ATTUALITÀ

ANTONIO GULLO

Compliance[*]

La parola *compliance* ha rappresentato negli ultimi vent'anni la formula magica nel contrasto alla criminalità economico-affaristica, nel solco di una generale tendenza del legislatore a puntare non più solo sulla repressione, ma anche sul momento della prevenzione. L'espressione si è poi colorata di diverse sfumature a seconda delle sue modalità di manifestazione, divenendo familiare per i penalisti ben oltre il terreno 'd'elezione' della *corporate criminal liability*. Muovendo da tale prospettiva, il lavoro si sofferma in particolare sui c.d. sistemi integrati di *compliance*, analizzando dapprima scenari di convergenza più tradizionali – quale quello 'naturale' tra compliance 231 e controlli interni – verso ambiti d'interferenza di più recente emersione – dal settore della *human rights due diligence*, sino all'ambito della *digital criminal compliance*.

Compliance

Over the last twenty years, the word compliance has represented the magic formula in the fight against economic and business crime, in the wake of a general regulatory trend focused no longer only on repression, but also on prevention. This expression has also taken different nuances depending on its manifestation, becoming familiar to criminal law scholars far beyond the corporate criminal liability field. Starting from this perspective, the contribution focuses on the so-called integrated compliance systems, first analysing more traditional scenarios of convergence – such as the 'natural' one between compliance 231 and internal controls – towards more recently emerged areas of interference – from the sector of human rights due diligence to digital criminal compliance.

1. *Un inquadramento del tema.* La parola *compliance* ha rappresentato negli ultimi vent'anni la formula magica nel contrasto alla criminalità economico-affaristica.

Molte sono le ragioni alla base di questo successo.

Un primo motivo è da ricercare nel mutato approccio alla lotta ai fenomeni in considerazione: le strategie elaborate in tempi più recenti dal legislatore nel fronteggiare tali forme di manifestazione criminosa hanno smesso di puntare solo sulla repressione e hanno riservato particolare attenzione al momento della prevenzione. Un filo rosso che lega oramai una pluralità di settori – che

[*] Il presente contributo è stato pubblicato negli *Studi in onore di Carlo Enrico Paliero*, a cura di Piergallini-Mannozzi-Sotis-Perini-Scoletta-Consulich, Milano, 2022.

vanno dal riciclaggio alla corruzione, per lambire, come diremo, quello dei reati tributari ed estendersi a campi meno tradizionali, solo indirettamente e in via eventuale legati alla criminalità del profitto, quali la *data protection* e la sicurezza cibernetica nazionale – è costituito dalla cooperazione pubblico-privato[1], che è il precipitato del cambiamento in discorso.

L'organizzazione si libera definitivamente dello stigma di (possibile) fattore di dispersione della responsabilità, per candidarsi ad alleato dell'Autorità statuale nel disegno normativo appena accennato. "Lotta di Judo contro lotta di Sumo", questa la filosofia trapiantata nel dibattito scientifico interno, oramai diversi anni addietro, da un Maestro del diritto penale, facendo propri concetti già affermati oltreoceano[2]: abbandonare la infruttuosa prospettiva della contrapposizione muscolare con la *corporation* per piuttosto sfruttarne la struttura reticolare al fine di presidiare il rischio reato.

Un secondo motivo, come di recente ben lumeggiato[3], è da ricercare nell'ampia gamma di significati riportabili al lemma qui in esame. La parola *compliance* si è rivelata un luogo ospitale in grado di accogliere e dare senso alle diverse sfumature della *partnership* pubblico-privato e capace di etichettarne in modo efficace le varie stagioni.

L'età dell'oro della *compliance* nel nostro ordinamento ha inizio in una data precisa, che coincide con l'entrata in vigore del d.lgs. n. 231 del 2001. L'introduzione nel sistema italiano di un modello di responsabilità diretta dell'ente di chiara matrice punitiva (senza qui indugiare sulle questioni di qualificazione) è coincisa con la prima diffusione del termine oggetto di analisi. L'espressione '*compliance program*' ha iniziato a divenire familiare per i penalisti, ben oltre il più ristretto novero degli specialisti della *corporate criminal liability*, e il ruolo che il legislatore ha inteso assegnarvi è alla base del carattere innovativo della soluzione progettata in Italia.

---

[1] Per una recente, articolata panoramica in materia v. *I nuovi volti del sistema penale fra cooperazione pubblico privato e meccanismi di integrazione fra* hard law *e* soft law, a cura di Gullo-Militello-Rafaraci, Milano, 2021.

[2] L'espressione di J. Coffee («The judo wrestler relies not on brute force, but rather turns his opponent own strenght against him») è ripresa da STELLA, *Criminalità d'impresa: lotta di sumo e lotta di judo*, in *Riv. trim. dir. pen. econ.*, 1998, 2-3, 471.

[3] V. MONGILLO, *Presente e futuro della* compliance *penale*, in *www.sistemapenale.it*, 11 gennaio 2022, 1 ss.

L'idea di un modello organizzativo che assolve a una funzione di esclusione della responsabilità dell'ente ma che, al contempo, laddove il fatto sia realizzato e la *societas* non sia per l'appunto *compliant*, interviene *ex post* con funzione riparatoria, è stata la linfa del 'decreto 231'. La logica di un modello 'supporto materiale' della colpa di organizzazione dell'ente[4], declinata nella prospettiva nostrana, ha consentito di andare oltre quella nordamericana di una valorizzazione del *compliance program* sul piano, in avvio, della sola commisurazione della pena e oggi quale tassello di una più articolata strategia volta a promuovere la collaborazione dell'ente (*cooperation* e *self-reporting*), in un orizzonte in cui si staglia, sullo sfondo, la tematica dei *settlements-agreements*[5].

E su questo fronte, quello del modello come perno dell'illecito dell'ente, rimangono fondamentali i contributi del Prof. Paliero[6] che qui onoriamo, il quale è stato subito in grado di delineare con sicurezza i tratti di questo innovativo meccanismo di imputazione della responsabilità e di metterne in luce le ragioni di compatibilità con il principio di colpevolezza.

L'espressione *compliance* ha iniziato a essere il mantello per dare copertura e legittimazione nel campo largo del diritto punitivo a concetti e approcci — *risk assessment*, *risk management*, procedimentalizzazione etc. —, destinati a successo, facendo anch'essi capolino in celebri decisioni della Cassazione[7].

Le fortune della *compliance* sono in seguito andate moltiplicandosi, dando origine a epifenomeni con cui il legislatore sarà chiamato a confrontarsi in sede di futura messa a punto della normativa.

Limitandosi qui a prendere in considerazione alcune linee di sviluppo della *compliance*, essa ha anzitutto seguito l'evoluzione, registratasi anche a livello

---

[4] V. PALIERO-PIERGALLINI, *La colpa di organizzazione*, in *Resp. amm. soc. ed enti*, 2006, 3, 170.

[5] V. per tutti, nell'oramai cospicua letteratura in materia, ARLEN, *The Potential Promise and Perils of Introducing Deferred Prosecution Agreements Outside the U.S.*, in *Negotiated Settlements in Bribery Cases: A Principled Approach*, a cura di Søreide-Makinwa, The Hague, 2020, 156 ss.

[6] V., oltre al contributo prima citato, *La società punita: del come, del perché, e del per cosa*, in *Riv. it. dir. proc. pen.*, 2008, 4, 1516 ss.; *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale*, in *Riv. trim. dir. pen. econ.*, 2018, 1-2, 175 ss.; voce *Colpa di organizzazione e persone giuridiche*, in *Reato colposo, Enciclopedia del Diritto*, diretto da Donini, Milano, 2021, 64 ss.

[7] Il riferimento è alle Sezioni Unite *ThyssenKrupp*, Cass., Sez. un., 18 settembre 2014, n. 38343.

internazionale, delle modalità di coinvolgimento dell'ente e di implementazione della strategia richiamata in apertura.
Si ha così:
— una *compliance* a 'trazione pubblica', in cui la struttura organizzativa dialoga con agenzie istituzionali di *enforcement*. L'esempio più evidente è quello dell'impianto prefigurato dalla legge anticorruzione del 2012, fondato sul piano nazionale quale riferimento dei piani triennali e su un ruolo centrale dell'Anac, a seconda dei casi, di indirizzo (determine, linee guida etc.), di controllo, o sanzionatorio;
— una *compliance* 'a trazione privata', nella quale la *soft law* domestica è appannaggio delle Associazioni di categoria e la vigilanza sul modello è affidata a un 'organismo interno all'ente dotato di autonomi poteri di iniziativa e controllo', ovverosia il noto Organismo di vigilanza;
— una *compliance* 'a trazione mista', in cui convivono, seppure solo per specifici settori, le due anime sopra illustrate — è questa l'architettura disegnata dalla *Loi Sapin II*, con l'Agenzia nazionale anticorruzione (*AFA*) che spazia dal settore pubblico a quello privato e, in qualche misura, quella dei sistemi che hanno adottato modalità di verifica di fonte pubblica dei modelli[8].
Si innesta su questo ceppo la *cooperative compliance* — argomento negli ultimi anni 'caldo' e arricchitosi di recente di interessanti innovazioni nel campo della lotta alla criminalità mafiosa —, nel cui ambito, oltre a ricadere i temi della 'messa alla prova' dell'ente[9], trovano collocazione i variegati strumenti che, con intensità e caratteristiche diverse, promuovono forme di collaborazione/interlocuzione con l'Autorità pubblica *ante delictum* volte a costruire percorsi condivisi di *compliance*[10].

---

[8] Ad esempio, nella legge peruviana che disciplina la responsabilità dell'ente (*Ley* n. 30424 del 2016), v. la valutazione tecnica del *modelo de prevención* da parte della *Superintendencia del Mercado de Valores*, con valore probatorio di perizia. In argomento, nel quadro di una articolata analisi dei modelli di validazione dei *compliance programs* in ottica comparata, v. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Torino, 2022.

[9] V., limitandosi ai lavori monografici, RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, Torino, 2018; FED. MAZZACUVA, *L'ente premiato. Il diritto punitivo nell'era delle negoziazioni: l'esperienza angloamericana e le prospettive di riforma*, Torino, 2020.

[10] Il riferimento è agli strumenti di "bonifica aziendale" di cui agli artt. 34 e 34-*bis* del d.lgs. n. 159 del

Su altro versante, la *compliance* continua a connotare le modalità attraverso cui l'ente traduce gli *input* normativi. La dicitura *cosmetic compliance*, diffusa nel dibattito statunitense e per tale via penetrata in quello italiano[11], identifica il fenomeno del modello, pur in teoria ben confezionato (e dunque *tailor made*), che risulti carente di effettiva traduzione nelle dinamiche operative dell'ente[12], secondo un approccio valutativo ben presente, ad esempio, nelle Linee guida del *Department of Justice* indirizzate ai *prosecutors.*

Chiudiamo infine questa rapida rassegna gettando lo sguardo su un'ultima accezione della *compliance* che negli ultimi tempi inizia a farsi largo nella riflessione in atto negli ordinamenti di importanti economie emergenti. Il riferimento è all'espressione *overcompliance*, che descrive il fenomeno distorsivo della artificiosa burocratizzazione della *compliance* frutto dell'influenza esercitata, in quei contesti, dalle *big corporations* sul decisore pubblico, quale potente strumento per tagliare fuori dal mercato *competitors* di più ridotte dimensioni, non in grado di ottemperare agli adempimenti richiesti (in una dimensione in cui, peraltro, l'ossequio reale a questi ultimi da parte dei 'promotori' di tale approccio si rivela di facciata)[13].

2011 (c.d. Codice Antimafia), alle misure di cui all'art. 32 del d.l. n. 90 del 2014, nonché da ultimo, in particolare, alla misura della c.d. prevenzione collaborativa (nuovo art. 94-*bis* Codice Antimafia, introdotto dal d.l. n. 152 del 2021) prevista come una sorta di '*probation*' disposta dal Prefetto nei confronti dell'ente in alternativa all'emissione dell'interdittiva antimafia (per un recente inquadramento, v. BIRRITTERI-TATÌ, *Cooperative Compliance Measures to Prevent Organised Crime Infiltrations and the Protection of the EU's Financial Interests. A New Gold Standard in the Implementation of the Italian Recovery and Resiliance Plan?*, in *Jean Monnet Network on EU Law Enforcement Working Paper Series*, No. 02/22; MAUGERI, *Prevenire il condizionamento criminale dell'economia: dal modello ablatorio al controllo terapeutico delle aziende*, in *Dir. pen. cont.*, 2022, 1, 106 ss.), nonché al c.d. *Tax Control Framework*, introdotto dal d.lgs. n. 128 del 2015 e adesso modificato, nell'ottica di un ampliamento del suo raggio di azione, dal d.m. 30 marzo 2022.

[11] V. LAUFER, *Corporate Liability, Risk Shifting, and the Paradox of Compliance*, in *Vanderbilt Law Rev.*, 1999, 52, 1344 ss.; ID., *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in *La responsabilità «penale» degli enti. Dieci proposte di riforma*, a cura di Centonze-Mantovani, Bologna, 2016, 11.

[12] Per ulteriori dettagli sia consentito rinviare a GULLO, *I modelli organizzativi*, in *Responsabilità da reato degli enti*, I, *Diritto sostanziale*, a cura di Lattanzi-Severino, Torino, 2020, 253 s.

[13] V. il contributo di FAGUNDES DE AZEVEDO-SAAD-DINIZ, *Overcompliance, Regulatory Policies and Environmental Crime*, in *Revue Internationale de Droit Pénal*, 1, 2020, 155 ss., fascicolo che raccoglie gli atti del VII Simposio dei Giovani penalisti dell'AIDP, svoltosi a Roma (11-12 novembre 2019).

Non proseguo oltre nell'illustrare le capacità di prestazione della parola *compliance* che, del resto, sono state da ultimo abilmente esplorate[14].
Sposterò qui l'attenzione su un fenomeno più di recente delineatosi e che comincia a essere oggetto di interesse da parte degli studiosi, che va sotto il nome di 'sistemi integrati di *compliance*'.
In questa sede non potrò affrontare *funditus* il tema, ma cercherò di illustrarne i tratti di fondo, facendo emergere le implicazioni sul piano della lettura del diritto positivo e su quello delle prospettive di riforma del decreto 231.

2. Compliance *231 e sistema di controllo interno: una integrazione naturale.*
La prima forma di integrazione cui intendo far riferimento è, a dire il vero, inscritta nel patrimonio genetico della normativa di settore e prima delle altre ha conquistato un suo posto tra gli studiosi della responsabilità degli enti. Alludo all'inserimento armonico dei presidi '231' nel sistema di controllo interno dell'ente; coabitazione, o meglio interazione fruttuosa che non a caso è stata sollecitata nell'ultima versione delle Linee Guida di Confindustria[15].
Ho prima accennato al fenomeno, che qui tuttavia merita qualche considerazione più distesa. Su questo terreno aggallano le venature della parola *compliance* che più guardano alla progettazione delle misure preventive e alla verifica della loro tenuta.
Il circuito virtuoso al quale dovrebbe ispirarsi l'ente è, questo sì, evincibile dalla lettura dell'art. 6, in combinato disposto con l'art. 7, del d.lgs. n. 231 del 2001. Se le previsioni in questione falliscono nel fornire indicazioni al soggetto collettivo sui contenuti dei presidi, esse delineano invece un percorso per la costruzione del modello; un itinerario che ha come sue tappe principali la mappatura dei rischi, la procedimentalizzazione, la tracciabilità dei flussi finanziari e la strutturazione di adeguati flussi informativi[16].
Si tratta di un lessico proprio degli esperti di *audit* e di controllo interno e che, in quegli ambiti, ha ricevuto una formalizzazione attraverso il c.d. *Coso*

[14] V. lo stimolante itinerario proposto da MONGILLO, *Presente e futuro*, cit., 1 ss.
[15] V. *Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231* del 25 giugno 2021.
[16] Volendo v. ancora il nostro *I modelli organizzativi*, cit., 254 ss.

Report il quale, significativamente, costituisce, almeno nelle imprese di medio-grandi dimensioni, la pietra angolare dell'architettura di controllo[17].
Il necessario approccio multidisciplinare ha consentito di sviluppare una visione della *compliance* così intesa, che ha come elementi centrali la valutazione dinamica dei rischi – avvalendosi della c.d. *gap analysis* –, un sistema articolato di *enterprise risk management* e dei successivi controlli (di primo, secondo e terzo livello), finendo con il diffondere un linguaggio comune tra giuristi, aziendalisti, esperti di controllo interno etc.
Un disegno complessivo che permette sia di tradurre nella prassi delle imprese in modo chiaro quanto meno la logica preventiva alla base della 231 sia, sul piano della elaborazione dei presidi, di costruire cautele che percorrono la struttura dell'ente, replicando le diverse cadenze appena richiamate[18]. Al contempo, esso consente di meglio intendere il ruolo dell'Organismo di vigilanza, il quale si staglia quale interlocutore privilegiato della funzione di *internal audit*, ove presente, e crocevia dei flussi informativi in punto di mitigazione del rischio e di verifica sul sistema di controllo interno; una figura che, letta attraverso questa lente, non risulta *attore* della gestione del rischio quanto piuttosto *controllore*, per i profili di propria competenza, dell'ordito organizzativo[19].
Infine, la prospettiva di analisi qui menzionata permette di sfatare un mito generato da una formalistica lettura dell'art. 6, ovverosia di chiedere al modello di impedire la commissione di reati del tipo di quello considerato. L'ambiguo concetto di idoneità del modello quale parametro sulla cui base

[17] V. BOZZOLAN-COSTANZO, Corporate governance*, sistemi di* risk management *e rischi di* compliance, in *La gestione della* compliance*. Sistemi normativi e controllo dei rischi*, a cura di Adotti-Bozzolan, Roma, 2020, 28 ss.
[18] Il richiamo è qui alla felice partizione tra cautele procedimentali, sostanziali e di controllo operata da PIERGALLINI, *I modelli organizzativi*, in *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001, n. 231*, a cura di Lattanzi, Milano, 2010, 188 s.
[19] V. VALENZANO, *L'illecito dell'ente da reato per l'omessa o insufficiente vigilanza. Tra modelli preventivi e omesso impedimento del reato*, Napoli, 2019, 24. In argomento, per una puntuale ricostruzione del ruolo dell'Organismo di vigilanza nel sistema di responsabilità da reato dell'ente, v. da ultimo Cass, Sez. VI, 15 giugno 2022, n. 23401 nella nota vicenda *Impregilo*, in *www.sistemapenale.it*, 20 giugno 2022. V. a commento della pronuncia PIERGALLINI, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda "Impregilo"*, in *www.sistemapenale.it*, 27 giugno 2022, 1 ss.; FUSCO-PALIERO, *L'*happy end *" di una saga giudiziaria: la colpa di organizzazione trova (forse) il suo tipo*, in *www.sistemapenale.it*, 27 settembre 2022, 1 ss.

saggiare le *chances* di esclusione della responsabilità dell'ente ha finito per essere di fatto inteso nel senso di azzeramento del rischio-reato. Eppure sappiamo bene, come anche autorevolmente ricordato, che il rischio zero non esiste[20] e — qui sono maestri i nordamericani — il fatto che il reato si sia realizzato non può di per sé certificare l'inidoneità del modello[21].
Come insegnano ancora una volta gli studiosi di controllo interno, la gestione del rischio è un processo misurabile con variabili — la propensione al rischio, il rischio tollerabile etc.[22] — calibrate su una prospettiva affatto diversa dalla (irrealistica) neutralizzazione del rischio.
Dovremmo dunque già da ora fare nostra questa chiave di lettura, incoraggiando nella ricostruzione teorica e nella prassi applicativa una interpretazione delle disposizioni sopra citate nel senso di doversi richiedere all'ente una riduzione significativa del rischio[23]; su questo aspetto bisognerebbe imparare dall'esperienza spagnola che, come noto, tributaria fortemente della nostra, ha saputo su tale specifico punto distaccarsi dall'impianto normativo italiano[24].

3. *Obblighi di* compliance *e obblighi 231: una combinazione su cui puntare in futuro?* Il secondo sistema di integrazione al quale desidero rivolgere l'attenzione è rappresentato dai casi, sempre più numerosi, in cui coesistono (per l'appunto si integrano o, forse meglio, dovrebbero integrarsi in ottica futura) obblighi di *compliance*, sottoposti in ipotesi di violazione ad autonoma

[20] V. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, 225. V. altresì SERENI, *L'ente guardiano. L'autorganizzazione del controllo penale*, Torino, 2016, 51, che opportunamente parla di eliminazione del 'rischio ragionevole'.
[21] V. le Linee Guida del *Department of Justice* sopra citate (§ 8B2.1(a)).
[22] Sul punto, anche per i necessari richiami, sia permesso rinviare al nostro *I modelli organizzativi*, cit., 256.
[23] Sul tema generale v. le chiare parole di MONGILLO, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 134 ss. e 425 ss. V. altresì le osservazioni adesso svolte da Cass., Sez. VI, 15 giugno 2022, n. 23401, cit., che parrebbe adottare un siffatto approccio, seppur con note che dischiudono possibili profili di problematicità: v. al riguardo PIERGALLINI, *Una sentenza "modello" della Cassazione*, cit., specie 4 ss.
[24] V. art. 31-*bis* del codice penale spagnolo. Da ultimo, suggerisce di rendere esplicito lo standard di validazione dei modelli organizzativi nel decreto 231, in termini di riduzione significativa del rischio di verificazione del reato, SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi*, cit., 320 s.

sanzione amministrativa, e obblighi di prevenzione di reati presupposto *ex* d.lgs. n. 231 del 2001.

Su questo versante l'analisi guarda all'assetto vigente ma si presenta particolarmente stimolante se ci proiettiamo verso scenari futuri di disciplina.

L'attualità non manca di segnalare obblighi di *compliance* oggetto di specifica sanzione: la normativa anticorruzione contempla una sanzione amministrativa per il responsabile della trasparenza e della prevenzione della corruzione che non abbia adottato il piano; prevede altresì una risposta analoga nel settore del *whistleblowing* in presenza della mancata predisposizione di procedure per la gestione delle segnalazioni oppure di mancata attivazione di dette procedure[25]. Allo stesso modo l'oramai celebre GDPR — e qui ci avviciniamo peraltro ad ambiti in cui, solo per mutamenti dell'ultima ora degli indirizzi di politica legislativa, non siamo dinanzi a reati 231[26] — non manca di rendere destinatario anche l'ente (che anzi sembra essere il naturale interlocutore del legislatore eurounitario) di numerosi obblighi di *compliance* presidiati da sanzioni la cui afflittività ha condotto i primi commentatori a 'denunciarne' subito la natura sostanzialmente penale[27].

I più recenti interventi nel campo della sicurezza nazionale cibernetica costituiscono invece un primo esempio in cui, accanto a una nutrita serie di obblighi di *compliance* di vario genere finalizzati all'adozione da parte dei destinatari della disciplina (in primo luogo infrastrutture critiche) di idonee misure tecniche[28], è stata introdotta la responsabilità dell'ente rispetto a una specifica figura di delitto di ostacolo.

---

[25] Art. 54-*bis* del d.lgs. n. 165/2001, come novellato dalla l. n. 179/2017. Sul punto, v. GULLO, *L'interesse pubblico come giusta causa della rivelazione nei delitti in materia di segreto*, in Whistleblowing *e prevenzione dell'illegalità (Atti del I Convegno annuale del Dipartimento di Scienze giuridiche C. Beccaria dell'Università degli Studi di Milano)*, a cura di Della Bella-Zorzetto, Milano, 2020, 269.

[26] Emblematica la circostanza che la rubrica dell'art. 24-*bis* menzioni l'illecito trattamento dei dati personali, sebbene, come noto, all'interno della norma sia stato alla fine espunto il richiamo alla relativa disposizione del codice della *privacy*.

[27] V. artt. 82 e 83 del Regolamento 2016/679/UE. Per un commento, già all'indomani della riforma, in cui emergono bene i profili segnalati nel testo, v. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Arch. pen.*, 2019, 1, 51 ss.; MANES-MAZZACUVA, *GDPR e nuove disposizioni penali del Codice "privacy"*, in *Dir. pen. proc.*, 2019, 2, 176 ss.

[28] Per una rassegna di tali disposizioni v. MELE, *Il Perimetro di Sicurezza Nazionale Cibernetica*, in *Dir. Internet*, 2020, 1, 15 ss.; v. altresì PICOTTI, Cybersecurity: quid novi?, *ivi*, 13 s.

Si è dunque in presenza, o si potrebbe essere in presenza prossimamente, di una *compliance* cogente per l'ente, con meccanismi di controllo e sanzionatori in 'mano pubblica' (nei casi prima prospettati, rispettivamente, Autorità Garante dei dati personali e, dopo le ultime modifiche normative[29], Agenzia per la sicurezza cibernetica nazionale) e focalizzata sulla gestione di un astratto rischio, per rifarsi ai casi considerati, *privacy* o *cyber*, e di una *compliance* su base volontaristica[30], in cui si torna alle consuete dinamiche '231' con autonormazione e controllo dell'Organismo di vigilanza, e in cui il fuoco della prevenzione è uno dei reati presupposto, pur secondo le maglie ampie proprie della logica della responsabilità dell'ente.

Vengo adesso agli orizzonti futuri che iniziano a dischiudere interessanti prospettive di utilizzo di questo tipo di sistemi integrati di *compliance*.

L'area di riferimento è quella della *corporate social responsibility* su cui, come noto, esiste una pluridecennale letteratura aziendalistica ma che, in tempi recenti, ha attirato l'attenzione del giurista nell'ambito del più esteso capitolo della 'sostenibilità'.

Il protagonista da questo angolo visuale è il gruppo multinazionale, e il tema al centro dell'attenzione diviene quello delle dinamiche tra impresa madre e società figlie nella predisposizione di misure a protezione dei diritti umani[31].

La *human rights due diligence* si è infatti progressivamente imposta nei diversi fori internazionali tradizionalmente sensibili alla lotta a fenomeni criminosi connessi all'attività d'impresa (un esempio sono le Linee Guida OCSE destinate alle imprese multinazionali) e ha permeato la strategia degli ultimi anni delle Nazioni Unite in materia di promozione del coinvolgimento delle grandi *corporations* nella diffusione di una cultura della *compliance*, iniziando poi a far breccia nella legislazione di diversi Paesi.

Innumerevoli sono gli esempi più o meno recenti in cui gli ordinamenti hanno cominciato a occuparsi *ex professo* di questi temi, spingendo le imprese a

---

[29] V. l. istitutiva dell'ACN n. 109/2021, di conversione del d.l. n. 82 del 2021.

[30] Per i concetti di *compliance* cogente e volontaristica v. ancora MONGILLO, *Presente e futuro*, cit., 7.

[31] Sul tema, per un affresco generale, v. gli atti del XX AIDP International Congress of Penal Law, tenutosi a Roma (13-16 novembre 2019) pubblicati nella sezione "*Corporate Liability, Business Integrity and Human Rights Protection*" della *Revue Internationale de Droit Pénal*, 2021, 2, nonché quelli raccolti nella *Special Issue* di *European Criminal Law Review*, 2021, 1.

rivelare le loro politiche di settore: il *California Transparency in Supply Chains Act*, il *Modern Slavery Act* britannico e la Direttiva 2014/95/UE sulle informazioni di carattere non finanziario – implementata in Italia con il d.lgs. n. 254 del 2016 – sono altrettanti punti di emersione del fenomeno qui cursoriamente descritto.

Si è trattato in avvio di un approccio *soft* fondato sul modello *comply or explain* che, anche rispetto agli enti obbligati alla presentazione di siffatti *statements*[32], ha condotto, se si guarda all'esperienza straniera, a forme anche qui, in un certo senso, di *compliance* cosmetica.

Ultimamente si assiste tuttavia a un fermento riformatore a livello sia di singoli Stati, ove si affacciano corpi normativi ispirati piuttosto alla *mandatory due diligence* – emblematiche la nota *Loi sur le devoir de vigilance* del 2017 che, pur andata incontro a censure del *Conseil Constitutionnel*[33], ha rappresentato la prima punta avanzata di tutela, e la recente *Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten* –, sia di legislazione eurounitaria, in cui si assiste alla revisione della direttiva UE prima richiamata, significativamente dedicata in prospettiva alla sostenibilità, nonché alla presentazione di una proposta di direttiva sulla *corporate sustainability due diligence*.

Le indicazioni che emergono sono quelle di un intervento indirizzato a imprese con determinate caratteristiche dimensionali; della previsione di obblighi in capo alla controllante di presidiare la *supply chain*; dell'impiego di (in-

[32] Nel nostro sistema, ai sensi del d.lgs. n. 254 del 2016, risultano obbligati alla presentazione della dichiarazione di carattere non finanziario gli enti di interesse pubblico qualora abbiano avuto, in media, durante l'esercizio finanziario un numero di dipendenti superiore a cinquecento e, alla data di chiusura del bilancio, abbiano superato almeno uno dei due limiti dimensionali prescritti (totale dello stato patrimoniale superiore a venti milioni di euro; totale dei ricavi netti delle vendite e delle prestazioni superiore a quaranta milioni di euro). Gli enti di interesse pubblico che siano società madri di un gruppo di grandi dimensioni sono tenuti alla redazione della dichiarazione finanziaria consolidata.

[33] V. *Décision n. 2017-750 DC du 23 mars 2017*, con cui il *Conseil Constitutionnel* ha ritenuto carente di precisione la disposizione che sanciva il perimetro dei nuovi obblighi di vigilanza, rilevando nella specie il carattere punitivo dell'*amende* (fino a dieci milioni di euro) originariamente prevista – pur sottolineando che il legislatore è libero di assoggettare le società rientranti nel campo di applicazione della *Loi sur le devoir de vigilance* a obblighi diversi, con l'obiettivo di promuovere il rispetto, da parte di dette società e dei loro partner commerciali, di differenti diritti e libertà. Per un inquadramento v. SABIA, *The Accountability of Multinational Companies for Human Rights Violations. Regulatory Trends and New Punitive Approaches Across Europe*, in *European Criminal Law Review*, cit., 48 ss.

cisive) sanzioni civili o amministrative; della coesistenza di siffatti obblighi con l'impianto di responsabilità criminale degli enti.
Si tratta di un processo di traduzione normativa degli obblighi in discorso non semplice — l'esperienza francese ne è chiara testimonianza —, ma che potrebbe dar vita a un interessante sistema in grado di differenziare il piano della costruzione a livello di gruppo di una *compliance* proiettata sulla protezione dei diritti umani da quello della prevenzione del singolo reato. Sul primo versante, una volta selezionati i destinatari — e le normative in questione ci dicono di far riferimento a imprese con certe caratteristiche —, gli obblighi investirebbero direttamente la capogruppo e potrebbero essere oggetto di *enforcement* da parte di Agenzie *ad hoc*; sul secondo versante, continuerebbe, se guardiamo al nostro ordinamento, a trovare applicazione la disciplina 231 — in questo caso dovremmo trovarci spesso alle prese con ipotesi di applicazione extraterritoriale della normativa — sulla scorta del modello sperimentato in giurisprudenza che alla fine propone soluzioni equilibrate e in grado di evitare automatiche risalite di responsabilità[34].
Sono scenari non futuribili, viste le iniziative legislative attuate altrove o in atto a livello UE, che richiederanno tra l'altro di individuare meccanismi tali da scongiurare rischi di duplicazioni sanzionatorie e che potrebbero agevolare la riflessione da tempo esistente riguardo alla struttura dell'illecito dell'ente[35].

4. Digital Criminal Compliance*: verso nuovi orizzonti della responsabilità da reato degli enti?* L'ultima modalità di integrazione di cui mi occupo punta dritto al futuro — anche se già adesso vi sono profili di emersione del fenomeno all'interno delle imprese — e si riferisce all'impiego delle nuove tecnologie nella *compliance* preventiva di cui si è discusso: la parola *compliance* qui si presenta nella sua versione '*digital*'.

---

[34] V. SCAROINA, *Verso una responsabilizzazione del gruppo di imprese multinazionale?*, in *Dir. pen. cont.*, 2018, 2, 75 ss.; PIERGALLINI, *Globalizzazione dell'economia, rischio-reato e responsabilità* ex crimine *delle multinazionali*, in *Riv. trim. dir. pen. econ.*, 2020, 1-2, 158 ss.
[35] V. PALIERO, *La società punita*, cit., 1531 ss.; DE VERO, *Il nesso causale e il diritto penale del rischio*, in *Riv. it dir. proc. pen.*, 2016, 2, 696 s.; DI GIOVINE, *Il criterio di imputazione soggettiva*, in *Responsabilità da reato degli enti*, cit., 224 ss.

Il riferimento immediato è agli algoritmi di intelligenza artificiale che anche nel campo in esame stanno conquistando l'attenzione degli studiosi[36]. Negli ultimi tempi però si è arricchito il novero degli strumenti in teoria utilizzabili e l'attenzione si sta indirizzando anche verso *blockchain* e *smart contracts*.

La ragione alla base dell'interesse verso i menzionati strumenti è di facile intuizione: i punti cardinali della *compliance* sono qui rappresentati da dati, flussi finanziari, informazioni. Se dunque un modello che si candidi all'idoneità deve assicurare un adeguato processamento dei dati, un'affidabile tracciabilità dei flussi finanziari e un efficiente circuito informativo, i 'ritrovati' tecnologici si rivelano piuttosto efficaci per il perseguimento dei fini in questione.

La capacità degli algoritmi di *machine learning* di elaborare una mole enorme di dati (i c.d. *big data*) in spazi temporali davvero ridotti apre la strada a forme di controllo in passato impensabili: verifiche massive su *mail* dei dipendenti dell'impresa, analisi di interi comparti documentali e ricerca di eventuali comportamenti anomali, verifica degli adempimenti e *report* in *real time* al *top management* (ma anche agli organi di controllo) circa indicatori di allarme (c.d. *red flags*), accurata *due diligence* delle terze parti anche attraverso l'*intelligence* su fonti aperte, sono solo alcune delle prestazioni che l'intelligenza artificiale può garantire[37].

Tutto ciò secondo modalità che potrebbero accomunare tanto il settore privato quanto il settore pubblico dove, per effetto anche della più recente norma-

[36] Pare sufficiente rilevare il numero dei contributi di recente pubblicati nella dottrina italiana, nel quadro di una letteratura più frastagliata oltreoceano: v. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Dir. pen. cont.*, 2019, 2, 289 ss.; SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, in *Dimensione tecnologica e prova penale*, a cura di Lupària-Marafioti-Paolozzi, Torino, 2019, 217 ss.; NISCO, *Riflessi della* compliance *digitale in ambito 231*, in *www.sistemapenale.it*, 14 marzo 2022, 1 ss.; MORGANTE-FIORINELLI, *Promesse e rischi della* compliance *penale digitalizzata*, in *Arch. pen.*, 2022, 2, 1 ss. Nel dibattito internazionale v. LAUFER, *The Missing Account of Progressive Corporate Criminal Law*, in *New York University Journal of Law & Business*, 2017, 14, 71 ss.; DIAMANTIS, *The Extended Corporate Mind: When Corporations Use AI to Break the Law*, in *North Carolina Law Review*, 2019, 98, 893 ss.; BURCHARD, *Digital Criminal Compliance*, in *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70*, vol. II, a cura di Engelhart-Kudlich-Vogel, Berlin, 2021, 741 ss.

[37] Più nel dettaglio v. BIRRITTERI, Big Data Analytics, cit., 290 s.

tiva in tema di obblighi di trasparenza, l'amministrazione ha notevolmente ampliato il proprio patrimonio di dati.

Su questa trama si inserisce la *blockchain* che può concorrere, grazie alla sua capacità di permettere la tracciabilità dell'operazione e la immodificabilità del dato, a irrobustire la *compliance* preventiva edificata dall'ente.

Gli impieghi recenti della *blockchain*, guardando ad ambiti di nostro interesse, nel settore degli appalti e della destinazione di fondi pubblici, confermano le potenzialità dello strumento.

La proposta avanzata è quella della costruzione di una *blockchain* privata con un governo centrale (c.d. *permissioned*), identificato nell'organo gestorio, e diversi nodi collocati nella struttura organizzativa (coincidenti anche con organi di controllo: ad esempio Collegio sindacale e Organismo di vigilanza), secondo un'architettura che consenta a ogni nodo di scrivere informazioni sul registro e preveda la necessità del consenso di tutti i nodi per la modifica e/o cancellazione del dato[38].

Immediato accesso alle informazioni, dislocazione di 'radar' più affidabili lungo la dorsale organizzativa dell'ente, conservazione del dato (con ovvi corollari in punto di ricostruzione di possibili violazioni e, in prospettiva, di *self-reporting* dell'ente) diventerebbero altrettanti punti di forza legati al ricorso a siffatto strumento.

Infine, l'integrazione potrebbe spingersi sino a implementare sistemi di controllo che utilizzino sinergicamente algoritmi di intelligenza artificiale (o addirittura di *machine learning*), *blockchain* e *smart contracts*[39], ovverosia contratti che, al ricorrere delle condizioni scritte nel codice, sarebbero suscettibili di esecuzione automatica (con l'effetto dunque che l'ente potrebbe affidare a

[38] V. GULLO, *I modelli organizzativi*, cit., 287; LETIZI-SOANA, *Le potenzialità del modello di* corporate compliance *integrato basato sulla tecnologia* Blockchain, in *Norme e Tributi Plus, www.ilsoleole24ore.com*, 21 dicembre 2020; nella letteratura in lingua inglese, v. ANJUM-SPORNY-SILL, *Blockchain Standards for Compliance and Trust*, in *IEEE Cloud Computing*, 2017, 4, 84 ss.; TRELEAVEN-B. BATRINCA, *Algorithmic Regulation: Automating Financial Compliance Monitoring and Regulation Using AI and Blockchain*, in *The Capco Institute Journal of Financial Transformation*, 2017, 4, 15 ss.

[39] Sul diverso versante, invece, dei rischi legati, in una prospettiva patologica, all'impiego di tali tecnologie per la commissione di reati, v. la relazione di ACCINNI, *L'utilizzo criminogeno della* blockchain: *gli* smart contract, tenuta in occasione del convegno *I profili penalistici dei* cryptoassets *tra diritto sostanziale e processuale*, svoltosi presso l'Università Luiss Guido Carli in data 3 maggio 2022.

queste tipologie contrattuali la realizzazione di una pluralità di operazioni societarie).

Ed è per l'appunto l'automazione della *compliance* che si realizzerebbe in tal modo, assicurando anzitutto prestazioni del sistema di controllo in punto di rapidità e 'accorciamento' delle linee sino a poco tempo fa non ipotizzabili, nonché rafforzando la capacità di intervento e gestione delle 'situazioni di crisi'.

Come si sa, però, non è tutto oro quello che luccica. Non manca infatti, come efficacemente rilevato, un lato oscuro della *compliance* digitale così raffigurata.

Dovendo qui ridurre all'osso gli aspetti da segnalare, il primo è, come intuibile, quello del controllo occulto dei lavoratori.

Su questo profilo si registrano già interessanti contributi che hanno iniziato ad ammonire sull'esigenza di rispettare i vincoli posti dalla normativa di settore e dai principi elaborati dalla Corte Edu in materia, a partire in primo luogo dal *leading case López Ribalda*[40].

Il secondo aspetto è, se vogliamo, preliminare e ha a che vedere con la qualità dei dati. Tema che si pone probabilmente in modo ancora più stringente nella Pubblica Amministrazione ma che esiste anche nel settore privato, già solo per eliminare i *bias* che un utilizzo indiscriminato dei dati può alimentare[41].

Venendo adesso a questioni più attinenti alla struttura della responsabilità dell'ente, uno scenario quale quello prospettato potrebbe portare in futuro a rivedere il ruolo dell'Organismo di vigilanza e, a monte, lo stesso obiettivo richiesto all'ente: ancora, come si sottolineava, quello di una realistica riduzione significativa del rischio, oppure le nuove tecnologie di cui si discute potranno condurre davvero a un azzeramento, almeno in certi settori, del rischio?

---

[40] Sul piano normativo a venire in rilievo è l'art. 4 dello Statuto dei lavoratori: v. BIRRITTERI, *Controllo a distanza del lavoratore e rischio penale*, in *www.sistemapenale.it*, 16 febbraio 2021; NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, *www.sistemapenale.it*, 20 dicembre 2021, 1 ss.

[41] V. ancora BIRRITTERI, Big Data Analytics, cit., 292.

Così pure si ripropone il tema legato ai costi di una siffatta *compliance* che, se non limitata a enti con certe caratteristiche, finirebbe per richiedere a numerose imprese condotte inesigibili.

E ancora il problema già avanzato in dottrina di possibili reati presupposto la cui integrazione risulti agevolata dal cattivo funzionamento dell'algoritmo: chi sarà in questi casi chiamato a rispondere?[42]

Tanti sono dunque gli interrogativi, come sempre accade nei differenti ambiti di impiego di queste tecnologie; domande alle quali al momento non è facile dare una risposta univoca.

Vi sono però, accanto a quelle prima richiamate, ulteriori opportunità che già sono state messe in evidenza: il ricorso all'intelligenza artificiale risulterebbe prezioso allorché, come accade in contesti quali quello ambientale, la *compliance* dell'ente passa dall'osservanza di parametri tecnici e soglie quantitative[43].

Allo stesso modo, i menzionati strumenti rivelano tutte le loro potenzialità nel campo, ancora da esplorare compiutamente, delle *internal investigations*[44], prodromiche a un'eventuale collaborazione con l'Autorità giudiziaria.

Inoltre, sul piano della valutazione giudiziale del modello, l'impiego dell'AI potrebbe candidarsi, almeno in certi settori, a integrare quelle *best practices* condivise in grado di legittimare una presunzione relativa vincibile dal giudice con motivazione rafforzata[45].

Insomma, un terreno da arare e sicuramente promettente dove però — e anche questo sta diventando un *leitmotiv* quando ci misuriamo con questioni in cui sullo sfondo si staglia la tutela di rilevanti interessi degli individui coinvolti

---

[42] SABIA, *Artificial Intelligence and Environmental Criminal Compliance*, in *Revue Internationale de Droit Pénal*, 2020, 1,186 ss.

[43] Sul punto v. SABIA, *Artificial Intelligence and Environmental Criminal Compliance*, cit., 192 e 196.

[44] NISCO, *Riflessi della* compliance *digitale in ambito 231*, cit., 8. Più in generale sulle fasi operative di una indagine interna, anche avuto riguardo ai meccanismi di *data analytics*, v. FORTUNATO, *La prassi di* internal investigation, in Internal Investigations. Best practices *e istanze di regolamentazione*, a cura di Centonze-Giavazzi, Torino, 2021, 161 ss.

[45] Il riferimento è alla tesi di PIERGALLINI, *Premialità e non punibilità nel sistema della responsabilità degli enti*, in *Dir. pen. proc.*, 2019, 4, 536. Per una applicazione al campo qui esplorato v. D'AGOSTINO, *Relazione finale alle attività di ricerca* nell'ambito del progetto "Go For It" della Fondazione Crui, dal titolo *Criminal Compliance and New Technologies*, nonché BIRRITTERI, Big Data Analytics, cit., 297 s.

– le soluzioni da ricercare dovranno avere come bussola costante il rispetto dei diritti fondamentali della persona.