Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

1/2023

Editore Associazione “Progetto giustizia penale”, c/o Università degli Studi di Milano,
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157
ANNO 2023 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Intelligenza artificiale e diritto penale
Inteligencia artificial y derecho penal
Artificial Intelligence and Criminal Law

Criminal compliance e nuove tecnologie *

Criminal compliance *y nuevas tecnologías*

Criminal Compliance and New Technologies

Luca D'Agostino
Dottore di ricerca in diritto penale
ldagostino@luiss.it

Responsabilità da reato degli enti, Intelligenza artificiale

Responsabilidad penal personas jurídicas, Inteligencia artificial

Corporate Criminal Liability, Artificial Intelligence

Abstracts

Il contributo ha per oggetto all'analisi di una possibile automazione della compliance penale per la prevenzione di illeciti all'interno delle imprese. L'indagine mira ad esaminare i possibili benefici e i rischi derivanti dall'utilizzo di *smart technologies* (es. *big data*, intelligenza artificiale, *blockchain*) in chiave preventiva, attraverso l'integrazione di tali strumenti innovativi nei modelli organizzativi e gestionali adottati dagli enti *ex* art. 6 D. Lgs. 231/2001. Partendo dall'analisi di strumenti già esistenti (quali quelli per la *detection* di minacce, vulnerabilità e anomalie), lo studio valuta la specifica applicabilità dei nuovi ritrovati tecnologici nei processi di controllo 231. L'obiettivo è dunque quello di analizzare – *de iure condito* e sulla base dell'attuale stato della tecnica – le possibili applicazioni tecnologiche per prevenire la commissione di *corporate crimes*.

El artículo analiza la posible automatización del compliance penal para la prevención de actuaciones ilícitas en el seno de las empresas. La investigación tiene como objetivo examinar los posibles beneficios y riesgos derivados del uso de tecnologías inteligentes (por ejemplo, big data, inteligencia artificial, blockchain) de forma preventiva, a través de la integración de estas herramientas innovadoras en los modelos organizativos y de gestión adoptados por las personas jurídicas en virtud del Art. 6 del Decreto 231/2001. Partiendo del análisis de las herramientas existentes (aquellas para la detección de amenazas, vulnerabilidades y anomalías), el estudio evalúa la aplicabilidad de los nuevos medios tecnológicos en los mecanismos de prevención y control corporativos. También se pretende analizar, las posibles aplicaciones informáticas para prevenir la comisión de delitos corporativos.

The essay examines the potential automation of criminal compliance to prevent illegal activities within companies. The investigation aims to explore the potential benefits and risks associated with the utilization of smart technologies (e.g., big data, artificial intelligence, blockchain) in a proactive manner. This involves integrating these innovative tools into the organizational and management models adopted by entities under Article 6 of the Italian Legislative Decree 231/2001. By analyzing existing tools used for threat detection, vulnerability assessment, and anomaly detection, the study assesses the feasibility of implementing new technological means in corporate compliance. Furthermore, the objective is to analyze and reflect on the current state of the art regarding IT applications for preventing corporate crimes.

* Il presente contributo nasce dalla rielaborazione dei risultati della ricerca "Criminal Compliance and New Technologies", nell'ambito del progetto "Go for IT" finanziato dal Ministero dell'Istruzione e attuato dalla Fondazione CRUI.

Sumario

1. *Digital Criminal Compliance*. Opportunità e rischi dell'automazione nei processi di controllo.

Alcuni studi recenti hanno elaborato la nozione di "Digital Criminal Compliance"[1] per indicare la tendenza alla digitalizzazione della tradizionale *compliance* aziendale nella prevenzione dei reati[2]. Un concetto che, secondo alcuni, potrebbe diventare centrale nel campo del diritto penale economico. Tale disciplina – che per brevità indicheremo con l'acronimo DCC – si basa essenzialmente sull'analisi di dati ottenuti attraverso strumenti di rilevazione che, grazie all'intelligenza artificiale, sono aggregati e resi fruibili per determinate attività di monitoraggio e controllo[3].

Nonostante si parli icasticamente di una "automazione" della *compliance* penale, nella realtà si tratta di applicazioni tecnologiche di supporto a funzioni aziendali gestite dall'uomo, non sostituibili con il lavoro del *software*. Pertanto, appare preferibile definire la DCC come un *empowerment organizzativo*: la tecnologia amplifica il potenziale del sistema di gestione e permette di massimizzare i risultati delle funzioni di controllo e *internal auditing*.

La DCC si rivela certamente più efficace ed efficiente rispetto alla *compliance* soltanto "analogica", che spesso presenta debolezze riconducibili al fattore umano. Di regola i modelli organizzativi mirano a prevenire la commissione di reati attraverso la diffusione della "cultura della legalità" e la segmentazione dei processi decisionali e di controllo[4]. Questo secondo elemento porta all'irrigidimento dell'assetto organizzativo, e si pone spesso in contrasto con le dinamiche del mercato e dell'impresa[5].

Le *smart technologies* consentono di elaborare grandi quantità di dati in modo coerente, più veloce e preciso degli esseri umani; ciò porta a un significativo incremento dell'efficienza e conduce verso una progressiva semplificazione delle procedure. Inoltre, grazie all'analisi in tempo reale dei flussi di informazioni, si incentiva la leva preventiva permettendo all'ente di intervenire non appena si abbia notizia di indici di sospetto o anomalia[6]. Ciò segna una svolta significativa nella *governance* del rischio, poiché consente all'ente di reagire in un tempo in cui il reato non è ancora stato commesso.

Laddove l'illecito non possa essere prevenuto neppure da sistemi evoluti di monitoraggio attivo, il vantaggio della DCC consiste nella registrazione degli "eventi informatici" occorsi[7] che permette di svolgere una accurata analisi *ex post* per individuare i responsabili o ricostruire le modalità di commissione del reato.

Occorre tuttavia essere consapevoli anche dei rischi della DCC, e del possibile contrasto con alcune disposizioni di legge sul trattamento dei dati personali e sui diritti del lavoratore. Invero, l'utilizzo di sistemi "intelligenti" a supporto alla *compliance* penale può dar luogo – in via diretta o anche solo incidentalmente – a forme di monitoraggio del personale addetto ai

[1] Gullo (2022), p.1289 ss.
[2] Burchard (2021), p. 741 ss.
[3] L'intelligenza artificiale è qui da intendersi in senso ampio, v. *infra* § 3.2.
[4] Severino (2020), p. 531
[5] Burchard (2021), p. 746.
[6] Si segnerebbe così il passaggio da una *compliance* penale statica e "reattiva" verso un modello più dinamico e fortemente preventivo.
[7] Si consideri al riguardo il caso esemplificato al § 3.1. e l'utilizzo di SIEM per l'analisi dei dati di traffico (§ 4.2.).

processi a rischio[8]. Si pensi al controllo del traffico di mail attraverso algoritmi di *Natural Language Processing* (NLP), alla registrazione di chiamate telefoniche o telematiche, al tracciamento dei file di navigazione, o alla rilevazione delle coordinate GPS. Si tratta, come evidente, di applicazioni che presentano rischi significativi per gli individui, in grado di ledere diritti costituzionalmente tutelati.

A ben vedere, la *compliance* penale digitale[9] si differenzia da quella "analogica" non soltanto per elementi quantitativi (numero di dati raccolti e trattati, tempi di risposta e reazione etc.), ma soprattutto per elementi qualitativi (tipologia di dati analizzati, funzioni e personale coinvolto). Sarebbe dunque opportuno procedere a una valutazione preventiva di conformità normativa per evitare che, da incentivo alla legalità aziendale, la tecnologia divenga il volano di prassi illecite[10] o discriminatorie[11]. Inoltre, la DCC non dovrebbe trasmodare in una modalità "post-panottica" di esercizio del potere in funzione di *Big Data* ottenuti monitorando in modo sempre più penetrante i comportamenti dei dipendenti.

Infine, si prospettano alcuni rischi "sociali" correlati alla *compliance* digitale. Essendo questa basata sul controllo preventivo, ne potrebbe derivare una sistematica sfiducia nei confronti del personale aziendale. Dipendenti e lavoratori finiscono per essere considerati un rischio da monitorare, anziché persone dotate di indipendenza e libertà di azione[12].

1.1. RegTech *e automazione della compliance penale. Lo stato dell'arte.*

La trasformazione digitale rappresenta una delle principali sfide per la *corporate compliance*. Se si considera la *compliance* come quel metodo per l'applicazione delle regole nei processi interni, appare chiaro come l'innovazione digitale sia destinata a mutare profondamente l'assetto organizzativo e dei controlli.

La dottrina nordamericana si interroga già da diversi anni sulle sorti della *compliance* penale dell'era del progressismo tecnologico, mettendo in evidenza il delicato equilibrio tra opportunità e rischi dell'automazione dei controlli societari[13]. Si parla in particolare di *RegTech*[14] per definire quelle tecnologie che supportano le imprese nel rispetto dei requisiti normativi, in modo da assicurare un alto grado di conformità alle regole. Secondo alcuni autori[15] il *RegTech*, non è un semplice strumento di potenziamento della *compliance*, ma un vero e proprio cambiamento di paradigma per il business del ventunesimo secolo[16]; secondo altri[17] esso rappresenta la base fondamentale e la prossima evoluzione in molti settori, tra cui in particolare quello dei servizi finanziari.

Il *RegTech* migliora la *performance* dei sistemi di gestione aziendale, automatizzando parte dei compiti attribuiti alle funzioni di *compliance* e riducendo i rischi operativi associati all'agire umano. Inoltre, permette al personale incaricato di agire in modo informato basandosi sui dati raccolti e processati dagli algoritmi[18]. Diverse applicazioni tecnologiche – quali il *machine*

[8] Sul tema, in generale, Burchard (2019), p. 1909
[9] Di recente sull'argomento v. Morgante- Fiorinelli (2022) p. 1; Nisco (2022); Mongillo (2022); Selvaggi (2019), p. 217
[10] Per trattamento illecito di dati (art. 167 D. Lgs. 196/2003) o per violazione delle disposizioni in materia di controlli a distanza dei lavoratori (art. 171 D. Lgs. 196/2003 in relazione all'art. 8 L. 300/70).
[11] Si pensi alla problematica dei *bias* algoritmici dovuti alle generalizzazioni statistiche. Tra gli esempi più noti si ricorda l'esperienza statunitense degli algoritmi predittivi per la commisurazione della pena, laddove tra le variabili rilevanti ai fini della determinazione del livello di rischio, si tiene spesso conto di fattori demografici, socioeconomici, familiari, che contribuiscono a caratterizzare come individui più pericolosi quelli appartenenti a determinate minoranze o classi sociali. L'output dell'algoritmo risulta così "contaminato" dal trend storico al trattamento deteriore e al pregiudizio nei confronti di alcune figure di criminali. Sia consentito rinviare, per richiami alla dottrina nordamericana, a D'Agostino, (2019), p. 354 ss.; Franssen -Berrendorf (2021), p.199. Il tema dei *bias* algoritmici interessa anche l'impiego per finalità di prevenzione dei reati. In dottrina si riporta l'esempio della multinazionale che intende utilizzare i dati del sistema giudiziario statunitense per individuare i dipendenti con maggiore possibilità di delinquere, che renderebbero verosimilmente più alto l'indice di pericolosità per gli individui appartenenti a talune classi sociali o minoranze razziali. Cfr. Burchard (2021), p. 746
[12] Zuboff (2019), p. 2
[13] Laufer (2017), p. 71
[14] Packin (2018), p. 193 ss.
[15] Arner *et al.* (2017), p. 373.
[16] Secondo la definizione comune, il Regtech è l'uso delle nuove tecnologie per assicurare il rispetto dei requisiti normativi in modo più efficace ed efficiente.
[17] Mohamed- Yildirim (2021), p. 153
[18] Gli strumenti tecnologici riducono la probabilità di errori umani e promuovono il miglioramento continuo dei processi organizzativi e gestionali. Il supporto alla *compliance* è caratterizzato da complesse analisi documentali e correlazioni tra dati, che grazie all'uso di strumenti e tecnologie intelligenti sono rese più performanti, facendo venir meno le inefficienze collegate al fattore umano.

learning, la crittografia, la *big data analytics* – rendono disponibili informazioni pertinenti e specifiche sulle attività della società, che in nessun altro modo sarebbe possibile ottenere[19].

É noto come l'Intelligenza Artificiale (IA)[20] abbia oggi molteplici applicazioni nella prevenzione e nel perseguimento dei reati e, in genere, nel sistema di giustizia penale[21] e nel *law enforcement*[22]. Alcune di queste, già radicate nella giudiziaria statunitense[23], pongono questioni sul fronte criminologico[24], etico e legale[25].

Di recente si è anche discusso dell'impiego dell'IA per la prevenzione dei reati, mettendo in evidenza alcune possibili criticità sul piano dei principi generali della responsabilità dell'ente[26]. La dottrina ha iniziato a interrogarsi sulla responsabilità per c.d. *algorithmic misconduct,* nei casi in cui una determinata violazione o un omesso controllo siano causati da una "scelta" del *software*. In questi casi risulterà complesso stabilire a quali condizioni l'ente debba rispondere dell'illecito, poiché si deve distinguere in base al modello di responsabilità oggettiva (*strict liability*) o di responsabilità vicaria (basato sul principio del *respondeat superior*)[27]. Mentre il primo non richiede la prova di alcun elemento soggettivo, essendo sufficiente il fatto nella sua oggettività, il secondo attribuisce rilevanza allo status psicologico del personale aziendale.

Questo secondo modello – sul quale è imperniato il sistema statunitense di responsabilità degli enti – pone alcune criticità nel caso di *algorithmic misconduct,* che gli studiosi hanno tentato di risolvere senza travolgere lo schema della responsabilità vicaria. L'ente risponderà dell'illecito a condizione che il fatto sia stato commesso attraverso informazioni "conosciute" dall'algoritmo, e quindi dalla società, per essere state prodotte o elaborate nelle attività aziendali devolute all'algoritmo stesso. Inoltre, le informazioni processate e l'output del *software* devono portare un qualche vantaggio all'ente[28].

Quando la violazione è causata dall'algoritmo, l'indagine sull'elemento psicologico diviene complessa, non essendo possibile far riferimento all'*animus* del personale aziendale incaricato di certe funzioni (ad esempio il programmatore o il responsabile IT).

Vi sono poi quei modelli di responsabilità dell'ente nei quali si valorizza la colpa di organizzazione, come nel sistema italiano disciplinato dal D. Lgs. 231/2001[29]. Secondo questo schema di responsabilità, in caso di violazione ascrivibile al *software*, l'ente sarà responsabile soltanto se la commissione dell'illecito dipende da una carenza organizzativa. Si è parlato a tal proposito dell'intelligenza artificiale come "arma a doppio taglio"[30] in grado potenziare le attività di *compliance* e, al tempo stesso, di esporre al rischio di deficit organizzativi. Sebbene, in linea di massima, l'uso della tecnologia renda i sistemi di gestione più affidabili, l'ente dovrà definire procedure e controlli specifici sul funzionamento degli strumenti informatici e sul trattamento delle eventuali anomalie[31].

La transizione digitale ha aumentato vertiginosamente la mole di dati a disposizione degli enti, che opportunamente elaborati, divengono informazioni preziose per il *decision making* aziendale. Per questo motivo l'intelligenza artificiale diviene uno strumento via via sempre più efficace per la prevenzione dei reati. Si va verso il tramonto dei processi tradizionali *human-based*, sostituiti dall'automazione nelle attività di *risk analysis*.

I *software* di IA permettono di individuare le aree critiche, attribuire un punteggio di

[19] Van Liebergen *et al.* (2016), p. 1
[20] *Amplius,* § 2.2.
[21] Ferguson (2015), p. 327; Osvald *et al.* (2018), p. 227; Gialuz (2019)
[22] United Nations Interregional Crime and Justice Research Institute's (UNICRI), *Artificial Intelligence and Robotics for law enforcement*, in unicri.it
[23] Si citano al riguardo le parole di Justice Roberts, giudice della Corte Suprema USA, che in una intervista del 2018 alla domanda se potesse immaginare un giorno in cui le macchine intelligenti saranno utilizzate per supportare il processo decisionale del giudice rispose: «*Questo giorno è già arrivato e sta mettendo a dura prova il modo in cui la magistratura fa le cose*». Cfr. Liptak (2017), citato da Burchard (2019), p. 1909.
[24] King *et al.* (2020), p. 89
[25] Vermeulen *et al.* (2021), p. 7. Gli autori affermano che l'uso legittimo dell'IA e dei *big data* nella giustizia penale dipende da una serie di fattori, tra cui la trasparenza algoritmica, l'affidabilità, la non discriminazione, la protezione dei dati, l'accesso alla giustizia, l'esistenza di rimedi effettivi.
[26] Sabia (2020), p. 179. Secondo l'autrice l'impiego dell'IA per migliorare la *compliance* aziendale e prevenire il rischio di reato è una tematica emergente, un campo di indagine ancora largamente inesplorato.
[27] Per una analisi accurata si veda Mazzacuva (2021), p. 143
[28] Diamantis (2020), p. 893 ss.
[29] Paliero (2018), p. 175 ss.
[30] Mazzacuva (2021), p. 150.
[31] Non si può infatti ignorare l'incidenza di tali strumenti nella organizzazione del lavoro e nell'assegnazione di ruoli e responsabilità all'interno dell'azienda. La dirigenza deve avere una conoscenza piena della tecnologia per poter strutturare al meglio i processi operativi; parimenti gli organismi di vigilanza dovranno comprenderne a fondo le logiche per esperire gli opportuni controlli.

rischio[32] e, grazie all'apprendimento automatico, di fare previsioni su eventi futuri. Gli enti possono così migliorare nel tempo le loro strategie di *compliance*, utilizzando la tecnologia, come detto, per l'*empowerment* organizzativo.

Altro tema discusso è il rapporto tra *digital compliance* e responsabilità da reato. Ci si è chiesti, nell'ipotesi in cui la società si affidi all'IA, se sia responsabile laddove il reato commesso rappresenti la concretizzazione di un rischio non rilevato dal *software*[33]. Facendo applicazione dei principi desumibili dall'art. 6 D. Lgs. 231/2001, l'ente andrà esente da responsabilità se, avendo adottato un modello organizzativo idoneo[34], non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Il vero *core* della questione rimane dunque il sindacato sull'idoneità del modello[35], attraverso il quale si esprime un giudizio sulla colpevolezza dell'ente[36]. Si dovrà compiere una valutazione relativa al caso concreto, per stabilire se l'automazione di determinate attività fosse coerente rispetto allo scopo e sia stata inserita in un processo tale da permettere l'acquisizione di informazioni e l'attivazione dei controlli da parte dell'organismo di vigilanza. L'aver acriticamente assegnato al *software* determinate funzioni – in assenza, ad esempio, di adeguata formazione del personale o di procedure specifiche di analisi dei dati – è indice sintomatico della colpa di organizzazione.

Guardando invece alle prospettive *de iure condendo* l'IA potrebbe offrire al legislatore una soluzione all'annosa questione del sindacato giudiziale, attraverso la previsione di una presunzione (relativa) di idoneità dei modelli che, in determinati ambiti, siano conformi alle *best practices* di settore[37].

Le potenzialità dei *Big Data* sono tanto maggiori quanto più grande è il flusso di informazioni[38]; grazie alle capacità computazionali e predittive degli algoritmi anche le società di grandi dimensioni possono analizzare i dati in modo accurato.

Numerosi sono tuttavia i profili critici. Secondo alcuni autori la bontà delle decisioni prese dal *software* dipende dalla quantità di dati processati in *input*[39]. Tuttavia, l'incremento di questi ultimi rende sempre più impegnativa l'attività di analisi da parte del personale umano. Spesso poi gli algoritmi di IA risultano *impenetrabili*[40], non essendo possibile determinare quanto peso abbia ogni singola variabile nella decisione finale[41]. Il problema è dunque quello della opacità del programma, che può produrre il c.d. effetto *black box*[42]. Si distinguono diversi tipi di opacità del *software*: (i) è intenzionale quando risponde a una scelta del programmatore (si pensi al *trade secret* per proteggere gli interessi economici dell'azienda); (ii) in atri casi potrebbe essere dovuta alla mancanza di competenze tecniche da parte degli utilizzatori; (iii) vi è poi l'opacità necessaria, legata alla complessità dei *software* di AI e al *deep learning*[43]. Mentre le prime due possono essere superate – scegliendo ad es. *software* non proprietari o acquisendo le opportune competenze tecniche – l'ultima è allo stato una costante ineliminabile.

[32] Si veda in argomento il paper di Deloitte, *AI and Risk Management*, *Center for regulatory strategy*, in www2.deloitte.com.

[33] Sabia (2020), p. 186 sostiene che, indipendentemente dal modello di riferimento, sia complesso attribuire la responsabilità in base alle norme esistenti. I criteri di ascrizione della responsabilità penale dell'ente potrebbero rivelarsi inadeguati di fronte alle sfide poste dalle nuove tecnologie.

[34] Sulla valutazione relativa all'idoneità del modello v. Morgante-Fiorinelli (2022), p. 13

[35] *Infra*, § 1.2.

[36] L'errore dell'algoritmo non può determinare *ex se* la responsabilità penale dell'ente, dovendosi all'opposto dimostrare l'assenza di procedure interne di valutazione e riesame. Se la società ha adottato un *compliance program* ben strutturato, prevedendo gli opportuni controlli, non dovrebbe sussistere alcuna colpa di organizzazione.

[37] La codificazione delle regole cautelari e il sindacato giudiziale sull'idoneità dei modelli sono temi assai discussi in dottrina. È autorevolmente sostenuta la tesi della "validazione" del modello attraverso la positivizzazione di protocolli cautelari, imperniati sulle *best practices* di settore. In particolare, Piergallini (2019), p. 536 ritiene che i modelli conformi allo standard del settore dovrebbero essere assistiti da una presunzione, *iuris tantum*, di idoneità preventiva, superabile dal giudice solo attraverso l'assolvimento di un onere motivazionale rafforzato. Nello stesso senso v. anche Piergallini (2015), p. 266.
A nostro modo di vedere, nella positivizzazione delle cautele, ampio spazio andrebbe riconosciuto all'impiego di strumenti tecnologici a supporto della *compliance*. Così, ad esempio, l'adozione di alcuni programmi (per la *due diligence* di terze parti o per monitorare il traffico di mail), in linea con gli standard di settore, potrebbe ragionevolmente fondare una presunzione relativa di idoneità del modello nel prevenire i reati di corruzione.

[38] Severino (2020), p. 536.

[39] Dombalagian (2016)

[40] Mozzarelli (2022), p. 259 ss.

[41] Da un punto di vista tecnico, comprendere le ragioni di una previsione basata su un numero limitato di variabili (come avviene di solito nella statistica tradizionale) è fattibile. Al contrario, le previsioni basate su Big Data e reti neurali non sono facilmente spiegabili *a posteriori*, essendo estremamente difficile ottenere informazioni sul peso di un singolo nodo nel determinare la decisione. *Amplius*, § 2.2.

[42] Sabia (2020), p. 185.

[43] Niklas (2020), p. 527.

Tra i punti deboli dei sistemi automatizzati vi sono anche la c.d. *standardizzazione dei controlli* e i malfunzionamenti derivanti da errori di programmazione o da inadeguata formazione. Il personale addetto ai sistemi non dovrà accomodarsi sugli *output* del programma, dovendo al contrario vagliare in modo critico e costruttivo la determinazione dell'algoritmo. In sostanza, l'automazione della *compliance* deve rappresentare l'occasione per dismettere le attività umane di supervisione e controllo[44].

Per superare tali criticità, una parte della dottrina ha plasmato la nozione di "controllo umano significativo"[45] per descrivere un approccio all'IA caratterizzato dal costante monitoraggio dell'uomo sui risultati della decisione algoritmica.

Altri autori ritengono necessario un intervento dei legislatori nazionali, o anche semplicemente la creazione di regole tecniche e standard di settore (es. norme ISO), per incentivare le aziende a dotarsi di strumenti digitali a supporto della *compliance*[46].

Vi è anche chi propone un approccio basato sulla *forward compliance*[47] secondo cui, per limitare i predetti rischi, l'ente dovrebbe adottare linee guida e istruzioni operative specifiche ed accurate, senza necessariamente attendere l'emanazione di una regolazione di settore. La tesi muove dal condivisibile assunto per cui qualsiasi nuova tecnologia presenta margini di rischio, e necessita l'adozione di particolari cautele. Affinché il percorso di automazione della *compliance* sia sicuro e sostenibile, gli enti dovranno interiorizzare le *smart technologies* nei processi esistenti scegliendo la soluzione che meglio riesca a conciliare le contrapposte esigenze.

Nonostante l'opinione prevalente sia favorevole al *RegTech*, non mancano voci di segno contrario. Vi è chi sostiene che la tecnologia possa ostacolare l'impegno umano nelle attività di *risk assessment* e nei processi decisionali dell'ente[48]. Si parla di *technology judgement rule* per indicare, in senso negativo, quelle scelte di *governance* basate unicamente sull'*output* algoritmico[49].

1.2. *Strumenti digitali a supporto della* compliance *231. Alcuni esempi derivanti dalle* best pratices *in materia di anticorruzione e antiriciclaggio.*

L'utilizzo di strumenti tecnologici a supporto della *compliance* aziendale si inserisce in un quadro di regole in cui è preponderante il ruolo dell'autodisciplina[50]. In molti settori il legislatore si affida al c.d. approccio basato sul rischio lasciando ai soggetti privati l'onere di individuare, in base al contesto di riferimento, le modalità concrete per l'attuazione degli obblighi di legge[51].

Pur non essendovi espresse disposizioni circa la doverosità di mettere in atto misure tecnologiche per mitigare il rischio di reati, può ritenersi che un tale adempimento rientri nel più ampio concetto di "best practice di settore" per assicurare l'adeguatezza in concreto dei sistemi di controllo aziendali. Da questa prospettiva l'automazione della *compliance* rappresenta una grande opportunità per gli enti, che potranno dimostrare di aver attuato controlli e procedure di mitigazione del rischio affidandosi alle più avanzate tecniche di monitoraggio e *intelligen-*

[44] Alcuni studiosi temono che gli uffici di compliance possano abbandonarsi a prassi lassiste, rimettendo tutto alle previsioni/decisioni algoritmiche. Cfr. Dombalagian (2016), p. 87.
[45] Ubertis (2020), p. 75 ss.; Sorbello (2019), p. 374 ss.
[46] Niklas (2020), p. 539.
[47] Armour (2018)
[48] Bamberger (2009), p. 669
[49] La dottrina da ultimo richiamata sostiene che i sistemi di *compliance* digitale siano sviluppati sulla base dell'interpretazione della legge fornita dal programmatore. I processi che portano alla creazione di tali sistemi nascono dalla interazione di diversi gruppi di professionisti che, spesso, comunicano tra loro in modo imperfetto.
[50] Nel sistema di responsabilità da reato degli enti si pensi ai codici elaborati dalle associazioni di categoria (le "Linee Guida") in base ai quali poter costruire, ai sensi dell'art. 6, comma 3, d.lgs. 231/2001, i modelli organizzativi e gestionali.
[51] L'approccio basato sul rischio assicura una certa flessibilità, proporzionalità e adeguatezza in concreto; in questo modo ciascun operatore dovrà valutare il rischio e adottare misure che siano adeguate e proporzionate al rischio stesso Nell'ordinamento vigente possono citarsi esempi afferenti a diversi ambiti: l'art. 6 D. Lgs. 231 /2001 indica genericamente le esigenze da considerare nella costruzione dei modelli organizzativi, senza prescrivere specifiche cautele o misure per le attività a rischio; in materia di antiriciclaggio l'art. 16, comma 1, D. Lgs. 231/2007 dispone che i soggetti obbligati debbano «*adottare i presidi e attuare i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo*»; in materia di trattamento dei dati personali l'art. 12, par. 1, GDPR prevede che «*Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*».

ce sui dati[52]. Affinché la transizione delle imprese verso il digitale sia sicura e sostenibile, è auspicabile che anche i modelli organizzativi e gestionali 231 si conformino alla progressiva informatizzazione dei processi. Il sistema di controlli dovrebbe evolvere di pari passo rispetto alle modalità di lavoro e di gestione dell'azienda[53], non potendo restare legato a dinamiche tradizionali.

Nel presente studio saranno considerati due principali benefici della *compliance* penale digitale: (i) la riduzione dei tempi di emersione degli indizi di reato e di attivazione degli opportuni controlli; (ii) il potenziamento dei canali informativi e degli elementi di valutazione a disposizione del personale incaricato di svolgere determinate funzioni. Rispetto al primo saranno considerati gli strumenti di *real time analytics*, in grado di generare *alert* automatici in caso di anomalie comportamentali o di contenuti sospetti. Il secondo vantaggio riguarda l'agire informato della società, che potrà disporre di efficienti strumenti per la *due diligence* nei confronti di terze parti, tutte le volte in cui un determinato affare possa essere considerato a rischio.

Come noto, l'esclusione della responsabilità dell'ente opera laddove l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi, secondo le cadenze prospettate agli artt. 6-7 del D. Lgs. 231/2001 a seconda che il *predicate crime* sia commesso da apicali o sottoposti. L'impiego di strumenti tecnologici rappresenta un fattore da considerare nel sindacato sull'idoneità del modello[54], poiché rafforza la tenuta complessiva del sistema di *compliance.* Il supporto offerto da tali strumenti si andrà progressivamente affermando a livello internazionale come *best practice*[55] in vari settori, fungendo da criterio guida per una efficace gestione del rischio[56]. Le buone pratiche aziendali, frutto dell'esperienza maturata negli anni, sono molto diffuse nella realtà socio-economica e, talvolta, sono cristallizzate in standard internazionali.

Si pensi, ad esempio, alla norma ISO 37001 sui sistemi di prevenzione della corruzione[57], che impone di pianificare processi di *due diligence* sui soci in affari per valutare il rischio di corruzione[58], ricorrendo a indagini sulle fonti disponibili per esaminare il coinvolgimento in atti di corruzione, condotte fraudolente, altri illeciti analoghi. I programmi di *decision intelligence* per le analisi su fonti aperte rappresentano, in questa direzione, una valida modalità di verifica delle informazioni sui fornitori.

In altri casi, l'utilizzo della tecnologia a supporto della *compliance* trova fondamento in discipline settoriali o nelle disposizioni delle autorità di vigilanza. Un esempio è dato dalle Linee Guida Confindustria che, nella parte dedicata alle modalità operative di gestione dei rischi, sottolineano la necessità di compiere *due diligence* sui fornitori qualora sia rilevato un "indicatore di sospetto"[59]. Nel settore della prevenzione del riciclaggio si possono richiamare le disposizioni della Banca D'Italia in materia di adeguata verifica del 30 luglio 2019 laddove prevedono che le informazioni per la determinazione del rischio *«possono essere tratte da ogni fonte e documento utile, tra cui fonti giornalistiche autorevoli»* (Sez. II, n. 2, lett. b), con particolare riguardo alle informazioni *«provenienti da organismi e autorità pubbliche, anche di altri paesi comunitari acquisibili anche attraverso siti web»* (Sez. V, n. 2, *sub* iii). Inoltre, gli intermediari sono tenuti a verificare la compatibilità dei dati e delle informazioni fornite dal cliente con le informazioni da essi acquisite autonomamente (Sez. VI)[60], anche per valutare la reputazione

[52] In argomento v. Gullo (2022), p. 1301 secondo cui, sul piano della valutazione giudiziale del modello, l'impiego delle nuove tecnologie potrebbe integrare quelle *best practice* condivise in grado di legittimare una presunzione relativa vincibile dal giudice con motivazione rafforzata.
[53] Per un studio sulle strategie di prevenzione e risposta ai rischi per la sicurezza informatica v. Baskerville *et al.* (2014), p. 138
[54] Di quest'avviso Gullo (2022), p. 1301; Birritteri (2019), p. 294.
[55] Sul tema delle *best pratice* v. Mongillo (2011), p. 75.
[56] Con riferimento alla colpa in organizzazione, la dottrina ha da tempo denunciato la mancanza di regole precauzionali ritenute efficaci secondo il parametro della *societas eiusdem professionis.* Pertanto, nell'effettuazione del giudizio di prevedibilità ed evitabilità del reato da prevenire ci si affida all'attività di autoregolazione societaria. In questo modo l'ente, che è il destinatario della regola cautelare, diviene anche il suo artefice.
[57] UNI ISO 37001:2016. La norma specifica i requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione.
[58] Si vedano i paragrafi 8.1, 8.2 e l'appendice A.10.1 e seguenti.
[59] Linee Guida Confindustria per la costruzione dei modelli di organizzazione gestione e controllo, parte II, par. 4, in www.confindustria.it
[60] L'Allegato II lett. a) delle Disposizioni riporta tra i fattori di rischio elevato la presenza di indici reputazionali negativi relativi al cliente o la sussistenza di procedimenti penali noti e procedimenti per danno erariale, procedimenti per responsabilità amministrativa 231 e sanzioni amministrative, notizie negative provenienti dai media o da altre fonti informative attendibili.

del cliente e del titolare effettivo[61]. Queste fonti settoriali incoraggiano l'uso di *software* di analisi per l'indagine su fonti aperte, che permettono agli operatori finanziari di acquisire informazioni sulla clientela.

In sintesi, nell'attuale società dell'informazione sembra che le migliori tecniche di prevenzione degli illeciti non possano ignorare le potenzialità della rete e degli algoritmi, che diventeranno la base delle *best practice* cui conformarsi per l'adozione di modelli organizzativi e gestionali all'avanguardia.

Alcuni autori sostengono che l'impiego di sistemi automatizzati possa incidere anche sull'accertamento della colpa in organizzazione[62], nei casi in cui la verificazione dell'illecito sia in concreto dovuta al malfunzionamento o a difetti di programmazione dei sistemi informatici adottati[63]. In questi casi l'ente che dimostri di aver attuato le migliori misure tecnologiche di prevenzione andrà esente da responsabilità, difettando l'elemento soggettivo di ascrizione dell'illecito. Si prospettano tuttavia scenari di indubbia complessità per l'accertamento concreto della colpa di organizzazione, la cui sussistenza dipenderà dal grado di affidabilità degli strumenti informatici utilizzati e dalla corretta implementazione degli stessi nelle procedure indicate dal modello 231[64].

1.3. *Sistemi di monitoraggio e prevenzione dei reati.*

Con riferimento alla prevenzione dei reati presupposto nella responsabilità degli enti, si è parlato di "modello matematico 231" per descrivere un sistema automatizzato di presidi e controlli[65]. Tuttavia, ai fini che qui interessano, saranno prese in considerazione soltanto alcune attività di *compliance*, e precisamente quelle necessarie alla acquisizione di indizi di reato nelle aree di maggiore rischio.

Sulla scorta di tali premesse, il presente studio vuole fornire una panoramica dei possibili impieghi di sistemi evoluti di monitoraggio e tracciamento nell'utilizzo delle risorse informatiche aziendali, al fine di rilevare possibili anomalie nei comportamenti del personale coinvolto in processi a rischio di reato (**§2**). Si proseguirà con l'analisi pratico-applicativa delle concrete modalità di implementazione delle nuove tecnologie, ipotizzando alcuni casi d'uso in settori particolarmente critici (es. appalti pubblici, settore bancario, società quotate, **§3**).

Al riguardo è utile precisare che tra i numerosi strumenti automatizzati di raccolta, confronto e analisi dei dati, saranno prese in considerazione tre principali applicazioni: (i) quelle per la rilevazione di indicatori di anomalia e possibili segnali d'allarme – la c.d. *behavior analysis* – in base allo scostamento rispetto ai canoni ordinari di comportamento attesi in base ai modelli aziendali; (ii) il monitoraggio del traffico di dati all'interno all'azienda, allo scopo di individuare situazioni sintomatiche di condotte illecite; (iii) le tecniche di *decision intelligence* su fonti aperte, al fine di elaborare report e generare *alert* per responsabili di funzione circa eventuali rischi nella relazione con terze parti. Con riferimento a queste applicazioni saranno esaminati possibili benefici e rischi, concentrandosi in particolare sulla legittimità *de iure condito* dei sistemi più evoluti di monitoraggio e sulle possibili frizioni con i principi in materia di trattamento dei dati personali (**§4**).

La disamina sulle potenzialità delle *smart technologies* permette di giungere alla conclusione che, allo stato, esse sono uno strumento fondamentale di supporto alla *compliance* aziendale, purché siano implementate in modo attento e consapevole (**§5**).

2. La tecnologia a supporto delle funzioni aziendali.

Prima di procedere all'analisi casistica, occorre inquadrare le principali innovazioni tecnologiche utilizzate per lo sviluppo di strumenti a supporto della *compliance* aziendale. Essi saranno di seguito indicati anche con la locuzione sintetica "Strumenti di Monitoraggio Au-

[61] Gli operatori acquisiscono e valutano informazioni sulla reputazione del cliente e titolare effettivo (parte quarta, sezione II delle Disposizioni).
[62] Nisco (2022), p. 11.
[63] Birritteri (2019), p. 294
[64] Sul tema v. Gullo (2020), p. 283 ss.
[65] Trezza (2021), p. 2

tomatico" (SMA) in modo da mettere in evidenza la loro concreta applicazione nei processi di controllo aziendali.

Tali strumenti si basano su tecniche e *software* innovativi, quali l'*intelligence* su fonti aperte, gli algoritmi di Intelligenza Artificiale, e i sistemi a registro distribuito. I prodotti più complessi ed evoluti nascono dalla combinazione di più innovazioni tecnologiche, così da permettere la generazione di output maggiormente aggiornati ed affidabili.

2.1. *Analisi su fonti aperte e OSINT.*

L'*intelligence* è definita come l'insieme delle attività di raccolta, valutazione e analisi delle informazioni al fine di produrre "il sapere" necessario per il raggiungimento di determinati obiettivi. Essa può assumere connotati differenti, in base all'oggetto[66]. Ai fini della presente analisi rileva in particolare la *Open Source Intelligence* (OSINT), che si fonda sull'attività di analisi delle fonti "aperte", ovvero le fonti pubbliche, liberamente accessibili, non classificate[67]. Oggi Internet rappresenta un formidabile collettore di informazioni poiché, oltre a portali web di mass media (quotidiani online, siti di divulgazione, radio e televisione) e istituzioni[68], raccoglie una grossa mole di *user generated contents*. Per effetto della crescita imponente dei *social network*, si è delineato un nuovo concetto di *Social Media Intelligence* (SOCMINT)[69], per indicare le tecniche basate sulle informazioni che vengono prodotte e scambiate attraverso le piattaforme social, mediante il monitoraggio e l'analisi dei contenuti e delle reazioni condivisi dagli utenti. Dai canali social possono trarsi elementi utili per identificare gli utenti e cogliere eventuali relazioni tra individui e organizzazioni, ricostruire scenari e accertare la corrispondenza rispetto ad altre informazioni presenti nel web.

Tali tecniche assumono grande importanza per la *compliance* penale digitale poiché – come si avrà modo di approfondire[70] – la maggior parte degli strumenti di *decision intelligence* si basa sulla raccolta e l'analisi delle fonti pubbliche. Per fornire un significato ai dati dispersi nel web i risultati della ricerca sono rielaborati da appositi programmi o algoritmi di intelligenza artificiale.

Va peraltro rimarcato come gli orizzonti dell'OSINT stiano divenendo sempre più estesi in ragione del *favor* legislativo per l'apertura dei dati pubblici. La Direttiva 2019/1024/UE (c.d. direttiva sugli *Open Data*) promuove l'utilizzo di dati aperti e favorisce il loro riutilizzo, a fini commerciali e non commerciali, con particolare riguardo alle informazioni detenute da pubbliche amministrazioni, da organismi di diritto pubblico e imprese pubbliche[71]. Si vuole in tal modo accrescere l'offerta di dati pubblici, rendendoli più facilmente disponibili per le imprese[72], assicurando disponibilità di fonti dinamiche e in tempo reale.

Con il D. Lgs. 200/2021 il legislatore italiano ha provveduto a dare attuazione alla Direttiva, predisponendo un sistema di regole volte a incentivare la divulgazione dei dati pubblici[73]

[66] Si distingue, ad esempio, tra *Human Intelligence* (HUMINT) che ha per oggetto le fonti umane e si basa sulla raccolta delle informazioni da soggetti in possesso di informazioni rilevanti per il caso; *Imagery Intelligence* (IMINT), vale a dire l'attività di raccolta informazioni attraverso l'elaborazione e l'analisi di immagini aeree provenienti da satelliti, aerei spia, droni etc.; *Measurement and Signature Intelligence* (MASINT), riferita all'analisi scientifica e tecnica di tracce chimiche, spettrografiche e radiologiche riferite a vettori e sistemi strategici militari; *Signals Intelligence* (SIGINT), basata sull'intercettazione e l'analisi delle comunicazioni sia tra esseri umani, sia tra macchine intelligenti. Cfr. Sagliocca (2017) p. 171

[67] Nel dettaglio l'OSINT è quella disciplina dell'*intelligence* che si occupa della ricerca, raccolta e analisi di dati e informazioni disponibili in fonti aperte, legalmente accessibili al pubblico.

[68] Basti pensare alla quantità di documenti di istituzioni pubbliche reperibili online (es. atti parlamentari, rapporti dell'esecutivo, conferenze stampa, atti giudiziari, pubblicazioni accademiche, atti di convegni, relazioni annuali, albi professionali, documenti programmatici etc).

[69] Massaro *et al.* (2017), p. 425

[70] *Infra* § 4.1.

[71] Secondo la Commissione europea l'adozione della Direttiva era necessaria per rinnovare il quadro giuridico in considerazione delle rilevanti evoluzioni delle tecnologie per la condivisione dei dati e per stimolare ulteriormente l'innovazione digitale, promuovendo nello stesso tempo, la concorrenza e la trasparenza nel mercato dell'informazione pubblica.

[72] Secondo quanto si legge nella Relazione tecnica al D. Lgs. 200/20212 (camera.it) l'intervento normativo sancisce il principio generale secondo cui i dati pubblici e quelli finanziati con fondi pubblici dovrebbero essere riutilizzabili a fini commerciali o non commerciali, perseguendo anche la finalità di renderle più facilmente disponibili per le start-up e le piccole e medie imprese, aumentando l'offerta di dati dinamici e di set di dati con un impatto economico particolarmente elevato e promuovendo la concorrenza e la trasparenza nel mercato dell'informazione.

[73] Il decreto delegato è intervenuto apportando rilevanti modifiche al D. Lgs. 24 gennaio 2006 , n. 36, che già conteneva alcune disposizioni sul riutilizzo di dati pubblici. La citata Relazione tecnica al D. Lgs. 200/2021 riporta alcune statistiche degne di nota sul totale dei dati di tipo aperto resi disponibili nel Catalogo Nazionale (che ammontano a 46.1442), messi a disposizione da 559 pubbliche amministrazioni.

entro limiti ben definiti per categorie particolari di documenti[74]. Benché la finalità principale della normativa sia quella di incentivare il riutilizzo dei dati a beneficio della concorrenza, le imprese potranno utilizzare il *dataset* pubblico anche per rafforzare i sistemi interni *compliance* e le procedure di controllo attraverso l'*intelligence* su fonti pubbliche.

2.2. Machine learning *e intelligenza artificiale.*

Secondo una nota definizione l'Intelligenza Artificiale consiste in *«una scienza e un insieme di tecniche computazionali che vengono ispirate dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire»*[75]. Nel linguaggio comune spesso si utilizza tale concetto per indicare forme di apprendimento automatizzato. Giova pertanto effettuare alcuni chiarimenti concettuali, partendo dalla differenza tra IA e robotica. Mentre la prima si riferisce alla riproduzione di alcune funzioni tipiche della mente umana, la seconda si riferisce alla sostituzione del lavoro corporale dell'uomo[76] con dispositivi meccanici che, nelle applicazioni più evolute, riescono anche a interagire con il mondo esterno (c.d. macchine intelligenti)[77].

Va parimenti tracciata una distinzione tra intelligenza artificiale e algoritmi. Si suole definire "algoritmo" quell'insieme di istruzioni ordinate, funzionali alla produzione di un determinato risultato. In informatica viene indicato come quel procedimento per risolvere un problema attraverso un numero finito di passi elementari, chiari e non ambigui, in un tempo ragionevole[78]. Nel descrivere il funzionamento di un algoritmo viene spesso richiamato il Teorema di Bohm-Jacopini[79] che individua tre strutture principali di elaborazione dei dati: sequenziale, alternativa e iterativa. Nella prima le istruzioni di assegnazione o di calcolo sono eseguite una dopo l'altra; nella seconda vi è una condizione che determina la scelta tra due strutture diverse da eseguire ("se la condizione è vera esegui la struttura 1, altrimenti la struttura 2"). La struttura iterativa invece è costituita dalla ripetizione di un *task* fino a che non è soddisfatta una determinata condizione ("ripeti struttura finché la condizione è vera").

Già queste semplici nozioni aiutano a comprendere come l'algoritmo e l'apprendimento automatico siano concetti non sovrapponibili[80]. Certo, anche l'algoritmo (specie se molto complesso) può essere considerato una forma di intelligenza artificiale, in quanto riproduce alcune categorie logiche della mente umana; ma non tutti gli algoritmi sono anche algoritmi di *machine learning*.

L'apprendimento automatico è quella branca dell'intelligenza artificiale che raccoglie un insieme di metodi e statistiche per migliorare progressivamente la *performance* di un algoritmo. Tecnicamente si suole parlare di apprendimento "supervisionato" quando al *software* vengono forniti esempi in forma di possibili *input* e rispettivi *output* desiderati con l'obiettivo di estrarre una regola generale che associ l'*input* all'*output* corretto. A esso si contrappone l'apprendimento "non supervisionato" dove l'algoritmo è impostato per trovare una struttura negli input forniti, senza che gli input vengano etichettati in alcun modo[81]. Infine nell'apprendimento "semi-supervisionato" si fornisce un *dataset* incompleto per allenare il *software*, cioè un insieme di dati per l'allenamento tra i quali ci sono dati senza il rispettivo *output* desiderato.

Con riferimento a queste forme di apprendimento automatico si è sviluppato il concetto di "rete neurale" per descrivere quei sistemi di elaborazione che, nel trattamento delle infor-

Con l'estensione dell'ambito soggettivo anche alle imprese pubbliche, la platea è destinata ad aumentare notevolmente poiché, dalle ultime rilevazioni dell'ISTAT, le società partecipate sarebbero circa 8.510, delle quali circa 6.085 sono imprese attive operanti nel settore dell'industria e dei servizi.

[74] L'art. 3 del D. Lgs. 36/2006, come modificato dall'art. 1 D. Lgs. 200/2021, elenca i documenti esclusi dall'ambito di applicazione del decreto tra cui quelli detenuti per finalità che esulano dall'ambito dei compiti istituzionali della PA, quelli nella disponibilità di imprese pubbliche non prodotti nella prestazione di servizi di interesse generale o connessi ad attività direttamente esposte alla concorrenza, quelli esclusi dall'accesso ai sensi dell'articolo 24 L. 7 agosto 1990, n. 24 o ai sensi dell'articolo 5-*bis* D. Lgs. 14 marzo 2013, n. 33 etc.

[75] *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence,* Stanford University, 2016, 5, in ai100.stanford.edu/2016-report.

[76] Secondo alcuni robotica deriva dal ceco *robota* che significa "lavoro forzato"; altri ritengono sia una flessione del sostantivo latino *vis-roboris* (forza, energia).

[77] Sul tema di recente v. Minneci *et al.* (2021)

[78] Per approfondimenti sugli algoritmi si rinvia al saggio di Laura (2019)

[79] Bianchini (2007) p. 23

[80] Gillespie (2014), p. 167 ss.

[81] Mozzarelli (2022), p. 266

mazioni, presentano alcune analogie con l'intelligenza naturale tra cui quella di ponderare i fattori di ingresso per giungere a un *output*[82]. Si deve al filosofo Searle[83] la distinzione tra IA debole e forte: la prima svolge alcune funzioni semplici dell'intelletto umano, mentre la seconda è dotata di una capacità cognitiva assimilabile a quella umana.

Ai fini del presente studio, si farà riferimento alla nozione giuridica di Intelligenza Artificiale contenuta nell'art. 3 della Proposta di Regolamento 2021/0106 (COD). É considerato "sistema di intelligenza artificiale" quel software sviluppato secondo uno o più degli approcci elencati *«che sia in grado di generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce alla luce degli obiettivi definiti dall'uomo»*. L'allegato I della Proposta indica tre gruppi di tecnologie: (a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, tra cui l'apprendimento profondo (*deep learning*); (b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; (c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione. Si tratta di una nozione molto elastica, che attrae nell'ambito dell'IA tutte le applicazioni, i servizi, e i dispositivi che riflettono le categorie di ragionamento della mente umana.

Nella materia penalistica l'intelligenza artificiale solleva numerosi interrogativi sul fronte del diritto penale sostanziale (imputabilità, rilevanza causale del danno provocano da sistemi intelligenti, rischio consentito, rapporto di autoria tra agente e fatto di reato)[84] e processuale (utilizzo di algoritmi predittivi per la commisurazione della pena o per determinare la pericolosità sociale di un individuo)[85]. Alcuni autori hanno trattato il tema dalla prospettiva della prevenzione attiva dei reati (c.d. *predictive policing*), facendo riferimento a particolari applicazioni progettate per coadiuvare le forze dell'ordine[86]. Sulla medesima scia si colloca l'oggetto di questo studio, che effettua una ricognizione delle potenzialità offerte dall'IA per la prevenzione dei reati nelle organizzazioni complesse[87], attraverso applicazioni che potremmo definire di *predictive compliance*.

2.3. *Tecnologia a registro distribuito* (Distributed Ledger Technology – DLT).

Le tecnologie a registro distribuito (*Distributed Ledger Technology* o anche DLT) costituiscono una classe di tecnologie complesse fondate sulla combinazione di diverse tecniche informatiche. Tra esse la specie più nota è quella comunemente denominata *blockchain.* Quest'ultima nasce dalla combinazione di due tecnologie diverse, la crittografia asimmetrica e i protocolli di comunicazione *peer-to-peer*, all'interno di una rete interconnessa di elaboratori[88].

Pur racchiudendo soluzioni tecnologiche molto diverse tra loro, le *blockchain* presentano una serie di proprietà comuni riassumibili in quattro principali caratteristiche: (i) la *resilienza* (c.d. *tamper resistance*), poiché ogni nodo reca in sé copia di tutte le transazioni precedenti, sicché, non esistendo alcun singolo punto di fallimento, il sistema è in via generale impossibile o comunque difficile da compromettere nella sua interezza; (ii) la *tendenziale irreversibilità e non ripudiabilità* delle transazioni, che una volta iscritte nel *ledger*, non possono essere modificate se non con il concorso di una maggioranza qualificata di nodi; (iii) l'*immediatezza e automaticità delle transazioni*, che sono processate istantaneamente e automaticamente dai nodi

[82] La rete neurale è costituita da unità elaborative che presentano collegamenti di varia intensità. Partendo dalle unità di input il calcolo si propaga in parallelo nella rete fino alle unità di output, che forniscono il risultato. La rete non viene programmata con istruzioni *ex ante* sull'output, ma addestrata mediante una serie di esempi che consentono l'affinamento dell'output nel tempo. Si parla a tal proposito di *deep learning* per indicare l'insieme di tecniche basate su reti neurali complesse, che permettono l'affinamento della ponderazione, affinché l'informazione finale sia il più possibile completa e affidabile.
[83] Searle (1980), p. 417
[84] Sul tema sia pur con diversità di prospettive v. Consulich (2018), p. 195 ss.; Basile (2019), p. 24 ss.; Borsari (2020); Ubertis, (2020), p. 75.
[85] Nella letteratura straniera v. Burchard (2019b), p. 3 ss.; Starr (2014), p. 809; Kehl *et al.,* (2017). Nella dottrina italiana v. Gialuz (2019); Maugeri (2021); Manes (2020).
[86] Bennett Moses e Chan (2018), p. 806.; Birritteri (2019), p. 291.
[87] Sull'utilizzo dell'IA nella prevenzione della corruzione v. di recente De Simone (2022), p. 51.
[88] Gambino e Bomprezzi (2019), p. 623

validatori; (iv) l'*attribuzione univoca dell'informazione*, assicurata dall'utilizzo della crittografia asimmetrica[89].

Richiamando in estrema sintesi il funzionamento della più nota *blockchain*, quella di Bitcoin, essa si basa sulla marcatura temporale delle transazioni, raggruppate progressivamente in blocchi per formare una vera e propria catena. Le nuove transazioni sono trasmesse a nodi della rete che, previa verifica della validità del trasferimento, si attivano per trovare un numero casuale che possa risolvere una predeterminata funzione algebrica.

Le caratteristiche sin qui esaminate sono proprie della *blockchain* c.d. pubblica in cui manca un titolare del sistema: il connotato essenziale è la decentralizzazione dell'infrastruttura in una pluralità di nodi gestiti da soggetti diversi[90]. Nei sistemi totalmente decentralizzati nessun utente ha privilegi sugli altri, o può controllare le informazioni che vengono memorizzate nei registri, modificarle o eliminarle. Nei sistemi pubblici la fiducia nella rete sembra giustificarsi proprio in virtù della disintermediazione negli scambi, che rappresenta un fattore di garanzia contro i possibili abusi da parte dell'autorità centrale.

Nell'ottica dell'automazione della *compliance* penale, assume particolare rilevanza l'archiviazione di dati informatici sui sistemi DLT, che assicura la certezza della data, l'identificazione univoca del firmatario della transazione, e la tendenziale immodificabilità del registro. Si tratta di una delle caratteristiche di maggior pregio della tecnologia a registro distribuito, tanto che il legislatore vi ha fatto espresso riferimento nella L. 11 febbraio 2019, n. 12 di conversione del D.L. 14 dicembre 2018, n. 135. L'art. 8-*ter* definisce le DLT[91] e pone le basi per attribuire valore legale alle registrazioni di dati informatici in *blockchain*. Si prevede che la memorizzazione di un documento informatico su un registro distribuito produca gli «*effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014*»[92], purché siano rispettati gli standard tecnici fissati dall'Agenzia per l'Italia Digitale[93].

Nel contesto qui in esame, appaiono evidenti i vantaggi delle DLT nella gestione dei dati all'interno dell'ente[94], non solo per la possibilità di "notarizzare" alcune informazioni rilevanti (es. conferimento di deleghe, comunicazioni ufficiali agli organi di controllo etc.) senza ricorrere a soggetti terzi, ma anche per potenziare il controllo dei responsabili sulle diverse procedure previste dal modello organizzativo (es. tracciamento dei passaggi intermedi per l'approvazione di una autorizzazione di spesa).

3. Prevenzione dei reati *ex* D. Lgs. 231/2001. Individuazione di possibili casi d'uso.

Possiamo ora esaminare da vicino le potenzialità offerte dalle *smart technologies* per la prevenzione di reati all'interno delle organizzazioni complesse. La casistica d'uso che segue è stata elaborata sulla falsariga degli elementi ricavabili da modelli organizzativi e gestionali 231 pubblicati sui siti web di importanti società nazionali. Prendendo spunto dai sistemi interni di controllo (es. flussi informativi verso l'OdV, gestione dei flussi finanziari etc.) nelle aree ritenute a rischio di reato, si è delineato uno scenario ipotetico di applicazione degli SMA nelle

[89] Si suole definire la *blockchain* come un registro tendenzialmente inalterabile, poiché nessuno dei nodi dispone – né potrà mai ragionevolmente disporre – di una potenza computazionale sufficiente a imporre un "monopolio" sul processo di verifica delle transazioni. La decentralizzazione diviene così un presidio contro il c.d. attacco del 51%, che si verificherebbe laddove uno o più soggetti, avendo il controllo della maggioranza dei nodi, potessero falsificare *ex post* le registrazioni, decidere unilateralmente quali trasferimenti validare o eludere i presidi contro il *double spending*. Tale caratteristica è propria delle reti pubbliche ad accesso libero, in cui chiunque può mettere a disposizione le proprie risorse per entrare a far parte del *network*.

[90] L'accesso alla rete può essere *permissionless* o *permissioned:* nel primo caso chiunque può prendere parte alla rete, semplicemente scaricando il *software* base e mettendo a disposizione un *hardware* connesso al sistema; nel secondo caso sono previste delle particolari condizioni per il rilascio dell'autorizzazione da parte di una autorità che verifica il rispetto delle condizioni di accesso e definisce il ruolo di ciascun partecipante.

[91] La disposizione definisce le DLT come quelle «*tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*».

[92] La materia è oggi disciplinata dal Regolamento 910/2014/UE che, in un'ottica di armonizzazione delle legislazioni nazionali, individua i requisiti e gli effetti giuridici della validazione temporale elettronica. Circa gli effetti giuridici della validazione temporale il Regolamento prevede che ad essa «*non possano essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali*». Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora, e di integrità dei dati ai quali tale data e ora sono associate.

[93] Ad oggi si resta ancora in attesa della pubblicazione della normativa secondaria dell'AgID sui requisiti tecnici che le DLT debbono possedere in fini indicati dall'art. 8-*ter* D.L. 135/2018. Per approfondimenti v. Piselli e D'Agostino (2019), p. 13

[94] De Simone, (2022), p. 67 ss.

procedure descritte dai modelli organizzativi.

3.1. *Gestione di sistemi informatici di pubblica utilità e appalti pubblici.*

Il primo *case study* riguarda la gestione di un sistema informatico utilizzato da una Centrale di committenza per lo svolgimento di procedure a evidenza pubblica. Gli operatori economici che intendono partecipare alle gare acquisiscono tutte le informazioni utili e accedono al sistema di deposito delle domande di partecipazione direttamente dalla piattaforma messa a disposizione da una società terza.

All'esito delle attività di *risk assessment* tale società ha ritenuto che alcuni processi interni – e in particolare quelli relativi alle attività di supporto tecnico e manutenzione della piattaforma – siano particolarmente esposti al rischio di reato. Nel dettaglio, si è ritenuto concreto il rischio di commissione dei seguenti delitti: (a) frode informatica a danno dello Stato o di altro ente pubblico (art. 24 D. Lgs. 231/2001 in relazione all'art. 640-*ter* c.p.), poiché i dipendenti addetti al supporto sono dotati dei privilegi di amministratore di sistema e possono intervenire sulle informazioni pubblicate sulla piattaforma, modificandole a propria discrezione. Si teme in particolare che vi possa essere un intervento senza diritto sui dati relativi alle coordinate per i pagamenti (es. spese per la partecipazione, versamento di cauzioni provvisorie alle Stazioni appaltanti), al fine di ottenere un profitto; (b) accesso abusivo a sistema informatico (art. 24-*bis* D. Lgs. 231/2001 in relazione all'art. 615-*ter* c.p.) con riferimento alle informazioni e ai segreti commerciali contenuti nelle offerte tecniche formulate dagli operatori economici in sede di gara. Difatti il Sistema gestisce anche procedure per l'acquisto di servizi informatici, che potenzialmente rientrano nel business della Società concessionaria. Si teme quindi un accesso non autorizzato finalizzato ad acquisire informazioni commerciali (es. soluzioni tecniche, *know-how* etc.) da poter riutilizzare a vantaggio della società in altre gare pubbliche; (c) danneggiamento informatico (art. 24-*bis* D. Lgs. 231/2001, in relazione agli artt. 635-*bis* ss. c.p.), falso informatico (art. 24-*bis* D. Lgs. 231/2001, in relazione all'art. 491-*bis* c.p.) e frode informatica a danno dello Stato o di altro ente pubblico, relativamente al rischio di cancellazione o alterazione di dati dal Sistema per favorire alcuni partecipanti (es. imprese con cui sussistono buoni rapporti commerciali o di collaborazione).

Ciò posto, la società vorrebbe dotarsi di alcuni applicativi che consentano di rilevare anomalie e segnalarle ai competenti organi di controllo. In particolare, con riferimento alle ipotesi *sub* (a), un sistema di *alert* nel caso in cui, durante una sessione, siano in qualsiasi modo modificati o alterati parametri relativi a spese e pagamenti (importi, coordinate bancarie, termini di pagamento, e altre informazioni economicamente rilevanti). Inoltre, per agevolare l'emersione di eventuali condotte illecite, l'applicativo dovrebbe poter effettuare un controllo automatizzato e un *matching* con le comunicazioni effettuate all'interno dell'azienda (es. rilevare che nei giorni precedenti, in un messaggio di posta si discuteva di modificare un importo o una coordinata bancaria)[95].

Quanto all'ipotesi *sub* (b), si ipotizza l'impiego di un *software* in grado di riconoscere per parole chiave le procedure e le offerte in qualche modo connesse e collegate al business della società, esposte al rischio di accesso abusivo. In tal caso l'applicativo dovrebbe limitare l'accesso a utenze predeterminate (es. ai soli responsabili incaricati) e tenere traccia di eventuali copie o *download* di documenti dalla piattaforma.

Infine, avuto riguardo ai reati *sub* (c), si prospetta l'utilizzo di un applicativo "intelligente" che possa segnalare agli organi di controllo della società l'avvenuta registrazione nel Sistema (oppure la presentazione di un'offerta) di un'impresa potenzialmente affiliata o comunque nota alla Società. Il *software* dovrebbe essere in grado di associare la denominazione dell'impresa all'elenco dei fornitori oppure alle registrazioni contabili della Società, ovvero di consultare fonti aperte (es. motori di ricerca, *web crawling*, etc.) per trovare dei collegamenti tra due o più aziende (es. si riesce a riconoscere che l'impresa partecipante alla gara fa parte di un gruppo affiliato etc.). L'applicativo dovrebbe anche consentire di segnalare eventuali scambi di messaggi, in entrata o in uscita, con indirizzi riconducibili all'impresa affiliata nei giorni precedenti o successivi rispetto alla registrazione nella piattaforma.

[95] Un tale applicativo potrebbe essere utile anche per far emergere possibili dinamiche corruttive nel caso in cui l'intervento senza diritto sui dati di pagamento sia stato oggetto di trattative illecite con un funzionario pubblico.

3.2. Compliance *nel settore bancario-creditizio.*

Un secondo caso d'uso riguarda da vicino il settore bancario-finanziario. Nel modello organizzativo e gestionale di una Banca sono individuate alcune attività a rischio di reato, tra cui le seguenti: (a) corruzione attiva (art. 25 D. Lgs. 231/2001, in relazione all'art. 321 c.p.), poiché la società intrattiene rapporti economici con molti Comuni ed enti pubblici, gestendo fondi per centinaia di milioni di Euro. Si ritiene particolarmente concreto il rischio che i dirigenti della società possano pagare tangenti per ottenere una proroga nell'affidamento dei servizi; (b) ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza (art. 25-*ter* D. Lgs. 231/2001 in relazione all'art. 2638 c.c.) con riferimento in particolare alla mancata comunicazione mensile dei dati relativi ad alcune operazioni alla Banca D'Italia; (c) riciclaggio (art. 25-*octies* in relazione agli artt. 648-*bis* e seguenti c.p.), finanziamento del terrorismo (art. 25-*quater* in relazione all'art. 270-*quinquies.1* c.p.) o delitti di criminalità organizzata (art. 24-*ter* D. Lgs. 231/2001) nell'instaurazione di relazioni di affari con nuovi clienti.

Visti gli esiti dell'ultima valutazione dei rischi, la Banca vorrebbe integrare alcuni SMA nei processi aziendali per facilitare l'emersione di prassi o flussi finanziari a rischio di reato. Segnatamente, avuto riguardo al rischio di corruzione attiva *sub* a), un sistema in grado di individuare attraverso tecniche di OSINT o sulla base di istruzioni predeterminate, i nominativi dei vertici amministrativi (dirigenti, alti funzionari) e politici (sindaci, presidenti etc.) di enti pubblici con cui la Banca intrattiene rapporti economici. Il sistema dovrebbe monitorare le comunicazioni che intercorrono tra la Banca e gli indirizzi istituzionali dei funzionari coinvolti, in modo da segnalare eventuali anomalie (ad es. uno scambio di mail tra indirizzi con richieste di incontro o di appuntamento).

Con riferimento alla prevenzione del reato *sub* (b), un SMA in grado di segnalare le anomalie comportamentali rispetto alle procedure ordinarie seguite dalla Banca e alle tempistiche individuate dalla legge. Tale sistema dovrebbe prevedere *alert* e segnalazioni automatizzate qualora, ricevuta una richiesta qualificata da un indirizzo istituzionale, l'organizzazione non segua il pattern di comportamento atteso (es. non si osservino le procedure previste dal modello o vi siano comunicazioni sintomatiche della volontà di occultare certe informazioni).

Infine, rispetto al rischio di commissione dei reati *sub* (c), si vorrebbe implementare un sistema in grado di estrapolare dati da fonti *open source* per calcolare un punteggio di rischio associato alla persona fisica o giuridica che richiede di entrare in affari con la Banca. Nella specie, il *software* dovrebbe essere in grado di: sintetizzare in un report le notizie disponibili online sul cliente, relativi a possibili coinvolgimenti in atti illeciti (es. legami con la criminalità organizzata, indagini per fatti di riciclaggio); confrontare le risposte fornite dal cliente in sede di acquisizione di informazioni AML con le notizie disponibili online (es. sul profilo di rischio o sulla professione del cliente); fornire un *alert* ogniqualvolta, successivamente alla instaurazione della relazione d'affari, sopravvengano nuove notizie sulla posizione del cliente[96].

L'applicativo dovrebbe avere due funzionalità essenziali: la generazione di report reputazionali *one-shot* prima di entrare in affari con il cliente; il monitoraggio periodico alla ricerca di nuove informazioni online. Con riferimento a questa seconda funzione, il nominativo del cliente inserito in "black-list" sarà oggetto di successivi controlli automatizzati; il sistema provvederà ad inviare in tempo reale un *alert* non appena risulteranno disponibili in rete informazioni potenzialmente rilevanti.

3.3. *Società quotate, redazione di bilanci e conflitti di interessi.*

Si è infine ipotizzato il caso di una società quotata, facente parte di un gruppo, il cui modello organizzativo e gestionale – adottato ai sensi dell'art. 6 del D. Lgs. 231/2001 – individua alcuni processi a rischio di reato tra cui: (a) quelli collegati all'ufficio acquisti, con particolare riferimento ai delitti di falso in bilancio (art. 25-*ter* D. Lgs. 231/2001 in relazione agli artt.

[96] Le analisi reputazionali saranno attivate soltanto in casi specifici (es. quando vengono richieste operazioni superiori a un certo ammontare) o quando si abbia motivo di ritenere che l'attività esercitata dal Cliente presenta il rischio di interferenze illecite.
Per *software* di questo tipo si veda ad es. il sistema CERICO, offerto da Dow Jones Risk & Compliance; oppure il software World Check della Thomson-Reuters che comparano dati provenienti da svariati fonti pubbliche al fine di valutare i rischi legali e reputazionali che l'impresa può correre intraprendendo una certa operazione. Sul tema, anche per riferimenti alla letteratura statunitense v. Birritteri (2019), p. 295.

2621 e seguenti c.c.) e corruzione (art. 25 D. Lgs. 231/2001, in relazione all'art. 321 c.p.), stante la verificazione in passato di fenomeni di *overpricing* e di *downpricing* (stipulazione di contratti e iscrizione a bilancio di prezzi per acquisiti molto superiori rispetto alla media del mercato); (b) quelli relativi alle deliberazioni del CdA su particolari materie, limitatamente al reato di omessa comunicazione del conflitto di interessi (art. 25-*ter* D. Lgs. 231/2001 in relazione all'art. 2629-*bis* c.c.), tenuto conto del consistente numero e della frequente alternanza dei membri del CdA (che durano in carica tre anni e che spesso, in passato, hanno ricoperto posizioni analoghe in primarie società nazionali).

La società intende automatizzare parte dei compiti di controllo attribuiti all'OdV e ai revisori contabili e dotarsi di strumenti di analisi preventiva di possibili rischi. Nella specie, con riferimento ai reati *sub* (a) utilizzare un applicativo integrato nel gestionale in uso, che possa confrontare in modo automatico e in tempo reale i prezzi di acquisto con il prezzo medio di mercato desumibile da listini, mercuriali o tariffari (specialmente per acquisti standardizzati). A tal fine si prevede che per ogni acquisto debba essere compilato un *form* in formato *excel* nel quale sono riportate quantità e prezzi di acquisto. L'applicativo dovrà pertanto estrarre questi dati e confrontarli con quelli desumibili da fonti aperte e inviare un *alert* ai responsabili in caso di anomalie.

Quanto al reato *sub* (b), la società vorrebbe sfruttare le potenzialità dell'OSINT per rivelare l'esistenza di potenziali conflitti di interessi nelle relazioni con terze parti. Il *software* dovrà essere in grado di rivelare l'esistenza di pregressi rapporti (professionali, imprenditoriali, amicali etc.) tra gli amministratori o i componenti del Consiglio di Gestione e terzi fornitori o controparti contrattuali. Tra i criteri rivelatori del "conflitto di interessi" saranno considerati anche i precedenti professionali del vertice aziendale in una data materia (es. se l'operazione riguarda l'acquisto di autovetture, si potrà fornire al *software* una istruzione per verificare un *linkeability* tra l'amministratore e il settore automotive). In sostanza l'analisi verterà tanto su rapporti personali diretti (associazione per soggetto), quanto su legami indiretti (associazione per oggetto).

4. Applicazione delle nuove tecnologie ai casi d'uso considerati.

I casi d'uso sopra esemplificati rappresentano soltanto alcune possibili applicazioni dei SMA per l'automazione della *compliance* penale. Le soluzioni tecnologiche ivi descritte non sono strettamente legate a tali contesti, e possono essere applicate per la prevenzione di reati anche in ambiti e settori economici diversi.

Poiché i *software* di raccolta e analisi dei dati non sono stati sviluppati per offrire supporto alla *compliance* penale, ci si interroga sul possibile impiego di tali programmi al fine prevenire la commissione di reati all'interno dell'azienda[97]. La soluzione affermativa dipende, in buona misura, dalla capacità dell'ente di riadattare gli applicativi di uso comune (es. SIEM, sistemi di *Data Classification* etc.) per favorire i controlli sui processi a rischio di reato. Si tratta di un'attività complessa che richiede competenze tecniche adeguate per mettere in funzione e supervisionare l'utilizzo dei sistemi. Si dovranno inoltre individuare i *cluster* di dati rilevanti ai fini della elaborazione di un *output*, e predisporre le dotazioni *hardware* (sistemi, *workstation*, *server* etc.) e di connessione (es. intranet aziendale) necessarie per l'utilizzo degli applicativi.

Nel prosieguo, gli strumenti di supporto alla *compliance* sono analizzati in base alle diverse tipologie di *software* utilizzabili.

4.1. Software *di* decision intelligence *e OSINT.*

L'imponente mole di dati reperibile online rappresenta un vero e proprio patrimonio informativo che gli enti possono impiegare a supporto della *compliance* penale. I programmi di analisi su fonti aperte sono stati elaborati per agevolare la raccolta di informazioni sulle controparti contrattuali (c.d. *due diligence* di terze parti) in modo da rendere più consapevole la decisione di entrare in affari con determinati soggetti. Più in generale di parla di *decision*

[97] Morgante e Fiorinelli (2022), p. 8

intelligence (o *decision support*) per descrivere quei *software* in grado di mettere in relazione due o più chiavi semantiche ordinando i risultati della ricerca secondo impostazioni predefinite[98]. Il principale scopo di tali programmi è quello di comporre un quadro conoscitivo per assumere scelte consapevoli nella gestione societaria.

Di regola questi software eseguono uno *scraping*[99] delle risorse del web, passando in rassegna i risultati forniti dai motori di ricerca, ordinati secondo filtri e criteri specifici. Ciò consente di cogliere la relazione tra due o più elementi testuali e di rendere intellegibile la correlazione tra essi; talvolta si utilizza la trasposizione in grafi[100] per illustrare in modo figurato l'associazione logica tra i risultati e consentire la c.d. *link analysis*.

Gli applicativi più evoluti permettono di eseguire ricerche per chiavi semantiche non soltanto su fonti aperte ma anche su database privati (es. archivi e risorse informatiche dell'azienda)[101], e di porre eventualmente in relazione i relativi risultati. La ricerca può avere ad oggetto dati strutturati o non strutturati[102] come emerge dalla casistica d'uso sopra esemplificata[103].

Per la raccolta e l'analisi delle informazioni si utilizzano tecniche di intelligenza artificiale applicate all'analisi semantica e multimediale, mediante algoritmi di *data mining* molto avanzati. Questi aggregano i dati in modo massivo, offrendo agli analisti un quadro generale ottenuto dalla correlazione di una pluralità di fonti e la visualizzazione di relazioni complesse tra le chiavi di ricerca. I programmi più avanzati si servono del *machine learning* anche per raffinare i risultati della query escludendo falsi negativi e falsi positivi dalla correlazione semantica[104].

Una volta elaborato il sistema di correlazione tra i dati, gli applicativi in esame permettono di analizzare i trend in tempo reale, aggiornandosi in base ai nuovi dati inseriti nel database o rintracciati online. L'analisi dinamica e continuativa delle fonti si rivela fondamentale per i processi di controllo aziendali poiché consente di generare automaticamente segnali di anomalia[105]. I modelli organizzativi dovrebbero prevedere specifiche procedure di riesame degli *alert*, attivando gli opportuni presidi nel caso in cui la segnalazione risulti attendibile.

La nota di maggior pregio degli strumenti in esame consiste nella possibilità di costruire ricerche "mirate" per argomento selezionando una o più categorie da una lista predefinita. Alcuni *software* prodotti da società americane sono stati sviluppati per la *due diligence* in determinati ambiti disciplinari attraverso la previa selezione di tutte le parole chiave e le forme flesse di uso comune in tali ambiti. Sarà dunque sufficiente inserire il nome di una persona fisica o di un ente per ottenere, all'esito della *query*, ogni possibile correlazione tra questi e i settori considerati[106]. Le imprese potranno così prevenire l'instaurazione di rapporti con soggetti coinvolti in affari illeciti e verificare la veridicità di quanto dichiarato da clienti e fornitori.

Sul versante giuridico emergono tuttavia alcune criticità collegate al trattamento dei dati personali, laddove il sistema attribuisca alle persone fisiche una classificazione di rischio[107]. Se-

[98] Alcuni applicativi permettono di fare ricerche non soltanto in pagine del *surface web*, ma persino nella parte "oscura" (il c.d. *dark web*) della rete.

[99] Lo *scraping* è una tecnica che consiste nel prelevare dati dal web. Il processo di estrazione è automatizzato grazie all'uso di un software che, dopo aver visitato un sito per ottenere dati, compila un database e analizza i risultati. Si pensi, ad esempio, ai siti che mettono a confronto i prezzi di alcuni prodotti (es. viaggi, assicurazioni etc.) mediante *web scraping* dei portali di vendita online.

[100] Il grafo in informatica descrive una figura geometrica (bidimensionale o tridimensionale), costituita da un insieme finito di punti, detti nodi (o vertici), e da segmenti o archi che congiungono coppie di nodi.

[101] Alcune piattaforme disponibili sul mercato si basano su tecniche OSINT e SOCMINT per integrare i dati ricavabili da fonti aperte con le informazioni dei database aziendali. Il matching tra i dati è effettuato impartendo le istruzioni fondamentali al software e dettando criteri specifici. A tal fine è indispensabile il ruolo dell'analista dei dati nell'impostare il sistema a seconda delle specifiche esigenze.

[102] Con "dati strutturati" si suole indicare quelli organizzati secondo schemi e tabelle (es. un file excel). Sono invece "non strutturati" i dati privi di schema (come quelli contenenti testi a carattere narrativo o file multimediali).

[103] Nel caso del software che mette in relazione i tabulati dell'ufficio acquisti con i listini prezzi ufficiali (v. *supra* §3.3 lett. a) i dati saranno disponibili in forma strutturata. Diversamente, per la valutazione del punteggio di rischio associato a determinate operazioni (v. § 3.2. lett. c) e in genere in tutti i casi di due diligence di terze parti si tratta di dati non strutturati.

[104] Ipotizzando una ricerca sull'affiliazione commerciale (v. § 3.1., lett. c) tra l'impresa Alfa e Beta, l'utilizzo del *machine learning* permette di non inquinare la ricerca con risultati in cui "Alfa" e "Beta" sono utilizzati in altri contesti lessicali. Il Natural Language Processing (NLP) indica gli algoritmi di IA in grado di analizzare il linguaggio naturale per comprenderne il contenuto, estrapolarne il significato, tradurlo in altra lingua etc., a partire da dati o documenti forniti in input. Si parla anche di linguistica computazionale per indicare lo studio del linguaggio naturale in modo da elaborare programmi eseguibili dalle macchine.

[105] Così, nei casi pocanzi esemplificati il sistema genera un *alert* quando sopravvengono notizie su un cliente ritenuto a rischio (v. § 3.2. lett. c) o sui rapporti tra un apicale della banca e un cliente coinvolto in una operazione economicamente molto rilevante.

[106] Per valutare il coinvolgimento di un socio in affari in traffici illeciti si potrà spuntare la categoria "criminalità organizzata" per ottenere l'associazione del nominativo a parole chiave come mafia, art. 416-*bis,* concorso esterno, scambio elettorale, boss, intimidazione, misura di prevenzione, DIA, etc.

[107] Sul tema del rating reputazionale, sia pur prospettive diverse, v. Sciascia (2021), p. 317 ss.; Ammannati e Greco (2021), p. 290

condo una recente sentenza di legittimità[108], gli strumenti di calcolo del rating reputazionale delle persone fisiche sono illegittimi in assenza di specifico ed espresso consenso dell'interessato. Nello specifico la Cassazione ha affrontato il caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche, col fine di contrastare fenomeni basati sulla creazione di profili artefatti o inveritieri e di calcolare, invece, in maniera imparziale la reputazione dei soggetti censiti, in modo da consentire a eventuali terzi una verifica di reale credibilità. Nell'accogliere il ricorso proposto dall'Avvocatura dello Stato, la Corte ritiene che il problema alla base del calcolo del rating è costituito dalla validità del consenso che si assume prestato al momento della registrazione. Non potrebbe dirsi valida l'adesione a un sistema automatizzato, che si avvale di un algoritmo per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili gli schemi con cui il software si esprime né i fattori considerati.

Nel giudizio di merito il Tribunale di Roma[109] aveva riconosciuto l'illegittimità del rating reputazionale riferito a soggetti che non avevano prestato il consenso per accedere al servizio, i cui nominativi potevano desumersi dai documenti inseriti nella piattaforma.

Nell'applicare tali principi alla raccolta di dati ricavabili da fonti aperte e alle attività di OSINT, emergono sostanziali differenze rispetto al caso affrontato dalla Corte. *In primis* perché il trattamento ha ad oggetto unicamente dati pubblicati sul web accessibili a chiunque finché l'interessato non eserciti i propri diritti (es. limitazione o cancellazione); in secondo luogo perché la maggior parte dei programmi non elabora un punteggio reputazionale, limitandosi a mettere in correlazione notizie, link e immagini. Pur non essendo dubitabile che l'impiego di tali *software* possa dar luogo a un "trattamento" in senso tecnico-giuridico[110], è altrettanto vero che esiste una base giuridica che legittima le operazioni[111].

4.2. *SIEM e analisi dei dati di traffico.*

L'analisi dei dati di traffico viene spesso utilizzata in chiave preventiva di possibili attacchi informatici ai danni dell'impresa; essa rappresenta una misura di *cybersecurity* particolarmente efficace per tenere traccia di tentativi di intrusione da parte di IP sconosciuti o per sventare minacce cibernetiche di vario genere.

In informatica si parla di *Security Information and Event Management* (SIEM)[112] per indicare quei *software* di monitoraggio in tempo reale degli eventi di rete, in grado di correlare, segnalare e reagire in modo automatico a determinati accadimenti. Il programma tiene traccia, all'interno di un registro, di tutti i dati di traffico al fine di rilevare possibili minacce alla sicurezza della rete aziendale. I prodotti più diffusi sul mercato prevedono l'installazione del SIEM all'interno di un *server* centralizzato nel quale confluiscono tutti i dati di traffico generati dalla rete locale[113]. I dati raccolti e processati non riguardano il contenuto delle comunicazioni informatiche, ma soltanto gli estremi delle comunicazioni intercorse[114]; nel registro degli eventi si tiene traccia dei log e degli indirizzi IP, dell'ora e della data della connessione ed eventualmente della quantità di dati scambiati. Dopo la fase di raccolta e acquisizione, il sistema procede al c.d. *arricchimento* dei dati, ricavando informazioni sulla localizzazione geografica dell'IP e sulla reputazione ad esso attribuitagli da fonti autorevoli.

[108] Cass. Civ., Sez. I, 25 maggio 2021 n. 14381 in *Media Laws*, 16 giugno 2021, con nota di Paolucci (2021); e in Federalismi.it, 11 agosto 2021, con nota di G. Lo Sapio (2021).
[109] Tribunale di Roma, Sez. I, 4 aprile 2018, n. 5715.
[110] L'art. 4, par 1, n. 2 GDPR definisce il "trattamento" come «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».
[111] Da rinvenirsi, a seconda dei casi, nel consenso dell'interessato (si pensi ai dati spontaneamente condivisi sui *social network*), nell'esistenza di un obbligo legale al quale è soggetto il titolare del trattamento (es. obblighi di identificazione della cliente e segnalazione delle operazioni sospette in base alla normativa antiriciclaggio), nel perseguimento del legittimo interesse dell'impresa o di terzi, O nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (cfr. sulle condizioni di liceità del trattamento, art. 6 GDPR).
[112] L'acronimo nasce dalla crasi di SIM (*Security Information Management*) e SEM (*Security Event Management*) per definire quei programmi che presentano entrambe le funzionalità (gestione della sicurezza delle informazioni e gestione degli eventi informatici).
[113] Le attività in entrata e in uscita tra i *device* all'interno della rete aziendale sono duplicate attraverso una porta SPAN (*Switched Port Analyzer*), che produce una copia *mirror* del traffico di rete per inviarlo al server SIEM di destinazione.
[114] Ai fini della normativa privacy "dato relativo al traffico" è «*qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione*» (art. 1, comma 1, lett. h D. Lgs. 196/2003).

Gli eventi sono classificati per tipologie e associati in base a regole di correlazione predefinite, ferma la possibilità di impartire istruzioni personalizzate a fronte di esigenze specifiche. Tali regole rendono fruibile il registro degli eventi che, anche in organizzazioni di ridotte dimensioni, conta migliaia di attività al giorno.

Laddove il SIEM dovesse individuare attività anomale, verrà emessa una notifica per segnalare la presenza di una possibile minaccia[115]. I programmi più evoluti attribuiscono un punteggio di rischio (es. in scala decimale) agli eventi di rete, così da far emergere immediatamente le attività maggiormente pericolose. Grazie all'uso del *machine learning* il SIEM perfeziona la regola di giudizio "allenandosi" su un database di eventi-tipo, nel quale gli analisti hanno valutato casi analoghi. Tra i principali indici di rischio si tiene conto della reputazione dell'indirizzo IP in base alla sua provenienza geografica, al numero di "visite" e alla prossimità temporale delle richieste di accesso[116]. Per rilevare anomalie il sistema tiene traccia di tutte le attività intercorse nei giorni precedenti, di modo che un evento considerato "neutro" sarà valutato come una potenziale minaccia laddove venga rilevato un pattern anomalo di comportamento.

Di regola i SIEM sono utilizzati per prevenire attacchi informatici mediante il blocco automatico delle attività sospette, respingendo ad es. le richieste di accesso e connessione ritenute sospette, o per rilevare la presenza di *malware*. Si tratta ora di comprendere se, ed eventualmente in che misura, applicativi di questo genere possano coadiuvare la prevenzione di reati commessi nell'esercizio dell'impresa. Attuando una sorta di capovolgimento di prospettiva, si dovrà chiarire se i SIEM siano in grado di fornire una qualche utilità nel caso di illecito commesso nell'interesse o a vantaggio dell'ente.

A ben vedere, l'analisi dei dati di traffico permette di rilevare anomalie anche nelle comunicazioni in uscita o interne all'azienda. Il sistema tiene traccia delle autenticazioni attraverso le periferiche di rete, individuando eventuali accessi non autorizzati o violazioni delle politiche interne all'impresa. Poiché la correlazione tra eventi si basa su criteri predefiniti, l'utilizzo dei SIEM nei sistemi di controllo *ex* D. Lgs. 231/2001 appare sicuramente plausibile dal punto di vista tecnico. Il sistema andrà customizzato per mettere in evidenza gli eventi ritenuti di interesse per la prevenzione di determinati reati presupposto.

Riprendendo la casistica d'uso pocanzi delineata, si pensi al sistema informatico per la presentazione delle domande di partecipazione a gare pubbliche[117]. L'ente che gestisce la piattaforma può utilizzare un SIEM per raccogliere i dati di traffico e registrare i log delle utenze dotate dei diritti amministrativi. Saranno così segnalati eventi che, sulla base delle istruzioni fornite, presentino indici di anomalia: tentativi ripetuti di accesso, attività in orari non abituali, autenticazione con account mai utilizzati in una determinata *workstation* etc. Per arricchire ulteriormente le informazioni ricavate dai log, esiste la possibilità di integrare i dati di traffico con sistemi di *Data Classification* e *Data Loss Prevention*[118]. La classifica dovrà tener conto degli esiti della valutazione dei rischi e attribuire particolare valore ai dati che presentano collegamenti più stretti con i reati presupposto indicati dal modello 231. Nel caso esemplificato, il sistema potrà "etichettare" in automatico i dati relativi ai pagamenti e quelli relativi alle offerte tecniche presentate per la fornitura di servizi informatici[119], avvisando i responsabili delle funzioni di controllo in caso di attività anomale. Ciò consente di prevenire efficacemente accessi abusivi e frodi informatiche commessi a vantaggio dell'ente nei processi ritenuti a più alto rischio.

[115] Gli avvisi sono recapitati tramite la dashboard del programma oppure utilizzando servizi di posta elettronica o telefonia.

[116] Così, ad esempio, sarà attribuito un punteggio di rischio elevato alle connessioni che provengono da un IP straniero sconosciuto che, nell'arco di pochi minuti, ha inoltrato decine di richieste di accesso. Parimenti, l'indice di rischio sarà via via più elevato se a cadenza periodica l'IP sospetto continua a tentare accessi ai server aziendali.

[117] Si veda § 3.1.

[118] Per *Data Classification* si intende quel processo volto a individuare i dati sensibili all'interno di un database, al fine di determinare i controlli di sicurezza necessari in base all'importanza delle informazioni. I sistemi di *Data Classification* effettuano ricerche testuali complesse (frasi, composti di parole e vocaboli polisenso) grazie ad algoritmi di NPL, indicizzando i dati sensibili in base ai risultati della *query*. La *Data Loss Prevention* indica quei sistemi che identificano e proteggono i dati aziendali (in uso o archiviati), al fine di prevenire l'uso non autorizzato e la trasmissione di informazioni riservate.

[119] I sistemi di classifica del dato sono basati su elementi testuali "inequivocabili" riconosciuti come sensibili a livello aziendale. Così, nel caso addotto ad esempio, una coordinata IBAN o le specifiche tecniche di un software presentano alcuni elementi semantici distinguibili dalla mole di dati presenti nella piattaforma.

4.3. *Domini aziendali e flusso di comunicazioni.*

Il SIEM non consente di vagliare il contenuto delle comunicazioni informatiche, ma soltanto di analizzare il traffico di rete che transita per i server aziendali. Per questo motivo esso non è in grado, ad esempio, di monitorare il contenuto delle e-mail scambiate all'interno dell'organizzazione[120]. Il controllo sui messaggi di posta rappresenta un efficace strumento di prevenzione, specialmente nei casi in cui l'*iter criminis* si articoli in più fasi e richieda una previa concertazione tra il personale aziendale. Astrattamente lo si potrà impiegare per qualsiasi processo a rischio di reato, purché vi siano degli elementi testuali inequivocabili – o quantomeno discriminanti – che lascino presagire l'imminente commissione di un reato. A tal fine si dovranno stabilire regole rigide sui processi comunicativi all'interno dell'azienda, privilegiando l'utilizzo della posta aziendale per tutte le comunicazioni lavorative in luogo degli account personali.

Dal punto di vista tecnico il monitoraggio è eseguito grazie ad algoritmi di NPL[121] che, una volta impostati e collegati con la casella gestita dal *service provider* di posta[122], sono in grado di "comprendere" il significato dei messaggi e segnalare eventuali contenuti sospetti. Ciò permette di irrobustire i processi di controllo, facilitando l'emersione di condotte illecite e l'invio di segnalazioni tempestive ai responsabili di funzione.

Alcuni prodotti utilizzano l'intelligenza artificiale per ottenere metriche e attribuire un punteggio di rischio ai messaggi scambiati all'interno dell'azienda, in modo da indirizzare il controllo umano verso le comunicazioni ritenute più pericolose. Il grado di affidabilità dell'*output* dipende dalle istruzioni di partenza e dal peso attribuito ai diversi fattori. Di regola gli algoritmi sono impostati per associazioni semantiche di parole o di altri elementi del messaggio[123], e funzionano in modo dinamico. L'indice di rischio non è legato al messaggio in sé, ma tiene conto delle possibili attività sospette rilevate nei giorni precedenti[124]. Il segnale di *alert* sarà generato soltanto laddove la valutazione algoritmica superi una certa soglia, predeterminata in base alle specifiche esigenze e al contesto in cui il software è impiegato.

Nonostante i numerosi vantaggi, devono essere considerati anche gli aspetti critici relativi alla riservatezza di alcune comunicazioni aziendali e alla *privacy* degli individui[125]. Il monitoraggio attivo delle mail rischia di sovvertire gli schemi di *governance* della società, in quanto anche i messaggi più delicati sulla gestione dell'impresa (es. una conversazione tra amministratori) potrebbero astrattamente essere "intercettati", con conseguente alterazione gli equilibri societari e del delicato rapporto tra organi di amministrazione e funzioni di controllo. Per non considerare quelle comunicazioni che, per loro natura, devono restare strettamente segrete per evitare che altri all'interno dell'azienda possano trovare occasione per commettere un reato (si pensi alla circolazione di informazioni privilegiate, quanto alla responsabilità *ex* art. 25-*sexies* D. Lgs. 231/2001). Trattandosi di un rischio concreto, si è dell'avviso che l'ambito di applicazione dei sistemi in esame dovrebbe essere circoscritto ai soli processi a più alto rischio[126], previa adozione delle cautele necessarie per impedire che si addivenga a forme di controllo generalizzato[127].

Venendo al secondo aspetto, si dovrà chiarire se il monitoraggio del traffico di mail possa ritenersi legittimo in base al diritto vigente. Circa il controllo a distanza dell'attività dei lavoratori la giurisprudenza più recente ha chiarito che l'art. 171 D. Lgs. 196/2003 non è

[120] Si vedano al riguardo i casi d'uso individuati in precedenza v. §3.1. lett. a) e lett. c); § 3.2. lett. a)
[121] Sul *Natural Language Processing* v. *supra* §4.1.
[122] Alcuni applicativi dialogano direttamente con il gestionale di posta elettronica attraverso interfacce di programmazione; altri invece leggono il contenuto delle mail archiviate in un database. In entrambi i casi l'elaborazione dei dati avviene in tempo reale, così da generare immediatamente *alert* in caso di anomalie.
[123] Ad esempio, nel caso esemplificato, vocaboli afferenti a "denaro" o "pagamenti" rispetto all'indirizzo del destinatario del messaggio (riconosciuto come istituzionale) o alle parole "Comune", "funzionario" etc.
[124] Così, nel caso in cui vi sia stato uno scambio tra colleghi per discutere dell'impugnazione di un provvedimento negativo di aggiudicazione, il sistema attribuirà al messaggio un profilo di rischio basso. Il punteggio diventerà via via più alto se nei giorni successivi un apicale dovesse scrivere alla Stazione appaltante parlando di denaro o altri vantaggi economici.
[125] Per un approfondimento del tema in chiave giuslavoristica v. Alagna (2018), p. 339 ss.
[126] Sarebbe opportuno limitare il monitoraggio del traffico di mail a uno o più indirizzi (dedicati alla gestione di determinati affari) in relazione alla tipologia di reato che si vuole prevenire.
[127] L'ente dovrà dotarsi di discipline specifiche (codici di condotta, istruzioni operative, accordi di riservatezza) per garantire che l'accesso al software sia dato al solo personale incaricato e nei limiti delle funzioni attribuite. Salvi gli obblighi di comunicazione previsti dal modello (es. flussi informativi all'organismo di vigilanza), le informazioni apprese nell'esercizio di tali funzioni dovrebbero essere considerate riservate e soggette a cancellazione dopo un tempo massimo di *retention*.

configurabile[128] laddove la sorveglianza – anche in assenza di accordo sindacale *ex* art. 4 L. 300/1970 o di autorizzazione dell'Ispettorato del lavoro[129] – sia strettamente funzionale alla tutela dell'azienda e non si declini in un «*significativo controllo sull'ordinario svolgimento dell'attività lavorativa*»[130], e il sistema sia riservato all'accertamento di gravi condotte illecite dei dipendenti. La pronuncia richiama l'orientamento della Corte di Strasburgo secondo cui tali forme di sorveglianza sono legittime purché vi sia il rischio di commissione di illeciti da parte dei dipendenti, i controlli siano limitati allo scopo di impedire i reati, e lo strumento sia proporzionato[131]. Si è dell'avviso che la facoltà riconosciuta al datore di lavoro di effettuare controlli difensivi renda pienamente legittima, alle condizioni previste dalla legge, anche la sorveglianza attiva nei processi a rischio di reato. Trattandosi di controlli finalizzati a prevenire la commissione di illeciti e di evitare conseguenze negative per l'impresa, appare irrilevante la finalità soggettiva perseguita dall'agente (danno per la società o interesse dell'ente).

Il monitoraggio delle mail pone anche l'ulteriore questione della violazione del c.d. domicilio informatico del lavoratore. Alcune pronunce hanno ritenuto configurabile il reato di cui all'art. 615-*ter* c.p. nel caso di accesso abusivo alla posta elettronica del dipendente[132]; ma si trattava di casi in cui l'agente aveva utilizzato senza consenso la password per introdursi in una area riservata personale.

Quando la casella di posta è gestita direttamente dell'organizzazione, le mail in entrata e in uscita transitano – e risultano visibili – agli indirizzi aziendali dotati di particolari privilegi. Si pensi ad esempio all'account di segreteria che, per ragioni connesse all'organizzazione del lavoro, può visualizzare tutti i messaggi di posta scambiati dai membri dell'organizzazione. Per quanto la casella di posta di ciascun utente sia protetta da password, al gestore del dominio aziendale è attribuito *by design* il potere di amministrare tutti gli *account* collegati e di supervisionare il contenuto dei messaggi. Ciò pare sufficiente a ritenere legittimo l'utilizzo di software che, analizzando il traffico di mail aziendali, supportino le funzioni di controllo e prevenzione di reati. L'affermazione trova conforto anche nella giurisprudenza della Corte EDU che – pronunciandosi in un caso riguardante i controlli del datore di lavoro sulle e-mail inviate e ricevute dai dipendenti tramite l'account di posta aziendale[133] – ha ritenuto insussistente la violazione dell'art. 8 della Convenzione, purché l'ordinamento nazionale preveda misure e garanzie per evitare abusi.

Infine, per quel che riguarda i dati personali dei destinatari dei messaggi, esterni all'impresa, si ritiene le operazioni di trattamento siano legittime perché effettuate nel perseguimento del legittimo interesse dell'impresa (art. 6 GDPR). I terzi – di fatto consapevoli di corrispondere con un indirizzo gestito dall'azienda – non potranno vantare una illimitata aspettativa di *privacy*, potendo ben prefigurarsi che i messaggi siano gestiti in modo centralizzato dall'azienda (es. attraverso l'inoltro automatico a altre caselle di posta in caso di assenza del lavoratore) o soggetti a controlli di vario tipo. Sarebbe comunque opportuno, per dovere di trasparenza, che le *policy* aziendali imponessero di inserire una informativa preimpostata in calce alle mail, al fine di avvisare i terzi che l'*account* con cui interagiscono è gestito direttamente dall'ente e che

[128] La disposizione, come modificata dal D. Lgs. 101/2018, prevede che per le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori prevede che si applichino le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 (arresto o ammenda, contravvenzione oblabile *ex* art. 162-*bis* c.p.).

[129] L'art. 23 del D. Lgs. 151/2015 (c.d. *Jobs Act*) è intervenuto sull'art. 4 dello Statuto dei lavoratori, aggiungendo, accanto agli impianti audiovisivi, il riferimento ad altri strumenti «*dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*». Il secondo comma precisa che l'accordo sindacale non è necessario per gli strumenti «*utilizzati dal lavoratore per rendere la prestazione lavorativa*». Alla luce della novella è si dovrà chiarire se il tracciamento nell'uso della rete aziendale ricada nell'ambito applicativo del primo ovvero del secondo comma dell'art. 4.

[130] Cass. Pen., Sez. III, 14 dicembre 2020, n. 3255 in *Sistema Penale*, 16 febbraio 2021, con nota di Birritteri (2021).

[131] Corte EDU, Grande Camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019, in *Rivista Labor,* 22 novembre 2019, con traduzione di F. Perrone.

[132] Si veda, anche per più ampi richiami giurisprudenziali, Cass. Sez. V Pen. 31 marzo 2016, n. 13057 secondo cui la casella di posta «*non è altro che uno spazio di memoria di un sistema informatico destinato alla memorizzazione di messaggi, o informazioni di altra natura (immagini, video, ecc.), di un soggetto identificato da un account registrato presso un provider del servizio. E l'accesso a questo "spazio di memoria" concreta, chiaramente, un accesso al sistema informatico, giacche' la casella non e' altro che una porzione della complessa apparecchiatura – fisica e astratta destinata alla memorizzazione delle informazioni. Allorche' questa porzione di memoria sia protetta – come nella specie, mediante l'apposizione di una password – in modo tale da rivelare la chiara volontà dell'utente di farne uno spazio a se' riservato ogni accesso abusivo allo stesso concreta l'elemento materiale del reato di cui all'articolo 615/ter cod. pen.*».

[133] Corte EDU, Grande Camera, Barbulescu c. Romania, 5 settembre 2017 «*[…] the Court takes the view that the Contracting States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse*» (§ 119, 120).

i messaggi scambiati potrebbero essere letti anche da personale diverso rispetto al destinatario.

5. Conclusioni.

La disamina sulle potenzialità offerte dalle *smart technologies* permette di giungere alla conclusione che, nella moderna società dell'informazione, esse sono uno strumento fondamentale di supporto alla *compliance* aziendale.

La tecnologia migliora la *performance* dei sistemi di gestione, automatizzando parte dei compiti attribuiti alle funzioni di controllo e riducendo i rischi operativi associati all'agire umano. Inoltre permette al personale incaricato di agire in modo informato basandosi sui dati raccolti e processati dagli algoritmi. Diverse applicazioni tecnologiche – quali il *machine learning*, la crittografia, l'analisi di *Big Data* – rendono disponibili informazioni pertinenti e specifiche sulle attività della società, che in nessun altro modo sarebbe possibile ottenere.

Dal punto di vista dei principi generali della responsabilità dell'ente, si è dell'avviso che la *digital compliance* sia un fattore positivo nella valutazione del modello organizzativo e gestionale adottato *ex* artt. 6 e 7 D. Lgs. 231/2001, potendo contribuire a rafforzare l'apparato di regole in chiave preventiva.

Peraltro, il supporto offerto da tali strumenti si andrà progressivamente affermando a livello internazionale come *best practice* in vari settori, fungendo da criterio guida per una efficace gestione del rischio. A tal riguardo, è da accogliere con favore la tesi di una maggiore positivizzazione delle regole cautelari per gli enti mediante un sistema che, valorizzando le *best practices* di settore, introduca una presunzione relativa di idoneità del modello[134].

Tuttavia, affinché il percorso di automazione della *compliance* sia sicuro e sostenibile, si dovrà svolgere una accurata analisi del caso concreto, valutando i possibili rischi derivanti dall'applicazione di certe tecnologie (es. l'intelligenza artificiale, con il suo alto grado di opacità). L'ente dovrà inoltre avere cura di definire il ruolo del personale "umano" nelle attività "digitalizzate", supervisionando in modo critico e costruttivo le determinazioni dell'algoritmo.

Tra le innovazioni tecnologiche sopra esaminate, certamente i programmi di *decision intelligence* su fonti aperte assumono particolare rilevanza per la semplicità con cui possono essere acquisiti e integrati nei processi aziendali. Gli enti potranno prevedere, nei propri modelli organizzativi, che il compimento di determinate operazioni a rischio di reato sia preceduto da una specifica *due diligence* mediante OSINT, o che situazioni particolari siano "monitorate" in tempo reale dall'algoritmo. Ciò consentirà di elaborare report e generare *alert* per responsabili di funzione circa eventuali rischi nella relazione con terze parti. Tali strumenti presentano anche il pregio di una piena conformità con la normativa in materia di *privacy*, laddove non siano utilizzati per la profilazione o per finalità non consentite.

Anche i SIEM e gli strumenti per il monitoraggio del traffico di dati (e delle mail) all'interno all'azienda si rivelano di grande utilità per prevenire la commissione di alcuni *corporate crimes*. Tuttavia, affinché tali software possano assolvere adeguatamente al compito di supportare la *compliance*, l'ente dovrà adattarli e/o customizzarli sulla base delle proprie esigenze. Si profilano, inoltre, alcuni rischi per la *privacy* dei lavoratori che, sebbene non ostativi al monitoraggio dei dati, dovrebbero richiedere quantomeno un'analisi di impatto preventivo.

In definitiva, la trasformazione digitale è un processo inarrestabile che investe, anzi deve investire, anche i modelli organizzativi e gestionali 231. Il sistema di *governance* e di controlli non può restare ancorato a logiche tradizionali, ma deve evolvere di pari passo rispetto alle nuove modalità di comunicazione e lavoro.

Bibliografia

Alagna, Ilenia Maria (2018): "Big data e People Analytics: nuove sfide e opportunità per liberare valore", *Ciberspazio e diritto*, 2018, vol. 19, p. 339 ss.

[134] *Amplius*, § 1.1

Ammannati Laura e Greco Gian Luca (2021): "Piattaforme digitali, algoritmi e "big data": il caso del "credit scoring", *Rivista Trimestrale di Diritto dell'Economia*, 2, p. 290 ss.

Armour, John (2018): The Case for "Forward Compliance", *The British Academy Review*, 1 november 2018, in www.thebritishacademy.ac.uk

Arner, Douglas W, Barberis Janos, e Buckley Ross (2017): "FinTech, RegTech and the Reconceptualization of Financial Regulation", *Northwestern Journal of International Law & Business*, vol. 37, 3, p. 373

Bamberger, Kenneth A. (2009): "Technologies of Compliance: Risk and Regulation in a Digital Age", *Texas Law Review*, vol. 88, p. 669 ss.

Baskerville, Richard, Spagnoletti, Paolo e Kim, Jongwoo (2014): "Incident-centered information security: Managing a strategic balance between prevention and response", *Information & Management*, vol. 51, 1, p. 138 ss.

Bennett Moses, Lyria e Chan, Janet (2018): "Algorithmic prediction in policing: assumptions, evaluation, and accountability", *Policing and Society,* vol. 28, 7, p. 806 ss.

Bianchini, Francesco (2007): "L'IA e il linguaggio fra storia ed epistemologia", in Bianchini, Francesco, Gliozzo, Alfio, e Matteuzzi Maurizio (editor), *Instrumentum vocale: intelligenza artificiale e linguaggio*, Bologna

Birritteri, Emanuele (2019): "Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2, p. 294 ss.

Birritteri, Emanuele (2020): "Controllo a distanza del lavoratore e rischio penale", nota a Cass. Pen., Sez. III, 14 dicembre 2020, n. 3255, *Sistema Penale*, 16 febbraio 2021

Basile, Fabio (2019): "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", *Diritto Penale Uomo*, 29 settembre 2019

Borsari, Riccardo (2020): "Intelligenza Artificiale e responsabilità penale: prime considerazioni", *Discrimen,* 14 febbraio 2020

Burchard, Christoph (2021): "Digital Criminal Compliance", in Engelhart, Marc, Kudlich, Hans, und Vogel, Benjamin (editor), *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber*, Berlin, p. 741

Burchard, Christoph (2019a): "Künstliche Intelligenz als Ende des Strafrechts? Zur algorithmischen Transformation der Gesellschaft" , *Normative Orders Working Paper*, in www.publikationen.ub.uni-frankfurt.de

Burchard, Christoph (2019b): "L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società", *Rivista italiana di diritto e procedura penale*, 4, p. 1909 ss.

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, p. 195 ss.

D'Agostino, Luca (2019): "Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.d. evidence-based sentencing", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2, p. 354 ss.

Dombalagian, Onnig H. (2016): "Preserving Human Agency in Automated Human Compliance, in Tulane University School of Law Public Law and Legal Theory", *Working Paper Series Working Paper n. 11/2016,* in brooklynworks.brooklaw.edu

Diamantis, Mihailis E. (2020): "The Extended Corporate Mind: When Corporations Use AI to Break the Law", *North Carolina Law Review,* vol. 98, 4, p. 893 ss.

Ferguson, Andrew Guthrie (2015): "Big Data and predictive reasonable suspicion", *University of Pennsylvania Law Review*, Vol. 163, p. 327;

Franssen, Vanessa, and Berrendorf, Alyson (2021): "The Use of AI Tools in Criminal Courts: Justice Done and Seen to Be Done?", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 199 ss.

Gambino, Alberto Maria, e Bomprezzi, Chantal (2019): "Blockchain e protezione dei dati personali", *Diritto dell'informazione e dell'informatica,* 3, p. 623

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

Gillespie, Tarleton (2014): "The Relevance of Algorithms", in Gillespie, Tarleton, and Boczkowski, Pablo J. (editor), *Media Technologies: Essays on Communication, Materiality, and Society,* MIT Press, p. 167 ss.

Gullo, Antonio (2022): "Compliance", in Piergallini, Carlo, Mannozzi, Grazia, Perini, Chiara, Scoletta, Marco, Sotis, Carlo, e Consulich Federico, (editor), *Studi in onore di Carlo Enrico Paliero*, Milano, p.1289 ss.

Gullo, Antonio (2020): "I modelli organizzativi", in Lattanzi, Giorgio, e Severino, Paola (editor), *Responsabilità da reato degli enti,* vol. I, *Diritto sostanziale*, Torino, p. 283 ss.

Kehl, Danielle, Guo, Priscilla, and Kessler, Samuel (2017): "Algorithms in the Criminal Justice System: Assessing the use of Risk Assessments in Sentencing", *Responsive Communities Initiative, Berkman Klein Center for Internet and Society, Harvard Law School*, in dash.harvard.edu

King, Thomas, Aggarwal, Nikita, Taddeo, Mariarosaria, and Floridi, Luciano (2020): "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", *Science and Engineering Ethics,* 26, p. 89-120

Laufer, William S. (2017): "The missing account of progressive corporate criminal law", *New York Journal of Law and Business*", vol. 14, 1, p. 71 ss.

Laura, Luigi (2019): *Breve e universale storia degli algoritmi*, Luiss University Press

Liptak, Adam (2017): "Sent to prison by a Software Program's secret algorithms", *New York Times*, May 1st 2017

Lo Sapio, Germana (2021): "Rating reputazionale, consenso valido e comprensione dell'algoritmo alle prese con l'era digitale", *Federalismi.it*, 11 agosto 2021, nota a Cass. Civ., Sez. I, 25 maggio 2021 n. 14381

Manes, Vittorio (2020): "L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia", *Discrimen,* 15 maggio 2020

Massaro, Alessandro, Icardi, Simone, e Mele, Fabio: (2017): "La Social Media Intelligence nell'era dei social network", *Ciberspazio e diritto,* 2, p. 425 ss.

Mazzacuva, Francesco (2021): "The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 143 ss.

Maugeri, Anna Maria (2021): "L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali", *Archivio Penale,*1, p. 2 ss.

Minneci, Ugo, Ammannati, Laura, Canepa, Allegra, e Greco, Gianluca (2021): *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione,* Giappichelli

Mohamed, Hazik, and Yildirim, Ramazan (2021): "RegTech and Regulatory Change Management for Financial Institutions", in Hamdan, Allan, Hassanien, Aboul Ella, and Razzaque, Anjum (editor), *The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success*, Studies in Computational Intelligence, p. 153 ss.

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*, 3, p. 75 ss.

Mongillo, Vincenzo (2022): "Presente e futuro della compliance penale", *Sistema Penale,* 11 gennaio 2022

Morgante, Gaetana, e Fiorinelli, Gaia (2022): "Promesse e rischi della compliance penale digitalizzata", *Archivio Penale Web,* 2

Mozzarelli, Michele Cesare Maria (2022): "Digital Compliance: The Case for Algorithmic Transparency", in Centonze, Francesco, e Manacorda, Stefano (editor), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness,* Springer

Niklas, Jędrzej (2020): "Human Rights-Based Approach to AI and Algorithms", in Barfield Woodrow (editor), *The Law of Algorithms*, p. 527 ss.

Nisco, Attilio (2022): "Riflessi della compliance digitale in ambito 231", *Sistema Penale*, 14 marzo 2022

Oswald, Marion, Grace, Jamie, Urwin, Sheena, and Barnes, Geoffrey (2018): "Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality", *Information and Communications Technology Law*, p. 227

Packin, Nizan Geslevich (2018): "RegTech, Compliance and Technology Judgment Rule", *Chicago Kent Law Review*, vol. 93, 1, p. 193-218

Paolucci, Federica (2021): "Consenso, intelligenza artificiale e privacy", *Media Laws*, 16 giugno 2021, con nota a Cass. Civ., Sez. I, 25 maggio 2021 n. 14381

Paliero, Carlo Enrico (2018): "La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale", *Rivista trimestrale di diritto penale dell'economia*, 1-2, p. 175 ss.

Piergallini, Carlo (2015): "Autonormazione e controllo penale", *Diritto penale e processo*, 3, p. 266 ss.

Piergallini, Carlo (2019): "Premialità e non punibilità nel sistema della responsabilità degli enti", *Diritto penale e processo,* 4, p. 530 ss.

Piselli, Riccardo, e D'Agostino, Luca (2019): "La definizione di tecnologia a registro distribuito e di smart contract nella legge di conversione del "Decreto semplificazioni". Un primo commento critico", in Nuzzo, Antonio (editor), *Blockchain e autonomia privata – Fondamenti giuridici,* Luiss University Press, 2019, p. 13-22

Sabia, Rossella (2020): "Artificial Intelligence and Environmental Criminal Compliance", *Revue Internationale de Droit Pénal*, 1, p. 179 ss.

Sagliocca, Antonio (2017): "Open Source Intelligence e Deep Web: scenari moderni delle investigazioni digitali", *Ciberspazio e diritto*, 1, p. 171 ss.

Sciascia, Giuseppe (2021): "Reputazione e potere: il social scoring tra distopia e realtà", *Giornale di diritto amministrativo*, 3, p. 317 ss.

Searle, John R. (1980): "Minds, brains, and programs", *Behavioral and Brain Sciences*, 3, p. 417-457

Selvaggi, Nicola (2019): "Dimensione tecnologica e compliance penale: un'introduzione", in Lupària, Luca, Marafioti, Luca, e Paolozzi, Giovanni, (editor), *Dimensione tecnologica e prova penale,* Giappichelli, p. 217 ss.

Severino, Paola (2020): "Intelligenza artificiale e diritto penale", in Ruffolo, Ugo (editor), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, p. 531 ss.

Sorbello, Pietro (2019): "Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto", *Diritto penale contemporaneo – Rivista trimestrale,* 2, p. 374 ss.

Starr, Sonja B. (2014): "Evidence -based Sentencing and the Scientific Rationalization of Discrimination", *Stanford Law Review*, vol. 66, p. 809 ss.

Trezza, Remo (2021): "L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi possibili e rischi celati", *Giurisprudenza Penale*, 1-*bis,* 2 ss.

Ubertis, Giulio (2020): "Intelligenza artificiale, giustizia penale, controllo umano significativo", *Diritto penale contemporaneo – Rivista trimestrale*, 4, p. 75 ss.

Van Liebergen, Bart (2016): "RegTech in financial services: technology solutions for compliance and reporting", 22th march 2016, *Institute of International Finance Publications*, in www.iif.com

Vermeulen, Gert, Peršak, Nina, e Recchia, Nicola (2021): "Capabilities and limitations of ai in criminal justice", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 7 ss.

Zuboff, Shoshana (2019), *Il capitalismo della sorveglianza,* Luiss University Press (trad. Paolo Bassotti)

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu