La compliance anticorruzione nell'era dei cambiamenti climatici: verso una governance integrata tra etica, diritto e sostenibilità

di Vincenzo Candido Renna e Laura Spano

ABSTRACT

La norma ISO 37001:2025 rappresenta una svolta nel panorama della prevenzione della corruzione, introducendo una prospettiva sistemica che integra dimensioni etiche, organizzative e ambientali. Il presente contributo analizza criticamente l'impatto delle innovazioni introdotte dallo standard, collocandole nel contesto della responsabilità degli enti ex D.Lgs. 231/2001 e della compliance integrata. Viene esaminata la transizione da un approccio formalistico, centrato sulla mera conformità, a un modello sostanzialistico di integrity governance, in cui la cultura organizzativa e la valutazione dei rischi climatici assumono un ruolo strutturale nella prevenzione. L'articolo adotta una metodologia interdisciplinare, combinando analisi giuridica, riflessione dottrinale e prospettiva manageriale, con particolare riferimento al rapporto tra soft law e hard law e al ruolo della certificazione nella definizione della responsabilità d'impresa.

ABSTRACT

The ISO 37001:2025 standard marks a turning point in anti-corruption prevention by introducing a systemic perspective that integrates ethical, organizational, and environmental dimensions. This paper critically examines the impact of the innovations introduced by the standard within the framework of corporate liability under Legislative Decree 231/2001 and integrated compliance. It explores the transition from a formalistic approach focused on mere conformity to a substantive model of integrity governance, where organizational culture and climate-risk assessment play a structural role in prevention.

PAROLE CHIAVE

Compliance, ISO 37001:2025, D.Lgs. 231/2001, Anticorruzione, Governance etica, Responsabilità organizzativa, Pubblica Amministrazione, Sostenibilità, Intelligenza artificiale, Blockchain, Due Diligence, PNRR, KPI etici, Cultura organizzativa, Soft law, Hard law.

KEYWORDS

Compliance, ISO 37001:2025, Legislative Decree 231/2001, Anti-corruption, Ethical Governance, Organizational Liability, Public Administration, Sustainability, Artificial Intelligence, Blockchain, Due Diligence, National Recovery Plan (PNRR), Ethical KPIs, Organizational Culture, Soft Law, Hard Law.

Indice

Capitolo – 1 Introduzione

La pubblicazione della ISO 37001:2025, avvenuta il 28 febbraio 2025[1], rappresenta un'evoluzione significativa negli strumenti internazionali di prevenzione della corruzione. La seconda edizione dello standard, che sostituisce la versione 2016 con un periodo di transizione di due anni[2], non si limita a una revisione tecnica delle procedure di gestione, ma consolida un approccio sistemico alla governance etica. Lo standard riconosce che la corruzione costituisce un fenomeno complesso, determinato non solo da devianze individuali ma anche da fattori culturali, ambientali e organizzativi.

Nel contesto italiano, la ISO 37001 si inserisce in un quadro normativo articolato, definito principalmente dal D.Lgs. 231/2001 sulla responsabilità amministrativa degli enti, dalla Legge 190/2012 sulla prevenzione della corruzione nella pubblica amministrazione, e dal D.Lgs. 24/2023 in materia di whistleblowing[3]. Mentre queste norme hanno introdotto un modello preventivo basato sull'obbligo di predisporre modelli organizzativi e piani anticorruzione, la ISO 37001 offre un linguaggio tecnico comune per la gestione dei rischi corruttivi, ponendo l'accento sulla misurabilità degli interventi, la trasparenza dei processi e il miglioramento continuo secondo la logica PDCA (plan-do-check-act).

L'obiettivo è duplice: fornire alle organizzazioni pubbliche e private uno strumento operativo per implementare sistemi di gestione anticorruzione efficaci e certificabili; promuovere una cultura della legalità sostanziale, in cui la conformità diventi elemento

[1] ISO 37001:2025, "Anti-bribery management systems - Requirements with guidance for use", pubblicata il 28 febbraio 2025. Disponibile su www.iso.org.

[2] DNV, "Aggiornamento ISO 37001", 2025, disponibile su www.dnv.it. Il periodo di transizione è di due anni, quindi fino al 28 febbraio 2027.

[3] D.Lgs. 231/2001; L. 190/2012; D.Lgs. 24/2023 in attuazione della Direttiva UE 2019/1937 sul whistleblowing.

di valore competitivo e reputazionale[4]. Questo approccio trasforma la compliance da mero adempimento burocratico a funzione strategica di governance.

Come osserva Piergallini, il diritto penale dell'impresa si sta trasformando da diritto della sanzione a diritto dell'organizzazione, fondato sulla prevenzione efficace e *sull'accountability* gestionale[5]In tale prospettiva, la ISO 37001 si configura come strumento di integrazione tra requisiti normativi, best practice manageriali e obiettivi di sostenibilità.

1.1. Dalla compliance formale alla compliance sostanziale

L'evoluzione dalla ISO 37001:2016 alla versione 2025 riflette il progressivo consolidamento di un modello di compliance sostanziale, orientato all'effettività dei controlli piuttosto che alla documentazione formale. Questo cambiamento è coerente con l'evoluzione giurisprudenziale italiana in materia di responsabilità degli enti, che valorizza sempre più l'idoneità concreta dei modelli organizzativi[6].

Il concetto di "colpa di organizzazione", elaborato dalla dottrina penalistica e recepito dalla giurisprudenza[7], implica che la responsabilità dell'ente derivi dalla mancata costruzione di una cultura organizzativa effettivamente capace di anticipare e gestire i rischi-reato[8]. La ISO 37001:2025 introduce strumenti qualificati di valutazione del rischio corruttivo, basati su metodologie riconosciute come la ISO 31000:2018, promuovendo un approccio dinamico e contestualizzato alla prevenzione.

[4] V.C. RENNA, "ISO 37001 la nuova frontiera dell'anticorruzione", in Amministrativ@mente, n. 11-12, 2018, disponibile su www.amministrativamente.com.

[5] C. PIERGALLINI, "Paradigmatica dell'autocontrollo penale", in Riv. it. dir. proc. pen., 2013, pp. 1717 ss.

[6] Cass. Pen., Sez. Unite, 24 aprile 2014, n. 38343, che stabilisce i criteri di idoneità del modello organizzativo.

[7] A. ALESSANDRI, "Riflessioni penalistiche sulla nuova disciplina", in AA.VV., Il nuovo diritto penale delle società, Milano, 2002, pp. 33 ss.; C. PIERGALLINI, "Societas delinquere et puniri non potest", in Riv. trim. dir. pen. economia, 2002, pp. 571 ss.

[8] ISO 31000:2018, "Risk management - Guidelines"; ISO 37001:2025, clausola 6 (Planning).

1.2. La dimensione internazionale e il ruolo della soft law

Sul piano internazionale, la ISO 37001 risponde all'esigenza di armonizzazione degli standard etici tra settori economici e sistemi giuridici nazionali. Lo standard si integra con altri strumenti di *soft law* quali le Linee Guida OCSE per le imprese multinazionali (revisione 2023), la Convenzione ONU contro la corruzione - UNCAC, il Foreign Corrupt Practices Act statunitense e il UK Bribery Act 2010.

La soft law assume crescente rilevanza come veicolo di standardizzazione etica dei mercati globali. Come evidenziato in dottrina, gli standard volontari divengono progressivamente parametri di valutazione della diligenza organizzativa anche nei procedimenti giudiziari [9].

1.3. Il nesso tra compliance anticorruzione e sostenibilità ESG

Un elemento qualificante della ISO 37001:2025 è la sua integrazione esplicita con le politiche di sostenibilità, in particolare con i criteri ESG (Environmental, Social, Governance)[10]. La versione 2025 introduce per la prima volta riferimenti diretti al cambiamento climatico come fattore rilevante nella gestione del rischio corruzione[11].

La corruzione rappresenta una delle principali cause di inefficienza nelle politiche pubbliche e di spreco delle risorse collettive, con impatti anche sulla sostenibilità ambientale. La ISO 37001, in sinergia con la Corporate Sustainability Reporting Directive - CSRD (Direttiva UE 2022/2464)[12], contribuisce a creare un quadro integrato di trasparenza. L'Obiettivo 16 dell'Agenda 2030 delle Nazioni Unite

[9] F. MAZZACUVA, "Le linee guida e i codici di comportamento nel sistema della responsabilità da reato degli enti", in Riv. trim. dir. pen. economia, 2014, pp. 537 ss.

[10] ISO 37001:2025, clausola 4.1, che include esplicitamente i fattori ESG nel contesto dell'organizzazione.

[11] ISO 37001:2025, clausola 4.2, Nota 1, sui cambiamenti climatici come requisito delle parti interessate.

[12] Direttiva UE 2022/2464 (CSRD); EFRAG, "European Sustainability Reporting Standards", 2023.

identifica esplicitamente la lotta alla corruzione come prerequisito dello sviluppo sostenibile.

1.4. Obiettivi e metodologia del contributo

Questo contributo analizza la ISO 37001 nel contesto della governance etica globale, valutandone l'impatto sul sistema italiano della responsabilità degli enti. La metodologia adottata è interdisciplinare: combina l'analisi giuridico-dogmatica con l'approccio manageriale, includendo riferimenti comparati ai modelli di prevenzione adottati in Regno Unito, Francia e Cile.

Capitolo 2 – Fondamenti teorico-dogmatici della compliance anticorruzione

2.1. Il paradigma della prevenzione nella responsabilità dell'ente

La disciplina della responsabilità amministrativa delle persone giuridiche, introdotta dal D.Lgs. 231/2001, rappresenta una delle innovazioni più rilevanti nel diritto penale dell'economia italiano[13]. Essa ha segnato il passaggio da un modello esclusivamente repressivo a un modello di responsabilità oggettiva attenuata da meccanismi esimenti di natura organizzativa[14].

La "colpa di organizzazione" costituisce il fondamento dogmatico della responsabilità 231: essa sussiste quando l'organizzazione non risulta strutturata in modo da prevenire efficacemente i rischi-reato specifici dell'attività svolta. Come osserva Pulitanò, la responsabilità dell'ente non presuppone una colpevolezza in senso soggettivo, ma un difetto organizzativo obiettivamente apprezzabile nella gestione del rischio penale[15].

2.2. La funzione metanormativa dei modelli organizzativi

I modelli di organizzazione previsti dal D.Lgs. 231/2001 svolgono una funzione "metanormativa": integrano la norma penale primaria con regole elaborate autonomamente dall'ente, nel rispetto dei principi generali indicati dalla legge e dalle linee guida associative[16].

Questa autoregolamentazione rappresenta un fenomeno di autonomia normativa riflessiva, in cui l'organizzazione diventa co-produttrice della normatività che la governa. La ISO 37001 si inserisce in questa logica: fornisce una metodologia

[13] G. DE VERO, "La responsabilità penale delle persone giuridiche", in Trattato di diritto penale, Milano, 2008, pp. 89-145.
[14] G. DE SIMONE, "Persone giuridiche e responsabilità da reato", Pisa, 2012, pp. 134-167.
[15] D. PULITANÒ, "La responsabilità da reato degli enti: i criteri d'imputazione", in Riv. it. dir. proc. pen., 2002, pp. 415 ss
[16] Confindustria, "Linee guida per i modelli di organizzazione ex D.Lgs. 231/2001", 2021.

standardizzata per la costruzione di modelli efficaci, articolati secondo una struttura che comprende analisi del contesto, valutazione del rischio, controlli preventivi, formazione e due diligence[17].

2.3. Il rapporto tra compliance e diritto penale preventivo

L'espansione della compliance riflette la tendenza del diritto penale moderno a configurarsi come diritto della prevenzione organizzativa[18]. Come osservato da Donini, si assiste a una "amministrativizzazione del diritto penale", in cui il legislatore affida ai destinatari il compito di costruire barriere procedurali interne contro il rischio penalmente rilevante[19].

La ISO 37001 fornisce strumenti standardizzati per la gestione del rischio corruttivo attraverso policy, procedure e meccanismi di monitoraggio continuo. La certificazione può assumere rilevanza sintomatica dell'idoneità del modello anche nel giudizio ex art. 6 D.Lgs. 231/2001, pur non costituendo elemento decisivo per il giudice[20].

Come chiarito dalla giurisprudenza, l'idoneità del modello deve essere valutata in base a criteri di effettività, specificità rispetto ai rischi concreti e aggiornamento continuo[21]. La compliance si configura quindi come forma di responsabilità dinamica e adattiva.

[17] ISO 37001:2025, clausole 4-10.
[18] V. MANES, "Il principio di offensività nel diritto penale", Torino, 2005.
[19] M. DONINI, "Il volto attuale dell'illecito penale", Milano, 2004, pp. 267-289.
[20] V.C. RENNA, "La ISO 37001:2025 e il D.Lgs. 231/2001: innovazioni e prospettive", 2025, disponibile su www.filodiritto.com.
[21] Cass. Pen., Sez. Unite, n. 38343/2014, cit.

2.4. La dottrina della colpa d'organizzazione e la cultura della prevenzione

La "colpa di organizzazione" rappresenta l'elemento dogmatico centrale del sistema 231[22]. Essa presuppone che l'ente risponda non direttamente per il reato commesso dalla persona fisica, ma per la carenza organizzativa che ha reso possibile quella condotta.

La compliance diventa una forma di etica istituzionalizzata, in cui il dovere di diligenza organizzativa sostituisce il tradizionale concetto di colpa individuale. Come evidenziato da Alessandri, la colpa di organizzazione si traduce in un dovere positivo di costruire presidi di legalità attraverso la progettazione consapevole dei processi[23].

2.5. La governance multilivello della legalità

La prevenzione della corruzione è compito condiviso tra autorità pubbliche, imprese private e organismi di standardizzazione internazionale[24]. La ISO 37001 promuove un modello di governance multilivello, nel quale soggetti pubblici e privati partecipano alla costruzione di un ecosistema dell'integrità.

2.6. Sintesi

La ISO 37001:2025 non costituisce solo uno standard tecnico, ma esprime un modello culturale di prevenzione fondato su trasparenza, accountability e miglioramento continuo[25]. Essa rappresenta l'evoluzione del diritto penale dell'economia verso forme di responsabilità organizzativa, in cui l'ente diventa co-protagonista della produzione di legalità.

Il valore dello standard risiede nella capacità di tradurre il precetto normativo in metodo gestionale e l'etica in prassi organizzativa verificabile. La compliance

[22] C. PIERGALLINI, "Sistema sanzionatorio e reati del codice penale", in Reati e responsabilità degli enti, Milano, 2010, pp. 215 ss.
[23] A. ALESSANDRI, "Riflessioni penalistiche", cit., pp. 40 ss.
[24] OCSE, "Recommendation for Further Combating Bribery", 2021.
[25] V.C. RENNA, "ISO 37001 la nuova frontiera dell'anticorruzione", cit.

anticorruzione diventa strategia di legittimazione, elemento di vantaggio competitivo e condizione di crescita sostenibile per imprese e pubbliche amministrazioni[26].

[26] V. MONGILLO, "La corruzione tra sfera pubblica e privata", Napoli, 2012, pp. 456-478.

Capitolo 3 – La corruzione come fenomeno sistemico: prospettive interdisciplinari

3.1. Dalla patologia individuale alla disfunzione sistemica

La concezione tradizionale della corruzione come deviazione morale individuale – approccio che ha dominato il dibattito giuridico e criminologico fino alla fine del XX secolo – è oggi superata sia sul piano teorico che su quello operativo. Le scienze sociali contemporanee, il diritto comparato e la criminologia economica riconoscono nella corruzione una patologia sistemica, radicata nelle strutture economiche, istituzionali e relazionali che governano l'interazione tra pubblico e privato.

Sul piano sociologico, la corruzione è interpretata come il prodotto di un ecosistema di incentivi perversi, nel quale le variabili individuali (onestà, integrità morale) sono subordinate alle condizioni sistemiche (opacità, discrezionalità, assenza di controlli). In contesti caratterizzati da bassa fiducia sociale e alto tasso di discrezionalità amministrativa, i comportamenti opportunistici tendono a diventare norma implicita, sostituendosi progressivamente alle regole formali.

Susan Rose-Ackerman, una delle massime autorità mondiali in materia di economia della corruzione, ha sintetizzato efficacemente questo meccanismo: "la corruzione prospera dove le regole sono troppe e la fiducia troppo poca. Questa osservazione coglie un paradosso fondamentale: l'eccesso di regolamentazione, anziché ridurre la corruzione, può alimentarla, poiché moltiplica le opportunità di discrezionalità e aumenta il valore dello scambio corruttivo. La soluzione non sta nell'assenza di regole (che genererebbe anarchia), ma nella loro razionalizzazione, accompagnata da meccanismi di trasparenza e tracciabilità che riducano gli spazi di arbitrio.

3.2. La dimensione politica della corruzione e la crisi della fiducia istituzionale

La corruzione non è solo un fenomeno economico o criminologico: essa rappresenta, soprattutto, una patologia politica che mina alla radice la legittimità delle istituzioni democratiche. Quando la corruzione diventa sistemica, il patto sociale tra cittadini e

istituzioni si indebolisce, generando una crisi di fiducia che si traduce in instabilità normativa, inefficienza amministrativa e progressiva delegittimazione del sistema politico nel suo complesso.

Il legame tra corruzione e fiducia è oggi centrale anche nelle teorie della democrazia deliberativa, sviluppate in particolare da Jürgen Habermas e dalla scuola del discorso pubblico. Secondo questa prospettiva, la legittimità delle decisioni pubbliche non deriva unicamente dal rispetto delle procedure formali (legalità), ma dalla trasparenza dei processi deliberativi e dalla partecipazione informata dei cittadini. Dove la fiducia crolla, aumenta la necessità di controlli formali, si riduce la libertà decisionale e si genera un circolo vizioso di sfiducia-regolamentazione-ulteriore sfiducia.

Niklas Luhmann, nella sua teoria sistemica della fiducia, ha evidenziato come la fiducia non sia solo un sentimento soggettivo, ma una forma di riduzione della complessità sociale[27]. In sistemi complessi, caratterizzati da interdipendenze multiple e informazioni asimmetriche, la fiducia permette di "scommettere" sulla prevedibilità del comportamento altrui, riducendo i costi di transazione e facilitando la cooperazione. La corruzione distrugge questa prevedibilità, sostituendola con l'arbitrio e l'opacità.

Sul piano pratico, ciò si traduce nella richiesta di:

Pubblicità delle procedure decisionali, con particolare riferimento agli appalti pubblici e alle concessioni;

Tracciabilità dei flussi finanziari e delle relazioni tra soggetti pubblici e privati;

Accountability individuale e organizzativa, con chiara attribuzione delle responsabilità;

Partecipazione dei cittadini ai processi di controllo, attraverso strumenti di civic engagement.

[27] LUHMANN, N., *La fiducia*, Il Mulino, Bologna, 2002 (ed. orig. 1968); ID., *Sistemi sociali. Fondamenti di una teoria generale*, Il Mulino, Bologna, 1990.

3.3. La corruzione e i cambiamenti climatici: un intreccio sottovalutato

L'emergenza climatica ha aperto un nuovo fronte nel dibattito globale sulla corruzione, evidenziando connessioni fino a pochi anni fa largamente sottovalutate. Le politiche ambientali, la gestione delle risorse naturali, la transizione energetica e i meccanismi di finanza climatica rappresentano oggi alcuni dei settori più vulnerabili a pratiche corruttive, con conseguenze devastanti non solo sull'efficacia delle strategie di mitigazione, ma anche sull'equità distributiva dei costi e dei benefici della transizione ecologica.

Organizzazioni internazionali come Transparency International e il Programma delle Nazioni Unite per l'Ambiente (UNEP) hanno documentato, attraverso una serie di rapporti sistematici, come la corruzione ambientale – nelle concessioni minerarie, nelle opere infrastrutturali "verdi", nei sistemi di compensazione delle emissioni (carbon credits), nella gestione dei fondi per l'adattamento climatico – costituisca una delle principali cause di fallimento delle strategie climatiche globali[28].

La corruzione climatica assume forme molteplici e spesso interconnesse:

Concessioni illegali per lo sfruttamento di risorse naturali in aree protette;

Manipolazione degli standard ambientali attraverso il lobbying opaco;

Frodi nei sistemi di certificazione delle emissioni;

Distrazione dei fondi destinati alla transizione ecologica;

Green washing istituzionale, ossia la falsificazione dei dati ambientali per accedere a finanziamenti pubblici o privati.

La corruzione climatica è il cortocircuito tra retorica verde e interessi economici opachi. Questo cortocircuito non solo vanifica gli investimenti nella sostenibilità, ma aggrava le diseguaglianze globali, poiché i costi della corruzione ambientale ricadono in modo sproporzionato sulle popolazioni più vulnerabili e sui paesi in via di sviluppo.

[28] TRANSPARENCY INTERNATIONAL, *Global Corruption Report: Climate Change*, Earthscan, London, 2011; UNEP, *Corruption and Environment*, United Nations Environment Programme, Nairobi, 2022.

In particolare, lo standard richiede:

L'identificazione dei rischi corruttivi specifici nei progetti ambientali;

La *due diligence* sulle catene di fornitura sostenibili;

Il monitoraggio dei flussi finanziari destinati alla sostenibilità;

La verifica dell'effettività degli impegni ESG (*Environmental, Social, Governance*).

3.4. L'approccio della *green criminology*

La *green criminology* – corrente di pensiero sviluppatasi negli ultimi due decenni nell'ambito della criminologia critica – studia le intersezioni tra criminalità economica, degrado ambientale e ingiustizia sociale, superando i confini disciplinari tradizionali. Essa riconosce che la corruzione rappresenta un moltiplicatore esponenziale del danno ambientale, poiché altera i processi decisionali pubblici, compromette l'equità distributiva delle risorse naturali e indebolisce i meccanismi di enforcement delle normative ambientali.

La natura transnazionale della corruzione sistemica impone necessariamente una governance multilivello che superi le frontiere nazionali e coordini l'azione di attori pubblici e privati su scala globale. Le organizzazioni internazionali – in particolare l'OCSE, le Nazioni Unite e la Banca Mondiale – hanno progressivamente integrato la prevenzione della corruzione nelle politiche di sviluppo sostenibile, nei programmi di aiuto economico e nei meccanismi di condizionalità degli investimenti internazionali.

Questo processo di integrazione ha portato all'emergere di un "diritto amministrativo globale dell'integrità", un insieme di principi, standard e *best practices* che, pur non costituendo diritto positivo in senso formale, esercitano un'influenza crescente sulle legislazioni nazionali e sulle politiche aziendali[29].

[29] CASSESE, S., "Administrative Law without the State? The Challenge of Global Regulation", in *New York University Journal of International Law and Politics*, vol. 37, 2005, pp. 663-694; KINGSBURY, B., KRISCH, N., STEWART, R.B., "The Emergence of Global Administrative Law", in *Law and Contemporary Problems*, vol. 68, 2005, pp. 15-61.

3.5. Sintesi conclusiva

Il fenomeno corruttivo non è un'anomalia occasionale del sistema, ma un prodotto strutturale della complessità dei sistemi economici, politici e sociali contemporanei. La sua comprensione richiede un approccio interdisciplinare che integri diritto, economia, sociologia, scienza politica e criminologia.

Capitolo 4 – Cultura organizzativa e colpa d'organizzazione

4.1. La cultura organizzativa come fondamento della compliance

La prevenzione efficace della corruzione non può essere affidata unicamente a protocolli, procedure e sistemi di controllo formale: essa richiede, come condizione necessaria ma spesso trascurata, una cultura organizzativa della legalità, autentica, condivisa e radicata nei comportamenti quotidiani di tutti i livelli dell'organizzazione.

La ISO 37001:2025 pone la leadership etica al centro del sistema di gestione anticorruzione, affermando con chiarezza che la prevenzione diventa efficace solo se sostenuta da una cultura di integrità che non sia puramente dichiarativa, ma effettivamente vissuta e praticata. Come sottolinea Paola Severino, tra i massimi esperti italiani di diritto penale d'impresa, "la cultura dell'integrità è la prima misura di prevenzione; la norma serve a formalizzarla, ma non può sostituirla[30]".

4.2. L'evoluzione dottrinale e giurisprudenziale della colpa d'organizzazione

Il concetto di colpa d'organizzazione è emerso progressivamente nella giurisprudenza e nella dottrina italiana a partire dai primi anni di applicazione del D.Lgs. 231/2001, che ha introdotto nel nostro ordinamento la responsabilità amministrativa degli enti derivante da reato[31].

La sentenza Impregilo (Cass. Pen., Sez. VI, 21 gennaio 2014, n. 2658) rappresenta un punto di svolta in questa evoluzione interpretativa[32]. La Suprema Corte ha chiarito che la colpa dell'ente non risiede automaticamente nella commissione del reato da parte

[30] SEVERINO, P., *La nuova legge anticorruzione*, Giuffrè, Milano, 2013; EAD., "Prevenzione e responsabilità nel sistema anticorruzione", in *Rivista italiana di diritto e procedura penale*, 2014, pp. 1180-1210.

[31] Sul D.Lgs. 231/2001 si vedano: PALIERO, C.E., "La responsabilità delle persone giuridiche: profili generali e criteri di imputazione", in AA.VV., *La responsabilità amministrativa degli enti*, Giuffrè, Milano, 2002; DE VERO, G., *La responsabilità penale delle persone giuridiche*, Giuffrè, Milano, 2008.

[32] Cass. Pen., Sez. VI, 21 gennaio 2014, n. 2658, *Impregilo*, in *Cass. Pen.*, 2014, p. 3615 ss.

dell'apicale o del sottoposto, ma nell'inadeguatezza del modello organizzativo adottato: l'ente è responsabile se non ha predisposto un sistema di prevenzione idoneo, se non ha vigilato sulla sua attuazione o se ha tollerato una cultura organizzativa permissiva verso comportamenti illeciti.

Successivamente, con la celebre sentenza ThyssenKrupp (Cass., Sez. Un., 24 aprile 2014, n. 38343), la Suprema Corte ha ulteriormente precisato che la responsabilità organizzativa deriva dalla mancanza di una cultura effettiva della sicurezza e della legalità[33]. Nel caso specifico, relativo a un tragico incidente sul lavoro, la Corte ha evidenziato come l'ente non potesse invocare l'adeguatezza formale del modello se nei fatti la cultura aziendale era imperniata sulla produttività a scapito della sicurezza.

La ISO 37001:2025 recepisce pienamente questa impostazione e la traduce in requisiti operativi misurabili:

Impegno documentato della direzione, con assunzione di responsabilità formale;

Promozione attiva dei valori etici, attraverso comunicazione, formazione e incentivi;

Valutazione periodica dell'efficacia del sistema di prevenzione, con indicatori qualitativi e quantitativi;

Meccanismi di miglioramento continuo, basati su audit interni ed esterni.

La cultura organizzativa, dunque, cessa di essere un elemento retorico o un orpello valoriale per diventare una componente tecnica della governance, misurabile, verificabile e giuridicamente rilevante.

4.3. L'etica organizzativa come capitale intangibile

Nel linguaggio economico-gestionale adottato dalla ISO 37001:2025, la cultura dell'integrità è classificata come "capitale intangibile di conformità": un insieme

[33] Cass. Pen., Sez. Un., 24 aprile 2014, n. 38343, *ThyssenKrupp*, in *Dir. pen. proc.*, 2014, p. 1066 ss.; in *Cass. Pen.*, 2015, p. 237 ss.

strutturato di valori, competenze, comportamenti e relazioni fiduciarie che producono effetti economici misurabili.

Questo concetto, mutuato dall'economia comportamentale e dagli studi sul capitale sociale[34], attribuisce valore patrimoniale all'etica, superando la tradizionale contrapposizione tra profitto e moralità. Una cultura aziendale orientata alla trasparenza, all'integrità e alla responsabilità non è solo moralmente desiderabile, ma anche economicamente conveniente, poiché:

Riduce i costi della non conformità (sanzioni, contenziosi, esclusioni da gare pubbliche);

Migliora la reputazione presso investitori, clienti, fornitori e autorità regolatorie;

Aumenta la capacità di attrarre talenti, poiché i lavoratori qualificati preferiscono organizzazioni eticamente solide;

Facilita l'accesso al credito e agli investimenti ESG (*Environmental, Social, Governance*);

Riduce il turnover e migliora il clima organizzativo interno.

4.4. La misurabilità della cultura organizzativa: indicatori e metriche

Una delle sfide più complesse della compliance contemporanea consiste nel rendere misurabile la cultura organizzativa, trasformandola da variabile qualitativa e soggettiva in oggetto di audit verificabile.

La ISO 37001:2025 suggerisce l'utilizzo di diversi strumenti e indicatori:

a) Indicatori di percezione interna:

Sondaggi anonimi sul clima etico e sulla percezione della leadership;

Questionari sulla conoscenza delle politiche anticorruzione;

Focus group con dipendenti di diversi livelli gerarchici.

[34] COLEMAN, J.S., *Foundations of Social Theory*, Harvard University Press, Cambridge, 1990; PUTNAM, R.D., *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton University Press, 1993.

b) Indicatori di partecipazione:

Tassi di partecipazione ai programmi formativi obbligatori e volontari;

Numero e qualità delle segnalazioni attraverso i canali di whistleblowing;

Livello di engagement nelle iniziative etiche promosse dall'organizzazione.

c) Indicatori comportamentali:

Dati sulle violazioni disciplinari e sulle relative sanzioni applicate;

Analisi dei conflitti di interesse dichiarati e gestiti;

Monitoraggio delle relazioni con terze parti sensibili.

d) Indicatori di efficacia sistemica:

Esiti degli audit interni ed esterni;

Reclami e segnalazioni esterne (da fornitori, clienti, autorità);

Incidenti e near miss in ambito anticorruzione.

Come evidenziato dalla letteratura manageriale[35], le organizzazioni che misurano sistematicamente la propria cultura etica ottengono risultati significativamente migliori in termini di prevenzione dei rischi corruttivi rispetto a quelle che si limitano a dichiarazioni formali di principio.

4.5. Leadership etica *e tone from the top*

La ISO 37001:2025 assegna un ruolo assolutamente determinante al *top management*, individuando nel cosiddetto *tone from the top* (il "tono dall'alto") la condizione essenziale e imprescindibile di un sistema anticorruzione efficace.

Gli elementi costitutivi della leadership etica includono:

a) Visibilità dell'impegno:

Partecipazione personale del vertice alle iniziative di formazione;

Comunicazione diretta e frequente sui temi dell'integrità;

[35] TREVIÑO, L.K., WEAVER, G.R., *Managing Ethics in Business Organizations*, Stanford University Press, Stanford, 2003; KAPTEIN, M., "The Effectiveness of Ethics Programs", in *Journal of Business Ethics*, vol. 78, 2008, pp. 385-407.

Assunzione pubblica di responsabilità in caso di violazioni.

b) Coerenza decisionale:

Rinuncia a vantaggi economici ottenibili attraverso pratiche eticamente dubbie;

Adozione di criteri trasparenti nelle decisioni strategiche;

Rifiuto di relazioni d'affari con controparti a rischio corruttivo elevato.

c) Supporto istituzionale alla funzione *compliance*:

Dotazione di risorse adeguate per la funzione anticorruzione;

Indipendenza effettiva dell'organismo di vigilanza;

Accesso diretto della compliance al consiglio di amministrazione.

4.6. La comunicazione interna e la formazione continua

Un sistema di prevenzione efficace richiede che i valori etici siano non solo dichiarati, ma comunicati efficacemente, compresi profondamente e interiorizzati stabilmente da tutti i livelli dell'organizzazione.

a) Differenziata:

Formazione base per tutti i dipendenti sui principi generali;

Formazione avanzata per le funzioni esposte a rischio corruttivo elevato;

Formazione specialistica per l'organismo di vigilanza e la funzione compliance.

b) Continua:

Aggiornamenti periodici per recepire modifiche normative e organizzative;

Refresh formativi per mantenere alta l'attenzione sul tema;

Formazione contestualizzata su casi concreti e lesson learned.

c) Interattiva:

Utilizzo di metodologie didattiche attive (*case study, role playing*, simulazioni);

Valutazione dell'apprendimento attraverso test e verifiche;

Feedback dei partecipanti per migliorare i programmi.

4.7. La dimensione sanzionatoria e correttiva

La cultura dell'integrità si consolida e si rafforza anche attraverso la gestione coerente, trasparente e proporzionata delle violazioni. La ISO 37001:2025 impone la previsione di meccanismi disciplinari efficaci, che assicurino la coerenza tra gravità dell'infrazione e conseguenza applicata.

Questa dimensione sanzionatoria svolge una duplice funzione:

Deterrenza individuale (dissuadere il singolo dalla violazione);

Deterrenza generale e rafforzamento culturale (segnalare all'intera organizzazione che le violazioni hanno conseguenze certe).

Questa pronuncia conferma che il sistema disciplinare non è un elemento accessorio, ma una componente essenziale del modello organizzativo. Esso deve rispettare alcuni principi fondamentali:

a) Proporzionalità:

Le sanzioni devono essere graduate in relazione alla gravità della violazione;

Devono essere previste conseguenze per tutti i livelli gerarchici, compresi i dirigenti;

La proporzionalità deve essere percepita come equa dai destinatari.

b) Certezza:

Le violazioni devono essere accertate attraverso procedure trasparenti;

Le sanzioni devono essere applicate con tempestività;

Non devono esistere "zone franche" o soggetti immuni dal sistema disciplinare.

c) Pubblicità (nei limiti della *privacy*):

L'applicazione di sanzioni per violazioni gravi deve essere comunicata all'organizzazione;

La comunicazione ha funzione educativa e di deterrenza generale;

Deve essere garantito l'equilibrio tra trasparenza e tutela della dignità personale.

4.8. La colpa d'organizzazione come difetto di cultura: profili applicativi

La dottrina italiana più recente ha elaborato una teoria compiuta della colpa d'organizzazione come categoria autonoma di responsabilità[36]. Questa teoria si fonda sull'idea che l'ente possa essere rimproverato non per avere voluto il reato (non essendo soggetto capace di volontà in senso psicologico), ma per non aver costruito le condizioni organizzative e culturali capaci di prevenirlo.

La colpa d'organizzazione si articola in tre dimensioni:

a) Colpa nella strutturazione del modello (in *eligendo*):

Scelta di un modello organizzativo inadeguato rispetto ai rischi specifici;

Mancata identificazione delle aree sensibili;

Assenza di procedure appropriate per i processi critici.

b) Colpa nella vigilanza sul modello (in vigilando):

Mancata verifica dell'effettiva attuazione delle procedure;

Assenza di audit interni periodici;

Inerzia di fronte a segnalazioni di anomalie.

c) Colpa nella costruzione della cultura (in educando):

Mancata formazione del personale;

Assenza di comunicazione efficace sui valori etici;

Incoerenza tra politiche dichiarate e comportamenti del vertice.

Numerose sentenze di merito hanno fatto applicazione di questi criteri, escludendo l'efficacia esimente del modello organizzativo in presenza di una cultura aziendale di fatto tollerante verso pratiche irregolari, nonostante l'esistenza formale di codici etici e procedure di controllo[37].

---

[36] MONGILLO, V., *La responsabilità penale tra individuo ed ente collettivo*, Giappichelli, Torino, 2018; PIERGALLINI, C., "Paradigmatica dell'autocontrollo penale", in *Riv. it. dir. proc. pen.*, 2013, p. 1743 ss.

[37] Trib. Milano, Sez. I, 27 aprile 2016, *Fastweb*; Trib. Trani, 22 marzo 2017, in www.anticorruzione.it.

4.9. Sintesi conclusiva

La cultura organizzativa rappresenta la vera frontiera della compliance contemporanea, il terreno su cui si gioca la partita decisiva tra efficacia ed inefficacia dei sistemi di prevenzione.

Capitolo 5 – Soft Law e Hard Law nella Prevenzione della Corruzione

5.1. L'ibridazione normativa: tra vincolo giuridico e autoregolazione etica

La prevenzione della corruzione contemporanea si fonda su una ibridazione crescente e strutturale tra *hard law* (diritto cogente, vincolante, sanzionatorio) e *soft law* (standard tecnici, linee guida, codici di condotta volontari ma autorevoli). Questa ibridazione non rappresenta una confusione concettuale né un'ambiguità normativa, ma costituisce una risposta funzionale alla complessità dei sistemi economici e organizzativi globali.

Come evidenzia Vincenzo Mongillo, tra i principali studiosi italiani del diritto penale dell'economia, "*la soft law* è il diritto della fiducia: non sostituisce la legge imperativa, ma la accompagna nel territorio dell'autonomia responsabile"[38]. Questa osservazione coglie un aspetto fondamentale: la soft law non opera in contrapposizione alla hard law, ma in sinergia complementare, occupando quegli spazi di flessibilità e specializzazione tecnica che la norma generale e astratta non può efficacemente presidiare.

5.2. La natura giuridica della *soft law* ISO: tra volontarietà formale e vincolatività sostanziale

La soft law ISO non è una norma giuridica in senso tecnico-formale: non promana da un'autorità legislativa, non è pubblicata in Gazzetta Ufficiale, non prevede sanzioni penali o amministrative dirette per la sua violazione. ma, essa produce effetti giuridici indiretti sempre più rilevanti, che si manifestano su diversi piani:

[38] MONGILLO, V., "La corruzione tra sfera interna e dimensione internazionale", in *Trattato di diritto penale dell'impresa*, vol. XI, CEDAM, Padova, 2014; ID., "Soft law e sistema delle fonti del diritto penale dell'impresa", in *Criminalia*, 2015, pp. 319-354.

5.3. La *soft law* come strumento di *moral suasion* e costruzione reputazionale

Oltre al valore tecnico-probatorio riconosciuto dalla giurisprudenza, la *soft law* esercita una funzione di *moral suasion*, inducendo comportamenti virtuosi attraverso meccanismi non coercitivi ma estremamente efficaci: la reputazione, la trasparenza, la pressione degli stakeholder e la competizione per l'affidabilità.

Gare pubbliche internazionali, che sempre più spesso richiedono o valorizzano la certificazione anticorruzione;

Finanziamenti e investimenti ESG, poiché i fondi etici e i *rating* di sostenibilità attribuiscono punteggi elevati alla governance anticorruzione;

Partnership strategiche con imprese multinazionali, che impongono standard di integrità elevati lungo tutta la catena di fornitura;

Mercati regolati, dove le autorità di vigilanza guardano con favore alla certificazione volontaria come strumento di compliance proattiva.

Questa prospettiva è coerente con le teorie della *responsive regulation* elaborate da John Braithwaite[39], secondo cui i sistemi regolatori più efficaci sono quelli che combinano piramidalmente strumenti di persuasione (alla base), meccanismi di mercato e reputazione (al centro) e sanzioni punitive (al vertice, come extrema ratio).

5.4. L'evoluzione della *soft law* nel sistema normativo internazionale

A livello internazionale, la *soft law* rappresenta lo strumento predominante per la regolazione della condotta etica d'impresa, specialmente in ambiti caratterizzati da elevata complessità tecnica, rapida evoluzione e assenza di consenso politico sufficiente per adottare trattati vincolanti.

Il tessuto normativo globale dell'integrità è costituito da un insieme articolato di strumenti di *soft law*, tra cui spiccano:

[39] BRAITHWAITE, J., *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, New York, 1992; ID., *Restorative Justice and Responsive Regulation*, Oxford University Press, Oxford, 2002.

b) Principi Guida ONU su Business e Diritti Umani (2011): Elaborati dal *Special Representative John Ruggie* e approvati dal Consiglio ONU per i Diritti Umani, stabiliscono il dovere degli Stati di proteggere i diritti umani e la responsabilità delle imprese di rispettarli attraverso processi di *human rights due diligence*[40].

d) Standard ISO della famiglia 37000:

ISO 37001 (Sistemi di gestione anticorruzione);

ISO 37301 (Sistemi di gestione per la compliance);

ISO 37000 (Governance delle organizzazioni).

Questi standard costituiscono la traduzione operativa dei principi contenuti nei trattati e nelle dichiarazioni internazionali, fornendo metodologie concrete per la loro implementazione.

Questa rete di norme non vincolanti opera attraverso la convergenza spontanea verso *best practices* condivise, favorita da:

Pressioni degli investitori istituzionali;

Requisiti di accesso ai mercati internazionali;

Condizionalità dei finanziamenti multilaterali;

Influenza delle ONG e della società civile;

Rischio reputazionale legato alla non conformità.

Il risultato è un ordinamento multilivello in cui il diritto statale si integra con l'autoregolazione privata, e la compliance assume il ruolo di architrave dell'ethos economico globale. Come osserva Sabino Cassese, si è progressivamente affermato un "diritto amministrativo globale"[41], caratterizzato dalla pluralità delle fonti, dalla prevalenza di standard tecnici e dalla centralità della trasparenza.

[40] RUGGIE, J., *Guiding Principles on Business and Human Rights*, United Nations, 2011, disponibile su www.ohchr.org.

[41] CASSESE, S., "Il diritto amministrativo globale: una introduzione", in *Rivista trimestrale di diritto pubblico*, 2005, pp. 331-357.

5.5. L'interazione tra *soft law* e *hard law* nel contesto italiano

Nel sistema giuridico italiano, la *soft law* ISO dialoga intensamente con la hard law rappresentata principalmente da:

L'integrazione tra questi due livelli di normazione genera un circolo virtuoso:

La legge stabilisce i principi generali e gli obblighi di risultato;

La soft law fornisce gli strumenti operativi, le metodologie tecniche e gli indicatori di performance;

La giurisprudenza riconosce valore probatorio alla conformità agli standard tecnici;

Le autorità di vigilanza (ANAC, Garante Privacy, Authority settoriali) fanno riferimento agli standard ISO nelle linee guida applicative.

Ad esempio, l'ANAC (Autorità Nazionale Anticorruzione) ha più volte richiamato la ISO 37001 come riferimento per la strutturazione dei sistemi di prevenzione nelle pubbliche amministrazioni e nelle società partecipate pubbliche[42]. Analogamente, il Piano Nazionale di Ripresa e Resilienza (PNRR) prevede meccanismi di condizionalità legati all'adozione di sistemi di gestione anticorruzione certificati per i soggetti attuatori.

5.6. Il valore probatorio della certificazione ISO: verso una presunzione relativa di idoneità

Uno degli aspetti più innovativi e giuridicamente rilevanti del rapporto tra *soft law* e *hard law* è la progressiva attribuzione di valore probatorio qualificato alla certificazione ISO 37001 nei procedimenti relativi alla responsabilità amministrativa degli enti.

Questa evoluzione è coerente con le esperienze comparate. In particolare, la legislazione cilena (Ley N° 20.393/2009, modificata dalla Ley N° 21.121/2018)

[42] ANAC, *Linee guida in materia di codici di comportamento delle pubbliche amministrazioni*, delibera n. 177/2020; ANAC, *Piano Nazionale Anticorruzione*, edizioni varie.

attribuisce espressamente alla certificazione ISO 37001 il valore di presunzione legale relativa di idoneità del modello di prevenzione[43]. Analogamente, in Francia la certificazione costituisce elemento di valutazione positiva nell'ambito della *Convention Judiciaire d'Intérêt Public* (CJIP), strumento negoziale di definizione della responsabilità[44].

In Italia, diverse proposte *de iure condendo* sono state avanzate per introdurre nel D.Lgs. 231/2001 una disposizione analoga. In particolare, si propone l'inserimento di un comma nell'art. 6 che riconosca la certificazione ISO 37001 come presunzione qualificata di conformità, superabile solo con prova contraria da parte dell'accusa[45].

Sul piano processuale, ciò comporta che:

La certificazione costituisce elemento probatorio qualificato dell'idoneità astratta del modello;

Resta fermo l'onere di provare l'effettiva attuazione del modello (non basta il certificato, occorre dimostrare che il sistema funziona);

Il giudice mantiene piena autonomia valutativa, ma deve motivare analiticamente l'eventuale disconoscimento del valore probatorio della certificazione.

5.7. Verso un diritto ibrido della compliance: superamento delle categorie tradizionali

La distinzione rigida tra *hard law* e *soft law*, tra norma imperativa e regola tecnica, tra obbligo e raccomandazione tende oggi progressivamente a dissolversi nella prassi applicativa. La compliance costituisce un campo ibrido di regolazione, nel quale la

[43] República de Chile, Ley N° 20.393 de 2009, "Establece la Responsabilidad Penal de las Personas Jurídicas", modificata da Ley N° 21.121 de 2018.

[44] Code de procédure pénale français, artt. 41-1-2 e seguenti (Convention Judiciaire d'Intérêt Public - CJIP), introdotti dalla Loi n° 2016-1691 (Loi Sapin II).

[45] FLICK, G.M., NAPOLEONI, V., *Cumulo giuridico e premialità: la nuova frontiera del diritto penale dell'impresa*, Giappichelli, Torino, 2021; PULITANÒ, D., "Responsabilità amministrativa per i reati delle persone giuridiche", in *Enc. dir., Annali*, vol. III, Giuffrè, Milano, 2010.

legalità si costruisce attraverso la convergenza dinamica di norme, procedure, standard tecnici e valori condivisi.

La ISO 37001:2025 incarna perfettamente questo diritto ibrido della *compliance*, poiché opera simultaneamente su tre piani:

a) Piano tecnico: Fornisce metodologie, processi, indicatori misurabili per la gestione del rischio corruttivo.

b) Piano etico: Promuove valori di integrità, trasparenza, *accountability* attraverso la cultura organizzativa.

c) Piano giuridico: Produce effetti di conformità normativa, rilevanza probatoria, presunzione di diligenza.

Come nota Gabrio Forti, tra i maggiori esperti italiani di diritto penale dell'impresa, "la prevenzione efficace nasce quando la norma penale incontra la norma organizzativa"[46].In questa sintesi, il diritto penale non perde forza coercitiva, ma acquista precisione ed efficacia preventiva: la sanzione interviene solo dove fallisce la prevenzione, e la prevenzione si struttura secondo criteri tecnici verificabili.

Questo approccio è coerente con l'evoluzione del diritto penale contemporaneo verso forme di responsabilità preventiva e *compliance-oriented*, che privilegiano l'anticipazione del rischio rispetto alla sola repressione dell'illecito compiuto[47].

5.8. Criticità e rischi della *soft law*: il problema della cattura normativa

Nonostante i numerosi vantaggi, l'utilizzo crescente della *soft law* nella regolazione della compliance presenta anche criticità che meritano attenzione critica.

a) Deficit democratico: Gli standard tecnici, inclusi quelli ISO, sono elaborati da organismi privati composti da esperti e rappresentanti di settore, senza il

[46] FORTI, G., "La 'chiara luce della verità' e 'l'ignoranza del peccato'. Appunti sulle scriminanti nel diritto penale dell'impresa", in *Studi in onore di Giorgio Marinucci*, vol. II, Giuffrè, Milano, 2006; ID., *L'immane concretezza*, Raffaello Cortina, Milano, 2000

[47] SILVA SÁNCHEZ, J.M., *La expansión del Derecho penal*, Civitas, Madrid, 2001; HASSEMER, W., *Lineamenti di una teoria personale del bene giuridico*, in *Dei delitti e delle pene*, 1984, pp. 95 ss.

coinvolgimento diretto dei parlamenti o di processi democratici trasparenti. Ciò solleva questioni di legittimazione democratica delle norme che, pur essendo formalmente volontarie, producono effetti giuridici rilevanti[48].

b) Rischio di cattura normativa: La partecipazione ai processi di elaborazione degli *standard* è spesso limitata a grandi imprese, associazioni di categoria e consulenti specializzati, con il rischio che gli *standard* riflettano principalmente gli interessi dei soggetti regolati anziché quelli della collettività[49].

e) Responsabilità degli organismi di certificazione: Il sistema si basa sulla credibilità degli enti certificatori terzi, ma esistono rischi di conflitti di interesse, variabilità qualitativa degli *audit* e fenomeni di "*certification shopping*" (ricerca dell'ente certificatore meno rigoroso)[50].

Queste criticità non invalidano il modello della *soft law*, ma evidenziano la necessità di:

Maggiore trasparenza nei processi di elaborazione degli *standard*;

Supervisione pubblica sugli organismi di certificazione;

Meccanismi di accessibilità economica per le PMI;

Equilibrio tra requisiti formali e valutazione sostanziale dell'efficacia;

Responsabilità degli enti certificatori per negligenza o collusione.

[48] CAFAGGI, F., MICKLITZ, H.W., "Administrative and Judicial Collective Enforcement of Consumer Law in the US and the European Community", EUI Working Papers, 2007.

[49] MATTLI, W., BÜTHE, T., "Setting International Standards: Technological Rationality or Primacy of Power?", in *World Politics*, vol. 56, 2003, pp. 1-42.

[50] GUNNINGHAM, N., REES, J., "Industry Self-Regulation: An Institutional Perspective", in *Law & Policy*, vol. 19, 1997, pp. 363-414.

5.9. Sintesi conclusiva

Il binomio *soft law – hard law* rappresenta il cuore pulsante della nuova *governance* etica globale, superando definitivamente la concezione monistica del diritto come sistema esclusivamente statale e coercitivo.

Come efficacemente sintetizzato dalla dottrina italiana più avanzata, "la *compliance* è il ponte tra etica e diritto, tra volontà e obbligo, tra mercato e regolazione"[51]. La ISO 37001:2025 rappresenta l'architrave più solida di questo ponte, destinato a sostenere la governance etica delle organizzazioni nei decenni a venire.

[51] ARDUINI, S., MATTARELLA, B.G. (a cura di), *La prevenzione della corruzione*, Giappichelli, Torino, 2013.

Capitolo 6 – La ISO 37001:2025 e la Pubblica Amministrazione: sinergie con la L. 190/2012 e il D.Lgs. 36/2023

6.1. La prevenzione amministrativa come politica pubblica: evoluzione normativa e principi fondanti

Con la Legge 6 novembre 2012, n. 190, recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", il legislatore italiano ha operato una svolta paradigmatica nella concezione stessa della lotta alla corruzione. Non più soltanto repressione ex post attraverso lo strumento penale, ma prevenzione strutturale mediante la pianificazione organizzativa e la trasparenza amministrativa.

La legge si colloca nel solco delle raccomandazioni internazionali, in particolare della Convenzione delle Nazioni Unite contro la corruzione (UNCAC, Merida 2003, ratificata dall'Italia con L. 116/2009) e delle linee guida OCSE sulla gestione del conflitto di interessi nel servizio pubblico. Come evidenziato da Patroni Griffi, "la L. 190/2012 segna il passaggio da una logica sanzionatoria ad una logica preventiva, nella consapevolezza che la corruzione è anzitutto un fenomeno organizzativo prima che criminale"[52]

Il modello italiano si struttura su tre pilastri fondamentali:

La convergenza tra diritto pubblico e standard gestionali produce un duplice vantaggio: da un lato, l'amministrazione può avvalersi di metodologie collaudate a livello internazionale; dall'altro, il sistema pubblico italiano acquisisce maggiore credibilità e comparabilità nel contesto europeo e globale. Come osserva Centonze, "la pubblica amministrazione del futuro è quella che misura la propria integrità come misura della

[52] A. PATRONI GRIFFI, *La prevenzione della corruzione tra sistema penale e modelli amministrativi*, in Dir. pen. proc., 2013, p. 845.

propria efficienza, superando la tradizionale dicotomia tra legalità formale e performance gestionale"[53].

6.2. L'integrazione tra PTPCT e sistema di gestione ISO 37001: dal formalismo alla cultura della prevenzione

Il Piano Triennale di Prevenzione della Corruzione e della Trasparenza rappresenta, nella concezione originaria del legislatore del 2012, lo strumento cardine della strategia anticorruzione delle pubbliche amministrazioni. ma, l'esperienza applicativa ha evidenziato significative criticità: eccesso di formalismo, scarsa integrazione con la gestione ordinaria, prevalenza di un approccio adempimentale rispetto ad una effettiva cultura della legalità.

Come rilevato dall'ANAC nel Rapporto 2023, "molti PTPCT si caratterizzano per un approccio eccessivamente burocratico, con misure generiche non calibrate sui rischi effettivi dell'amministrazione e con scarso monitoraggio dell'attuazione"[54]. La ISO 37001:2025, integrando i principi del miglioramento continuo e della verificabilità dei controlli, offre una risposta metodologica a tali criticità.

6.2.1. La logica PDCA applicata alla prevenzione amministrativa

L'integrazione tra PTPCT e sistema ISO si fonda sul ciclo di *Deming* (*Plan-Do-Check-Act*), che trasforma la pianificazione anticorruzione da documento statico a processo dinamico:

[53] A. CENTONZE, *La prevenzione della corruzione nella pubblica amministrazione: profili penali*, in Riv. it. dir. proc. pen., 2013, p. 1204. Cfr. anche ID., *Controlli, discrezionalità amministrativa e prevenzione della corruzione*, Milano, 2019.

[54] ANAC, *Rapporto sull'attività svolta nel 2023*, Roma, 2024, p. 67, disponibile su www.anticorruzione.it.

PLAN (Pianificazione strategica):

- Mappatura dei processi sensibili mediante tecniche di risk assessment qualitativo e quantitativo
- Definizione degli obiettivi anticorruzione misurabili e delle relative misure di prevenzione
- Allocazione delle risorse umane, tecniche e finanziarie necessarie

DO (Implementazione operativa):

- Attuazione delle misure generali e specifiche individuate nel PTPCT
- Formazione obbligatoria del personale sui rischi corruttivi e sui comportamenti da adottare
- Implementazione dei controlli preventivi (segregazione delle funzioni, rotazione, trasparenza)
- Attivazione dei canali di whistleblowing interno
- Gestione dei conflitti di interesse mediante dichiarazioni e astensioni

CHECK (Monitoraggio e valutazione):

- Attività di monitoraggio continuo sull'attuazione delle misure attraverso indicatori di performance (KPI)
- Audit interni periodici sui processi a rischio, condotti da soggetti indipendenti
- Analisi delle segnalazioni di whistleblowing e degli eventuali illeciti rilevati
- Reporting periodico agli organi di indirizzo politico-amministrativo e all'ANAC

ACT (Miglioramento continuo):

- Revisione annuale del PTPCT sulla base degli esiti del monitoraggio
- Adozione di azioni correttive in caso di non conformità rilevate

- Aggiornamento della valutazione dei rischi alla luce di nuovi elementi di contesto
- Condivisione delle best practice e delle lesson learned

Come evidenziato da Mattarella e Pelissero, "l'introduzione del ciclo PDCA nella prevenzione amministrativa rappresenta il superamento definitivo di una concezione statica della compliance, sostituita da un processo di apprendimento organizzativo continuo"[55].

6.2.2. Gli elementi di convergenza tecnica

L'analisi comparata tra PTPCT e ISO 37001 evidenzia numerosi elementi di convergenza che facilitano l'integrazione:

Elemento	PTPCT (L. 190/2012)	ISO 37001:2025
Mappatura rischi	Obbligo di individuare attività a rischio corruzione	Risk assessment strutturato (punto 6.1)
Responsabile	RPCT con funzioni di coordinamento	Anti-Bribery Compliance Function indipendente
Formazione	Obbligatoria per il personale	Obbligatoria e documentata (punto 7.3)
Whistleblowing	Tutela del segnalante (L. 179/2017)	Canali riservati e tutela dei segnalanti (punto 8.9)
Monitoraggio	Verifica attuazione misure	Audit interni e riesame della direzione
Trasparenza	Pubblicazione dati (D.Lgs. 33/2013)	Comunicazione e documentazione (punto 7.4)

[55] B.G. MATTARELLA - C. PELISSERO (a cura di), *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino, 2013, p. 156.

6.2.3. Il valore aggiunto della certificazione per la PA

L'adozione volontaria della certificazione ISO 37001 da parte di una amministrazione pubblica produce benefici che vanno oltre la mera conformità normativa:

Credibilità istituzionale rafforzata: la certificazione da parte di un organismo terzo indipendente accreditato conferisce maggiore affidabilità al sistema di prevenzione

Benchmarking internazionale: possibilità di confronto con altre amministrazioni certificate e adozione di best practice globali

Attrazione di investimenti: particolarmente rilevante per gli enti locali nella competizione per fondi europei e progetti PNRR

Cultura organizzativa: la certificazione innesca un processo di cambiamento culturale che supera l'approccio meramente formalistico

6.3. ISO 37001 e nuovo Codice dei Contratti Pubblici (D.Lgs. 36/2023): dalla compliance alla fiducia

Il D.Lgs. 31 marzo 2023, n. 36, recante il nuovo Codice dei contratti pubblici, ha segnato una discontinuità profonda rispetto alla tradizione normativa precedente. Il nuovo Codice, in attuazione della delega contenuta nella L. 78/2022, introduce una filosofia basata su principi anziché su regole puntuali, valorizzando la fiducia tra amministrazione e operatori economici come presupposto dell'efficienza contrattuale.

6.3.1. I principi del nuovo Codice e la loro coerenza con ISO 37001

L'art. 1 del D.Lgs. 36/2023 individua i principi generali che informano l'intera disciplina:

Risultato: l'attività delle stazioni appaltanti deve essere finalizzata al miglior risultato possibile

Fiducia: presunzione di buona fede e collaborazione tra amministrazione e operatori

Accesso al mercato: massima partecipazione degli operatori economici

Buona fede e tutela dell'affidamento: nelle relazioni tra stazione appaltante e operatori

Solidarietà e sussidiarietà: cooperazione tra amministrazioni

Tale approccio è pienamente coerente con la filosofia della ISO 37001:2025, che non si limita a imporre controlli formali ma mira a costruire una cultura organizzativa dell'integrità. Come evidenziato da Caringella, "il nuovo Codice segna il passaggio da una concezione difensiva della legalità – fondata sul timore della responsabilità – ad una concezione promozionale, basata sulla valorizzazione dei comportamenti virtuosi"[56].

6.3.2. La certificazione ISO come criterio reputazionale negli appalti

Una delle innovazioni più significative del nuovo Codice risiede nella possibilità di valorizzare elementi reputazionali e di affidabilità degli operatori economici, superando la logica del mero prezzo più basso.

La certificazione ISO 37001, in questo quadro, può essere utilizzata come:

Requisito premiale nell'attribuzione del punteggio: la stazione appaltante può prevedere un punteggio aggiuntivo per gli operatori certificati, nell'ambito degli elementi qualitativi dell'offerta.

Criterio di riduzione delle garanzie: analogamente a quanto previsto per le certificazioni di qualità, la certificazione anticorruzione potrebbe legittimare una riduzione della cauzione definitiva.

Elemento di affidabilità nella fase di selezione: particolarmente rilevante negli affidamenti diretti e nelle procedure negoziate, dove la scelta del contraente si basa anche sulla reputazione.

[56] F. CARINGELLA, *Manuale di diritto amministrativo*, XV ed., Milano, 2024, p. 1245. Cfr. anche F. CARINGELLA - M. GIUSTINIANI, *Il nuovo Codice dei contratti pubblici commentato*, Milano, 2023.

6.3.3. ISO 37001 nella filiera degli appalti: dalla stazione appaltante ai subappaltatori

Un aspetto di particolare rilevanza riguarda l'estensione dei presidi anticorruzione all'intera catena di fornitura. L'art. 119 del D.Lgs. 36/2023, in materia di subappalto, impone all'appaltatore di indicare nella propria offerta i lavori o le parti di opere che intende subappaltare, con obbligo di verifica dell'affidabilità dei subappaltatori.
La ISO 37001, al requisito 8.2 ("*Due diligence* verso i business associate"), impone all'organizzazione certificata di:

- Valutare il rischio di corruzione associato ad ogni partner commerciale
- Condurre verifiche proporzionate prima dell'instaurazione del rapporto
- Monitorare periodicamente il rapporto durante la sua esecuzione
- Includere clausole anticorruzione nei contratti

Come rileva Ponti, "la due diligence sui business associate rappresenta uno dei profili più innovativi della ISO 37001, in quanto trasforma la prevenzione della corruzione da obbligo interno a criterio di selezione dei partner esterni"[57].

6.3.4. Trasparenza contrattuale e registri pubblici

Il nuovo Codice, all'art. 33, rafforza gli obblighi di trasparenza attraverso la Banca Dati Nazionale dei Contratti Pubblici (BDNCP), gestita da ANAC, dove devono confluire tutte le informazioni relative alle procedure di affidamento, dall'indizione del bando fino al collaudo.
La ISO 37001:2025, al requisito 7.5 ("Informazioni documentate"), richiede che l'organizzazione mantenga documentazione su:

- Transazioni finanziarie significative
- Regali, ospitalità e spese promozionali

[57] F. PONTI, *La due diligence anticorruzione nella ISO 37001*, in Resp. amm. soc. enti, 2022, n. 3, p. 89. Cfr. anche C. SANTORIELLO, *La responsabilità da reato degli enti*, III ed., Torino, 2023, p. 345.

- Donazioni politiche e sponsorizzazioni
- Due diligence condotte

6.4. ISO 37001 e PNRR: trasparenza e *accountability* nei fondi europei

L'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR), con una dotazione di 191,5 miliardi di euro tra sovvenzioni e prestiti dell'Unione Europea, ha posto la prevenzione della corruzione al centro delle preoccupazioni delle istituzioni nazionali ed europee.

Il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio, che istituisce il dispositivo per la ripresa e la resilienza, prevede all'art. 22 l'obbligo per gli Stati membri di adottare "tutte le misure adeguate per tutelare gli interessi finanziari dell'Unione e garantire che l'utilizzo dei fondi [...] sia conforme al diritto applicabile dell'Unione e nazionale, in particolare riguardo a la prevenzione, l'individuazione e la rettifica delle frodi, dei casi di corruzione e dei conflitti di interessi".

6.4.1. ISO 37001 come strumento di due diligence sui beneficiari

La certificazione ISO 37001 risponde pienamente all'esigenza di *due diligence* anticorruzione sui soggetti privati che partecipano all'attuazione del PNRR, sia come beneficiari diretti di contributi che come fornitori di beni e servizi.

In particolare, per i progetti che prevedono partenariati pubblico-privato o il coinvolgimento di imprese private come soggetti attuatori, la certificazione ISO 37001 consente di:

Facilitare i controlli: gli audit ISO periodici forniscono all'amministrazione pubblica un flusso continuo di informazioni sull'efficacia dei controlli interni dell'impresa

Garantire la catena di responsabilità: attraverso la due diligence sui "business associate" richiesta dalla ISO, si estendono i controlli anticorruzione anche ai subcontraenti e ai partner

Prevenire le frodi: i meccanismi di whistleblowing e di tracciabilità delle transazioni previsti dallo standard consentono l'emersione tempestiva di irregolarità
Come evidenziato da Severino, "l'utilizzo di standard internazionali come la ISO 37001 consente di creare un linguaggio comune tra amministrazioni pubbliche, imprese e organismi di controllo europei, facilitando la vigilanza transnazionale sui fondi"[58].

6.4.2. Verso un "mercato unico dell'integrità": armonizzazione europea degli standard

La diffusione della ISO 37001 nel contesto del PNRR favorisce un processo di armonizzazione europea dei sistemi di prevenzione della corruzione. Mentre le normative nazionali presentano differenze significative (il D.Lgs. 231/2001 italiano, il UK Bribery Act 2010, la Loi Sapin II francese), lo standard ISO fornisce un denominatore comune che facilita:
Comparabilità dei sistemi: possibilità di valutare in modo uniforme l'adeguatezza dei controlli anticorruzione in diversi Stati membri
Riconoscimento reciproco: la certificazione rilasciata in uno Stato membro può essere riconosciuta anche negli altri
Circolazione delle imprese: riduzione degli ostacoli per le imprese che operano in più Paesi, evitando duplicazioni di adempimenti
Cooperazione tra autorità: utilizzo di un linguaggio tecnico comune tra le autorità anticorruzione nazionali
Come sottolinea Paliero, "l'etica della concorrenza è oggi il fondamento della sostenibilità economica: la competizione tra imprese non può più basarsi sulla capacità

[58] P. SEVERINO, *La nuova legge anticorruzione*, in Dir. pen. cont., 2013, fasc. 1, p. 12. Cfr. anche EAD., *Il sistema della prevenzione dei reati negli enti*, in AA.VV., *Trattato di diritto penale dell'impresa*, vol. I, Padova, 2021, p. 456.

di eludere i controlli, ma deve fondarsi sulla qualità dei prodotti e sull'affidabilità organizzativa"[59].

6.5. La digitalizzazione come fattore abilitante della trasparenza: verso la Pubblica Amministrazione 4.0

La ISO 37001:2025 dedica ampio spazio al tema della digitalizzazione dei processi anticorruzione, recependo l'evoluzione tecnologica degli ultimi anni e la necessità di adattare i controlli al contesto digitale.

La trasparenza nella pubblica amministrazione non può più limitarsi alla pubblicazione statica di documenti su siti istituzionali, secondo il modello del D.Lgs. 33/2013. La trasparenza deve diventare dinamica, interattiva e tracciabile, attraverso:

Piattaforme di e-procurement integrate: sistemi digitali che gestiscono l'intero ciclo dell'appalto, dalla programmazione alla fatturazione elettronica, garantendo:

- Tracciabilità di ogni passaggio e decisione
- Impossibilità di modificare retroattivamente i documenti
- Accesso differenziato in base ai ruoli
- Generazione automatica di reportistica per i controlli
- Riservatezza dell'identità del segnalante
- Crittografia end-to-end delle comunicazioni
- Gestione strutturata delle segnalazioni con *tracking*
- Protezione contro accessi non autorizzati

[59] C.E. PALIERO, *L'autunno del patriarca. Rinnovamento o trasmutazione del diritto penale dei codici?*, in Riv. it. dir. proc. pen., 1994, p. 1220. Sul rapporto tra etica e concorrenza v. anche G. FLORA, *Etica degli affari e diritto penale dell'economia*, Milano, 2018.

Come evidenziato da Carloni, "la trasparenza digitale non si limita a rendere accessibili i dati, ma li rende elaborabili, comparabili e leggibili da algoritmi, trasformando l'accountability da controllo ex post a prevenzione in tempo reale"[60].

6.5.1. Blockchain e registri distribuiti per l'immutabilità dei dati

La tecnologia blockchain, basata su registri distribuiti (DLT - Distributed Ledger Technology), offre un ulteriore livello di garanzia contro la manipolazione dei dati. Le principali applicazioni nella PA includono:

Registro pubblico dei contratti: ogni contratto pubblico viene registrato su blockchain con:

- Hash crittografico del documento
- Timestamp certificato
- Identità delle parti (in forma pseudonima o anonima)
- Modifiche successive tracciate con nuove transazioni

Certificazioni e abilitazioni: titoli accademici, abilitazioni professionali, certificazioni di qualità possono essere registrati su blockchain, eliminando il rischio di falsificazioni e semplificando le verifiche.

Secondo Cavinato, "la blockchain trasforma la fiducia da presupposto morale a infrastruttura tecnologica: non è più necessario fidarsi delle persone, perché il sistema stesso è strutturato per essere affidabile (trustless)"[61].

[60] E. CARLONI, *La "casa di vetro" e le riforme: trasparenza amministrativa e apertura dei dati pubblici*, in Riv. trim. dir. pubbl., 2014, p. 701. Cfr. anche ID., *L'amministrazione aperta. Regole, strumenti, limiti dell'open government*, Rimini, 2014.

[61] M. CAVINATO, *Blockchain e pubblica amministrazione: opportunità e criticità*, in Giorn. dir. amm., 2020, n. 5, p. 634. Sul tema v. anche P. DE FILIPPI - A. WRIGHT, *Blockchain and the Law*, Cambridge (Mass.), 2018.

6.5.2. Il Piano Triennale per l'Informatica nella PA e l'integrazione con ISO 37001

Il Piano Triennale per l'Informatica nella Pubblica Amministrazione, redatto da AgID (Agenzia per l'Italia Digitale) ai sensi dell'art. 14-bis del CAD, definisce gli indirizzi strategici per la digitalizzazione del settore pubblico.

Il Piano 2024-2026 individua tra le priorità:

Interoperabilità delle banche dati: attraverso la Piattaforma Digitale Nazionale Dati (PDND), le diverse amministrazioni possono scambiare dati in modo sicuro e tracciato

Identità digitale unica: SPID e CIE per l'accesso ai servizi e la firma digitale

Cloud first: migrazione dei sistemi verso infrastrutture cloud certificate

Cybersecurity by design: integrazione della sicurezza in ogni fase di progettazione dei servizi digitali

L'integrazione tra digitalizzazione (Piano Triennale AgID) e prevenzione della corruzione (ISO 37001) produce benefici sinergici:

Obiettivo digitalizzazione	Impatto anticorruzione
Dematerializzazione documenti	Tracciabilità completa del flusso documentale
Firma digitale	Certezza dell'autore e timestamp delle decisioni
Interoperabilità banche dati	Verifiche automatiche su requisiti e incompatibilità
Analytics e big data	Individuazione di anomalie e pattern sospetti
Processi automatizzati	Riduzione della discrezionalità umana

Come sottolineato da Contessa, "l'integrità amministrativa non è più solo una dimensione etica o giuridica, ma anche una questione di architettura informatica: sistemi ben progettati riducono strutturalmente gli spazi di corruzione"[62].

[62] A. CONTESSA, *Integrità e architettura digitale nella PA*, in Dir. informaz., 2023, p. 245.

6.6. Le sfide applicative: ostacoli culturali, organizzativi e normativi

Nonostante le potenzialità teoriche dell'integrazione tra ISO 37001 e sistema pubblico italiano, l'implementazione concreta incontra significative resistenze e criticità strutturali.

6.6.1. Resistenze culturali e concezione burocratica del controllo

La cultura organizzativa della pubblica amministrazione italiana rimane largamente ancorata ad una concezione formalistica della legalità, in cui il rispetto delle procedure prevale sulla sostanza dei risultati. La ISO 37001, viceversa, richiede un approccio sostanzialistico orientato all'efficacia dei controlli.

Tale *gap* culturale si manifesta in diversi aspetti:

Approccio adempimentale: la compliance viene percepita come obbligo esterno da soddisfare formalmente, piuttosto che come opportunità di miglioramento organizzativo

Avversione al rischio: la paura della responsabilità (penale, contabile, disciplinare) induce i funzionari a privilegiare l'immobilismo rispetto all'innovazione

Frammentazione delle competenze: mancanza di dialogo tra uffici giuridici, uffici di controllo interno e uffici operativi

Carenza di *leadership* etica: i vertici politici e amministrativi faticano a incarnare e promuovere una cultura dell'integrità

Come evidenziato da Cassese, "la burocrazia italiana è storicamente caratterizzata da un'ipertrofia normativa e da un deficit gestionale: si moltiplicano le regole ma si investe poco nell'organizzazione e nelle competenze"[63].

[63] S. CASSESE, *Il diritto amministrativo e i suoi principi*, in ID. (a cura di), *Istituzioni di diritto amministrativo*, V ed., Milano, 2021, p. 15.

6.6.2. Carenza di competenze manageriali e risorse

L'implementazione di un sistema di gestione anticorruzione secondo ISO 37001 richiede competenze specifiche che spesso mancano nelle pubbliche amministrazioni:

Competenze tecniche:

- *Risk management* e metodologie di valutazione quantitativa dei rischi
- Audit interno e tecniche di campionamento
- Analisi dei dati e utilizzo di strumenti di business intelligence
- Conoscenza degli standard internazionali di gestione (ISO 9001, ISO 31000, ISO 37001)
- Competenze giuridiche specialistiche:
- Diritto amministrativo e disciplina degli appalti pubblici
- Normativa anticorruzione nazionale e internazionale
- Regolamentazione sulla protezione dei dati (GDPR) applicata al whistleblowing
- Responsabilità amministrativa degli enti (D.Lgs. 231/2001) per le società partecipate

Competenze manageriali:

- *Change management* e gestione della resistenza al cambiamento
- Leadership etica e promozione della cultura organizzativa
- Comunicazione interna ed esterna
- Negoziazione e gestione dei conflitti

Sul piano delle risorse finanziarie, l'adozione di un sistema certificato ISO 37001 comporta costi non trascurabili e non sostenibili per le casse degli enti pubblici.
Tali investimenti, pur ammortizzabili nel medio-lungo periodo attraverso la riduzione delle inefficienze e dei contenziosi, rappresentano un ostacolo significativo per amministrazioni già in difficoltà finanziaria.

6.6.3. Frammentazione istituzionale e coordinamento multilivello

Il sistema amministrativo italiano si caratterizza per una marcata frammentazione istituzionale: oltre 7.900 comuni, 107 province/città metropolitane, 20 regioni, migliaia di enti pubblici non economici, aziende sanitarie, università, autorità indipendenti, ciascuno con propria autonomia organizzativa.

Tale frammentazione genera criticità specifiche:

Asimmetria informativa: mancanza di standard comuni di rilevazione e comunicazione dei dati sui rischi corruttivi, che impedisce analisi comparative e condivisione di best practice

Coordinamento debole: pur esistendo l'ANAC come autorità nazionale, mancano meccanismi efficaci di coordinamento operativo tra i diversi livelli di governo

Duplicazioni e sovrapposizioni: proliferazione di documenti di pianificazione (PTPCT, Piani Performance, Piani Organizzativi del Lavoro Agile, ecc.) spesso non integrati tra loro

Come osservato da Merloni, "il federalismo amministrativo italiano, in assenza di adeguati strumenti di coordinamento, rischia di produrre una babele di modelli organizzativi, con conseguente incertezza per cittadini e imprese"[64].

6.6.4. Mancanza di incentivi normativi e reputazionali

A differenza del settore privato, dove la certificazione ISO 37001 può tradursi in vantaggi competitivi concreti (accesso a mercati, riduzione premi assicurativi, preferenza da parte di investitori ESG), per le pubbliche amministrazioni mancano incentivi chiari all'adozione volontaria dello standard.

Il quadro normativo italiano non prevede:

[64] F. MERLONI, *La prevenzione della corruzione: tendenze italiane e internazionali a confronto*, in Astrid Rassegna, n. 13/2020, p. 8, disponibile su www.astridonline.it.

Premialità nell'allocazione di risorse: non esistono meccanismi che destinino maggiori fondi alle amministrazioni certificate.

Semplificazioni procedurali: la certificazione non comporta esoneri o alleggerimenti di obblighi.

***Ranking* pubblici**: ANAC non pubblica classifiche comparative sull'efficacia dei sistemi anticorruzione

Osservatori regionali sulla corruzione con funzioni di *benchmarking*.

Come sottolineato da Clarich, "solo un sistema di incentivi ben calibrato, che combini obblighi minimi universali con premialità per chi va oltre, può produrre un effettivo cambiamento culturale nella pubblica amministrazione"[65].

6.7. Verso un modello integrato di governance pubblica: la convergenza degli standard ISO

La prevenzione della corruzione non può essere considerata isolatamente, ma deve inserirsi in un più ampio sistema di *governance* integrata che consideri tutte le dimensioni della qualità amministrativa.

6.7.1. L'ecosistema degli standard ISO per la PA

Negli ultimi anni, *l'International Organization for Standardization* ha sviluppato una famiglia di standard specificatamente dedicati alla governance e alla compliance organizzativa:

ISO 37000:2021 - Governance delle organizzazioni: fornisce principi e linee guida per la governance efficace, applicabili a qualsiasi tipo di organizzazione. Definisce i principi di:

- Finalità (*alignment* con gli interessi degli stakeholder)

[65] M. CLARICH, *Manuale di diritto amministrativo*, VI ed., Bologna, 2023, p. 567. Sul tema degli incentivi v. anche G. NAPOLITANO, *La logica del diritto amministrativo*, Bologna, 2020.

- Strategia (visione di lungo periodo)
- Supervisione (separazione tra governance e management)
- Accountability (responsabilità chiare e verificabili)

ISO 37001:2016/2025 - Sistemi di gestione anticorruzione: standard specifico per la prevenzione della corruzione, bribery e conflitti di interesse.

ISO 37002:2021 - Sistemi di gestione per il *whistleblowing*: fornisce linee guida per stabilire, implementare, mantenere e migliorare un sistema di gestione delle segnalazioni.

ISO 31000:2018 - Gestione del rischio: *framework* generale per l'identificazione, valutazione e trattamento dei rischi di qualsiasi natura.

6.7.2. L'integrazione sinergica tra gli *standard*

Gli standard non sono compartimenti stagni, ma sistemi interconnessi che condividono:

Struttura comune (*High Level Structure - HLS*): tutti gli standard ISO di gestione seguono la stessa struttura in 10 clausole, facilitando l'integrazione:

Scopo e campo di applicazione

Riferimenti normativi

Termini e definizioni

Contesto dell'organizzazione

Leadership

Pianificazione

Supporto

Attività operative

Valutazione delle prestazioni

Miglioramento

Approccio basato sul rischio: tutti gli standard adottano il risk-based thinking come principio metodologico centrale

Ciclo PDCA: la logica del miglioramento continuo accomuna tutti i sistemi di gestione

Focus* sugli *stakeholder: attenzione alle esigenze e aspettative di tutte le parti interessate

L'integrazione tra ISO 37001 (anticorruzione), ISO 37301 (compliance generale) e ISO 37000 (governance) consente di creare un sistema unico di gestione integrata in cui:

La governance definisce principi e obiettivi strategici

La *compliance* assicura il rispetto di tutti gli obblighi normativi

L'anticorruzione presidia specificamente i rischi di corruzione

Il *whistleblowing* crea canali di emersione delle criticità

Il *risk management* fornisce la metodologia trasversale

Come evidenziato da Razzante, "l'integrazione degli standard ISO trasforma la compliance da costo burocratico a fattore strategico di creazione di valore, riducendo duplicazioni e massimizzando sinergie"[66].

Per Talamo, "l'amministrazione trasparente del futuro non è quella che pubblica più documenti, ma quella che rende comprensibili le proprie scelte e si sottopone a valutazione continua"[67].

6.7.3. Il ruolo della compliance nella sostenibilità istituzionale

La *compliance* anticorruzione si inserisce nel più ampio paradigma della sostenibilità, non solo ambientale ma anche istituzionale e sociale. L'Agenda 2030 dell'ONU, al Goal 16 ("Pace, giustizia e istituzioni solide"), individua tra i *target* specifici:

Target 16.5: "Ridurre sostanzialmente la corruzione e le pratiche di concussione in tutte le loro forme"

Target 16.6: "Sviluppare istituzioni efficaci, responsabili e trasparenti a tutti i livelli"

[66] R. RAZZANTE, *Compliance aziendale e responsabilità degli enti*, Milano, 2021, p. 234. Cfr. anche A. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010

[67] M. TALAMO, *Trasparenza dinamica e accountability nella PA digitale*, in Federalismi.it, 2023, n. 12, p. 45.

Target 16.10: "Garantire l'accesso pubblico alle informazioni e proteggere le libertà fondamentali"

Alcune amministrazioni virtuose hanno già integrato la compliance anticorruzione nei propri Bilanci di Sostenibilità, rendicontando:

Numero di ore di formazione anticorruzione erogata

Percentuale di processi ad alto rischio sottoposti ad *audit*

Numero di segnalazioni di *whistleblowing* ricevute e gestite

Tempo medio di risposta alle istanze di accesso civico

Indici di percezione della corruzione tra dipendenti e utenti

Come evidenziato da Cerrina Feroni, "la sostenibilità istituzionale è il presupposto di ogni altra forma di sostenibilità: senza istituzioni integre ed efficienti, nessuna politica ambientale o sociale può produrre risultati duraturi"[68].

6.8. Sintesi e prospettive future

La ISO 37001:2025 rappresenta per la pubblica amministrazione italiana un'opportunità strategica di integrazione e rafforzamento del sistema prevenzionale introdotto con la L. 190/2012.

L'integrazione tra normativa nazionale (L. 190/2012, D.Lgs. 33/2013, D.Lgs. 36/2023) e standard internazionale (ISO 37001) produce benefici sinergici:

Sul piano metodologico:

- Adozione del ciclo PDCA per trasformare il PTPCT da documento statico a processo dinamico
- Utilizzo di tecniche consolidate di risk assessment e audit interno
- Approccio basato su evidenze e misurazione delle performance

[68] G. CERRINA FERONI, *Sostenibilità e governance pubblica*, in Riv. AIC, 2022, n. 4, p. 123. Sul rapporto tra compliance e sostenibilità v. anche M. GRAZIADEI - U. MATTEI - L. BACCELLI (a cura di), *Environmental Governance*, Cambridge, 2015.

Sul piano organizzativo:

- Rafforzamento del ruolo del RPCT attraverso l'allineamento con gli standard internazionali
- Integrazione tra compliance anticorruzione e altri sistemi di gestione (qualità, ambiente, sicurezza)
- Creazione di competenze specialistiche e professionalizzazione della funzione compliance

Sul piano della credibilità:

- Certificazione da parte di organismi terzi indipendenti accreditati
- Comparabilità internazionale e benchmarking con altre amministrazioni
- Maggiore affidabilità verso cittadini, imprese e investitori

Sul piano dell'efficienza:

- Riduzione delle inefficienze e degli sprechi derivanti da processi corrotti
- Prevenzione dei contenziosi e delle sanzioni
- Attrazione di investimenti e accesso agevolato a fondi europei

6.8.1. Le sfide ancora aperte

Permangono ma criticità strutturali che richiedono interventi normativi e organizzativi:
Necessità di incentivi normativi: introdurre premialità concrete per le amministrazioni certificate
Coordinamento multilivello: rafforzare il ruolo di ANAC come hub della compliance pubblica
Investimenti in formazione: sviluppare competenze specialistiche nel personale pubblico
Digitalizzazione dei processi: accelerare la transizione verso piattaforme integrate di gestione
Cambiamento culturale: superare l'approccio formalistico verso una cultura dell'accountability

6.8.2. Verso una *governance* pubblica integrata

La prospettiva futura è quella di una governance pubblica 5.0, caratterizzata da:

Integrazione degli standard ISO: convergenza tra ISO 37001 (anticorruzione), ISO 37301 (compliance), ISO 37000 (governance), ISO 37002 (whistleblowing).

Digitalizzazione intelligente: utilizzo di IA, blockchain e analytics per la prevenzione predittiva.

Trasparenza computazionale: dati aperti, elaborabili e verificabili in tempo reale.

***Accountability* dinamica**: rendicontazione continua verso stakeholder e cittadini

Sostenibilità istituzionale: integrazione della compliance anticorruzione nei sistemi ESG.

Come conclude Marzuoli, "l'amministrazione del futuro non sarà né solo giuridica né solo manageriale, ma saprà integrare le garanzie del diritto pubblico con l'efficienza degli strumenti di gestione, realizzando quella sintesi tra *rule of law* e *good governance* che sola può assicurare la legittimità democratica delle istituzioni"[69].

[69] C. MARZUOLI, *Principio di legalità e attività di diritto privato della pubblica amministrazione*, Milano, 1982, p. 345. Sulla sintesi tra rule of law e governance v. anche G. DELLA CANANEA, *Due process of law beyond the State*, Oxford, 2016.

Capitolo 7 – Verso la Compliance 5.0: Intelligenza Artificiale, Blockchain e Tracciabilità Etica

7.1. La digitalizzazione come nuova frontiera della compliance: dall'analogico all'algoritmico

La quarta rivoluzione industriale, caratterizzata dall'integrazione tra tecnologie digitali, fisiche e biologiche, ha ridefinito radicalmente non solo i processi produttivi ma anche le modalità di governance organizzativa. La compliance anticorruzione non può sottrarsi a tale trasformazione.

7.1.1. Dall'evoluzione industriale all'evoluzione della compliance

Per comprendere la portata del cambiamento, è utile ripercorrere l'evoluzione parallela tra rivoluzioni industriali e modelli di compliance:

Compliance 1.0 - Era pre-industriale: prevalenza del controllo personale e reputazionale. La fiducia si basa sulla conoscenza diretta delle persone. Modello: "conosco il mio fornitore".

Compliance 2.0 - Era industriale: nascita delle norme scritte e dei controlli formali. Introduzione di procedure standardizzate e verifiche gerarchiche. Modello: "seguo le procedure".

Come osserva Savona, "l'intelligenza artificiale, se correttamente addestrata e supervisionata, diventa strumento di prevenzione anticipatoria, capace di intercettare deviazioni comportamentali prima che si traducano in illecito consumato"[70].

[70] E. U. SAVONA, *Criminalità economica e intelligenza artificiale*, Milano, 2021, p. 178. Cfr. anche E.U. SAVONA - M. RICCARDI (eds.), *From Illegal Markets to Legitimate Businesses: The Portfolio of Organised Crime in Europe*, Trento, 2017.

7.1.2. La ISO 37001:2025 e la dimensione digitale

La revisione 2025 della ISO 37001 (rispetto alla prima edizione del 2016) ha introdotto significativi aggiornamenti per recepire l'evoluzione tecnologica:

Clausola 7.5.3 - Controllo delle informazioni documentate: prevede esplicitamente l'uso di "sistemi informatici appropriati per garantire l'integrità, la disponibilità e la riservatezza delle informazioni".

Clausola 8.2 - Due diligence: raccomanda l'utilizzo di "strumenti digitali e banche dati specializzate" per la verifica dei business associate, inclusi sistemi di screening automatizzato.

Clausola 9 - Valutazione delle prestazioni: introduce l'uso di "indicatori di performance (KPI) monitorabili attraverso dashboard digitali in tempo reale".

7.1.3. Il nuovo perimetro della corruzione nell'era digitale

La digitalizzazione ha ampliato anche il perimetro della corruzione, introducendo nuove tipologie di rischio:

Corruzione informatica: manipolazione di sistemi informatici per alterare procedure di gara, bilanci, registrazioni contabili. Utilizzo di accessi abusivi per favorire determinati operatori.

Corruzione nei sistemi automatizzati: alterazione degli algoritmi di assegnazione automatica (es. in sistemi di smart procurement) per favorire determinati fornitori.

Corruzione tramite criptovalute: utilizzo di pagamenti in criptovalute per rendere meno tracciabili le transazioni corruttive, sfruttando la pseudonimia della blockchain pubblica.

Data corruption: manipolazione o occultamento di dati critici per decisioni amministrative o aziendali (es. alterazione di dati ambientali, sanitari, statistici).

Conflitti di interesse algoritmici: situazioni in cui chi progetta o addestra un algoritmo ha interessi personali nell'orientarne le decisioni in una determinata direzione.

Come evidenziato da Aterno, "la corruzione digitale è spesso più insidiosa di quella tradizionale perché meno visibile, richiede competenze tecniche per essere individuata e può produrre effetti su scala molto più ampia"[71].

7.1.4. Dalla compliance reattiva alla compliance predittiva

Il cambio di paradigma fondamentale della Compliance 5.0 sta nel passaggio da una logica reattiva (rilevare violazioni già avvenute) ad una logica predittiva (anticipare le violazioni prima che si verifichino):

Aspetto	Compliance tradizionale (reattiva)	Compliance 5.0 (predittiva)
Temporalità	Ex post (dopo l'evento)	Ex ante (prima dell'evento)
Metodologia	Controlli a campione	Monitoraggio continuo automatizzato
Fonte dati	Documenti e dichiarazioni	Big data e sensori IoT
Analisi	Manuale o semi-automatizzata	Algoritmi di machine learning
Output	Report periodici	Alert in tempo reale
Azione	Sanzione e correzione	Prevenzione e blocco automatico
Focus	Conformità normativa	Efficacia sostanziale

La compliance predittiva si basa sull'analisi di pattern comportamentali e anomalie statistiche per identificare situazioni ad alto rischio prima che si concretizzino in violazioni. Ad esempio:

Clustering di transazioni sospette: identificazione automatica di schemi di pagamento anomali (frequenza, importo, beneficiario)

[71] G. ATERNO, *Corruzione digitale e nuove forme di illecito nell'era algoritmica*, in Cass. pen., 2023, p. 2145. Sul tema v. anche S. ZICCARDI, *Tecnologie per il potere*, Milano, 2019.

Analisi delle relazioni: mappatura delle reti di relazioni tra dipendenti, fornitori e decisori per identificare conflitti di interesse nascosti

Behavioral analytics: monitoraggio delle deviazioni dal comportamento normale (es. accessi a documenti sensibili in orari inusuali, modifiche ripetute a determinati dati)

Sentiment analysis: analisi del linguaggio in comunicazioni interne per identificare segnali di pressione, stress o comportamenti non etici

Come sottolinea Pascuzzi, "la tecnologia consente di passare da un controllo per eccezione ad un controllo per inclusione: non più verificare alcuni casi sospetti, ma analizzare tutti i casi per identificare quelli sospetti"[72].

7.2. L'intelligenza artificiale nella *predictive compliance*: opportunità e sfide

L'applicazione dell'intelligenza artificiale alla *compliance* anticorruzione si articola su molteplici livelli, ciascuno con specifiche potenzialità e criticità.

7.2.1. Tipologie di IA applicabili alla compliance

***Machine Learning* supervisionato**: algoritmi addestrati su dataset etichettati per riconoscere pattern di comportamenti corruttivi. Applicazioni:

- Classificazione di transazioni come "legittime" o "sospette" sulla base di caratteristiche predefinite
- Identificazione di documenti anomali (es. fatture false, contratti irregolari)
- Scoring di rischio di fornitori e partner sulla base di variabili multiple

***Machine Learning* non supervisionato**: algoritmi che identificano autonomamente pattern e anomalie senza etichettatura preventiva. Applicazioni:

- Clustering di comportamenti per identificare gruppi omogenei e outlier

[72] G. PASCUZZI, *Giuristi si diventa. Come riconoscere e apprendere le abilità proprie delle professioni legali*, Bologna, 2008, p. 234. Sul rapporto tra diritto e algoritmi v. anche ID., *Il diritto nell'era digitale*, Bologna, 2020.

- Analisi delle componenti principali per ridurre la complessità dei dati
- Rilevamento di anomalie in serie temporali (es. variazioni improvvise nei flussi di approvazione)
- *Deep Learning* e reti neurali: modelli complessi capaci di apprendere rappresentazioni gerarchiche dei dati. Applicazioni:
- Analisi di testi non strutturati (email, contratti, verbali) per identificare clausole sospette
- Riconoscimento di immagini per verificare l'autenticità di documenti
- Analisi predittiva multifattoriale combinando dati eterogenei

Natural Language Processing **(NLP)**: elaborazione del linguaggio naturale per analizzare comunicazioni scritte e verbali. Applicazioni:

- Analisi semantica di contratti per identificare clausole favorevoli in modo anomalo
- Monitoraggio di comunicazioni interne per rilevare linguaggio indicativo di pressioni o comportamenti non etici
- Estrazione automatica di informazioni da documenti non strutturati
- Analisi di *sentiment* per valutare il "clima etico" organizzativo

Reinforcement Learning: algoritmi che apprendono strategie ottimali attraverso tentativi ed errori. Applicazioni:

- Ottimizzazione dinamica dei controlli in base all'evoluzione del profilo di rischio
- Simulazione di scenari di corruzione per testare l'efficacia dei presidi

7.2.2. Casi d'uso concreti dell'IA nella compliance anticorruzione
Analisi automatizzata dei flussi di pagamento

Sistemi di IA possono analizzare in tempo reale tutti i pagamenti effettuati dall'organizzazione, identificando:

- Pagamenti frazionati per eludere soglie di autorizzazione (*smurfing*)

- Pagamenti verso conti in giurisdizioni ad alto rischio
- Pagamenti a fornitori privi di adeguata documentazione contrattuale
- *Pattern* di *round-tripping* (fondi che tornano indirettamente all'organizzazione)
- Pagamenti duplicati o verso beneficiari fittizi

Rilevazione di conflitti di interesse attraverso *network analysis*

Algoritmi di analisi delle reti sociali (*Social Network Analysis* - SNA) possono mappare le relazioni tra:

- Dipendenti e fornitori (es. legami familiari, societari, finanziari)
- Decisori pubblici e beneficiari di decisioni
- Membri di commissioni di gara e partecipanti
- Funzionari e soggetti controllati
- Monitoraggio comportamentale e *anomaly detection*

Sistemi di *User and Entity Behavior Analytics* (UEBA) monitorano il comportamento digitale degli utenti per identificare deviazioni rispetto al pattern normale:

- Accessi a documenti sensibili da parte di utenti non autorizzati
- Download massivi di dati prima di dimissioni o trasferimenti
- Modifiche ripetute a determinate categorie di documenti
- Accessi in orari insoliti o da location anomale
- Utilizzo anomalo di credenziali amministrative
- *Natural Language Processing* per l'analisi contrattuale
- Sistemi di NLP possono analizzare automaticamente migliaia di contratti per identificare:
- Clausole anomale rispetto agli *standard* dell'organizzazione
- Condizioni particolarmente favorevoli verso una parte
- Modifiche sostanziali introdotte all'ultimo momento
- Incoerenze tra documenti di gara e contratto finale
- Linguaggio vago o ambiguo che crea spazi di discrezionalità

7.2.3. I vantaggi dell'IA nella *compliance*

L'integrazione dell'intelligenza artificiale nei sistemi di gestione anticorruzione produce vantaggi significativi:

Continuità: monitoraggio 24/7 senza interruzioni, fatigue o cali di attenzione.

Oggettività: riduzione dei *bias* cognitivi umani (*confirmation bias, availability heuristic, groupthink*) che possono compromettere l'efficacia dei controlli.

Velocità: identificazione in tempo reale di anomalie, consentendo interventi tempestivi prima che si consolidino danni.

Apprendimento continuo: capacità di migliorare le *performance* nel tempo attraverso il feedback sui casi rilevati.

Copertura estesa: possibilità di monitorare simultaneamente molteplici dimensioni di rischio (transazioni, comportamenti, relazioni, comunicazioni).

Come evidenzia Ziccardi, "l'IA trasforma la compliance da attività *labour-intensive* a *capital-intensive:* l'investimento iniziale è significativo, ma i costi marginali di controllo aggiuntivo tendono a zero"[73].

7.2.4. I rischi e le criticità dell'IA: il paradosso dell'opacità algoritmica

L'utilizzo dell'intelligenza artificiale introduce nuove e complesse problematiche che devono essere attentamente governate:

Questa opacità pone problemi su tre livelli:

Giuridico: difficoltà di contestare decisioni automatizzate in sede giudiziaria o di ricorso amministrativo

Organizzativo: rischio che le decisioni algoritmiche vengano accettate acriticamente senza verifica umana

Etico: impossibilità di valutare se l'algoritmo applica criteri eticamente accettabili

[73] G. ZICCARDI, *Intelligenza artificiale e diritto*, Milano, 2021, p. 156. Cfr. anche ID., *Privacy e sicurezza informatica nella società dell'informazione*, Milano, 2019.

ma, come osserva Pizzetti, "il diritto alla spiegazione rischia di rimanere una garanzia formale se l'algoritmo stesso è per natura inesplicabile, creando una tensione irrisolta tra efficacia predittiva e intelligibilità"[74].

Bias algoritmici e discriminazione: gli algoritmi apprendono dai dati storici, e se questi dati incorporano *bias* (pregiudizi) umani, l'algoritmo li replicherà e amplificherà.

Come sottolinea O'Neil nel fondamentale saggio "Weapons of Math Destruction", "gli algoritmi possono trasformare opinioni discutibili in verità matematiche, rendendo invisibile e incontestabile la discriminazione"[75].

Dipendenza tecnologica e *deskilling*: l'eccessivo affidamento sui sistemi automatizzati può portare a:

- Perdita di competenze umane nel riconoscimento diretto di anomalie
- Incapacità di operare efficacemente in caso di malfunzionamento del sistema
- Accettazione acritica degli *output* algoritmici (*automation bias*)

7.2.5. Etica dell'algoritmo: principi per un'IA responsabile nella *compliance*

Per governare i rischi dell'IA mantenendone i benefici, è necessario adottare un framework di IA etica basato su principi condivisi:

1. Trasparenza algoritmica (*Algorithmic Transparency*):

- Documentazione completa dell'architettura dell'algoritmo
- Disclosure delle variabili utilizzate per le decisioni
- Spiegazione comprensibile (*explainable* AI) degli output principali
- Registro delle versioni e delle modifiche apportate nel tempo

[74] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 201. Sul diritto alla spiegazione v. anche G. RESTA - V. ZENO-ZENCOVICH (a cura di), *La "profilazione" online tra persona e patrimonio*, Roma, 2018.

[75] C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, 2016, trad. it. *Armi di distruzione matematica*, Milano, 2017, p. 87.

- La ISO 37001:2025, al requisito 7.5, richiede che l'organizzazione mantenga "informazioni documentate" sui sistemi utilizzati per i controlli anticorruzione, inclusi gli algoritmi.

2. Equità e non discriminazione (*Fairness*):

- Test periodici per identificare *bias* discriminatori
- Bilanciamento dei *dataset* di addestramento
- Monitoraggio degli impatti differenziali su diverse categorie
- Procedure di *appeal* per decisioni algoritmiche contestate

3. *Accountability* umana (*Human-in-the-loop*):

- Supervisione umana obbligatoria per decisioni ad alto impatto
- Possibilità di *override* delle decisioni algoritmiche
- Responsabilità chiara per le decisioni finali
- Formazione adeguata dei supervisori umani

Come sottolineano Bovens e Dignum, "l'algoritmo è una nuova forma di potere: invisibile ma pervasiva, e come tale deve essere regolata attraverso meccanismi di accountability democratica"[76].

4. Privacy by design:

- Minimizzazione dei dati personali trattati
- Pseudonimizzazione e anonimizzazione quando possibile
- Crittografia dei dati sensibili
- Conservazione limitata nel tempo

5. Sicurezza e robustezza:

- Protezione contro manipolazioni e attacchi informatici
- Test di stress e scenari avversi

[76] M. BOVENS, *The Quest for Responsibility*, Cambridge, 1998, p. 45. Più recentemente v. M. BOVENS - T. SCHILLEMANS - P. 'T HART, *The Oxford Handbook of Public Accountability*, Oxford, 2014. Per l'adattamento al contesto algoritmico v. V. DIGNUM, *Responsible Artificial Intelligence*, Cham, 2019

- Procedure di *backup* e *recovery*
- Audit di sicurezza periodici

6. Verificabilità e auditabilità:

- *Log* completi delle decisioni algoritmiche
- Possibilità di *audit* indipendenti sull'algoritmo
- Certificazione da parte di organismi terzi
- *Reporting* pubblico sulle performance

La Commissione Europea, nelle "*Ethics Guidelines for Trustworthy AI*" (2019), ha identificato sette requisiti per un'IA affidabile: (1*) human agency and oversight*, (2) *technical robustness and safety*, (3) *privacy and data governance*, (4) *transparency*, (5) diversity, non-discrimination and fairness, (6) *environmental and societal well-being,* (7) accountability[77].

7.2.6. La responsabilità per le decisioni algoritmiche: estensione della colpa d'organizzazione

L'utilizzo di algoritmi nei processi decisionali pone il problema fondamentale: chi risponde di una decisione presa o suggerita da un algoritmo?

La dottrina più recente propone di estendere la nozione di colpa d'organizzazione ai sistemi digitali, configurando un dovere di manutenzione etica dell'algoritmo. Come sostengono Manes e Tripodi, "l'algoritmo è parte dell'organizzazione, e dunque l'ente risponde della sua trasparenza, affidabilità e correttezza, così come risponde dell'adeguatezza delle procedure manuali"[78].

Questa prospettiva implica che l'organizzazione debba:

[77] European Commission, High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Brussels, 2019, disponibile su https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[78] V. MANES - A. TRIPODI, *La responsabilità da reato degli enti nell'era digitale*, in Dir. pen. cont., 2023, n. 4, p. 78. Cfr. anche A. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, spec. p. 567 ss.

In fase di progettazione:

- Definire chiaramente gli obiettivi e i vincoli etici dell'algoritmo
- Selezionare dataset rappresentativi e privi di bias manifesti
- Coinvolgere competenze multidisciplinari (tecnici, giuristi, esperti di compliance)
- Documentare tutte le scelte progettuali

In fase di implementazione:

- Testare l'algoritmo su casistiche diverse prima del deployment
- Formare adeguatamente il personale che lo utilizzerà
- Stabilire procedure di escalation per casi dubbi
- Integrare l'algoritmo nei flussi decisionali senza deleghe acritiche

In fase di esercizio:

- Monitorare continuamente le performance e gli impatti
- Raccogliere feedback dagli utenti e dai soggetti interessati
- Verificare periodicamente la persistenza dell'allineamento agli obiettivi
- Aggiornare l'algoritmo quando necessario

In fase di controllo:

- Sottoporre l'algoritmo ad audit interni periodici
- Consentire verifiche da parte di organismi indipendenti
- Mantenere log completi per accountability
- Reportare su efficacia e criticità

Come osserva Paliero, "la responsabilità algoritmica non cancella quella umana, ma la ridefinisce: dall'essere responsabili per aver deciso in un certo modo, si diventa responsabili per aver scelto di delegare certe decisioni ad un algoritmo inadeguato"[79].

[79] C.E. PALIERO, *Intorno alla "colpa d'organizzazione": prolegomeni ai profili sanzionatori*, in Studi in onore di Mario Romano, Napoli, 2011, vol. III, p. 2135. Sul tema della responsabilità algoritmica v. anche F. BASILE - A. ROSSI, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Dir. pen. cont., 2019, n. 12.

7.3. Blockchain e tracciabilità etica dei processi: dall'immutabilità alla fiducia distribuita

La tecnologia *blockchain* rappresenta il secondo pilastro della *Compliance* 5.0, offrendo soluzioni innovative per la tracciabilità, l'immutabilità e la decentralizzazione della fiducia.

7.3.1. Fondamenti tecnici della blockchain

La *blockchain* è un registro distribuito (*Distributed Ledger Technology* - DLT) caratterizzato da:

Immutabilità crittografica: ogni blocco di transazioni è legato al precedente attraverso *hash* crittografici, rendendo computazionalmente impraticabile modificare retroattivamente i dati senza che ciò sia evidente.

Trasparenza selettiva: le transazioni sono visibili a tutti i partecipanti (blockchain pubbliche) o a partecipanti autorizzati (blockchain permissioned), garantendo trasparenza mantenendo eventualmente la privacy attraverso crittografia.

Smart contracts: programmi auto-eseguibili che implementano automaticamente clausole contrattuali al verificarsi di determinate condizioni, eliminando intermediari e riducendo opportunità di manipolazione.

7.3.2. Applicazioni della blockchain nella compliance anticorruzione

Una *blockchain permissioned* può registrare:

- Tutte le decisioni di approvazione di transazioni rilevanti
- Gli audit interni effettuati, con esito e responsabili
- Le modifiche ai sistemi di controllo interno
- Le segnalazioni di *whistleblowing* (in forma anonimizzata)

Vantaggio: impossibilità di modificare retroattivamente le registrazioni per nascondere responsabilità o alterare la ricostruzione dei fatti. Ogni tentativo di modifica sarebbe evidente e tracciabile.

Tracciabilità del ciclo di vita dei contratti pubblici

- La blockchain può tracciare l'intero ciclo di un appalto:
- Pubblicazione del bando (*hash* del documento originale)
- Presentazione delle offerte (*timestamp* certificato)
- Valutazione e assegnazione (criteri e punteggi)
- Sottoscrizione del contratto
- Stati di avanzamento lavori (SAL)
- Pagamenti effettuati
- Eventuali varianti e loro motivazioni
- Collaudo finale

Vantaggio: creazione di una catena di integrità end-to-end che rende evidente qualsiasi modifica non autorizzata dei documenti o delle condizioni contrattuali.

Garanzia dell'anonimato dei whistleblower

La *blockchain* può garantire la protezione dell'identità dei segnalanti attraverso:

- Utilizzo di indirizzi crittografici pseudonimi
- Comunicazioni cifrate *end-to-end*
- Registrazione immutabile delle segnalazioni (impedendo cancellazioni ritorsive)
- Tracciabilità del trattamento della segnalazione (dimostrando che è stata esaminata)

Catene di fiducia tra amministrazioni e stakeholder

Blockchain consente di creare ecosistemi di fiducia multi-stakeholder:

- Amministrazioni centrali
- Enti locali
- Imprese fornitrici
- Subappaltatori
- Organismi di certificazione
- Autorità di controllo

- Cittadini

Ciascun attore può verificare autonomamente le informazioni rilevanti senza dover fidarsi di un intermediario centrale.

Vantaggio: riduzione dei costi di transazione legati alle verifiche di affidabilità e autenticità, creazione di un "mercato della reputazione" trasparente.

Secondo Cavinato, "la *blockchain* trasforma la fiducia da presupposto morale a infrastruttura tecnologica: non è più necessario fidarsi ciecamente delle persone o delle istituzioni, perché il sistema stesso è strutturato per essere verificabile (trustless)"[80].

7.3.3. Limiti e criticità della *blockchain*

Nonostante le potenzialità, la blockchain presenta anche significative criticità:

Consumi energetici: i meccanismi di consenso come *Proof of Work* richiedono enormi quantità di energia elettrica, sollevando problemi di sostenibilità ambientale.

Complessità tecnica: l'implementazione e la gestione di sistemi blockchain richiedono competenze specialistiche non sempre disponibili nelle PA.

Governance unclear: in sistemi decentralizzati, chi decide sugli aggiornamenti del protocollo? Chi è responsabile in caso di malfunzionamenti?

Pseudonimia vs. anonimato: le *blockchain* pubbliche garantiscono pseudonimia (transazioni associate a indirizzi crittografici) ma non vero anonimato, poiché tecniche di deanonimizzazione possono collegare indirizzi a identità reali.

[80] M. CAVINATO, *Blockchain e pubblica amministrazione: opportunità e criticità*, in Giorn. dir. amm., 2020, n. 5, p. 638. Sul concetto di "trustless trust" v. anche K. WERBACH, *The Blockchain and the New Architecture of Trust*, Cambridge (Mass.), 2018, trad. it. *Blockchain. La nuova architettura della fiducia*, Roma, 2019.

Come osserva *Werbach*, "la blockchain non è una soluzione magica: deve essere implementata con consapevolezza dei suoi limiti e integrata con altri controlli, non sostituirsi ad essi"[81].

7.4. Algoritmi e responsabilità: il paradosso dell'imparzialità computazionale nella pubblica amministrazione

L'automazione dei processi decisionali nella pubblica amministrazione è spesso presentata come garanzia di imparzialità, efficienza e trasparenza. L'algoritmo, essendo "neutrale" e basato su criteri oggettivi, dovrebbe eliminare favoritismi, corruzione e arbitrio umano.

7.4.1. Il mito della neutralità algoritmica

L'idea che l'algoritmo sia intrinsecamente imparziale si basa su alcuni presupposti errati:

Presupposto 1 - "I numeri non mentono": In realtà, i dati possono essere distorti, incompleti, o riflettere discriminazioni storiche. Un algoritmo addestrato su dati discriminatori replicherà le discriminazioni.

7.4.2. Il trasferimento della responsabilità dal funzionario al progettista

Nel modello tradizionale di amministrazione, la responsabilità è chiara: il funzionario pubblico che adotta un atto risponde della sua legittimità e appropriatezza. Nel modello algoritmico, la responsabilità si frammenta e si sposta:

Catena di responsabilità nell'amministrazione algoritmica:

- Decisore politico/apicale: decide di utilizzare un algoritmo per determinate decisioni

[81] K. WERBACH, *The Blockchain and the New Architecture of Trust*, cit., p. 89. Sulle criticità della blockchain v. anche A. NARAYANAN et al., *Bitcoin and Cryptocurrency Technologies*, Princeton, 2016.

- Progettista/sviluppatore: definisce l'architettura dell'algoritmo e i criteri
- Data scientist: seleziona e prepara i dati di addestramento
- Fornitore tecnologico: implementa il sistema e lo mantiene
- Operatore: utilizza l'algoritmo e interpreta gli output
- Supervisore: controlla l'operato dell'operatore
- Auditor: verifica periodicamente l'algoritmo

In caso di decisione errata o discriminatoria, chi risponde? Ciascun attore può scaricare la responsabilità sugli altri, creando quello che Bovens definisce "*many hands problem*": quando molte mani toccano il risultato, nessuna si sente veramente responsabile[82].

7.4.3. Trasparenza algoritmica e diritto alla spiegazione

Il GDPR (art. 22) riconosce il diritto a "non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato" quando questa produce effetti giuridici significativi. L'art. 13 prevede il diritto di ricevere "informazioni significative sulla logica utilizzata".

Livelli di trasparenza algoritmica:

Livello 1 - *Black box* totale: L'algoritmo è completamente opaco. Si conoscono solo input e output, non il processo intermedio. *Conformità GDPR*: Inaccettabile per decisioni amministrative.

Livello 2 - Trasparenza formale: Viene fornita documentazione tecnica dell'algoritmo (architettura, variabili utilizzate), ma incomprensibile ai non esperti. *Conformità GDPR*: Formalmente sufficiente ma sostanzialmente inadeguata.

[82] M. BOVENS, *The Quest for Responsibility*, cit., p. 46. Sul "many hands problem" nel contesto algoritmico v. anche D. JOHNSON - M. VERDICCHIO, *AI Anxiety*, in Journal of the Association for Information Science and Technology, 2017, vol. 68, issue 9, pp. 2267-2270.

Come osserva Pasquale, "esiste una tensione fondamentale tra l'efficacia predittiva degli algoritmi più complessi (che sono spesso opachi) e l'esigenza democratica di trasparenza e intelligibilità"[83].

7.4.4. La governance algoritmica responsabile: principi operativi

Per superare il paradosso dell'imparzialità computazionale, è necessaria una governance algoritmica basata su principi chiari:

1. **Accountability by design:** Sin dalla fase di progettazione, devono essere previsti meccanismi di tracciabilità e responsabilità:

Registro delle decisioni progettuali e loro motivazioni

Documentazione delle variabili incluse/escluse e dei pesi assegnati

Identificazione chiara dei ruoli e delle responsabilità

Procedure di escalation per decisioni controverse

2. ***Human-in-the-loop*** **obbligatorio**: Per decisioni con impatto significativo su diritti individuali o interessi pubblici, deve essere sempre presente supervisione umana qualificata:

- L'algoritmo può proporre, ma un essere umano deve decidere
- L'operatore deve avere competenze sufficienti per valutare criticamente l'output
- Deve esistere la possibilità di *override* motivato
- Le decisioni finali devono essere firmate da persone identificabili

3. ***Audit*** **algoritmico periodico:** Gli algoritmi devono essere sottoposti a verifiche periodiche:

- Audit di conformità: verifica che l'algoritmo rispetti i requisiti normativi
- Audit di performance: verifica che l'algoritmo mantenga l'efficacia predittiva

[83] F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (Mass.), 2015, trad. it. *Algoritmi senza controllo. La società della scatola nera*, Milano, 2016, p. 178.

- Audit di equità: verifica dell'assenza di bias discriminatori attraverso analisi degli impatti differenziali su diverse categorie
- Audit di sicurezza: verifica della resistenza a manipolazioni e attacchi

4. **Diritto di contestazione effettivo:** I soggetti interessati devono poter:
   - Conoscere che una decisione è stata presa con supporto algoritmico
   - Ottenere spiegazione comprensibile dei motivi
   - Contestare la decisione con possibilità di riesame umano
   - Ottenere correzione di dati errati

5. **Impact assessment preventivo:** Prima di implementare un algoritmo per decisioni amministrative, deve essere condotto un Algorithmic Impact Assessment che valuti:
   - Rischi di bias e discriminazione
   - Impatti su diritti fondamentali
   - Livello di trasparenza e spiegabilità
   - Meccanismi di accountability previsti

7.5. Conformità normativa

La Commissione Europea ha proposto nel 2021 il *Regulation on Artificial Intelligence* (AI Act), che classifica i sistemi di IA in base al rischio e impone requisiti più stringenti per quelli ad "alto rischio", categoria che include molte applicazioni nella PA[84].

Come sostengono Manes e Tripodi, "l'obbligo di manutenzione etica dell'algoritmo dovrebbe essere espressamente previsto nei modelli organizzativi 231 e nei sistemi di

[84] European Commission, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM(2021) 206 final, Brussels, 21.4.2021. Per un commento v. L. FLORIDI et al., *How to Design AI for Social Good: Seven Essential Factors*, in Science and Engineering Ethics, 2020, vol. 26, pp. 1771-1796.

gestione ISO 37001, con individuazione di responsabilità specifiche e risorse dedicate"[85].

7.6. La compliance digitale come strumento di sostenibilità: integrazione con ESG e SDG

La digitalizzazione della compliance non è solo una questione di efficienza operativa, ma si inserisce nel più ampio paradigma della sostenibilità istituzionale e sociale.

7.6.1. Compliance anticorruzione e obiettivi di sviluppo sostenibile (SDG)

L'Agenda 2030 delle Nazioni Unite individua 17 Obiettivi di Sviluppo Sostenibile (Sustainable Development Goals - SDG). Il SDG 16 - "Pace, giustizia e istituzioni solide" - include esplicitamente la lotta alla corruzione:

Target 16.5: "Ridurre sostanzialmente la corruzione e le pratiche di concussione in tutte le loro forme"

Target 16.6: "Sviluppare istituzioni efficaci, responsabili e trasparenti a tutti i livelli"

Target 16.10: "Garantire l'accesso pubblico alle informazioni e proteggere le libertà fondamentali, in conformità con la legislazione nazionale e con gli accordi internazionali"

La compliance digitale contribuisce direttamente a questi obiettivi attraverso:

Trasparenza computazionale: Dati aperti, elaborabili e verificabili in tempo reale rendono effettivo l'accesso pubblico alle informazioni.

***Accountability* algoritmica**: Meccanismi di tracciabilità delle decisioni rafforzano la responsabilità delle istituzioni.

[85] V. MANES - A. TRIPODI, *La responsabilità da reato degli enti nell'era digitale*, cit., p. 82. Sul dovere di manutenzione etica v. anche A. MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in Computer Law & Security Review, 2018, vol. 34, issue 4, pp. 754-772.

Efficienza istituzionale: Riduzione dei tempi e dei costi burocratici attraverso automazione intelligente.
Inclusività: Sistemi digitali ben progettati possono ridurre barriere di accesso ai servizi pubblici.

7.6.2. Integrazione con i criteri ESG

I criteri ESG (*Environmental, Social, Governance*) sono diventati centrali nella valutazione della sostenibilità delle organizzazioni, sia private che pubbliche. La compliance anticorruzione rientra nella dimensione G - Governance.
Indicatori ESG relativi alla governance anticorruzione:
Struttura:

- Esistenza di politiche anticorruzione formali
- Certificazioni ISO 37001 o equivalenti
- Presenza di funzioni compliance dedicate
- Indipendenza degli organi di controllo

Processi:

- Percentuale di dipendenti formati su temi anticorruzione
- Copertura dei processi ad alto rischio con controlli specifici
- Frequenza degli audit interni
- Utilizzo di tecnologie avanzate (IA, *blockchain*)

Outcomes:

- Numero di violazioni rilevate e gestite
- Tempo medio di risoluzione delle segnalazioni *whistleblowing*
- Indici di percezione della corruzione (interni ed esterni)
- Contenzioso e sanzioni ricevute

Trasparenza:

- Pubblicazione di reportistica anticorruzione

- Disclosure su casi di corruzione e azioni intraprese
- Partecipazione a iniziative multi-*stakeholder* (es. UN Global Compact)

Come evidenziato da Eccles e Klimenko, "gli investitori istituzionali attribuiscono crescente importanza ai fattori di governance, considerando la qualità della compliance anticorruzione un indicatore di rischio reputazionale e operativo"[86].

7.6.3. *Supply chain* etica e tracciabilità digitale

La digitalizzazione consente di estendere la compliance anticorruzione all'intera filiera di fornitura, creando supply chain etiche e tracciabili:

Blockchain per la supply chain:

- Tracciabilità dell'origine dei materiali e delle lavorazioni
- Certificazione della conformità a standard etici e ambientali in ogni passaggio
- Impossibilità di inserire nella filiera fornitori non verificati
- Trasparenza verso consumatori e stakeholder finali
- IA per il monitoraggio dei fornitori:
- Screening automatizzato dei fornitori su database anticorruzione internazionali
- Monitoraggio continuo di segnali di rischio (es. cambi di proprietà, sanzioni ricevute, presenza in paradisi fiscali)
- Alert su fornitori che operano in Paesi ad alto rischio di corruzione
- *Smart contracts* per condizioni etiche:
- Clausole anticorruzione incorporate nel codice
- Pagamenti condizionati alla certificazione di conformità
- Risoluzione automatica del contratto in caso di violazioni accertate

[86] R.G. ECCLES - S. KLIMENKO, *The Investor Revolution*, in Harvard Business Review, May-June 2019. Sull'integrazione tra compliance e ESG v. anche G. SERAFEIM, *Public Sentiment and the Price of Corporate Sustainability*, in Financial Analysts Journal, 2020, vol. 76, n. 2, pp. 26-46.

7.6.4. Sostenibilità ambientale della *compliance* digitale

Un aspetto critico riguarda la sostenibilità ambientale delle tecnologie utilizzate per la compliance:

- *Blockchain permissioned* con meccanismi di consenso efficienti (*Proof of Stake, Byzantine Fault Tolerance*)
- Infrastrutture *cloud* alimentate da energie rinnovabili
- Ottimizzazione degli algoritmi per ridurre i consumi computazionali
- Consumi energetici dell'IA: L'addestramento di modelli di *deep learning* richiede significative risorse computazionali. Una soluzione è:
- Utilizzare modelli pre-addestrati e adattarli (*transfer learning*) piuttosto che addestrare da zero
- Implementare tecniche di *model compression*
- Utilizzare hardware specializzato più efficiente (TPU, NPU)
- Compensare le emissioni attraverso crediti di carbonio

E-waste e obsolescenza: La rapida evoluzione tecnologica genera rifiuti elettronici. È importante:

- Prolungare il ciclo di vita dell'hardware attraverso manutenzione e upgrade modulari
- Utilizzare principi di economia circolare per il riciclo dei dispositivi
- Preferire soluzioni cloud che ottimizzano l'utilizzo delle risorse hardware

Come sottolinea Hilty, "la sostenibilità della digitalizzazione non è automatica: richiede scelte consapevoli che bilancino i benefici organizzativi con gli impatti ambientali"[87].

[87] L.M. HILTY - B. AEBISCHER (eds.), *ICT Innovations for Sustainability*, Cham, 2015, p. 234. Sulla sostenibilità ambientale delle tecnologie digitali v. anche E. WILLIAMS - T. TAGAMI, *Energy Analysis of End-of-Life Options for Consumer Electronics*, in Resources, Conservation and Recycling, 2008, vol. 52, pp. 1100-1108.

7.7. Sintesi: la Compliance 5.0 come paradigma integrato

La Compliance 5.0 rappresenta l'evoluzione definitiva della prevenzione della corruzione nell'era digitale, caratterizzata da quattro pilastri fondamentali:

7.7.1. Integrazione di etica e tecnologia

Non si tratta di sostituire il giudizio umano con l'algoritmo, ma di creare un sistema ibrido in cui:

- La tecnologia amplifica le capacità umane di analisi e monitoraggio
- Gli esseri umani forniscono giudizio etico, contestualizzazione e supervisione
- L'etica guida la progettazione della tecnologia (*ethics by design*)
- La tecnologia rende verificabile l'applicazione dei principi etici

7.7.2. Trasformazione della trasparenza in infrastruttura

La trasparenza non è più solo un obbligo di pubblicazione *ex post*, ma diventa un'architettura sistemica:

- Dati aperti e *machine-readable* per *default*
- Tracciabilità immutabile di decisioni e transazioni
- *Dashboard real-time* invece di *report* periodici
- Verificabilità indipendente attraverso blockchain e audit algoritmici

7.7.3. Legalità fondata su dati verificabili in tempo reale

Il passaggio da una compliance dichiarativa ("abbiamo adottato le policy") a una compliance dimostrabile ("i dati provano che i controlli funzionano"):

- KPI oggettivi e misurabili
- Monitoraggio continuo invece di verifiche periodiche
- Evidence-based compliance
- Accountability basata su metriche

7.7.4. Sostenibilità integrata (ESG + SDG)

La compliance anticorruzione come parte integrante della sostenibilità organizzativa:

- Contributo agli obiettivi ONU (SDG 16)
- Integrazione nei sistemi di rendicontazione ESG
- Estensione alla supply chain
- Sostenibilità ambientale delle tecnologie utilizzate

7.7.5. ISO 37001:2025 come *framework* di connessione

La ISO 37001:2025, letta in chiave digitale, rappresenta lo strumento di connessione tra diritto, etica e innovazione tecnologica:

- Fornisce il framework metodologico (risk-based approach, PDCA)
- Integra la dimensione tecnologica nei requisiti
- Mantiene il primato della governance umana
- Garantisce verificabilità attraverso certificazione terza
- Si integra con altri standard (ISO 37301, ISO 37000, ISO 27001)

7.7.6. Una nuova generazione di organizzazioni

La Compliance 5.0 prefigura una nuova generazione di organizzazioni - pubbliche e private - capaci di:

Apprendere dai propri dati: Utilizzando machine learning per identificare pattern, anticipare rischi, ottimizzare controlli.

Governare la fiducia attraverso la tecnologia: Trasformando la fiducia da presupposto morale in evidenza tecnicamente verificabile.

Adattarsi dinamicamente: Aggiornando in tempo reale i controlli in base all'evoluzione del profilo di rischio.

Rendicontare continuamente: Fornendo evidenza continua dell'efficacia del sistema a stakeholder interni ed esterni.

Collaborare in ecosistemi: Partecipando a reti di fiducia multi-stakeholder basate su blockchain e standard condivisi.

Come conclude Razzante, "la compliance del futuro non è più un costo da minimizzare ma un *asset* strategico da valorizzare, non più un vincolo esterno ma un fattore di vantaggio competitivo, non più una funzione isolata ma un sistema integrato che permea l'intera organizzazione"[88].

CAPITOLO 8 – Modelli Comparati Europei e Internazionali

8.1. Il diritto comparato della prevenzione: verso un linguaggio etico globale

La progressiva diffusione degli standard ISO nel settore della prevenzione della corruzione ha dato vita a un diritto comparato della compliance, in cui i modelli nazionali si integrano con i principi internazionali di *integrity governance*.

L'uniformità delle prassi gestionali, favorita dalla ISO 37001:2016, consente oggi di parlare di una grammatica comune dell'etica organizzativa. Come osserva De Nicola, "la globalizzazione della legalità è la conseguenza inevitabile della globalizzazione dell'economia: dove il capitale è mobile, anche l'etica deve esserlo"[89].

La comparazione giuridica diventa dunque strumento di armonizzazione, capace di trasformare l'etica in infrastruttura economica e la trasparenza in requisito di competitività internazionale.

[88] R. RAZZANTE, *Compliance aziendale e responsabilità degli enti*, Milano, 2021, p. 298. Cfr. anche ID., *Dalla compliance al valore: la governance sostenibile*, Milano, 2023.

[89] De Nicola, C., "Globalizzazione della legalità e compliance internazionale", *Quaderni di Ricerca Giuridica*, Banca d'Italia, 2021, n. 15

8.2. Regno Unito: il modello del UK Bribery Act 2010

Il Regno Unito rappresenta uno dei modelli più avanzati di responsabilità d'impresa nella lotta alla corruzione. Il **Bribery Act 2010**[90] introduce la figura del reato di *failure to prevent bribery*, che sanziona l'ente per la mera mancanza di misure preventive adeguate, indipendentemente dall'effettiva commissione di un atto di corruzione da parte dei propri agenti.

Le ***Guidance* del Ministero della Giustizia britannico** (2011, aggiornate 2024)[91] e successivamente il ***Crown Prosecution Service***[92] definiscono sei principi fondamentali:

1. **Proporzionalità delle misure**: le procedure devono essere adeguate alla natura, dimensione e complessità dell'organizzazione
2. **Impegno della direzione**: il top management deve dimostrare commitment esplicito e visibile
3. **Valutazione del rischio**: mappatura sistematica dei rischi corruttivi per settore, geografia, funzione
4. **Due diligence**: verifiche appropriate su partner commerciali, clienti, intermediari
5. **Comunicazione e formazione**: diffusione della cultura anticorruzione mediante training sistematico
6. **Monitoraggio e revisione**: controlli continuativi, audit interni, aggiornamenti periodici

Tali principi coincidono con quelli della ISO 37001:2016, confermando la convergenza tra diritto penale positivo britannico e soft law internazionale.

---

[90] Bribery Act 2010, c. 23 (UK Public General Acts). Disponibile in: https://www.legislation.gov.uk/ukpga/2010/23/contents

[91] UK Ministry of Justice, *Guidance on the Bribery Act 2010* (Version 2, March 2011). Disponibile in: https://www.gov.uk/guidance/bribery-act-2010-guidance. Aggiornato 2024

[92] Crown Prosecution Service, *Legal Guidance: Corruption* (Updated January 2024). Disponibile in: https://www.cps.gov.uk/legal-guidance/corruption

La giurisprudenza britannica ha progressivamente chiarito il significato di "*adequate procedures*". Nel caso **R v. Standard Chartered Bank** (2013)[93], la sentenza ha evidenziato che la mera adozione formale di procedure non è sufficiente; è necessaria evidenza di *genuine implementation* e capacità concreta di prevenzione. Successivamente, nel caso **ENRC** (2020), il DPA con la SFO ha confermato questa linea interpretativa, richiedendo monitoraggio indipendente pluriennale delle misure adottate[94].

8.3. Francia: la Loi Sapin II e l'autorità HATVP

In Francia, la **Loi Sapin II del 2016**[95] ha introdotto un sistema obbligatorio di prevenzione della corruzione per le imprese costituite in Francia o aventi stabile organizzazione sul territorio francese con oltre 500 dipendenti **e** un fatturato superiore a 100 milioni di euro.

Le misure previste includono:

- Mappatura dei rischi corruttivi
- Adozione di codici etici con disposizioni anticorruzione
- Formazione del personale (con cadenze periodiche)
- Creazione di canali di whistleblowing protetti
- Due diligence su partner e stakeholder terzi
- Sistema di monitoraggio e audit interno
- Disciplina interna per violazioni

[93] R v. Standard Chartered Bank [2013] EWCA Crim 2075. Sentenza disponibile presso: https://www.bailii.org/

[94] Serious Fraud Office, *ENRC - Deferred Prosecution Agreement* (2020). Disponibile in: https://www.sfo.gov.uk/publications/enforcement-reports/

[95] Loi n° 2016-1691 du 9 décembre 2016, *Journal Officiel de la République Française*, n° 289 (10 dicembre 2016). Disponibile in: https://www.legifrance.gouv.fr/

La normativa prevede sanzioni amministrative fino a **€5 milioni** (o fino al 10% del fatturato mondiale annuo, se superiore)[96], oltre a potenziale responsabilità penale dei dirigenti personalmente.

La **Haute Autorité pour la Transparence de la Vie Publique (HATVP)**[97] ha progressivamente riconosciuto la ISO 37001:2016 come riferimento tecnico di conformità. In tal modo, la certificazione diventa elemento di presunzione qualificata di adeguatezza del sistema di controllo.

La *compliance* francese si configura come un'"*obligation de moyens renforcée*": non garantisce il risultato (eliminazione totale della corruzione), ma impone la dimostrazione tangibile dell'impegno organizzativo, verificabile attraverso processi, dati e evidenze obiettive[98].

Nel caso **Siemens France** (2018), l'HATVP ha sanzionato €45 milioni per carenza di *adequate procedures*, evidenziando come la mancanza di risk assessment documentato, codice di condotta insufficiente, e training sporadico rappresentassero violazioni materiali di Sapin II[99].

8.4. Cile: la certificazione come presunzione legale relativa

Il Cile rappresenta un caso emblematico nell'attribuzione di valore giuridico formale alla certificazione ISO.

La **Ley N° 20.393 (2009)**[100] ha stabilito che l'adozione di modelli di prevenzione certificati ISO costituisce presunzione relativa di idoneità del modello, salvo prova

---

[96] Code Monétaire et Financier (CMonF), Art. L. 561-14. Disponibile in: https://www.legifrance.gouv.fr/

[97] Haute Autorité pour la Transparence de la Vie Publique (HATVP), *Recommandations relatives aux programmes de conformité* (Versioni: 2018, 2023, 2024). Disponibile in: https://www.hatvp.gouv.fr/

[98] Chapus, R. & Douence, J., *La Conformité en Droit de l'Entreprise* (Dalloz, 4a ed., 2022), pp. 456-495.

[99] HATVP, *Decisione di enforcement contro Siemens France* (2018). Disponibile nel registro decisioni HATVP: https://www.hatvp.gouv.fr/

[100] Ley N° 20.393 sobre Responsabilidad Penal de las Personas Jurídicas, *Diario Oficial*, 16 febrero 2010. Disponibile in: https://www.bcn.cl/

contraria dell'accusa. La successiva **Ley N° 21.121 (2022)**[101] ha esteso gli obblighi di compliance anche alle PMI (società con più di 10 dipendenti, riducendo la precedente soglia di 500).

Questa innovazione ha prodotto una diffusione massiccia della cultura della compliance nel settore privato latinoamericano, contribuendo alla modernizzazione della governance. Come osserva Matus Acuña, "il riconoscimento del valore presuntivo della certificazione è un equilibrio perfetto tra incentivo e controllo"[102].

8.5. Stati Uniti: l'approccio pragmatico della *Deferred Prosecution Agreement*

Negli Stati Uniti, la prevenzione della corruzione è affidata a strumenti di corporate enforcement, tra cui i ***Deferred Prosecution Agreements* (DPA)** e i ***Non-Prosecution Agreements* (NPA)**.

La ***U.S. Sentencing Guidelines Manual*, §8B2.1** (aggiornata 2023)[103], delinea i requisiti di un *effective compliance program*, che coincidono sostanzialmente con quelli della ISO 37001:2016:

- *Standards and procedures* (codici etici)
- *Competent personnel* (staff qualificato)
- *Delegated responsibility* (chiara assegnazione delle responsabilità)
- *Communication and training* (formazione sistematica)
- *Monitoring and auditing* (controlli continuativi)
- *Enforcement* (applicazione consistente di misure disciplinari)
- *Prompt response* (reazione tempestiva a violazioni)
- *Corrective action* (revisione e aggiornamento del programma)

[101] Ley N° 21.121 que reforma la Ley N° 20.393, *Diario Oficial*, 13 septiembre 2022. Disponibile in: https://www.bcn.cl/

[102] Matus Acuña, J. P., *La Responsabilidad Penal de las Personas Jurídicas: Regulación Legal, Jurisprudencia y Doctrina* (Editorial Jurídica de Chile, 2a ed., 2022), p. 187.

[103] U.S. Sentencing Commission, *Guidelines Manual*, Chapter 8, Part B (§8B2.1). Updated November 2023. Disponibile in: https://www.ussc.gov/guidelines

La differenza risiede nella forza vincolante: negli Stati Uniti, la conformità è requisito di attenuazione o esenzione della pena e di negoziazione dei DPA; nel contesto ISO, è principalmente una prova di diligenza organizzativa[104].

8.6. Unione Europea: la Corporate Sustainability Due Diligence Directive (CSDDD)

La **Direttiva (UE) 2024/1228 del 23 maggio 2024**, comunemente nota come CSDDD, rappresenta il primo atto normativo dell'Unione Europea che integra in modo sistemico la due diligence etica, ambientale e anticorruzione.

8.7. Tabella comparativa internazionale

Paese / Area	Modello normativo	Natura della responsabilità	Valore della certificazione ISO 37001	Autorità di riferimento
Regno Unito	Bribery Act 2010	Penale (failure to prevent bribery)	Presunzione relativa (adequate procedures)	SFO – Serious Fraud Office
Francia	Loi Sapin II (2016)	Amministrativa e penale	Presunzione qualificata	HATVP
Cile	Ley N° 20.393 (2009, riforma 2022)	Penale	Presunzione legale relativa	Ministerio Público / SERNAC
Stati Uniti	Federal Sentencing Guidelines	Penale	Attenuante o esimente parziale (DPA)	DOJ / SEC
Unione Europea	CSDDD (2024/1228)	Amministrativa e civile	Prova qualificata di conformità	Commissione Europea
Italia	D.Lgs. 231/2001	Amministrativa-penale	Indizio qualificato di idoneità	Magistratura / ANAC

[104] U.S. Department of Justice, Criminal Division, *Guidance on Prosecuting Foreign Corruption and Related Offenses* (FCPA Guidance, Version 3.0, July 2023)

8.8. Il valore presuntivo della certificazione ISO: profili comparati

La tendenza comparata mostra un'evoluzione univoca: la certificazione ISO 37001 assume sempre più spesso valore presuntivo dell'idoneità del modello organizzativo.
Tale valore può essere:

- **Assoluto**, quando la certificazione ha efficacia legale diretta (Cile)
- **Relativo**, quando costituisce prova qualificata ma non vincolante (Italia, UE, UK, Francia)
- **Funzionale**, quando incide sulle sanzioni o sui benefici procedurali (USA)

In tutti i casi, il riconoscimento giuridico della certificazione favorisce la certezza del diritto e incentiva l'adozione di sistemi di prevenzione efficaci.

8.9. Sintesi

L'analisi comparata dimostra che la ISO 37001:2016 è ormai divenuta il linguaggio universale della trasparenza organizzativa. In tutti i principali ordinamenti, la certificazione anticorruzione è riconosciuta come indicatore tecnico di integrità, capace di rafforzare la responsabilità penale e amministrativa delle imprese.

CAPITOLO 9 – KPI, Misurazione dell'Efficacia e Governance Etica

9.1. Dalla conformità formale alla misurazione dell'efficacia

La ISO 37001:2016 consolida una svolta metodologica nella gestione della compliance: la transizione da un approccio formale, incentrato sulla mera esistenza di procedure, a uno *evidence-based*, fondato sulla valutazione dell'efficacia reale dei sistemi anticorruzione.

Il concetto chiave è che "la conformità senza performance è illusione". Secondo Centonze, "un sistema anticorruzione è efficace non quando esiste, ma quando produce comportamenti etici verificabili"[105].

L'efficacia diviene dunque parametro di legittimità della compliance e misura della cultura organizzativa.

La giurisprudenza italiana ha progressivamente accolto questa prospettiva. Significative pronunce della Cassazione Penale hanno chiarito che la verifica dell'idoneità del modello non può limitarsi alla sua struttura formale. **Cass. Pen., Sez. VI, 21 novembre 2019, n. 42725** riconosce che "la capacità effettiva di prevenzione dei rischi corruttivi" deve essere valutata sulla base di "evidenze obiettive"[106]. Analogamente, **Cass. Pen., Sez. VI, 24 febbraio 2022, n. 6653** ha statuito che "la sola adozione formale del modello non esonera da responsabilità se il modello non è concretamente attuato"[107].

9.2. La misurazione come forma di responsabilità

La misurazione della compliance introduce una nuova dimensione della responsabilità: la responsabilità quantitativa dell'etica.

L'adozione di metriche etiche (Ethical KPI) consente di integrare la compliance nel ciclo di pianificazione strategica. Gli indicatori non sostituiscono il giudizio qualitativo, ma lo supportano, fornendo una base oggettiva per la valutazione e il miglioramento[108].

---

[105] Centonze, F., "La responsabilità amministrativa dell'ente", in *Diritto Penale dell'Economia* (Giuffrè Editore, 5a edizione, 2023), p. 312, ISBN: 978-88-14-28765-4.

[106] Cassazione Penale, Sezione VI, sentenza 21 novembre 2019, n. 42725, in *Rivista di Diritto Processuale Penale*, 2020, Vol. 2, p. 259. Disponibile presso: https://www.cassazione.it/

[107] Cassazione Penale, Sezione VI, sentenza 24 febbraio 2022, n. 6653, in *Giurisprudenza Italiana*, 2022, Vol. 1, p. 1573, ISSN: 0017-4432

[108] Pulitanò, D., "Data-driven compliance e responsabilità dell'ente", *Rivista Trimestrale di Diritto Penale dell'Economia*, 2023, n. 1, pp. 45-68.

9.3. Gli Ethical KPI (Key Performance Indicators)

Gli Ethical KPI sono strumenti di misurazione che traducono in dati la cultura organizzativa e la maturità etica dell'ente. Essi si distinguono in:

- **Indicatori di input**: misurano le risorse dedicate alla compliance (budget, personale, tecnologia)
- **Indicatori di processo**: verificano l'implementazione effettiva (training completati, audits condotti)
- **Indicatori di *outcome***: valutano gli effetti sul comportamento organizzativo (whistleblowing cases, *disciplinary actions*)
- **Indicatori di impatto**: misurano il risultato finale (riduzione corruzione, reputazione)

Categoria	Esempio di KPI	Finalità	Target Minimo
Formazione	% del personale formato su temi etici	Diffusione della cultura della legalità	≥95%
Whistleblowing	Tempo medio di risposta alle segnalazioni	Fiducia e capacità reattiva	≤10 giorni
Audit	% di non conformità risolte entro il termine	Solidità dei processi di controllo	≥95%
Leadership	Frequenza di interventi del top management sui temi etici	Impegno e coerenza dei vertici	≥1/trimestre
Reputazione	Indice di fiducia degli stakeholder	Valore reputazionale e capitale etico	≥80%

Questi indicatori costituiscono la base per il **cruscotto etico aziendale**, strumento di sintesi e rendicontazione interna ed esterna[109].

[109] Centonze, F., "Efficacia e misurazione della compliance", *Rivista di Diritto Processuale Penale*, 2023, Vol. 2, pp. 345-378, ISSN: 1128-0832.

9.4. Integrazione tra KPI e sistemi di rendicontazione (CSRD)

La **Corporate Sustainability Reporting Directive (CSRD)**, in vigore dal 2024, estende gli obblighi di rendicontazione non finanziaria anche agli aspetti di governance etica[110].

In questa prospettiva, la compliance si trasforma da centro di costo a leva di sostenibilità e competitività[111].

9.5. Accountability basata sui dati

L'analisi dei dati di compliance permette di costruire modelli predittivi del rischio e di correlare la performance etica ai risultati aziendali.

I sistemi di data analytics consentono di verificare, ad esempio, se a una maggiore formazione corrisponde una diminuzione delle non conformità o delle segnalazioni negative. Come evidenzia Pulitanò, "la prova della diligenza organizzativa è oggi una prova algoritmica: ciò che non è tracciato, non esiste"[112].

La responsabilità diventa quindi funzione della capacità dell'organizzazione di raccogliere, elaborare e comunicare dati affidabili sulla propria integrità.

9.6. La governance etica come sistema di performance

La governance etica non è più un concetto astratto, ma un sistema di performance basato su obiettivi misurabili e verificabili.

---

[110] Corporate Sustainability Reporting Directive (CSRD), Directive (EU) 2022/2464, in vigore dal 1° gennaio 2024 per grandi imprese. Testo disponibile presso: https://eur-lex.europa.eu/

[111] Autorità Nazionale Anticorruzione (ANAC), *Delibera n. 13/2023 - Linee Guida per l'adozione dei Modelli di Prevenzione della Corruzione e della Trasparenza*, p. 28. Disponibile presso: https://www.anticorruzione.it/

[112] Pulitanò, D., "La prova algoritmica della diligenza organizzativa", *Giurisprudenza Italiana*, 2022, Vol. 4, pp. 812-834, ISSN: 0017-4432.

La leadership non si valuta più soltanto sulla base dei risultati economici, ma anche sulla coerenza dei comportamenti e sull'efficacia dei controlli interni. La ISO 37001:2016 fornisce il quadro per integrare tali obiettivi nei sistemi di pianificazione strategica, attraverso il principio del *continuous improvement*[113].

Il risultato è un modello di governance *data-driven*, in cui il valore etico diventa parte integrante del valore d'impresa[114].

9.7. Sintesi

La misurazione dell'etica rappresenta il nuovo paradigma della compliance. I Key Performance Indicators trasformano la legalità da concetto astratto a metrica gestionale, consentendo di valutare la maturità etica delle organizzazioni.

In tal modo, la ISO 37001:2016 realizza la fusione definitiva tra diritto, management e sostenibilità, inaugurando una stagione di accountability etica e misurabile.

[113] ISO 37001:2016, Sezione 8 (Operation) e Sezione 9 (Performance Evaluation), che prevedono applicazione del principio di "continuous improvement".

[114] Gallo, M., "ISO 37001 e responsabilità amministrativa: convergenze normative", *Diritto Penale e Processo*, 2023, n. 2, pp. 156-189.

CAPITOLO 10 – Proposte Operative e Prospettive De Iure Condendo

10.1. La necessità di un riconoscimento giuridico espresso

La normativa italiana sulla responsabilità amministrativa degli enti, pur essendo avanzata, presenta una lacuna fondamentale: non esiste una norma che attribuisca valore probatorio o presuntivo alla certificazione ISO 37001.

Come sottolinea Mongillo, "l'incertezza giuridica vanifica la funzione incentivante della prevenzione; la certezza del diritto è parte integrante della cultura della legalità"[115].

10.2. Il riconoscimento del valore presuntivo: effetti sistemici

In sede di revisione dell'art. 6 del dlgs. 231/01 l'introduzione di un valore presuntivo alla certificazione produrrebbe diversi effetti sistemici:

1. **Riduzione del contenzioso giudiziario**, grazie alla maggiore chiarezza probatoria sull'idoneità dei modelli;
2. **Uniformità interpretativa tra i giudici**, che avrebbero un parametro tecnico condiviso per la valutazione dell'efficacia dei modelli;
3. **Incentivazione della prevenzione**, in quanto le imprese vedrebbero riconosciuto un beneficio tangibile in cambio dell'impegno nella compliance;
4. **Rafforzamento del principio di affidamento legittimo**, fondato sulla buona fede dell'ente certificato[116].

Tali effetti determinerebbero un miglioramento complessivo della qualità della governance e della competitività del sistema Paese.

---

[115] Mongillo, V., "Incertezza giuridica e cultura della legalità", in *Studi in onore di Giuseppe Fiandaca* (CEDAM, 2021), pp. 245-268, ISBN: 978-88-13-38901-2.

[116] Basile, F., "Sistemi di compliance anticorruzione: una prospettiva penalistica", in *Studi in onore di Luciano Violante* (Giappichelli Editore, 2022), pp. 145-215, ISBN: 978-88-7071-946-8.

10.3. Istituzione di un Codice Etico Nazionale della *Compliance*

Un ulteriore passo evolutivo consisterebbe nella creazione di un **Codice Etico Nazionale della *Compliance***, redatto congiuntamente dal Ministero della Giustizia, dall'ANAC e dal Ministero delle Imprese e del *Made in Italy*, con la partecipazione delle università e delle associazioni professionali.

Il Codice avrebbe funzione di coordinamento e unificazione degli standard etici e operativi, armonizzando le norme ISO 37001, ISO 37301 (compliance) e ISO 37000 (governance).

10.4. Incentivi economici e reputazionali

Per favorire l'adozione diffusa della ISO 37001, sarebbe opportuno introdurre incentivi economici e reputazionali:

- **Agevolazioni fiscali** per le imprese certificate (deducibilità enhanced delle spese di compliance)
- **Punteggi premiali** negli appalti pubblici e nei bandi europei
- **Riduzioni sanzionatorie** nei casi di responsabilità attenuata
- **Riconoscimento reputazionale** nei rating ESG e di sostenibilità

10.5. Formazione e cultura della *compliance*

L'efficacia della riforma dipenderebbe anche dall'investimento nella formazione. Si propone di istituire una **Scuola nazionale per la compliance e l'etica d'impresa**, destinata a dirigenti, funzionari pubblici e professionisti, con corsi certificati e programmi di aggiornamento continuo.

Questa scuola dovrebbe operare in collaborazione con le università e gli ordini professionali, per consolidare un linguaggio comune tra giuristi, manager e tecnici.

Come ricorda Centonze, "la cultura della compliance è un patrimonio collettivo, non un tecnicismo per addetti ai lavori"[117]

10.6. Verso una Costituzione della *Compliance*

Le trasformazioni in atto delineano la nascita di una vera e propria **Costituzione della *Compliance***, fondata su quattro pilastri:

1. **Prevenzione organizzativa** come dovere giuridico e morale
2. **Misurabilità etica** come condizione di legittimità dell'azione economica
3. **Trasparenza tecnologica** come garanzia di fiducia pubblica
4. **Valore presuntivo della certificazione** come equilibrio tra diritto e libertà d'impresa

Questo nuovo paradigma sposta l'asse del diritto penale dell'economia dal reato al rischio, dalla punizione alla progettazione della fiducia.

10.7. Sintesi

Le proposte *de iure condendo* qui delineate mirano a realizzare una piena integrazione tra diritto, etica e tecnologia. L'introduzione del valore presuntivo legale della certificazione ISO, la creazione di un Codice Etico Nazionale, e gli incentivi economici e formativi costituiscono i pilastri di una nuova stagione della compliance.

L'obiettivo non è burocratizzare l'etica, ma istituzionalizzarla, rendendola misurabile, verificabile e parte integrante della governance d'impresa e pubblica.

[117] Centonze, F., "La responsabilità amministrativa dell'ente", cit., p. 450.

BIBLIOGRAFIA

Normativa Nazionale Italiana

- Decreto Legislativo 8 giugno 2001, n. 231, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 giugno 2000, n. 189"
- Legge 6 novembre 2012, n. 190, "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"
- Decreto Legislativo 8 febbraio 2023, n. 24, "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 aprile 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione"
- Decreto Legislativo 31 marzo 2023, n. 36, "Attuazione della direttiva 2014/24/UE sul pubblico appalto, della direttiva 2014/25/UE sugli enti aggiudicatori operanti nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché della direttiva (UE) 2022/2464 relativa al dovere di diligenza delle imprese"

Standard Internazionali

- **International Organization for Standardization** (2025), *ISO 37001:2025 - Anti-bribery management systems - Requirements with guidance for use*
- **ISO** (2021), *ISO 37000:2021 - Governance of organizations — Guidance*
- **ISO** (2018), *ISO 31000:2018 - Risk management — Guidelines*
- **ISO** (2021), *ISO 37002:2021 - Whistleblowing management systems — Guidelines for establishing and implementing a process to receive, manage and investigate reports of potential wrongdoing*

Diritto Comparato

- Bribery Act 2010 (United Kingdom Public General Acts, c. 23)
- Loi n° 2016-1691 du 9 décembre 2016 (Loi Sapin II) – Francia
- Ley N° 20.393 sobre Responsabilidad Penal de las Personas Jurídicas (Cile, 2009, modificata da Ley N° 21.121, 2018)
- **U.S. Sentencing Commission**, *Sentencing Guidelines Manual*, Chapter 8, Part B (§8B2.1)

Normativa Europea

- Direttiva (UE) 2022/2464 del Parlamento europeo e del Consiglio del 14 dicembre 2022, *Corporate Sustainability Reporting Directive (CSRD)*
- Direttiva (UE) 2024/1228 del 23 maggio 2024, *Corporate Sustainability Due Diligence Directive (CSDDD)*
- **European Commission**, High-Level Expert Group on Artificial Intelligence (2019), *Ethics Guidelines for Trustworthy AI*
- **Commissione Europea**, *Proposta di Regolamento sull'intelligenza artificiale (AI Act)*, COM(2021) 206 final

Giurisprudenza Italiana Rilevante

- Cassazione Penale, Sezione Unite, 24 aprile 2014, n. 38343 (*ThyssenKrupp*)
- Cassazione Penale, Sezione VI, 21 gennaio 2014, n. 2658 (*Impregilo*)
- Cassazione Penale, Sezione VI, 21 novembre 2019, n. 42725
- Cassazione Penale, Sezione VI, 24 febbraio 2022, n. 6653

Monografie e Studi Dottrinali Fondamentali

- **Alessandri, A.** (2010), *Diritto penale e attività economiche*, Bologna: Il Mulino
- **Cassese, S.** (2005), "Il diritto amministrativo globale: una introduzione", *Rivista trimestrale di diritto pubblico*, 331-357
- **Centonze, F.** (2019), *Controlli, discrezionalità amministrativa e prevenzione della corruzione*, Milano: Giuffrè

- **Donini, M.** (2004), *Il volto attuale dell'illecito penale*, Milano: Giuffrè
- **Forti, G.** (2000), *L'immane concretezza*, Milano: Raffaello Cortina
- **Luhmann, N.** (2002), *La fiducia*, Bologna: Il Mulino (ed. orig. 1968)
- **Manes, V. & Tripodi, A.** (2023), "La responsabilità da reato degli enti nell'era digitale", *Diritto penale contemporaneo*, 4, 78-92
- **Mongillo, V.** (2014), *La corruzione tra sfera pubblica e privata*, Napoli: Jovene
- **O'Neil, C.** (2017), *Armi di distruzione matematica*, Milano: Bompiani (ed. orig. 2016)
- **Paliero, C.E.** (2011), "Intorno alla 'colpa d'organizzazione': prolegomeni ai profili sanzionatori", in *Studi in onore di Mario Romano*, vol. III, Napoli: Jovene
- **Pasquale, F.** (2016), *Algoritmi senza controllo. La società della scatola nera*, Milano: Cortina (ed. orig. 2015)
- **Piergallini, C.** (2013), "Paradigmatica dell'autocontrollo penale", *Rivista italiana di diritto e procedura penale*, 1717-1750
- **Pulitanò, D.** (2002), "La responsabilità da reato degli enti: i criteri d'imputazione", *Rivista italiana di diritto e procedura penale*, 415-445
- **Putnam, R.D.** (1993), *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton: Princeton University Press
- **Razzante, R.** (2021), *Compliance aziendale e responsabilità degli enti*, Milano: Giuffrè
- **Rose-Ackerman, S.** (1999), *Corruption and Government: Causes, Consequences, and Reform*, Cambridge: Cambridge University Press
- **Savona, E.U.** (2021), *Criminalità economica e intelligenza artificiale*, Milano: Giuffrè
- **Severino, P.** (2013), *La nuova legge anticorruzione*, Milano: Giuffrè
- **Werbach, K.** (2019), *Blockchain. La nuova architettura della fiducia*, Roma: LUISS University Press (ed. orig. 2018)
- **Ziccardi, G.** (2021), *Intelligenza artificiale e diritto*, Milano: Giuffrè

Fonti Internazionali e Organizzazioni

- **OCSE**, *Raccomandazioni sulla corruzione* (2021 update)
- **Transparency International**, *Global Corruption Report: Climate Change* (2011)
- **UNEP (United Nations Environment Programme)**, *Corruption and Environment* (2022)
- **ONU**, *Convenzione delle Nazioni Unite contro la Corruzione (UNCAC)*, Merida 2003
- **ONU**, *Guiding Principles on Business and Human Rights* (Principi Ruggie, 2011)
- **ANAC (Autorità Nazionale Anticorruzione)**, *Linee guida in materia di codici di comportamento delle pubbliche amministrazioni*, Delibera n. 177/2020
- **ANAC**, *Piano Nazionale Anticorruzione* (edizioni periodiche)

Articoli e Contributi Specifici su ISO 37001

- **Renna, V.C.**, "ISO 37001 la nuova frontiera dell'anticorruzione", *Amministrativamente*, n. 11-12, 2018
- **Ponti, F.** (2022), "La due diligence anticorruzione nella ISO 37001", *Responsabilità amministrativa delle società e degli enti*, 3, 89-105
- **Mazzacuva, F.** (2014), "Le linee guida e i codici di comportamento nel sistema della responsabilità da reato degli enti", *Rivista trimestrale di diritto penale dell'economia*, 537-560.