

**RESPONSABILITÀ DEGLI ENTI:
PROBLEMATICHE E PROSPETTIVE
DI RIFORMA A VENTI ANNI
DAL D. LGS. 231/2001**

2021 / 1-BIS

**RegTech e Modelli 231: uno sguardo al futuro
per un'esigenza presente.**

di Andrea Vianelli e Francesca Valenti

di Andrea Vianelli e Francesca Valenti

Abstract

Il contributo si focalizza, in via pragmatica e propositiva, sul fenomeno c.d. di *Regulatory Technology* (“RegTech”) e le sue applicazioni nei modelli di organizzazione, gestione e controllo (“Modelli”). L’adozione e l’aggiornamento dei Modelli non rappresenta solo un investimento in termini di *good governance*, immagine o di accesso al sistema premiale ex d.lgs. n. 231/2001, ma altresì uno strumento di efficientamento dell’ente, agevolandone l’accesso a gare pubbliche, a concessioni di finanziamenti pubblici, al mercato di capitali e al credito bancario. A tal riguardo, le soluzioni *RegTech*, attraverso l’elaborazione dei dati normativi e l’automatizzazione dei processi di verifica e monitoraggio, semplificano e migliorano l’adozione e l’implementazione dei Modelli. Infatti, benché sia acclarata la primazia del settore finanziario nell’applicazione di soluzioni *RegTech* (e.g. procedure di *KYC*, *risk&control analytics*, *fraud detection*, autenticazione e gestione dei dati personali etc.), il *RegTech* si sta espandendo anche in settori non finanziari. Ciò è dovuto al complesso susseguirsi di disposizioni e protocolli a cui gli enti devono conformarsi per potersi esimere da responsabilità a proprio carico ed evitare ricadute sia economiche che reputazionali. Di fatto, il *RegTech* si pone come strumento di supporto pratico ed efficace che, grazie alla sua dinamicità, flessibilità e modellabilità, automatizza e riduce il margine del c.d. “errore umano” nello svolgimento di attività richiedenti un significativo impiego di risorse e tempo, come il monitoraggio della normativa, l’analisi dei rischi, la produzione di reportistica e l’inoltro di tali informazioni a soggetti terzi. Come è noto, l’Organismo di Vigilanza (“OdV”) e il Modello sono i cardini di un sistema che deve essere calato nella realtà aziendale, efficacemente attuato e idoneo, in concreto, a prevenire *malpractice* e reati ritenuti rilevanti per l’operatività dell’ente in sede di mappatura del rischio. In termini di *risk assessment*, il *RegTech* agevola la gestione delle verifiche di conformità, automatizzando il monitoraggio di specifici profili di rischio e generando *report* grafici, tabellari e descrittivi di sintesi, analitici o di *trend* storico. Inoltre, proponendosi quale strumento suppletivo e complementare all’OdV sia durante il *set-up* del Modello, in termini di *governance* e protocolli, che nelle fasi di monitoraggio e revisione, il *RegTech* ne rafforza i profili di imparzialità e indipendenza. Infine, agevola la trasparenza e la tracciabilità delle attività e delle procedure (ne si considerino anche i riflessi probatori) e favorisce la fruizione di *training* formativi sia in fase di ingresso alle dinamiche dell’ente, che su base continuativa. Concludendo, l’elaborato indaga le reali potenzialità del *RegTech* alla luce della possibile dotazione obbligatoria del Modello in un tessuto economico costellato di piccole e medie imprese in cui il bilancio costi-benefici riveste un ruolo di primaria importanza.

The article is focused, adopting a pragmatic and proactive approach, on the growth of the so-called Regulatory Technology phenomenon (“RegTech”) and its application within the corporate governance models (“Models”). The introduction and update of such Models should not be seen as a mere investment in terms of good governance, corporate image or benefit according to the framework set out under d.lgs. n. 231/2001, but also a tool for enhanced corporate efficiency with respect to public procurement access, public financing and access to funding.

In this respect, RegTech solution (through legal data analysis and compliance monitoring and automation), are suitable to simplify and improve the implementation of such Model. Whilst RegTech solutions are generally more common in the financial industry, RegTech is now reaching also non-financial players. This outcome is mainly dependent on the nuanced regulatory framework which, in the event of breaches, may negatively impact firms both under a financial and non-financial (i.e. reputational) standpoint.

RegTech solutions do represent a useful tool that, given its dynamic, flexible and tailored nature, would enable to reduce human errors during time consuming and labor intensive tasks, such as compliance



functions, risk management and reporting.

As generally accepted practice, the board of statutory auditors (“OdV”) and the Model are pillars in a system which needs to fit the real dynamics of the firm and as such would be useful, in concrete, to avoid malpractice and criminal charges in accordance to a detailed risk management process.

Under a risk assessment perspective, RegTech has the benefit to simplify compliance activities, monitoring of risks and risk mapping, generating interactive reports and offering useful insights on corporate performance and trends.

In addition to and together with the activities of the OdV both during the introduction of the Model and its implementation and review, RegTech is suitable to strengthen models under independence and unbiased actions, but also transparency and audit trails (useful also in order to challenge charges) and training purposes.

As conclusive remarks, the article investigates on RegTech potential within a framework of mandatory adoption of Models within the SME context, traditionally featured by cost-benefit analysis during the lifecycle of a firm’s business.

Sommario

1. Introduzione. - **2.** Regulatory Technology. - **3.** Modello 231 e Organismo di Vigilanza. - **4.** Trasparenza e Onere della prova. - **5.** Applicazione Pratica. - **6.** Corporate Culture - **7.** Rischi. - **8.** Conclusione Costi-Benefici.

1. Introduzione

A vent’anni dall’entrata in vigore del d.lgs. 8 giugno 2001, n. 231 nel panorama giuridico italiano, è possibile constatare la progressiva estensione del perimetro di applicazione della disciplina, attraverso, ad esempio, l’assunzione in vasta scala nel mondo delle medio-grandi imprese di modelli organizzativi e gestionali prescritti dalla normativa.

L’adozione e l’aggiornamento del modello di organizzazione, gestione e controllo (il “Modello”) non rappresenta solo un investimento in termini di *good governance*, immagine o di accesso al sistema premiale ai sensi del decreto, ma altresì uno strumento di efficientamento dell’ente, agevolandone l’accesso a gare pubbliche, a concessioni di finanziamenti pubblici, al mercato di capitali e al credito bancario.

Il Modello rappresenta la volontà di conseguire il rispetto della legalità non solo con la minaccia di sanzioni, ma soprattutto attraverso un’efficace prevenzione endosocietaria: il legislatore si è ispirato ai *compliance program* statunitensi¹, fondati sulla logica del sistema *stick and carrot* (il c.d. approccio del bastone e della carota)², e ha previsto l’adozione di modelli comportamentali adeguati allo scopo di scongiurare il rischio della commissione di specifici reati con il requisito indispensabile dell’*effettività*, al fine di ottenere un’esclusione di responsabilità.

Il legislatore ha optato, infatti, per una forma di «*parziale delocalizzazione e condivisione del*

controllo»³ da cui emerge la vocazione special-preventiva⁴ del processo, il cui scopo è, *in primis*, il recupero dell’ente alla legalità realizzato tramite l’adozione - anche tardiva⁵- di modelli comportamentali idonei ad arginare il rischio che l’impresa commetta - o ricommetta - reati e la previsione di «*strumenti di ravvedimento post factum*»⁶ che in determinate circostanze permettono all’ente, ad esempio, di evitare l’applicazione delle sanzioni interdittive.

Al contempo, tuttavia, è da rilevarsi la difficoltà per questa nuova realtà di trovare un solido terreno applicativo. Infatti, a causa della complessità della fattispecie, delle aporie interpretative, degli esiti incerti e delle lacune normative che rendono necessaria la strada dell’eterointegrazione, la normativa non si rende appetibile agli occhi delle procure della Repubblica. Ne consegue una frammentaria applicazione, alimentata dalla subordinazione alle discrezionali scelte del singolo procuratore.

Inoltre, nonostante i principali obiettivi normativi del legislatore nazionale ed europeo siano rimasti invariati nel corso degli anni (i.e. prevenzione dei reati, stabilità finanziaria, protezione dei consumatori, integrità del mercato, concorrenza e sviluppo del mercato), i mezzi di implementazione della disciplina sono diventati sempre più inadeguati. In aggiunta, particolarmente significativo è il mancato conseguimento di competenze e professionalità idonee nel settore delle consulenze aziendali, indice di una ancora non completa ricezione nel mercato della disciplina.

In questo contesto di frammentaria implementazione delle disposizioni di legge risiede il potenziale del c.d. *regulatory technology* o **'RegTech'**, ossia dell'utilizzo della tecnologia quale tramite per soddisfare le esigenze normative di controllo, *reporting* e *compliance*. In particolare, le soluzioni *RegTech*, attraverso l'elaborazione dei dati normativi e l'automatizzazione dei processi di verifica e monitoraggio, semplificano e migliorano l'adozione e l'implementazione del Modello.

Al lettore è proposta una ricognizione critica del fenomeno *RegTech*, accompagnata dalla prospettazione delle novità tecnologiche quali elementi di incontro tra l'esigenza del legislatore e quella dell'ente.

2. Regulatory Technology

Il termine *RegTech* ricomprende ogni genere di uso delle tecnologie a fini regolamentari, siano essi implementati a livello di autorità di vigilanza o di ente che svolge attività regolamentata. Inizialmente tale concetto si utilizzava per descrivere la tecnologia quale mezzo di supporto nell'ambito dei dipartimenti di *compliance* dei soggetti sottoposti all'applicazione di obblighi regolamentari – generalmente in gruppi finanziari particolarmente strutturati. Per questa ragione, la prima ondata di *RegTech* era per lo più focalizzata al supporto di realtà istituzionali di dimensioni importanti – sia in termini di espansione territoriale che di risorse umane – nel settore finanziario, con l'obiettivo di ridurre i costi di *compliance* oltre al rischio di incorrere in sanzioni amministrative e penali⁷.

In particolare, la progressiva adozione di soluzioni tecnologiche innovative, specialmente in ambito finanziario⁸, è strettamente correlata al mastodontico *corpus* di nuove disposizioni normative che gli operatori del settore finanziario hanno dovuto affrontare, in modo efficiente, efficace ed economico, dopo la crisi bancaria del 2008⁹. Pare opportuno però sottolineare come l'avvento di talune tecnologie (in uno allo sviluppo di soluzioni *hardware*, e.g. *smartphone* sempre più sofisticati) abbia permesso di migliorare servizi (o aspetti di essi) già esistenti e contribuire al lancio di nuovi servizi e/o prodotti *"tech-enabled"*. Questo fenomeno ha favorito l'interazione tra l'universo finanziario e la sua clientela grazie alla crescente accessibilità e rapidità nella fruizione dei predetti servizi¹⁰ e pare aver raggiunto il culmine durante l'emergenza sanitaria dovuta alla pandemia da Sars-Covid-2: l'*impasse* della crisi sanitaria ha comportato un aumento senza precedenti nelle richieste di esecuzione di transazioni finanziarie e accesso ai servizi di pagamento in tempo reale –

tra tutte, si veda il crescente uso di piattaforme di *brokerage retail* negli Stati Uniti.

Il ricorso alla tecnologia nel settore finanziario è noto come fenomeno del c.d. *FinTech* ovvero *"financial technology"*, ossia lo sviluppo di tecnologie innovative declinate alle esigenze della finanza¹¹. Infatti, la digitalizzazione dei processi di *reporting* manuale, di *Know-Your-Customer (KYC)*, i programmi di *risk&control analytics*, i sistemi di *fraud detection*, o di autenticazione e gestione dei dati personali hanno implicato enormi risparmi sui costi nei settori regolamentati.

Benché sia acclarata la primazia del settore finanziario nell'applicazione di soluzioni tecnologiche, il *RegTech* non deve essere inteso quale sottoinsieme o corollario del *FinTech*¹²: grazie all'automatizzazione e la razionalizzazione dei processi normativi¹³, il *RegTech* rende possibile la *compliance* con il quadro regolamentare vigente quasi in tempo reale e, soprattutto, in modo proporzionale alle peculiarità dell'ente che deve identificare, declinare e mitigare le fattispecie di rischio specifiche del suo settore operativo¹⁴. A ciò si aggiunga che, attraverso il monitoraggio continuo e costante, la tecnologia ha il potenziale di fornire una visione in tempo reale del funzionamento dei mercati a livello nazionale e globale, attraverso meccanismi di *machine learning*, *deep learning* e filtri di intelligenza artificiale che identificano le possibili implicazioni e non si limitano a prendere provvedimenti a posteriori.

L'emergere del *RegTech* è attribuibile (i) ai cambiamenti nella regolamentazione post-crisi che richiedono una massiccia divulgazione di dati supplementari da parte degli enti regolamentati, (ii) allo sviluppo nel campo della scienza dei dati, ad esempio l'intelligenza artificiale (*artificial intelligence*), il *machine learning* e il *deep learning*, che consentono di strutturare dati non organizzati¹⁵, (iii) agli sforzi delle autorità di regolamentazione per migliorare l'efficienza degli strumenti di vigilanza al fine di promuovere la concorrenza e l'integrità del mercato.¹⁶

Il *RegTech* rappresenta inoltre la crescente fiducia nella c.d. *information technology* quale principale strumento di regolamentazione, supervisione e dialogo, in grado di declinare e modellare le singole procedure e protocolli di conformità con il flusso di disposizioni normative di volta in volta applicabili. Con l'*information technology* è aumentata l'adozione di soluzioni di *cloud computing*, di *data analysis* tramite intelligenza artificiale e di integrazione di *feed* a fini di monitoraggio diretto degli enti regolamentati; questi sistemi sono spesso forniti da terze parti tramite modelli di servizio quali *software as a service (SaaS)* e/o *infrastructure as*

a service (IaaS), non venendo quindi prodotti *in-house* dall'ente.¹⁷

Ad oggi vi è chi suole distinguere tra due rami complementari del *RegTech*: la c.d. *Compliance Technology (CompTech)* e la c.d. *Supervisory Technology (SupTech)*¹⁸, benché tale distinzione pare riflettere più i destinatari del prodotto che la sostanza del medesimo. Infatti, oltre a comportare tagli sui costi in termini di *compliance* per gli enti e crea opportunità di mercato per le *start-up*, le aziende IT e le società di consulenza *FinTech/RegTech* emergenti, dal punto di vista delle autorità di vigilanza, il *RegTech* consente la prospettiva di un monitoraggio continuo e di più efficiente vigilanza, creando un flusso costante di informazioni utili per rimodellare e ridefinire gli ambiti di eccessiva regolamentazione e efficientando il tempo delle indagini inerenti alle potenziali violazioni rilevate.¹⁹ Ampliando la prospettiva ad un ambito non prettamente nazionale, la prova del potenziale del *RegTech* risiede nel crescente numero di c.d. *regulatory sandbox* e altre istanze proattive delle autorità locali e internazionali, che facilitano la transizione da un modello regolamentare all'altro. Le stesse autorità di vigilanza hanno iniziato gradualmente a considerare il *RegTech* quale strumento in grado di supportare i soggetti regolamentati a tenere il passo con il copioso e crescente numero di disposizioni normative applicabili sia a livello europeo che nazionale.

Di recente, la *Financial Conduct Authority (FCA)* nel Regno Unito ha lanciato una serie di conferenze ed eventi virtuali tra l'autunno (2020) e la primavera (2021) per approfondire l'ecosistema *RegTech*²⁰ soprattutto date le circostanze emergenziali dovute alla pandemia di Covid-19, la c.d. *digital transformation* nei settori regolamentati risulta essere quanto più necessaria²¹. Sembra infatti che gli sviluppi *RegTech* stiano provocando un cambiamento di paradigma della regolamentazione del sistema finanziario²² e per questa ragione, la FCA s'interroga ormai da anni sulla possibilità di adottare nuove tecnologie per agevolare la gestione e la comunicazione dei requisiti regolamentari.²³

Le autorità di regolamentazione si trovano ad affrontare la necessità di utilizzare la tecnologia per affrontare le sfide del monitoraggio e dell'applicazione di requisiti normativi sempre più esigenti su mercati in rapida evoluzione, in rapida crescita e transfrontalieri, oltre che di sviluppare approcci normativi in concerto con tutti gli *stakeholder* che non ostacolano lo sviluppo e l'innovazione dovute alla comparsa di nuove tecnologie e di nuovi operatori *FinTech*, ma che limitino al contempo i rischi per i consumatori e la stabilità finanziaria.²⁴

Possiamo quindi aspettarci che, sulla base dell'interesse dimostrato dalle autorità di vigilanza, il *RegTech* si concentri sempre più sulle soluzioni *business-to-business* ("B2B"), a differenza del settore *FinTech* in cui un gran numero di enti e, quindi, fornitori si concentra sulle soluzioni *business-to-consumer* ("B2C"), oltre che sul B2B.²⁵ Concludendo, le soluzioni tecnologiche permetterebbero (i) di modellare le politiche di regolamentazione simulando il probabile impatto delle nuove politiche prima dell'emanazione e raccogliendo un *feedback* immediato dall'applicazione della regolamentazione esistente, (ii) lo sviluppo di *standard* comuni di *reporting* e di *compliance tagging* in più giurisdizioni per supportare le richieste di condivisione obbligatoria delle informazioni tra le autorità di vigilanza, (iii) l'integrazione dei sistemi di monitoraggio finanziario nazionale, europeo e globale²⁶, (iv) incoraggiare lo sviluppo di una *suite* di strumenti di *compliance open-source*, (v) la collaborazione e condivisione di dati selezionati tra i diversi *regulator* internazionali, come nel caso del settore del antiriciclaggio e la lotta al terrorismo²⁷.

3. Modello 231 E Organismo Di Vigilanza

L'ente diviene nuovo destinatario di un rimprovero penalmente rilevante in un'ottica di prevenzione del rischio di reato e di recupero alla legalità mediante la sollecitazione all'adozione di regole di comportamento che sottopongono l'ente sia a risposte sanzionatorie, che a un sistema di diritto c.d. premiale.

Per questa ragione, il Modello e l'Organismo di Vigilanza ("OdV")²⁸, che ne permette un'efficace attuazione e vigilanza, sono il fulcro del sistema: la corretta strutturazione del Modello delinea i compiti dell'OdV e, al contempo, il non corretto operare dell'OdV, impedisce all'ente l'implementazione del Modello. Il Modello, infatti, deve essere efficacemente attuato e non bastano adempimenti cartacei, ma deve essere declinato sulle esigenze specifiche dell'ente in riferimento al quale deve operare.

Secondo le prassi consolidate anche in base alle indicazioni delle associazioni di categoria, il metodo da seguire per strutturare concretamente il Modello con connotati essenziali affinché possa ambire all'idoneità e ottenere l'esclusione dalla responsabilità, richiede lo svolgimento di una serie di attività che delincono i perimetri, i criteri e le prospettive che rendono il Modello «*cucito*»²⁹ su misura per l'ente che lo deve adottare.

Attraverso la strutturazione guidata dalle soluzioni

RegTech di protocolli e regole di condotta è possibile rintracciare e documentare, non solo quei comportamenti (azioni, operazioni, transazioni) maggiormente esposti al rischio di reato, ma anche offrire un valido strumento di supporto per l'OdV, monitorandone i meccanismi autorizzativi e di verifica dei diversi processi operativi.

In primis, è necessario condurre un'attività istruttoria in cui tutta la documentazione interna dell'ente (statuto, organigramma, *policy*, regolamenti, deleghe, contrattualistica, codice etico, ecc...) viene organizzata e riportata nel database della soluzione *RegTech*.

Sulla base di tale documentazione ha luogo la mappatura del rischio, che prevede un'analisi dettagliata delle attività poste in essere dall'ente comprendente la descrizione dei singoli passaggi operativi, delle aree di competenza e della gerarchia delle funzioni. Le soluzioni *RegTech* permettono uno screening preliminare dei possibili gap e hanno spesso già integrate delle *detecting rules* per individuare le aree o le operazioni a rischio, le stesse possono essere customizzate a seconda delle esigenze più o meno stringenti dell'ente.

Innanzitutto, si devono individuare le attività e i momenti in cui la possibilità di realizzazione di specifici reati tende a intensificarsi, prendendo in considerazione il tipo di ente, così come le dinamiche organizzative e produttive³⁰. La base di partenza per tale mappatura dei rischi consiste nell'osservazione a 360 gradi delle carenze all'interno della dinamica aziendale, attraverso l'identificazione di *breakpoint*, *malpractice* e dilemmi che i dipendenti possono trovarsi ad affrontare e che possono favorire comportamenti scorretti.

Le aree di rischio possono essere sia individuate empiricamente in termini astratti (i.e. attività e/o procedimenti notoriamente sensibili alla commissione di violazioni della disciplina interna e/o reati presupposto) o in termini concreti (i.e. i soggetti che svolgono tali funzioni individuano le aree grigie percepite nell'adempimento delle proprie mansioni). Lo scopo è la strutturazione di strumenti di gestione del rischio su misura a seguito della mappatura delle aree di rischio³¹ combinata alla c.d. *gap analysis*³².

Infatti, una volta acquisito un quadro delle varie dinamiche societarie e delle aree di rischio sarà necessario lo sviluppo di protocolli idonei a programmare la formazione e l'attuazione della decisione dell'ente, così come le modalità di gestione delle risorse³³.

Sulla base delle informazioni raccolte all'ente è richiesto di predisporre *policy* in grado di gestire e arginare le suddette aree sensibili, attraverso

procedure operative precauzionali, volte a prevenire il crearsi di situazioni suscettibili di scaturire in commissione di violazioni, e tempestive, con l'obiettivo di ripristinare e/o limitarne gli effetti.

Una base di partenza per la strutturazione del Modello possono essere i codici comportamentali redatti dalle associazioni rappresentative dell'ente e approvati dal Ministero della giustizia che, tuttavia, non sono sufficienti a soddisfare i requisiti di idoneità ed efficienza richiesti³⁴.

I protocolli vengono registrati e appresi dalle soluzioni di intelligenza artificiale e *machine learning* che, oltre a programmare la formazione dei soggetti coinvolti, contribuiscono a offrire un supporto concreto nell'attuazione dei protocolli predisposti dall'ente attraverso regole di condotta che possono rafforzare il sistema ideato contribuendo a rendere ancor più *tailored* il Modello. Infatti, il *RegTech*, interpretando queste informazioni, consente di supervisionare l'operatività dell'ente, suggerendo i punti di non conformità e automatizzando le metodologie di controllo dei rischi. Inoltre, non di rado, i fornitori di tecnologie *RegTech*, hanno già delle *policy* di monitoraggio integrate nella soluzione IT conformi a quelli della normativa vigente nel quale la soluzione si propone come strumento di supporto³⁵. L'ente dovrà riportare nei propri protocolli anche i dettagli sul funzionamento delle soluzioni *RegTech* adottate tenendo in considerazione le *policy* dalle stesse adottate. Inoltre, a fini di evitare eventi di *business disruption*, i protocolli dovranno esplicitare il piano di *back-up* qualora l'infrastruttura IT dovesse temporaneamente cessare di funzionare. Anche per questo aspetti legati al funzionamento del sistema *RegTech* dovrà essere preso in considerazione per la *gap analysis*. Il Modello deve inoltre presentare evidenze rispetto al principio di segregazione delle funzioni e di imparzialità dell'OdV. Infatti, l'OdV deve essere dotato di autonomi poteri di iniziativa e controllo, oltre che di autonomia e indipendenza, per vigilare sul funzionamento effettivo e l'osservanza del Modello, garantendo continuità e aggiornamento³⁶. Tuttavia, le operazioni di vigilanza sono rimesse alla discrezionalità dei componenti dell'OdV, i cui requisiti di imparzialità di giudizio e indipendenza sono intrinsecamente difficili da garantire. Non di rado i membri dell'OdV hanno rapporti consolidati negli anni con soggetti appartenenti alla funzione vigilata, che rischiano di smorzare l'efficienza e l'imparzialità dell'OdV, facilitando, ad esempio, atteggiamenti indulgenti rispetto agli apicali che hanno conferito l'incarico.

Oltre alla composizione plurisoggettiva, specie in presenza di componenti interni alla struttura

operativa dell'ente, anche le soluzioni *RegTech* possono contribuire a tale scopo. Infatti, le iniziative dell'OdV possono essere rafforzate dal supporto di tecnologie che ne favoriscono le funzioni, e garantiscono l'opportuna evidenza e trasparenza delle operazioni e dei rapporti sottostanti.

Per ciò che concerne la segregazione dei compiti e delle funzioni, il *RegTech* ha il potenziale di garantire tali esigenze attraverso la sistematizzazione dei protocolli di *governance* stabiliti *ex ante*, segnalando eventuali conflitti di interessi una volta registrate le funzioni dei singoli soggetti deputati ad assumere le decisioni all'interno di comitati e/o dell'OdV.

I ruoli assunti dai singoli funzionari, che devono essere dichiarati per motivi di trasparenza, possono essere rilevanti da parte di soluzione IT che hanno accesso a *database* pubblici, come ad esempio quelli delle pubbliche amministrazioni (registro delle imprese) e che possono rilevare ulteriori cariche assunte dai funzionari attraverso un'attività di *screening*. Non solo, è possibile anche procedere con attività di *screening* per identificare eventuali informazioni pubbliche negative (ad esempio sanzioni) o *adverse media* (ad esempio articoli di giornale). I risultati, aggregati ed elaborati in appositi *log*, possono contribuire al mantenimento di un modello organizzativo più trasparente e a monitorare possibili conflitti di interesse, oltre che a tutelare la società da potenziali danni di tipo reputazionale.

Inoltre, una volta registrati i parametri da rispettare nell'ambito dei processi decisionali, le soluzioni *RegTech* monitorano il rispetto del principio di segregazione dei compiti tra coloro che intervengono e/o partecipano nella fase operativa e nella fase di vigilanza, così da evitare che siano coinvolti sempre i medesimi soggetti e rafforzandone la trasparenza.

Fatto salvo quanto precedentemente esposto, tra i problemi emersi in questi anni di applicazione della disciplina vi è senza dubbio quello dell'individuazione dei criteri e delle linee guida capaci di soddisfare il requisito dell'idoneità. Non è possibile predeterminare il contenuto del Modello a causa dei differenti destinatari ed esigenze che richiedono la creazione di specifici protocolli in grado di mappare i rischi e soddisfare le esigenze di idoneità³⁷ del modello nel caso concreto³⁸.

Si consideri inoltre che non si ha modo di conoscere la *ratio* dei decreti di archiviazione e, quindi, non è possibile sapere se vi sia stata la constatazione da parte delle procure di un Modello idoneo. Risulta possibile solo una riflessione basata sui provvedimenti dei giudici che hanno espresso una valutazione negativa³⁹.

Concludendo, questa percepita «*anarchia di contenuti*»⁴⁰ non aiuta in termini di prova dell'efficace attuazione che deve superare positivamente la valutazione del giudice basata sul libero convincimento⁴¹. Di conseguenza, l'ampia discrezionalità riconosciuta in questo campo all'accertamento giurisdizionale, in mancanza di una normativa che descriva nel dettaglio il contenuto del Modello per i motivi soprammenzionati, inevitabilmente spaventa le imprese⁴².

4. Trasparenza e onere della prova

Il legislatore ha previsto che l'ente sia responsabile per i reati-presupposto commessi, nel suo interesse o vantaggio, da soggetti c.d. apicali o da soggetti sottoposti all'altrui direzione⁴³. La compresenza del criterio d'imputazione c.d. oggettivo⁴⁴, rappresentato dall'interesse o dal vantaggio dell'ente⁴⁵, e dei criteri d'imputazione c.d. soggettivi⁴⁶, i quali variano a seconda della qualifica dell'autore del reato-presupposto, permette di discernere i casi nei quali è il pubblico ministero è chiamato all'esercizio dell'azione penale *ex art. 112 Cost.* Infatti, i criteri di imputazione soggettiva dell'ente hanno come cardine il Modello e si differenziano a seconda della qualifica del soggetto autore del reato. Nei casi riguardati soggetti in posizione c.d. apicale⁴⁷, l'art. 6, comma 1 richiede, ai fini dell'esenzione di responsabilità dell'ente, che non solo si sia adottato ed efficacemente attuato il modello⁴⁸, ma che questo sia idoneo⁴⁹ alla prevenzione del reato commesso (lett. *a*)⁵⁰.

Il legislatore ha quindi ritenuto opportuno prevedere un'inversione dell'onere probatorio⁵¹ fondata sulle evidenze empiriche da cui si presume che il requisito soggettivo di imputazione sia soddisfatto, visto il rapporto di stretta immedesimazione tra l'apicale e l'ente. Ne consegue che l'ente possa «*rimanere immune dalla responsabilità se riesce ad ottemperare ad un complesso onere probatorio*»⁵². Sarà l'ente a dover dimostrare di essersi dotarsi di un organismo con poteri autonomi preposto alla vigilanza (lett. *b*)⁵³ (i.e. OdV), dimostrando che non vi siano state negligenze da parte di quest'ultimo e che si sia vigilato sul corretto funzionamento del complesso organizzativo (lett. *d*). Inoltre, dovrà dar prova del fatto che l'autore del reato si sia fraudolentemente sottratto alla vigilanza (lett. *c*)⁵⁴: il carattere di frodolenza deve caratterizzare il comportamento elusivo dell'autore del reato⁵⁵.

I reati commessi da c.d. sottoposti⁵⁶ *ex art. 7*, comma 1 riguardano il mancato adempimento degli obblighi di vigilanza e controllo e il fulcro è individuabile nel paradigma della *culpa in*

vigilando: l'ente contribuisce colpevolmente alla concretizzazione del rischio di commissione di un reato-presupposto. La colpa è esclusa in caso di adozione di modelli che garantiscano lo svolgimento dell'attività nel rispetto della legge e contrastino il rischio-reato (i.e. il Modello). Il Modello deve essere dotato di un sistema sanzionatorio e aggiornato costantemente per il suo effettivo funzionamento⁵⁷. Qualora il soggetto autore del reato sia un c.d. sottoposto, non è prevista alcuna inversione dell'onere probatorio come nel caso degli apicali.⁵⁸ Questi criteri sono rilevanti nell'ottica della funzione preventiva della sanzione e, combinati al regime premiale del sistema, aspirano a motivare all'osservanza di *standard* utili a prevenire la commissione di reati e a evitare che le sanzioni vengano recepite come un costo necessario e quindi calcolate come *spese* nel bilancio⁵⁹.

Il Modello diventa così un «*mezzo di prova tipico previsto per dimostrare l'idoneità organizzativa dell'ente*»⁶⁰ in funzione di fatto impeditivo.⁶¹

Per assolvere a tale funzione, il Modello deve essere orientato alla trasparenza e alla tracciabilità. La tracciabilità serve sia a garantire una maggiore trasparenza della gestione organizzativa, che alle Procure della Repubblica per permettere un'accurata ricostruzione degli eventi e di stabilire ed avere una comprensione più profonda e documentata del funzionamento del Modello, consentendo di individuare al meglio i *process owners* e i soggetti che intervengono in determinati processi operativi. In tale ottica, il *RegTech* ha il grande vantaggio di poter assicurare la tracciabilità in tempo reale, oltre che a conservare a posteriori, le dinamiche di attuazione dei protocolli, i percorsi di *decision making*, nonché i soggetti che vi hanno preso parte e, quindi, di rilevare le violazioni o le *suspicious activities* tempestivamente.

Come descritto in precedenza, il *RegTech* contribuisce, di fatto, alla raccolta, l'archiviazione, la visualizzazione e l'utilizzo dei dati utili sia per la pianificazione e l'esecuzione dei protocolli e delle regole di condotta, che per la documentazione degli eventi e delle misure intraprese dall'ente attraverso *log* strutturati e cronologicamente organizzati in cui gli accessi di coloro che hanno gestito le singole procedure e/o inserito e/o aggiornato e/o modificato e/o monitorato i dati vengono registrati e le ragioni alla base delle scelte compiute, siano in conformità al Modello o in eccezione alle procedure formalizzate (*comply or explain*), annotata. Queste informazioni così archiviate e organizzate possono diventare cruciali per la difesa dell'ente oltre a facilitare le indagini circa l'effettività e l'idoneità del Modello e la vigilanza sullo stesso,

5. Applicazione pratica

La c.d. *integrated compliance*⁶² rafforzata dall'uso degli strumenti *RegTech* può contribuire a contenere i costi e, soprattutto, agevolare agli enti il compito di districarsi tra il groviglio di disposizioni normative che, a seconda dei settori in cui operano, variano ed aumentano rapidamente.

Sia in termini di efficientamento che da un punto di vista economico: l'adozione di soluzioni tecnologiche pare essere in grado di ammortizzare i costi in termini di *compliance*. Pertanto, la natura dinamica della tecnologia, benché esponga chi ne fa uso (e non) a rischi e, quindi, necessita di un quadro normativo che ne regoli l'uso e l'esposizione, si sta dimostrando un'agile alleata in termini di *compliance* e *risk management*, grazie alla capacità di raccolta, organizzazione, elaborazione e comunicazione di un gran numero di dati.

Le soluzioni *RegTech* consentono l'automatizzazione delle attività che tradizionalmente richiedevano un significativo impiego di risorse e tempo, come ad esempio il monitoraggio della normativa, l'analisi dei rischi, fino alla produzione di reportistica dedicata.

Infatti, tra le possibili applicazioni del *RegTech*, identificate anche dal *EBA*⁶³, vi è l'*automated compliance*, l'*identity management and control*, il *risk management*, il *regulatory reporting* e il *transaction monitoring*.

In particolare, la *dynamic-compliance*, ovvero il controllo dei requisiti di *compliance* effettuati tramite protocolli IT nel contesto di un *automated real-time monitoring*, combinata alle procedure automatizzate di profilatura del cliente in ambito di *KYC* e agli strumenti di *advanced data analytics* e *machine learning* possono rendere più efficace e meno costoso il processo di gestione del rischio oltre che di implementazione del Modello. Si consideri, per esempio, che l'automazione e la digitalizzazione dell'attività di *reporting* comporta risparmio di costi oltre ad una maggiore accuratezza e tempestività, basti pensare che la tecnologia consente un monitoraggio *real-time* delle transazioni (*transaction monitoring*) che rileva eventuali discrepanze e segnala istantaneamente ai soggetti competenti l'evento, oltre che sospendere, laddove necessario, eventuali operazioni.

Inoltre, le attività di monitoraggio dell'applicazione dei protocolli possono essere automatizzate attraverso l'adozione di sistemi di *RPA* (*Robotic Process Automation*) e combinate all'implementazione di piattaforme di *GRC* (*Governance, Risk and Control*) che gestiscono il flusso delle informazioni, riducendo i tempi e i costi dei controlli e aumentandone al contempo l'efficacia. Queste tecnologie sono in

grado di rielaborare e armonizzare grandi volumi di dati provenienti da fonti diverse migliorando i processi di *decision-making* aziendale.

Le soluzioni *RegTech* hanno anche il grande vantaggio di proporsi quale soluzione pratica alle esigenze di *KYC*, monitoraggio, *screening*, *assessment* e gestione del rischio sia nella fase di *onboarding* che nell'arco della relazione con i clienti.⁶⁴ A questo riguardo, strumenti di *RegTech* come *streaming analytics* e tecnologie *DLT-based* possono essere impiegate per l'identificazione in tempo reale delle *suspicious transactions* e *suspicious activities*.⁶⁵

6. Corporate Culture

Attraverso lo studio dei *white-collar crimes*⁶⁶ e dei *corporate crimes*⁶⁷ che è emersa l'esigenza di una moderna strategia di contrasto alla criminalità d'impresa, specialmente alla luce delle nuove forme di criminalità non ancora perseguite penalmente⁶⁸ nei paesi economicamente sviluppati. Infatti, il giudizio della società civile e dell'ordinamento stesso rispetto a questa tipologia di illeciti ribalta le logiche del c.d. *labelling approach*⁶⁹ a causa del c.d. *organizational deviance defining process*⁷⁰: le imprese definiscono le proprie condotte in termini favorevoli, finendo con il minimizzare l'effetto deviante e tendendo ad annullare la percezione del danno prodotto dalle loro condotte.⁷¹

Si è iniziato a utilizzare il termine *corporate crime* poiché rimanda al ruolo importante della struttura organizzativa nella quale si origina il fenomeno⁷² e alla necessità di intervenire sul contesto sottoculturale⁷³ entro il quale le persone fisiche agiscono⁷⁴. La persona giuridica viene, quindi, concepita come un *soggetto a rischio* di commissione di reati⁷⁵: la distanza spazio-temporale tra l'evento dannoso e la condotta, *l'invisibilità della vittima*⁷⁶, così come il carattere di segretezza delle scelte⁷⁷, i *deficit* nei procedimenti decisionali dell'organizzazione e il *fenomeno del gruppo*⁷⁸ accrescono il c.d. *risky shift*⁷⁹ e alimentano meccanismi di neutralizzazione⁸⁰.

La struttura culturale e normativa dell'organizzazione va a costituire un'autonoma personalità dell'ente rispetto alle persone fisiche che ne manifestano la volontà⁸¹ e contribuisce ad aumentare le pressioni criminogene.

Pertanto, il Modello deve essere partecipativo e orientato al consenso: è necessario che i protocolli siano proporzionati alla natura e alle dimensioni dell'ente, che delineino e tengano in considerazione i comportamenti dei dipendenti⁸² e promuovano una cultura aziendale corretta. In questo contesto la tecnologia potrebbe essere utilizzata per rendere

più efficiente i profili di *corporate governance* e conformità, aumentando la trasparenza e la disponibilità di informazioni, velocizzando la comunicazione, riducendo i tempi di attività e migliorando il processo decisionale.

La sensibilizzazione può essere conseguita attraverso un approccio pragmatico in cui i *manager* promuovono e spiegano la cultura dell'azienda fin dall'inserimento del nuovo personale, premiano le persone che rappresentano dei modelli all'interno dell'azienda e stabiliscono degli incentivi, ossia dei bonus, che tengono conto non solo dei risultati finanziari dei dipendenti, ma anche della loro condotta nel rispetto delle politiche e delle procedure interne.⁸³

A questo fine i training sia in fase di inserimento che su base continuativa sono fondamentali non solo per mantenere il personale aggiornato e in grado di approcciarsi all'infrastruttura tecnologica in modo efficiente, ma anche per evitare che, in assenza di un'adeguata formazione, ponga in essere atti non in linea con i protocolli o altre *malpractice*. Spesso gli apicali, così come buona parte dei funzionari non hanno ore da dedicare per la formazione dei propri dipendenti, colleghi o sottoposti e per questa ragione esternalizzano questa funzione a terzi.

Le soluzioni *RegTech* spesso includono nei servizi prestati anche la formazione dei soggetti che ne fruiscono e offrono dei *tutorial* aggiornati sul funzionamento della soluzione. Infatti, esse stesse richiedono una formazione del personale per il loro corretto funzionamento.

Si combini quanto esposto con la possibilità da parte dei *manager* di programmare e registrare dei corsi da riproporre ai nuovi dipendenti attraverso piattaforme digitali, comprensivo di test finali a risposta multipla. Benché l'approccio *face-to-face* sia insostituibile, è innegabile l'utilità di una sezione di formazione continua accessibile a tutti i dipendenti tramite piattaforma digitale che li aiuti ad orientarsi in un quadro normativo non di facile interpretazione, oltre che ad avere una visione più chiara struttura organizzativa e del funzionamento dell'infrastruttura IT.

La *corporate culture*⁸⁴ e i valori trasmessi dalla *leadership* aziendale sono la *conditio sine qua non* per incentivare un atteggiamento di attenzione verso la disciplina in continuo cambiamento, non uniformemente applicata e che non di rado presenta discrepanze interpretative.

L'osservanza della normativa risulta essere un elemento imprescindibile di una cultura aziendale orientata al modello di *compliance culture* e su questo presupposto, la tecnologia può contribuire a disegnare i perimetri e incentivare l'assimilazione di comportamenti orientati alla conformità, oltre

che all'etica. Tuttavia, si consideri che la *compliance culture* deve mirare non solo a disincentivare le violazioni dei protocolli e delle norme, ma anche a non esautorare il senso del Modello e le esigenze del legislatore, in caso contrario, la tecnologia stessa rischia quindi di essere usata quale mezzo di conformità che vanifica lo scopo e la *ratio* delle prescrizioni normativa⁸⁵.

7. Rischi

Tra i rischi dell'utilizzo di soluzioni *RegTech* vi è il c.d. effetto scatola nera (*black-box*): in generale, ambienti e processi complessi e automatizzati rischiano di rendere opaco la trasparenza del processo dei dati. Se la metodologia sottostante che governa i processi decisionali degli strumenti tecnologici non viene adeguatamente spiegata, si può creare un fenomeno di asimmetrie del flusso di informazioni che può finire con l'alimentare l'impressione che, quando gli strumenti *RegTech* sono utilizzati dai *regulator*, gli obblighi imposti dalle autorità siano futili e le sanzioni emesse siano incontrollabili e ingiustificate. L'opacità nell'applicazione del *RegTech* può rendere difficile per revisori e per gli enti stessi comprendere non solo le esatte ragioni che hanno portato l'autorità a sanzionare la società, ma anche ostacolare anche l'impugnazione di tali decisioni, poiché questi non hanno accesso alle informazioni e al metodo di elaborazione delle stesse.⁸⁶

Dall'altro lato, l'adozione di queste tecnologie da parte degli enti può essere motivo di scetticismo da parte delle autorità di vigilanza e/o dalla Procura della Repubblica, oltre che dei revisori e della clientela, finendo con l'essere percepito come elemento di opacità circa il flusso e l'elaborazione delle informazioni.

Inoltre, considerando che solitamente sono terzi fornitori di servizi che mettono a disposizione le soluzioni *RegTech*⁸⁷ e vista la frequenza degli attacchi alla sicurezza informatica che provocano la perdita di dati e l'interruzione delle attività economiche o di vigilanza l'ente deve verificare che la sicurezza, la riservatezza e l'integrità dei dati siano adeguatamente presidiate. Inoltre, l'uso di tecnologie espone a maggiori rischi anche la *privacy* e la riservatezza aziendale. Sia le autorità di vigilanze che gli enti devono quindi dotarsi di un solido *business continuity plan* e di un *cybersecurity framework* in grado di far fronte ai rischi operativi⁸⁸, oltre che a solida *governance* dei dati e la messa in sicurezza delle infrastrutture IT. Un altro rischio che vale la pena di evidenziare riguarda l'automazione dei processi che da un lato riduce i rischi di errori manuali, ma non elimina in

toto gli errori umani derivanti dall'impostazione dei criteri applicativi delle soluzioni IT. Ad esempio, algoritmi non correttamente impostati potrebbero portare alla selezione di una strategia di gestione e/o mitigazione del problema rilevato scorretta o non adeguata, mettendo a rischio l'efficacia complessiva delle azioni di *compliance*.⁸⁹

Inoltre, le risorse umane sono fondamentali per valutare e interpretare i risultati degli *output* prodotti da soluzioni *RegTech*, oltre a garantire accuratezza e completezza. L'apprendimento automatico e processi basati su algoritmi necessitano di risorse umane adeguatamente qualificate.⁹⁰

Il *RegTech* è soggetto a un ulteriore problema, ossia l'allocazione delle responsabilità. Le autorità stesse, per esempio, rischiano di violare delle normative e di essere quindi esposte a potenziali responsabilità nei confronti dei vari *stakeholder*. Queste responsabilità potenzialmente derivanti da malfunzionamenti dell'infrastruttura IT, così come la copertura assicurativa per tali responsabilità, potrebbero non risultare di facile contrattazione⁹¹. Concludendo, le soluzioni *RegTech* consentono agli enti di automatizzare e rendere più effettiva la *compliance* con le esigenze della normativa vigente, tuttavia vi è il rischio che le piattaforme informatiche messe a disposizione degli enti, si traducano in tentativi delle società di eludere le normative.⁹²

8. Conclusione costi-benefici

Poiché i soggetti destinatari della normativa non sono solo le persone giuridiche private riconosciute ex artt. 14 ss. c.c., ma anche le associazioni non riconosciute e gli enti privati privi di personalità giuridica, come emerge dall'art. 1, comma 2 del d.lgs. n. 231 del 2001⁹³, anche entità di scarsa importanza⁹⁴ finiscono con il diventare destinatarie del sistema processuale dispendioso progettato per la responsabilità da reato degli enti.

Ne consegue che, questo sistema possa risultare «*alla prova dei fatti, addirittura diseconomico*»⁹⁵.

Altrettanto rilevanti sono le crescenti spinte, raccolte nel ddl n. 726/2018, per rendere obbligatoria l'adozione dei Modelli per determinate categorie di persone giuridiche⁹⁶.

Dall'altro lato, l'industria globale *RegTech* ha il potenziale di accelerare il perseguimento di un'innovazione normativa e finanziaria più sostenibile, efficace ed inclusiva. Non a caso, dal 2008, la combinazione tra nuove disposizioni regolamentari e tecnologia nel settore finanziario ha facilitato e diffuso una maggiore *compliance*, non solo grazie l'impiego di soluzioni *RegTech* da parte delle società, ma anche per via di un primo

approccio a tale fenomeno da parte di alcune autorità di vigilanza.

Tale processo non può che includere una trasformazione sia nel rapporto tra vari soggetti coinvolti (autorità e enti), che nelle infrastrutture che ne facilitino il dialogo e la vigilanza. Il nuovo paradigma, nel panorama italiano, offre un'ulteriore possibilità di incontro tra esigenze preventive (da parte dello Stato) e vantaggi premiali (da parte degli enti) che trascende la questione ente regolamentato e coinvolge a tutto tondo le persone giuridiche soggette al d.lgs. n. 231 del 2001.

Di non secondaria importanza sono i costi relative alle infrastrutture *RegTech* che possono essere considerevoli: il loro acquisto, corsi di preparazione e aggiornamento, le consulenze specialistiche e la necessità di ulteriori servizi ancillari da parte di terzi fornitori.

La convenienza delle soluzioni *RegTech* è direttamente proporzionale con la dimensione del *business* sottostante all'ente. *L'economy of scale* del *RegTech* è evidente, al crescere della quantità della produzione e della dimensione di un'impresa corrisponde una riduzione del costo medio.

Concludendo, sebbene il *RegTech* sia un grande strumento di supporto per gli enti, al tempo stesso potrebbe non essere considerato come economicamente sostenibile per le piccole-medio imprese.

Tuttavia, l'aumento di *player* sul mercato e la crescente offerta di soluzioni variegata possono offrire soluzioni proporzionali alle dimensioni e alle disponibilità economiche dell'ente acquirente, riducendo in generale i costi di accesso alle soluzioni *RegTech*.

1 Il sistema è stato messo a punto nelle *Federal Sentencing Guidelines for Organizations* nell'anno 1991 cfr. C. DE MAGLIE, *L'etica e il mercato. La responsabilità penale delle persone giuridiche*, Giuffrè, 2002, p. 66 ss.

2 Per tutti v. C. DE MAGLIE, *L'etica e il mercato. La responsabilità penale delle persone giuridiche*, cit., p. 73 ss.

3 A. ALESSANDRI, *Diritto penale e attività economiche*, Il Mulino, 2010, cit p. 221.

4 H. BELLUTA, *L'ente incolpato. Diritti fondamentali e processo 231*, in *Procedura penale*, collana diretta da M. BARGIS - G. GIOSTRA - G. ILLUMINATI - R.E. KOSTORIS - R. ORLANDI, Giappichelli, 2018, p. 107; G. LASCO, sub art. 12, in *Enti e responsabilità da reato*, a cura di G. LASCO - V. LORIA - M. MORGANTE, Giappichelli, 2017, p. 166; R. A. RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, in M. BARGIS - G. GIOSTRA - G. ILLUMINATI - R. KOSTORIS - R. ORLANDI, *Procedura Penale*, Giappichelli, 2018, p. 43 ss.; M. H. SCHETTINO - F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, Giuffrè, 2019, p. 57; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, in *Trattato di procedura penale*, diretto da G. UBERTIS - G. VOENA, Giuffrè, 2012, p. 92 ss.

5 H. BELLUTA, *L'ente incolpato. Diritti fondamentali e processo 231*, cit., p. 107; G. LASCO, sub art. 12, cit. p. 166; A. RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, cit., p. 43 ss.; M. H. SCHETTINO - F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 57.

6 G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit. p. 92.

7 L'Associazione Bancaria Italiana (ABI) ha avviato un cantiere dedicato all'analisi di soluzioni tecnologiche disponibili e i relativi trend. Accessibile al sito: <https://www.abi.it/Pagine/news/ParteFintech.aspx>. Ultimo accesso 19 Dicembre 2020. Nell'Agosto 2020, l'Associazione Bancaria Europea (EBA) ha pubblicato una consultazione sul tema. Accessibile al sito: <https://eba.europa.eu/eba-consults-use-regtech-solutions-and-ways-support-uptake-regtech-across-eu>. Ultimo accesso 19 Dicembre 2020.

8 L'emergere del *FinTech* è attribuibile a: (1) le carenze del mercato finanziario causate dal crisi finanziaria e dalla risposta normativa che ne è derivata, (2) la sfiducia del pubblico nell'industria dei servizi finanziari, in particolare negli Stati Uniti e nell'UE, (3) la pressione politica a favore di fonti di finanziamento alternative per le piccole e medie imprese, (4) la mercificazione della tecnologia e la penetrazione nel mercato di Internet e dei telefoni cellulari, in particolare degli *smartphone*. Vedi D.W. ARNER - J.N. BARBERIS - R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, in *Northwestern Journal of International Law & Business, Forthcoming, University of Hong Kong Faculty of Law Research Paper*, 35, 2016.

9 "Solo nel 2017, in Italia, sono state emanate ben 1.509 norme di diritto europeo e nazionale, considerando tutte le fasi normative si tratta di circa sei norme per ogni giornata lavorativa, con un incremento rispetto alle 1.247 del 2016" cfr. ABI. Accessibile al sito: <https://www.abi.it/Pagine/news/ParteFintech.aspx>. Ultimo accesso 19 Dicembre 2020.

Sul tema anche D.W. ARNER - J.N. BARBERIS - R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, in *Northwestern Journal of International Law & Business, Forthcoming, University of Hong Kong Faculty of Law Research Paper*, 35, 2016, p. 4 ss; J.W. BAGBY - N. PACKIN, *RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation*, 2020, p. 11.

- 10 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 2.
- 11 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 4 ss.; G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, cit., p. 2.
- 12 “RegTech is a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities”, FINANCIAL CONDUCT AUTHORITY, *Feedback Statement, Call for Input on Supporting the Development and Adopters of RegTech*, 2016, p. 3.
- 13 J.W. BAGBY – N. PACKIN, *RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation*, cit., p. 10.
- 14 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 4 ss.
- 15 L’institute of International Finance identifica una serie di soluzioni tecnologiche innovative che possono migliorare la gestione dei dati e l’analisi include *inter alia*, il *cryptographic technology*, *data mining algorithms*, *machine learning*, *blockchain*, *robotics* e *visual analytics*. Vedi D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 15.
- 16 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 15.
- 17 J.W. BAGBY – N. PACKIN, *RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation*, cit., p. 10.
- 18 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, cit., p. 2 ss.
- 19 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 15.
- 20 FCA, RegTech Forum Series: <https://web.cvent.com/event/cadb5e87-3dfb-4635-859d-7539f255a63f/summary?rp=00000000-0000-0000-0000-000000000000>. Ultimo accesso 4 Dicembre 2020.
- 21 FCA, *Moving your firm to RegData*: <https://www.fca.org.uk/firms/regdata/moving-your-firm-regdata> Ultimo accesso 4 Dicembre 2020. FCA, *The Digital Sandbox Pilot*: <https://www.fca.org.uk/firms/innovation/digital-sandbox>. Ultimo accesso 4 Dicembre 2020.
- 22 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 15.
- 23 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 2. La FCA è stata la prima a descrivere l’applicazione di nuove tecnologie che potrebbero aiutare a gestire meglio le sfide normative e i pericoli della sicurezza informatica.
- 24 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 17.
- 25 D.W. ARNER – J.N. BARBERIS- R. P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, cit., p. 17.
- 26 Una rendicontazione standardizzata e armonizzata potrebbe quindi essere vantaggiosa sia per gli enti che per le autorità di regolamentazione.
- 27 Un sistema globale di *reporting* e il KYC a disposizione dei partecipanti - sia le autorità di regolamentazione che l’industria - potrebbero trasformare gli sforzi anti-riciclaggio e i relativi costi di conformità, oltre a sostenere l’inclusione finanziaria, come evidenziato nel focus del G20/FSB sul *correspondent banking*. Da Gennaio 2020 è diventata attuativa la quinta direttiva antiriciclaggio e lotta al finanziamento del terrorismo che prevede l’istituzione di banche date per condividere le informazioni relative ai *beneficial owners*.
- 28 M. CERESA GASTALDO, *Procedura penale delle società*, Giappichelli, 2017, p. 24; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti. Il difficile equilibrio tra difesa e prevenzione*, in A. GIARDA- G. SPANGHER- P. TONINI, *Problemi attuali della giustizia penale*, CEDAM, 2016, p. 225-226; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, Ipsoa, 2017, p. 68 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 91 ss.
- 29 M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 73.
- 30 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 23; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 224 ss.; A. PRESUTTI-A. BERNASCONI, *Manuale della responsabilità degli enti*, cit., p. 102; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 54 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 67-68.
- 31 D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 221; A. PRESUTTI-A. BERNASCONI, *Manuale della responsabilità degli enti*, cit., p. 100 F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 58.
- 32 A. PRESUTTI-A. BERNASCONI, *Manuale della responsabilità degli enti*, cit., p. 101; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 74.
- 33 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 23; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 225-226.
- 34 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 24; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a*

carico degli enti., cit., p. 227; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 86 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 67-68.

35 Si pensi al caso di soluzioni per il monitoraggio delle transazioni, o per KYC.

36 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 24; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti.*, cit., p. 225-226; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 68 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 92 ss.

37 In tema di valutazione dell'idoneità *ex ante* ed *ex post* v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 22-23; D. GERONIMO, *Responsabilità da reato degli enti: l'adozione di modelli organizzativi post factum ed il commissariamento giudiziale nell'ambito delle dinamiche cautelari*, in *Cass. pen.*, 2004, p. 257 ss.; S. GIAVAZZI, sub art. 17-21, in A. Giarda- E.M. MANCUSO- S. SPANGHER- G. VARRASO, *Responsabilità «penale» delle persone giuridiche. D.lgs. 231/2001*, Ipsoa, 2007, p. 163 ss.; G. SALCUNI, *La valutazione di idoneità dei modelli ed il requisito dell'elusione fraudolenta*, in R. Borsari, *Responsabilità da reato degli enti. Un consuntivo critico*, Padova University Press, 2016, p. 111 ss.; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 94-95.

38 Sul tema v. A. PRESUTTI-A. BERNASCONI, *Manuale della responsabilità degli enti*, cit., p. 100 ss. In materia di linee guida si veda per esempio CONFINDUSTRIA, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del Decreto legislativo 8 giugno 2001, n. 231*, in www.confindustria.it; ABI, *Linee guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche*, in www.abi.it

39 Cfr. v. Cass. pen., sez. IV, 24 gennaio 2019, n. 16598; Cass. pen. sez. III, 23 gennaio 2019, n. 11518 § 18; Cass., Sez. un., 24 aprile 2014, n. 38343 Espenhahn e altri; Cass. pen., Sez. II, 20 giugno 2018, n. 41012, § 10.2

40 D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti.*, cit., p. 235; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 67-68.

41 D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti.*, cit., p. 235.

42 Cfr. v. Cass. pen., sez. IV, 24 gennaio 2019, n. 16598; Cass. pen. sez. III, 23 gennaio 2019, n. 11518 § 18; Cass., Sez. un., 24 aprile 2014, n. 38343 Espenhahn e altri; Cass. pen., Sez. II, 20 giugno 2018, n. 41012, § 10.2

43 *Ex multis* v. A. ALESSANDRI, *Diritto penale e attività economiche*, cit., p. 191; A. BERNASCONI, *Societas delinquere (et puniri) potest*, in *Manuale della responsabilità degli enti*, a cura di A. PRESUTTI-A. BERNASCONI, Giuffrè, 2018, p. 6; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 1 ss.; F. SBISA - E. SPINELLI- B. AGOSTINI, *La responsabilità amministrativa degli enti: origine, natura, principi e criteri d'imputazione*, cit., p. 28 ss.; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit. p. 18.

44 Quelli che la Relazione chiama *criteri di imputazione sul piano oggettivo*, e che sono previsti all'art. 5 del d. lgs. n. 231/2001, individuano i *soggetti qualificati* che, con la commissione di reati *per conto* dell'ente, ne innescano la responsabilità. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 14 ss.; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti.*, cit., p. 104 ss.; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 28 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 20 ss.; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 37. In giurisprudenza di recente v. Cass. pen., Sez. VI, 25 settembre 2018, n. 54640.

45 Sul tema v. A. BERNASCONI, sub art 5, cit., p. 97 ss.; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 16 ss.; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 104 ss.; C. SANTORIELLO, *I requisiti dell'interesse e del vantaggio della società nell'ambito della responsabilità dell'ente collettivo*, in *Resp. amm. soc. enti*, 2008, 49 ss.; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 32 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 20 ss. G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 41 ss.

46 I criteri di imputazione c.d. soggettiva, invece, riprendono l'idea di *colpevolezza* intesa come *riprovevolezza*, e si prepongono di attribuire all'ente una responsabilità che derivi da una *colpa di organizzazione* e che sia, comunque, espressione della *politica aziendale*. In tema v. A. ALESSANDRI, *Diritto penale e attività economiche*, cit., p. 216; A. BERNASCONI, sub art 5, cit., p. 113; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 20 ss.; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 114 ss.

47 Sul tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 39 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29. G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 51 ss. In giurisprudenza di recente v. Cass. pen., Sez. VI, 25 settembre 2018, n. 54640; Cass., Sez. un., 24 aprile 2014, n. 38343 Espenhahn e altri.

48 Sul tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; M. H. SCHETTINO- F. LUCARIELLO, *La difesa*

degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale, cit., p. 28-29. Per una maggiore concretizzazione dei modelli è necessario porre l'attenzione sulle possibili cause degli illeciti, che stanno alla base di una progettualità preventiva circa i rischi, e sulle dinamiche che permettono l'occultamento e che, se contrastate, possono favorirne l'emersione v. G. FORTI, *Percorsi di legalità in campo economico: una prospettiva criminologico-penalistica*, in *Ciclo di seminari "L'uomo e il denaro"*, 2009, p. 55.

49 Sul tema v. A. ALESSANDRI, *Diritto penale e attività economiche*, cit., p. 225; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22.

50 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

51 Sul tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti. Il difficile equilibrio tra difesa e prevenzione*, cit., p. 80-81; Ivi, p. 174 ss.; P. PAULESU, *L'accertamento della responsabilità penale degli enti: riflessioni in tema di dinamiche probatorie e regole decisorie*, in R. BORSARI, *Responsabilità da reato degli enti. Un consuntivo critico*, Padova University Press, 2016, p. 417 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

52 G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 52. In tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

53 M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 40; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

54 Sul tema M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 41; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

55 Sul tema A. BERNASCONI, sub art 6, cit., p. 148 ss.; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 21-22; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 41; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 28-29.

56 Sul tema v. A. BERNASCONI, sub art 7, in *La responsabilità degli enti*, a cura di A. PRESUTTI- A. BERNASCONI- C. FLORIO, Giuffrè, 2008, p.163 ss.; M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 22-23; F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, cit., p. 42 ss.; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 32; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, cit., p. 58 ss. In giurisprudenza di recente v. Cass. pen., Sez. VI, 25 settembre 2018, n. 54640; Cass., Sez. un., 24 aprile 2014, n. 38343 Espenhahn e altri.

57 Sul tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 22-23; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 32-33.

58 Sul tema v. M. CERESA GASTALDO, *Procedura penale delle società*, cit., p. 22-23; D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 175.

59 Con la conseguenza che il "costo" degli illeciti finisce con l'essere sostenuto dai clienti. «Il versarsi in re illecita si traduce in un disincentivo all'osservanza di cautele doverose» Relazione ministeriale di accompagnamento al d.lgs. n. 231/2001 § 3.3

60 D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 237

61 D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, cit., p. 237; A. PRESUTTI-A. BERNASCONI, *Manuale della responsabilità degli enti*, cit., p. 96; M. H. SCHETTINO- F. LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. n. 231/2001. Dal modello organizzativo al procedimento penale*, cit., p. 67 ss.

62 Deloitte, New Horizons. Compliance 2020 and beyond, 2020. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-compliance-thought-leadership-16.pdf>.

63 EBA, Accessibile al sito <https://eba.europa.eu/eba-consults-use-regtech-solutions-and-ways-support-uptake-regtech-across-eu> e <https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub/regtech-industry-survey>

64 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 7.

65 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 7.

66 Espressione con la quale si indicano i reati commessi da "una persona rispettabile e appartenente alle più alte classi sociali nel corso della sua occupazione" Cfr. E. H. SUTHERLAND, *White collar crime*, trad. it. a cura di G. Forti *Il crimine dei colletti bianchi. La versione integrale*, Giuffrè, 1987, p. 8. Per le critiche al concetto di *white collar crime*, considerato troppo vasta v.

P. TAPPAN, *Who is the Criminal?* in *Am. Soc. Rev.*, 1947, p. 12 ss.

67 Sul tema J. BRAITHWAITE - B. FISSE, *Corporations, crime and accountability*, Cambridge University Press, 1993; JOHN C. COFFEE, *Corporate criminal liability: An Introduction and Comparative Survey* in Eser-Heine-Huber, *Criminal Responsibility of Legal and Collective Entities*, 1999, p.10; P. TAPPAN, *Who is the Criminal?* in *Am. Soc. Rev.*, 1947.

68 All'epoca erano previste delle sanzioni amministrative pecuniarie. Per approfondire il concetto di relatività del reato v. G. FORTI, *L'immane concretezza. Metamorfosi del crimine e controllo penale*, Cortina Raffaello, 2000, p. 304 ss.

69 G. FORTI, *L'immane concretezza*, cit., p. 228 ss.; Ivi, p. 337 ss.

70 G. FORTI, *Percorsi di legalità in campo economico: una prospettiva criminologico-penalistica*, in *Ciclo di seminari "L'uomo e il denaro"*, 2009, p. 43.

71 Per comprendere il motivo per cui fenomeni patologici legati al mondo dei rapporti economici siano comunemente percepiti in modo "meno grave" rispetto alla criminalità c.d. di strada e, di conseguenza, la ragione per cui "l'intensità" della risposta penale risulta essere diversa, bisogna riprendere il concetto di euristica della disponibilità e di campo oscuro. Il primo concetto si basa su un tipico meccanismo attraverso cui l'uomo si rappresenta i rischi basandosi sulla facilità con cui la mente riesce a pensare a esempi pertinenti; il pubblico costantemente sottoposto alla spettacolarizzazione del crimine e alla brutalità dei reati c.d. di strada, dove la vittima è palesata e l'autore ha un volto da condannare, è più sollecitato da questi ultimi rispetto ai "noiosi" illeciti finanziari, in cui la vittima è invisibile e gli autori spesso non hanno un volto o si presentano come persone ben integrate nel complesso sociale. Il c.d. privilegio degli affari permette di tutelare la reputazione e condizionare le riforme legislative, contribuendo al mantenimento degli illeciti d'impresa nel campo oscuro, rallentandone l'emersione e sottraendoli alle istanze di controllo, sia a livello di criminalizzazione in c.d. astratto, attraverso la previsione di una normativa penale, che di criminalizzazione in c.d. concreto, poiché gli agenti istituzionali tendono a dare la precedenza ad altri autori di reato. Per queste ragioni si parla di una depenalizzazione di fatto che investe la criminalità degli affari e accresce la cifra nera.

72 Si passa quindi dalla visione antropomorfa alla visione c.d. strutturale, considerando l'ente capace di produrre determinati effetti criminosi. Sul tema C. DE MAGLIE, *L'etica*, cit., p. 249; R. A. RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, in M. BARGIS - G. GIOSTRA- G. ILLUMINATI- R. KOSTORIS- R. ORLANDI, *Procedura Penale*, Giappichelli, 2018, p. 87 ss; F. SBISA- N. MOTTA, *Uno sguardo comparato. La responsabilità degli enti nei paesi di common law*, in F. SBISA, *Responsabilità amministrativa degli enti (d.lgs. 231/01)*, Ipsoa, 2017, p. 492 ss.

73 Sutherland avvalendosi della figura dei *colletti bianchi* corroborò la sua teoria delle associazioni differenziali secondo cui "nelle condizioni adatte, una certa persona tiene un comportamento criminale solo se le definizioni favorevoli prevalgono su quelle sfavorevoli" cfr. E. H. SUTHERLAND, *Il crimine*, cit., p. 305. In tema v. A. CERETTI, *L'orizzonte artificiale. Problemi epistemologici della criminologia*, CEDAM, 1992, p. 217 ss. Sull'influenza delle dinamiche di gruppo sul comportamento individuale v. P. ZIMBARDO, *L'effetto lucifero. Cattivi si diventa*, trad. it., Cortina Raffaello, 2008.

74 In tema di *colpevolezza organizzativa* v. A. ALESSANDRI, *Commento all'art 27*, cit., p. 154.

75 In assenza di quella struttura organizzata difficilmente si commetterebbero i reati imputati al soggetto autore v. A. ALESSANDRI, *Diritto penale e attività economiche*, cit., p. 65; C. DE MAGLIE, *L'etica*, cit., p. 252.

76 J. BRAITHWAITE - B. FISSE, *Corporate*, cit., p. 4.

77 Sul tema C. DE MAGLIE, *L'etica*, cit., p. 254 ss.

78 J. BRAITHWAITE - B. FISSE, *Corporate*, cit., p. 2. L'autore individua il gruppo come "matrice essenziale" del reato d'impresa.

79 La c.d. sindrome da "ebbrezza da rischio", ossia la sottovalutazione del rischio di insuccesso e la sopravvalutazione della possibilità di successo quando questi soggetti agiscono in gruppo v. C. DE MAGLIE, *L'etica*, cit., p. 51.

80 A. CERETTI, *L'orizzonte artificiale*, cit., p. 228; Sulla teoria delle negazioni G. FORTI, *L'immane concretezza*, cit., p. 499 ss.

81 G. FORTI, *Percorsi*, cit., p. 42.

82 DELOITTE, *Compliance in the spotlight Challenges and opportunities for corporate compliance functions*, 2013. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-audit-compliance-in-the-spotlight.pdf>; T. HAUGH, *Harmonizing Governance, Risk Management, and Compliance through the Paradigm of Behavioral Ethics Risk*, in *University of Pennsylvania Journal of Business Law*, Vol. 21, No. 4, 2019.

83 HAUGH, T., *Harmonizing Governance, Risk Management, and Compliance through the Paradigm of Behavioral Ethics Risk*, in *University of Pennsylvania Journal of Business Law*, Vol. 21, No. 4, 2019; DELOITTE, *Compliance in the spotlight Challenges and opportunities for corporate compliance functions*, 2013.

84 DELOITTE, *Compliance in the spotlight Challenges and opportunities for corporate compliance functions*, 2013; HAUGH, T., *Harmonizing Governance, Risk Management, and Compliance through the Paradigm of Behavioral Ethics Risk*, in *University of Pennsylvania Journal of Business Law*, Vol. 21, No. 4, 2019.

85 L'etica intesa come spinta a prendere decisioni sulla base di una convinzione morale, e non tanto per il mero fine di obbedire alle disposizioni di legge, non esime di per sé l'ente dal commettere violazioni: per quanto etica, una condotta può

comunque essere non conforme alla disciplina vigente. Dall'altro lato, un atteggiamento conforme alla normativa vigente, può essere considerato non etico, ad esempio, si consideri che i profitti delle banche risentono delle decisioni in termini di gestione del livello di capitale e di liquidità nel modo più efficace possibile, per questo la tendenza è quella di individuare il metodo che consenta di abbassare il livello di capitale minimo richiesto.

86 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 18 ss.

87 Come normalmente avviene nei casi di strumenti di *data security* impiegati dalle autorità di vigilanza.

88 G. LOIACONO- A. MAZZULLO – E. RULLI, *ResTech: Innovative Technologies for Crisis Resolution*, in *Oxford Business Law Blog*, 2020, p. 18 ss.

89 *Ibidem*

90 *Ibidem*. L'insieme delle competenze umane di cui l'autorità di vigilanza e gli enti possono avere bisogno (a seconda della complessità del sistema adottato) è ampio e comprende le competenze tecnologiche, le competenze ingegneristiche e le competenze specifiche per la *compliance*. Il personale - che molto probabilmente ha un *background* legale o economico - potrebbe dover essere affiancato da un ingegnere finanziario e da un analista dei dati, le cui conoscenze sono fondamentali per decidere qualsiasi ulteriore azione in seguito all'uscita delle tecnologie innovative

91 *Ibidem*

92 Pertanto, tra i rischi del *RegTech* vi è un uso improprio della tecnologia al mero fine di non essere in violazione della disciplina attenendosi al minimo regolamentare o, nei casi più estremi, eludere la regolamentazione e frustrare gli obiettivi delle autorità di vigilanza, facendo sì che l'ente e la *compliance function* finisca con il promuovere quei medesimi comportamenti che la disciplina vigente intende prevenire.

93 Il legislatore ha evitato di stilare elenchi dei destinatari e si è limitato a indicare categorie di enti attraverso una «*formula elastica*». Sono state giurisprudenza e dottrina a cimentarsi nell'interpretazione della norma per individuare con maggiore precisione quali tra le numerose realtà dotate di qualifica giuridica siano da considerarsi soggette alla disciplina, nonostante il principio di legalità richieda anche la determinatezza dei destinatari e, pertanto, non dovrebbe essere ammessa l'interpretazione analogica o estensiva dell'articolo. È possibile desumere dei criteri sistematici che aiutino a interpretare l'inclusione o meno nel gruppo dei destinatari della disciplina. Innanzitutto, devono esserci un'apprezzabile complessità organizzativa e la capacità patrimoniale autonoma. Poiché le sanzioni colpiscono in via esclusiva il patrimonio dell'ente in quanto centro di imputazione soggettiva distinto dalla persona fisica si è considerato opportuno escludere le realtà individuali.

94 A. Rossi, *I soggetti persone giuridiche*, cit., p. 27

95 Relazione ministeriale del d.lgs. n. 231/2001 § 2

96 «*Pertanto, il presente disegno di legge intende introdurre l'obbligatorietà del citato modello 231 e della nomina dell'organismo di vigilanza di cui all'articolo 6, comma 1, lettera b), del decreto legislativo n. 231 del 2001 a tutte le società di capitali e cooperative che non rientrino nei limiti dimensionali e reddituali previsti dall'articolo 2435-bis, primo comma, numeri 1) e 2), del codice civile, nonché la previsione di sanzioni pecuniarie per le società inadempienti*» v. disegno di legge n. 726/2018, p. 4.

 **GIURISPRUDENZA PENALE**