna, il Mulino), pp. 73-85.

Severino, Paola (2018): "La responsabilità dell'ente ex d.lgs. n. 231 del 2001: profili sanzionatori e logiche premiali", in Paliero Carlo Enrico, Viganò Francesco, Basile Fabio, Gatta Gian Luigi (eds.): "La Pena, ancora, fra attualità e tradizione" (Milano, Giuffrè), pp. 1101-1127.

Severino, Paola (2019): "Strategie di contrasto alla corruzione nel panorama interno e internazionale", *Luiss Open*, 29 marzo 2019.

Starr, Sonja B. (2014): "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination", *Stanford Law Review*, vol. 66, pp. 803-872.

Tebano, Laura (2017): "Employees' Privacy and employers' control between the Italian legal system and European sources", *Labour & Law Issues*, vol. 3, n. 2, pp. 1-20.

Trapani, Matteo (2018): "La prevenzione e il controllo della corruzione e dell'etica pubblica mediante l'utilizzo delle nuove tecnologie", *Forum di Quaderni Costituzionali*, 15 aprile 2018, pp. 1-13.

Tripodi, Andrea Francesco (2013): "L'elusione fraudolenta nel sistema della responsabilità da reato degli enti" (Padova, Cedam).

Vona, Leonard W. (2017): "Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems" (Hoboken, John Wiley & Sons).

Vuona, Bridget (2019): "Foreign Corrupt Practices Act", *American Criminal Law Review*, vol. 53, pp. 979-1032.

Watcher, Sandra, Mittelstadt, Brent (2019): "A right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2, pp. 1-130.

White, Mary J. (2016): "A New Model for SEC Enforcement: Producing Bold and Unrelenting Results", *Compliance & Enforcement* (wp.nyu.edu), 21 novembre 2016.

Woody, Karen E. (2017): "No Smoke and No Fire: The Rise of Internal Controls Absent Anti-Bribery Violations in FCP Enforcement", *Cardozo Law Review*, vol. 38, pp. 101-139.

Zeno-Zencovich, Vincenzo (2018): "Dati, grandi dati, dati granulari e la nuova epistemologia del giurista", *La rivista di diritto dei media*, 2, pp. 1-7.

Zwiebel, Megan (2017): "Measuring Compliance: Gathering and Analyzing Data", *The Anti-corruption Report* (www.anti-corruption.com), v. 6, n. 18, september 2017.