GAETANA MORGANTE, GAIA FIORINELLI

Promesse e rischi della *compliance* penale digitalizzata*

La «digitalizzazione del mondo» che contraddistingue l'era contemporanea prospetta (*promette*, a detta di alcuni; *minaccia*, a detta di altri) anche per il diritto penale profonde trasformazioni: tra queste, è ora particolarmente vivace il dibattito sulle potenzialità (e i rischi) della c.d. «*compliance* digitale», ovverosia sul possibile impiego di nuove tecnologie (ad esempio: intelligenza artificiale, *blockchain* o *big data analytics*) da parte di società ed enti per la gestione dei propri processi interni ed esterni di "conformità normativa". Con il presente contributo, le Autrici intendono esplorare, nella prima parte, le "promesse" della digitalizzazione dei *compliance programs*, utilizzando quale banco di prova il d. lgs. 231/2001, per poi estendere lo sguardo *oltre* i modelli di prevenzione del rischio-reato. Nella seconda parte, invece, l'analisi si concentra sui rischi connessi alla *compliance* digitalizzata, quale strumento di *predictive policing* privato. Le riflessioni conclusive intendono, infine, mettere in luce i diversi piani d'intersezione – a livello di politiche globali ed europee – tra la nozione di «sostenibilità» e le prospettive della transizione digitale della *compliance*.

Promises and risks of technology-based compliance

The «digitalization of the world» characterizing the contemporary era envisages (promises, according to some; threatens, according to others) significant transformations also for criminal law: among these, there is now a lively debate on the potentials (and risks) of the so-called «digital compliance», i.e. of the possible use of new technologies (for example: artificial intelligence, blockchain or big data analytics) by companies and organizations for the management of their internal and external processes of regulatory compliance. The aim of this paper is thus to explore, in the first part, the 'promises' of the digitalization of compliance programs, using as a case study the model of criminal compliance outlined by the Italian decree n. 231/2001, and then extend the research to other models of compliance. In the second part, on the other hand, the analysis focuses on the risks connected with technology-based compliance programs, as tools for private predictive policing. Eventually, the final reflections intend to highlight the different intersection levels - at both a global and European policy level - between the category of 'sustainability' and the prospects of such a digital shift in the field of compliance programs.

* Benché il lavoro nel suo complesso sia frutto di riflessioni condivise tra le Autrici, i par. 1 e 5 sono da attribuire alla prof.ssa Gaetana Morgante e i par. 2, 3 e 4 sono da attribuire alla dott.ssa Gaia Fiorinelli.

tenzialità della *compliance* digitalizzata entro e oltre il d. lgs. 231/2001. - 3. I rischi della *compliance* digitalizzata. - 3.1. Il *predictive policing* aziendale tra protezione dei dati e tutela dei lavoratori. - 3.2. Il modello organizzativo digitalizzato quale oggetto di regolazione: spunti dall'*AI Act*. - 3.3. *Compliance* digitalizzata e teoria delle organizzazioni: dalla metafora meccanicistica alla cultura dell'integrità - 4. Profili di sostenibilità nella transizione digitale della *compliance*. – 5. Riflessioni conclusive: dalla conformità alla conformazione tecnologica dei comportamenti? Verso l'intersezione tra auto-normazione e digitalizzazione.

1. *Premessa: la «digitalizzazione del mondo» e la* compliance *digitale.* La «digitalizzazione del mondo»[1] che contraddistingue l'era contemporanea prospetta (*promette*, a detta di alcuni; *minaccia*, a detta di altri[2]) anche per il diritto penale profonde trasformazioni: tra queste, è ora particolarmente vivace il dibattito sulle potenzialità (e i rischi) della c.d. «*compliance* digitale»[3], ovverosia sul possibile impiego di nuove tecnologie (ad esempio: intelligenza artifi-

[1] In questi termini, cfr. FERRARESE, *Presentazione dell'edizione italiana* di GARAPON-LASSEGUE, *La giustizia digitale*, Bologna, 2021, 11.

[2] Cfr. ad es. GARAPON-LASSEGUE, *La giustizia digitale*, cit., 27, nel senso che le posizioni sull'argomento si dividono essenzialmente in due categorie: la prima include quanti sono entusiasticamente «orientat[i] verso le innovazioni in corso», la seconda invece annovera coloro che piuttosto «si preoccupano degli sconvolgimenti» che rischiano di derivarne.

[3] In dottrina, cfr. ad es. NISCO, *Riflessi della* compliance *digitale in ambito 231*, in *www.sistemapenale.it*, 14 marzo 2022; PREZIOSI, *Responsabilità da reato degli enti e intelligenza artificiale*, in *La responsabilità amministrativa delle società e degli enti*, 2020, 4, 173-179; SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, in *Dimensione tecnologica e prova penale*, a cura di Luparia-Marafioti-Paolozzi, Torino, 2019, 217 ss., che richiama la dicitura di «*e-compliance*»; VIANELLI-VALENTI, *RegTech e Modelli 231: uno sguardo al futuro per un'esigenza presente,* in *Giurisprudenza Penale Web*, 2021, 1-*bis*, 96-110; BURCHARD, *Digital criminal compliance*, in *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber zum 70. Geburtstag*, a cura di Engelhart-Kudlich-Vogel, Berlin, 2021, 741 ss. Cfr. anche EY, *Integrity in the Spotlight. The future of compliance. 15th Global Fraud Survey,* in *www.assets.ey.com*, 2018, in part. 23, che include tra le prospettive future della *compliance* la digitalizzazione, la proliferazione di strumenti di monitoraggio e prevenzione basati sulla *data analytics*, sulle capacità predittive dei *big data*, sull'individualizzazione delle soluzioni resa possibile dall'intelligenza artificiale. Ancora, cfr. PWC, *Re-inventing internal controls in the digital age*, in *www.pwc.com*, aprile 2019.

ciale, *blockchain* o *big data analytics*)[4] da parte di società e altri enti per la gestione dei propri processi interni ed esterni di "conformità normativa"[5].
Lungi dall'avere una dimensione meramente speculativa o ipotetica, la riflessione su questo tema è resa urgente dalla circostanza che il ricorso a modalità "digitali" per l'adempimento di obblighi di *compliance* sia talora raccomandato dalle stesse autorità di settore[6]: per citare un esempio, nel PNA 2019 l'ANAC ha suggerito che il monitoraggio sull'attuazione delle misure anticorruzione, adottate nell'ambito dei Piani Triennali di Prevenzione della Corruzione e della Trasparenza, possa essere attuato da parte delle singole amministrazioni «mediante sistemi informatici che consentano la tracciabilità del processo e la verifica immediata dello stato di avanzamento»[7]. Analogamente, il ricorso a «modalità informatiche» o a «strumenti di crittografia» è prescritto nell'ambito della disciplina del *whistleblowing* – tanto nel settore pubblico, quanto nel settore privato[8] – quale necessario presidio a garanzia della riserva-

[4] In proposito, cfr. ad es. RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, Milano, 2022. Si tratta di tecnologie basate ora su un «quadro epistemologico di ordine statistico», ora invece sul «determinismo» reso possibile dalla «crittologia», per cui cfr. GARAPON-LASSEGUE, *La giustizia digitale*, cit., 117. Più nel dettaglio, cfr. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, in *Rechtshandbuch Legal Tech*, a cura di Breidenbach-Glatz, München, 2018, 137 ss. e in part. 143, nel senso che la nozione di «*digital compliance*» ricomprende le diverse risorse del c.d. *legal tech* (*big data, machine learning,* etc.), integrate nel sistema aziendale di «*compliance-management*».

[5] Come rileva NISCO, *Riflessi della* compliance *digitale in ambito 231*, cit., 1, la questione dell'applicazione di «tecnologie emergenti ai sistemi di *compliance*» si pone non (sol)tanto per il suo potenziale impatto pratico, ma anche e soprattutto per il suo presumibile impatto teorico. Essenziale e pionieristico sul tema è lo scritto di BAMBERGER, *Technologies of Compliance: Risk and Regulation in a Digital Age*, in *Texas Law Review*, 2010, 88, 4, 669-739, che appunto analizza «*the automation of compliance with laws mandating risk management*».

[6] Sottolinea BAMBERGER, *Technologies of Compliance*, cit., 685, come tale «*turn to technology*» sia ormai reso vieppiù necessario dall'aumento del volume dei dati da analizzare, dalla sempre maggiore complessità delle transazioni, dall'incremento dei requisiti di *compliance* e di *reporting*, in misura tale da rendere i controlli "manuali" e "verticali" del tutto inadatti a tenere il ritmo con i crescenti oneri di *compliance* e con i crescenti livelli di rischio.

[7] Cfr. *Piano Nazionale Anticorruzione 2019*, Delibera n. 1064 del 13 novembre 2019, reperibile in *www.anticorruzione.it*.

[8] Cfr. gli art. 1 e 2 della l. 30 novembre 2017, n. 179, che hanno rispettivamente modificato l'art. 54-*bis* del d. lgs. 165/2001, disciplinando il *whistleblowing* del dipendente pubblico, e l'art. 6 del d.lgs. 231/2001, invece relativo alla tutela del dipendente che segnala illeciti nel settore privato. Al riguardo, si deve inoltre segnalare come la Direttiva UE 2019/1937 «riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione» - non ancora recepita nell'ordinamento italiano - preveda per il futuro l'applicazione generalizzata della disciplina del *whistleblowing* a tutte le imprese con più di 50 dipendenti, indipendentemente dall'adozione o meno del modello organizzativo "231"; la Direttiva

tezza circa l'identità del segnalante e il contenuto della segnalazione. Ancora, per volgere lo sguardo al di fuori dell'ordinamento italiano, la *Bank of England* e la *Financial Conduct Authority* stanno promuovendo nel Regno Unito lo sviluppo del c.d. «*Digital regulatory reporting*» (ovverosia, la digitalizzazione delle attività di *reporting* da parte delle società vigilate), sul presupposto che una nuova vigilanza *data-driven* possa allo stesso tempo alleggerire gli oneri di *compliance* per le società e rendere più efficienti i controlli da parte delle autorità[9].

Le questioni che derivano da una simile "incursione" delle tecnologie digitali nel settore della *compliance*[10], *lato sensu* inteso, sono – come si può ben immaginare – molteplici. In primo piano, emerge sicuramente l'esigenza di comprendere se e a quali condizioni un modello di *compliance* "digitale" (vale a dire, ad esempio, l'utilizzo da parte di una società di procedure o protocolli informatizzati, ovvero di strumenti digitali di tracciamento e monitorag-

---

precisa, inoltre, che i canali di segnalazione (interni) debbano essere «progettati, realizzati e gestiti in modo sicuro e tale da garantire la riservatezza dell'identità della persona segnalante» e che i canali di segnalazione (esterni) debbano analogamente essere «progettati, stabiliti e gestiti in modo da garantire la completezza, l'integrità e la riservatezza delle informazioni», così saldando la disciplina del *whistleblowing* alla tutela dei dati personali e alla *cybersecurity*, per cui cfr. BINCOLETTO, *Whistleblowing Application: Italian DPA Sanctions Non-Compliance with GDPR Principles*, in *European Data Protection Law Review*, 2021, 3, 429-434.

[9] Cfr. BANK OF ENGLAND, *What is regtech and why is it needed?*, in *www.bankofengland.co.uk*, 2021, nonché FINANCIAL CONDUCT AUTHORITY, *Digital regulatory reporting*, in *www.fca.org.uk*, 2020. Sul punto, cfr. anche EUROPEAN BANKING AUTHORITY, *EBA analysis of RegTech in the EU financial sector,* in *www.eba.europa.eu*, giugno 2021, nonché l'analisi di MICHELER-WHALEY, *Regulatory technology: replacing law with computer code*, in *European Business Organization Law Review*, 2020, 21, 349-377; BUTLER-O' BRIEN, *Understanding RegTech for Digital Regulatory Compliance*, in *Disrupting Finance. FinTech and Strategy in the 21st Century*, a cura di Lynn-Mooney-Rosati-Cummins, Cham, 2019, 85 ss.

[10] Giova precisare come, nel presente contributo, con la nozione di *compliance* si alluda, in senso ampio, a quel «vasto e composito universo» di «sistemi gestionali e protocolli decisionali» adottati dagli enti (*in primis* società ed enti privati, ma è recente la progressiva diffusione di modelli di *compliance* anche alle pubbliche amministrazioni) allo scopo di assicurare *dall'interno* il rispetto dei precetti e la prevenzione degli illeciti nell'ambito dell'attività aziendale: in tal senso, cfr. MONGILLO, *Presente e futuro della* compliance *penale*, in *www.sistemapenale.it*, 11 gennaio 2022. La *compliance* penale (da identificarsi, nell'ordinamento italiano, con il sistema della responsabilità amministrativa da reato degli enti) rappresenta perciò soltanto una delle possibili declinazioni del modello della *compliance* in senso ampio. In argomento, cfr. anche PRESTI, *What We Talk About When We Talk About Compliance*, in *Corporate Compliance on a Global Scale*, a cura di Manacorda-Centonze, Cham, 2022, 25 ss., che definisce la nozione di *compliance* in funzione del *particolare* tipo di rischio che essa presidia: «*the risk of incurring judicial or administrative sanctions, significant financial losses, or reputational damage as a consequence of violations of mandatory rules (laws of regulations) or self-regulatory rules*».

gio dell'attività aziendale) possa soddisfare i requisiti normativi previsti per l'adempimento degli obblighi-oneri di auto-organizzazione preventiva. Inoltre, il tema – come si vedrà – impone di indagare le complesse questioni connesse ai diversi segmenti della "filiera della *compliance*", dalla definizione di limiti e rischi del ricorso a sistemi di *predictive policing* in ambito aziendale all'indagine sulle diverse declinazioni della *sostenibilità* di modelli di *compliance* digitalizzati, che ad un tempo risultano più accessibili ed efficienti, ma anche più penetranti e invasivi; alla riflessione infine sullo stesso concetto di *compliance* e sul senso che ad esso imprime la possibilità di realizzare una conformazione *tecnologica* dei comportamenti.
Nella prima parte del presente contributo (par. 2), ci si concentrerà, dunque, sulle "promesse" della digitalizzazione dei *compliance programs*, per poi analizzare, nella seconda parte dello scritto (par. 3), i rischi che paiono invece connessi alla *compliance* digitalizzata. Nei paragrafi conclusivi (par. 4) si intende, infine, indagare come (e in quale misura) la digitalizzazione della *compliance* possa porsi in linea di continuità con gli obiettivi di «sostenibilità» e «transizione digitale», che guidano le più recenti politiche globali ed europee; da ultimo (par. 5), si raccoglieranno gli esiti della riflessione, tentando di comprendere quale sia l'impatto sistematico e concettuale di scelte organizzative che si avvalgono della normatività tecnologica per influenzare ed orientare la "conformità legale" di comportamenti individuali e processi aziendali.

2. *Le promesse della* compliance *digitalizzata: il d. lgs. 231/2001 come banco di prova per modelli organizzativi e controlli interni a base tecnologica.* Quanto alla prima delle questioni accennate – ovverosia, la definizione delle forme e dei limiti entro i quali le tecnologie informatiche e digitali possano essere utilizzate da società o altri enti per prevenire il rischio-reato –, tanto la prassi, quanto le prime riflessioni dottrinali suggeriscono invero per le nuove tecnologie una sorprendente varietà di possibili applicazioni nell'ambito della *compliance* aziendale: si pensi, ad esempio, all'integrazione dei controlli interni con strumenti di monitoraggio in tempo reale; all'automazione della fase di *risk assessment*; alla gestione di transazioni con tecnologie *blockchain*; alla capacità predittiva di eventuali comportamenti illeciti dei dipendenti suppor-

tata da tecnologie AI e *Machine Learning*; o ancora all'automatizzazione delle funzioni di *audit* e di *reporting*[11].

In ognuno di questi ambiti, il valore aggiunto derivante dall'impiego delle nuove tecnologie è intuitivo ed è generalmente individuato nella maggiore efficienza, effettività ed efficacia del sistema di organizzazione e controllo[12], rispetto alle modalità più "tradizionali" (*paper-based*) di gestione della *compliance*[13]. Invero, quanto all'*efficienza*, basti pensare, ad esempio, alla c.d. *big data analytics*, che si contraddistingue per il *volume* e la *varietà* dei dati che essa è in grado analizzare, nonché per la *velocità* con la quale può operare[14], determinando – ove impiegata per finalità di *compliance* – un evidente potenziamento delle capacità tecniche di analisi e di monitoraggio sulle quali

[11] Cfr. PWC, *Re-inventing internal controls in the digital age*, cit.; NEUFANG, *Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen*, in *Zeitschrift für Internationale Rechnungslegung*, 2017, 249-254; SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 221. Sui variegati rapporti tra le nuove tecnologie digitali e il diritto (penale), cfr. ad es., *Intelligenza artificiale - il diritto, i diritti, l'etica*, a cura di Ruffolo, Milano, 2020, e in part. i contributi di SEVERINO, *Intelligenza artificiale e diritto penale*, 531 ss.; MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, 547 ss. (anche in *www.discrimen.it*, 15 maggio 2020); *Intelligenza artificiale e diritti della persona*, a cura di Buzzelli-Palazzo, Pisa, 2022; *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia,* a cura di Giordano-Panzarola-Police-Preziosi-Proto, Milano, 2022; *Intelligenza artificiale: Politica, economia, diritto, tecnologia*, a cura di Severino, ed. e-book, Roma, 2022. Cfr. in part. SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in *Intelligenza artificiale: Politica, economia, diritto, tecnologia*, cit., 109 ss. e in part. 120 ss., ove l'A. rileva come le nuove tecnologie basate sui dati e sull'elaborazione algoritmica con la finalità di prevenzione dei reati abbiano ormai un'applicazione trasversale, ma richiedano riflessioni differenziate a seconda dei contesti (pubblico o privato) nei quali sono impiegate.

[12] Cfr. ad es. BAMBERGER, *Technologies of Compliance*, cit., 685, che si riferisce a «*both efficiency and effectiveness*».

[13] Cfr. ancora FERRARESE, *Presentazione dell'edizione italiana*, cit., 12, che fa per l'appunto riferimento alla «anima efficientistica della digitalizzazione». In relazione al rapporto tra attività umana e (più efficiente) *performance* del digitale, si chiedeva anche BODEI, *Dominio e sottomissione. Schiavi, animali, macchine e intelligenza artificiale*, Bologna, 2019, 297 ss., se al crescere delle capacità dei dispositivi digitali di «apprendere» e di «prevedere», l'essere umano «si limiterà a diventare [...] l'esecutore sia di un *logos* artificiale molto più capace di lui nell'elaborare informazioni e nel trovare soluzioni ai problemi, sia di un *bouleutikon* in grado di prendere decisioni rapide e precise». Con specifico riferimento all'uso di nuove tecnologie, cfr. ad es. BURCHARD, *Digital criminal compliance*, cit., 745, nel senso che la digitalizzazione "promette" di porre rimedio alle debolezze umane, eliminando l'errore e la possibilità di perdita di dati.

[14] RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 93. Cfr. anche TSAI-LAO-CHAI-VASILAKOS, *Big data analytics: a survey*, in *Journal of Big Data*, 2015, 2, 21, 1-32, nel senso che la c.d. *big data analytics* si distingue da precedenti tecniche di analisi dei dati in relazione alle tre "v", rappresentate da *volume*, *velocità*, *varietà*.

l'ente può fare affidamento[15]. Quanto, invece, al profilo dell'*efficacia*, si è rilevato come la digitalizzazione di procedure e protocolli importi un miglioramento non già soltanto quantitativo, ma anche essenzialmente qualitativo[16] nella gestione dei processi di *compliance*, riducendo il margine per l'errore umano e determinando l'integrazione costante (tramite sistemi c.d. *embedded*[17]) tra la funzione aziendale di *compliance* – sino ad ora esterna e separata – e le funzioni amministrative e gestionali, così incrementando le capacità predittive, preventive e impeditive dei presidi adottati, mediante un controllo *dall'interno* – e non più *dall'esterno* – dell'attività aziendale. Infine, ma su tale profilo ci si soffermerà meglio in seguito (v. *infra*, par. 2.2.1), è con riguardo all'*effettività* di regole e protocolli che la *compliance* digitalizzata pare distinguersi in maniera ancora più netta dalle altre forme di auto-regolazione, consentendo essa di incorporare tecnicamente le norme nei programmi informatici utilizzati per l'ordinaria gestione dell'attività aziendale e di renderle, in tale maniera, auto-esecutive e non eludibili[18].

In questa sede non è, tuttavia, il piano propriamente operativo a costituire, di per sé, oggetto d'interesse: ciò che si vuole piuttosto indagare e comprendere è come simili "alternative" digitali si collochino nell'attuale contesto teorico, normativo e giurisprudenziale in tema di *compliance* e di auto-organizzazione preventiva da parte di società e altri enti – tra i quali, come accennato, rientrano anche le pubbliche amministrazioni – così da valutare quali mutamenti di portata *strutturale* e *concettuale* esse possano determinare nel panorama dei sistemi di *compliance*. Ad esempio, proprio in considerazione delle grandi quantità di dati che le nuove tecnologie digitali possono raccogliere e ana-

[15] Consentendo, ad esempio, controlli pervasivi, costanti e in tempo reale, in luogo dei tradizionali controlli "a campione" effettuati nell'ambito di sistemi di *compliance* «manuali»: cfr. BAMBERGER, *Technologies of Compliance*, cit., 687.

[16] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 686-687, che individua in tale mutamento strutturale la ragione della maggiore *efficienza* della *compliance* digitalizzata.

[17] Cfr. ad es. RUHL-KATZ-BOMMARITO, *Harnessing legal complexity. Bring tools of complexity science to bear on improving law*, in *Science*, 31 marzo 2017, 355, 6332, 1377-1378, ove si fa specifico riferimento all'ipotesi di una «*embedded compliance*».

[18] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 692, che attribuisce ai modelli organizzativi digitalizzati la capacità di «*forcing compliance*»: «*GRC systems establish decision controls that automate business "rules" intended to mitigate those risks consistent with both operational and regulatory requirements*».

lizzare in tempo reale e, dunque, delle loro inedite capacità predittive[19], si è sostenuto che la digitalizzazione possa trasformare il funzionamento stesso dei modelli di *compliance*: i quali non dovrebbero più ridursi a una funzione di controllo *ex post* di dati "del passato", «quando la violazione è ormai già avvenuta da tempo»[20], ma consentirebbero addirittura di prevedere e *anticipare* la commissione dei reati, individuando anomalie e atti preparatori[21] e, in termini vieppiù anticipati, ambiti particolarmente a rischio di futuri illeciti in una fase ancora priva perfino di attività prodromiche rispetto all'illecito (c.d. *predictive policing*).

In altre parole, anziché riflettere sulle singole possibili applicazioni delle nuove tecnologie nelle attività di prevenzione del rischio-reato da parte di società ed enti, ci si domanderà piuttosto in quale modo e in quale misura i tratti qualificanti delle nuove tecnologie digitali interagiscano *su un piano concettuale* con il modello regolatorio della *compliance*, eleggendo a tal fine il paradigma delineato dal d. lgs. 231/2001 quale "banco di prova" per una riflessione che deve necessariamente confrontarsi anche con la prassi. Ciò non toglie, peraltro, che le considerazioni di volta in volta formulate possano estendersi anche agli altri sistemi di *compliance lato sensu* intesa come attività strutturata di conformazione ad un determinato apparato regolatorio o che i successivi riferimenti al contesto "aziendale" possano valere – con gli opportuni adattamenti – anche per altri enti privati o per le pubbliche amministrazioni. Com'è stato rilevato, infatti, la *compliance* digitale presenta una particolare affinità "strutturale" con tutti quei «modelli di regolazione» *«process-based»* o «*management-based*»[22] che si fondano sulla procedimentalizzazione della gestione dei rischi, cosicché i successivi riferimenti al d. lgs. 231/2001 intendono piuttosto assolvere una funzione *esemplificativa*, ma non certo *limitativa*, dei possibili ambiti di sviluppo del modello della *compliance* digitalizzata (per cui v. anche *infra*, par. 2.3).

---

[19] In ordine alle potenzialità predittive delle nuove tecnologie digitali, cfr. ZACCARIA, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, in *Ars Interpretandi*, 2021, 1, 29-52.

[20] Cfr. NEUFANG, *Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen*, cit., 249.

[21] Ancora, *ibid.*, 252.

[22] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 672.

2.1. *L'uso di tecnologie digitali nella* costruzione *(e nell'*aggiornamento*) del modello organizzativo: dal* risk assessment *al* risk management. Con riferimento alle diverse fasi della "vita" di un modello organizzativo (progettazione; attuazione; aggiornamento; eventuale valutazione giudiziale in presenza della contestazione di un illecito[23]), pare anzitutto indubbio che le tecnologie digitali possano fornire un proprio contributo già al momento della *costruzione* del sistema di *compliance*: e cioè, in primo luogo, quale strumento utile per la *mappatura* delle attività «nel cui ambito possono essere commessi reati», che l'art. 6, co. 2, lett a) d. lgs. 231/2001 pone quale primo requisito essenziale del modello organizzativo; inoltre, anche nella successiva fase di definizione dei *presidi* da adottare, per disciplinare e monitorare l'agire individuale e collettivo nel contesto aziendale, allo scopo di prevenire e impedire la commissione di reati.

Quanto al primo ambito (la *mappatura* del contesto aziendale), un tratto qualificante delle nuove tecnologie basate sui dati è appunto costituito dalla loro capacità di dipingere un «quadro iper-realista»[24] della realtà indagata, codificando in forma numerica ogni aspetto del mondo fisico, elaborando poi i dati raccolti e individuando infine correlazioni (e anomalie) tra di essi[25]. Pare perciò indiscutibile – ed è stato in tal senso già suggerito da alcuni "attori professionali" della *compliance*[26] – che le tecnologie digitali possano anzitutto supportare la fase preliminare del c.d. *risk assessment*, contribuendo alla "fotografia" del contesto e all'identificazione dei rischi, mediante la raccolta e

[23] In relazione a tali diverse fasi, cfr. ad es. le *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo* elaborate da CONFINDUSTRIA a giugno 2021 (*www.confindustria.it*), ove appunto si distingue tra il momento della costruzione del modello (suscettibile di una valutazione in termini di idoneità *astratta*) e la sua successiva implementazione ed efficace attuazione, che costituiscono invece l'oggetto di una valutazione *in concreto*.

[24] Cfr. FERRARESE, *Presentazione dell'edizione italiana* cit., 16. Anche GARAPON-LASSEGUE, *La giustizia digitale*, cit., 111-112, rilevano la capacità della tecnologia di realizzare una «scansione», di una istituzione o di un ente, ottenendone una sorta di "radiografia" digitale, una versione composta di dati che possono poi «essere incrociati e sfruttati all'infinito». Ancora, BODEI *Dominio e sottomissione*, cit., 333, equipara la funzione dei *big data* e degli algoritmi a quella di «un microscopio», così riconfermando come – anche su un piano teorico – alle nuove tecnologie digitali debba anzitutto riconoscersi una capacità di analizzare e "fotografare" la realtà.

[25] Cfr. ancora GARAPON-LASSEGUE, *La giustizia digitale*, cit., 43 ss. Cfr. anche BAMBERGER, *Technologies of Compliance*, cit., 688.

[26] Cfr. PWC, *Re-inventing internal controls in the digital age*, cit., 10.

l'analisi di tutti i dati relativi alla realtà aziendale[27]. In tale prospettiva, la digitalizzazione concorrerebbe ad assicurare l'idoneità del modello organizzativo, sul versante della necessaria "customizzazione" delle cautele organizzative alla «sagoma della singola impresa» e alla «"concretezza" del suo operare»[28].
Volgendo, invece, lo sguardo al secondo ambito di possibile rilevanza della digitalizzazione rispetto alla *progettazione* del modello organizzativo (ovverosia, alla fase di definizione dei *presidi*[29]), le nuove tecnologie rappresentano – come si anticipava – (inediti) strumenti organizzativi e di controllo, dei quali l'impresa può prevedere l'impiego per la prevenzione del rischio-reato: da un lato, quali dispositivi di monitoraggio in tempo reale dei processi interni di formazione e attuazione delle decisioni (come appunto prescritto dall'art. 6, co. 2, lett. b), d.lgs. 231/2001); dall'altro lato, e più in generale, quali strumenti per procedimentalizzare le attività aziendali in modo conforme ai rilevanti parametri normativi (ad esempio, incorporandovi obiettivi, soglie, divieti), così modellando e limitando tecnicamente il margine d'azione degli individui

[27] Evidenzia ad esempio VON BÜNAU, *Künstliche Intelligenz und Recht. Möglichkeiten und Mythos*, in *Rechtshandbuch Legal Tech*, cit., 47 ss. e in part. 50-51, la capacità dei sistemi "intelligenti" di analizzare i dati storici e di estrapolare, sulla base di essi, "modelli" di comportamento ai quali conformare il proprio funzionamento (c.d. programmazione implicita), ma anche di contribuire – sulla base di questa capacità di estrarre modelli analizzando set di dati storici – alla valutazione del rischio, individuando la probabilità di verificazione di un evento. In senso del tutto analogo anche BAMBERGER, *Technologies of Compliance*, cit., 690 ss., ove l'A. rileva come la fase del *risk assessment* si fondi tradizionalmente su valutazioni di carattere qualitativo, laddove invece le specifiche capacità di analisi delle tecnologie digitali ne rendono possibile una valutazione (anche) quantitativa. Sottolinea invece BURCHARD, *Digital criminal compliance*, cit., 748, come anche nella fase di *risk assessment* l'uso di tecnologie "intelligenti" ponga questioni di rilevanza etica, là dove – così come accade con gli strumenti di *risk assessment* utilizzati dalle autorità pubbliche – esso non abbia ad oggetto l'attività aziendale in sé considerata, ma costituisca strumento di valutazione del rischio-reato "individuale" connesso a ciascuno dei soggetti (dirigenti, dipendenti, etc.) coinvolti nell'attività aziendale (ma a tale riguardo cfr. anche par. 3). In proposito, cfr. anche ASSUMMA, LEI, *Sub Art. 6*, in *Il 231 nella dottrina e nella giurisprudenza*, a cura di Levis-Perini, Bologna, 2021, 232 ss. e in part. 235, in relazione alle preliminari attività di analisi della struttura organizzativa dell'ente, del suo modello di *business* e della sua *case history*, nonché dei processi interni e delle attività sensibili.

[28] Cfr. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo*, in *Giurisprudenza commerciale*, 2021, 4, 633-661 e in part. 639. Cfr. anche ARENA, *L'adozione e l'efficace attuazione di un idoneo modello organizzativo*, in *La responsabilità degli enti* ex *d. lgs. 231/2001 tra diritto e processo*, a cura di Piva, Torino, 2021, 351 ss., che individua i «sette requisiti» di idoneità del Modello organizzativo e appunto vi annovera, oltre all'analisi preliminare delle attività sensibili, anche la previsione di protocolli e procedure interni per la gestione e la procedimentalizzazione di tali medesime attività sensibili.

[29] In relazione alla fase di «Valutazione/costruzione/adeguamento del sistema di controlli preventivi», cfr. le già citate *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, 50 ss.

che operano all'interno dell'ente[30]. Per fare un esempio, rispetto alla gestione delle disposizioni di pagamento in uscita dall'ente, eventuali presidi digitali di *compliance* potrebbero non soltanto consentire di tracciare o monitorare in tempo reale le transazioni e di verificarne in modo automatizzato la corrispondenza con disposizioni di acquisto e fatture passive, ma potrebbero soprattutto rendere *tecnicamente impossibile* (e, dunque, *impedire*) l'esecuzione di pagamenti anomali o difformi rispetto ai protocolli aziendali: inabilitando, ad esempio, l'effettuazione di bonifici a favore di destinatari che non risultino già censiti e approvati nell'anagrafe aziendale, con l'effetto, dunque, di ridurre, se non addirittura eliminare, il rischio di comportamenti appropriativi, distrattivi, o financo corruttivi.

Nella medesima direttrice d'indagine, meritano infine un cenno anche le potenzialità delle tecnologie digitali nell'*aggiornamento* del modello organizzativo, da declinarsi sia in una forma, per così dire, "ancillare" o di supporto – nella quale, cioè, l'automazione è impiegata al limitato fine di rilevare tempestivamente i mutamenti normativi ovvero le modifiche del contesto aziendale[31] che debbano essere poi recepiti nell'ambito del modello organizzativo da parte delle funzioni competenti –, sia in una forma, al contrario, propriamente automatizzata – vale a dire, attraverso la predisposizione di sistemi di *machine learning* con i quali il modello organizzativo possa costantemente migliorare e ottimizzare il proprio funzionamento, ovvero adeguarsi autonomamente a eventuali mutamenti normativi[32] a seguito di un previo "addestramento" basato sull'esperienza pregressa e sui risultati del *continuous monitoring,* in una prospettiva di aggiornamento costante basato sulle evidenze proprie della realtà dell'ente.

Già tale rapida panoramica sul "valore aggiunto" dei sistemi di *compliance* digitalizzati porta allora a domandarsi – su un piano teorico – in quale misura l'innovazione tecnologica (e, segnatamente, la possibilità di ricorrere alle tecnologie informatiche e digitali nella costruzione del modello organizzativo)

[30] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 674-675.

[31] PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, in *www.pwc.com*, 2021, 8 ss.

[32] Cfr. RUHL-KATZ-BOMMARITO, *Harnessing legal complexity*, cit., 1378: «*for example, corporations with access to a real-time model of legal system complexity could develop more effective compliance strategies, including autonomous embedded compliance protocols that adjust as the law adjusts*».

possa incidere sulla definizione della regola cautelare e contribuisca, dunque, a individuare, anche nel settore della responsabilità degli enti, la misura della colpa (di organizzazione)[33].

A dispetto, tuttavia, di siffatte potenzialità, il tema dell'incidenza della digitalizzazione – e delle inedite capacità preventive che essa porta con sé – sulla definizione delle regole cautelari è stato sinora poco esplorato nella dottrina penalistica[34], sebbene non sia mancata qualche sporadica pronuncia di legittimità nella quale la Suprema Corte ha – ad esempio – qualificato espressamente in termini di *doverosità* l'adozione di un sistema *automatizzato* di sicurezza, funzionale a «ovviare agli errori umani»[35], in presenza del quale – secondo un giudizio controfattuale – l'evento lesivo non si sarebbe verificato.

Limitando per ora l'analisi al tema della colpa di organizzazione, si tratta dunque di comprendere se – quantomeno, in un prossimo futuro – la semplice possibilità di ricorrere a (più efficaci) presidi digitali[36] possa condizionare la valutazione dell'*idoneità preventiva* del modello organizzativo in sede di scrutinio giudiziale e imponga quindi, sin dal momento della sua *costruzione*, di considerare l'alternativa digitalizzata quale *best practice* cui sia doveroso conformarsi.

---

[33] Al riguardo, cfr. ad es. NISCO, *Riflessi della* compliance *digitale in ambito 231*, cit., 10, che per appunto riflette sui riflessi della *compliance* digitale sulla colpa di organizzazione, sottolineando come la promessa «di esattezza e di maggiore effettività» connessa all'uso delle nuove tecnologie sia destinata a «condizionare il giudizio di idoneità dei modelli organizzativi, che non adottano misure tecnologiche (ritenute non eludibili), o adottano sistemi (considerati) poco performanti».

[34] In argomento, cfr. essenzialmente, con riferimento al tema dell'innovazione tecnologica in senso ampio, G. MARINUCCI, *Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza*, in *Riv. it. dir. proc. pen.*, 2005, 29-59. Con specifico riguardo all'intelligenza artificiale, cfr. DI FLORIO, *Il diritto penale che verrà. Brevi considerazioni sul possibile impiego dell'IA per prevenire il rischio di disastri colposi*, in *Arch. pen.*, 2021, 2, 12 ss., che analizza le «implicazioni penalistiche per la colpa» derivanti dalla possibilità d'impiegare con funzioni cautelari o prevenzionistiche l'intelligenza artificiale e ipotizza «una "qualificazione" in termini di (super) agente modello dell'IA», atteso che «la cooperazione, per così dire, tra l'agire (creativo) umano e le "macchine intelligenti", pare ragionevolmente destinato ad incrementare lo standard di cautela nella gestione e nei controlli».

[35] Cfr. Cass., sez. IV, 19 ottobre 2006, n. 41944, in *Riv. pen.*, 2007, 10, 1065 ss.

[36] SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 143, ritengono che per le imprese di grandi dimensioni la *compliance* digitalizzata rappresenti l'*unica* modalità realmente adeguata (*alternativlos*) per adempiere agli obblighi-oneri di *compliance*: la crescente complessità e l'aumento dei dati da analizzare renderebbero, infatti, strutturalmente inadeguati e inefficaci sistemi di gestione e controllo «*papierbasiert*».

A tale riguardo, è noto come la valutazione relativa all'*idoneità* del modello organizzativo si appunti essenzialmente sulla considerazione della sua «effettiva capacità preventiva rispetto alla commissione futura di "reati della stessa specie di quello verificatosi"»[37]: la quale, beninteso, non postula «la capacità dello stesso di impedire e precludere *in termini assoluti* la commissione di illeciti nell'ambito dell'attività aziendale»[38], ma deve anzi mirare al «(più ragionevole) risultato dell'*abbassamento del rischio che venga commesso un illecito nell'ambito dell'attività aziendale*»[39].

Se ciò è vero, va nondimeno rilevato come la definizione dei criteri rilevanti per l'accertamento dell'idoneità del modello organizzativo rappresenti tuttora «uno degli aspetti più oscuri, se non un autentico punto di crisi della disciplina della responsabilità *ex delicto* delle società»[40], trattandosi di valutazione tendenzialmente rimessa all'apprezzamento del giudice, in assenza di parametri normativi predeterminati. Paradigma dogmatico di riferimento è, tuttavia, quello dell'illecito colposo di evento[41], che impone dunque di contemperare, da un lato, la valutazione di effettiva (o maggiore) capacità impeditiva del comportamento alternativo (nel caso in esame: l'adozione di un sistema digitalizzato di presidi e controlli interni) e, dall'altro lato, l'esigibilità e l'effettiva praticabilità di un siffatto sforzo cautelare da parte del soggetto agente.

Cosicché, anche nell'ambito che ci occupa, pur potendosi senz'altro supporre che le maggiori capacità delle tecnologie digitali siano destinate a «condiziona-

---

[37] Cfr. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive*, in *Riv. trim. dir. pen. econ.*, 2017, 1-2, 49-113 e in part. 67. In proposito, cfr. anche ASSUMMA, LEI, *Sub Art. 6*, cit., 232 ss.

[38] SANTORIELLO, *La valutazione giudiziale del modello. Un esempio di come legge e cosa cerca il pubblico ministero nei modelli organizzativi*, in *La responsabilità amministrativa delle società e degli enti*, 2019, 2, 193-213 e in part. 195.

[39] *Ibid.*, 196 (corsivo nel testo).

[40] In questi termini, cfr. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo*, cit., 633. Il tema dell'idoneità del modello organizzativo è stato da ultimo affrontato nella giurisprudenza di legittimità da Cass., sez. VI, 11 novembre 2021, n. 23401 (relativa alla c.d. vicenda Impregilo), in *www.sistemapenale.it*, 20 giugno 2022 (con nota di PIERGALLINI, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda "Impregilo"*, in *www.sistemapenale.it*, 27 giugno 2022), che per l'appunto parametra l'*idoneità* del modello alla capacità di esso di «*ridurre il rischio* di commissione dei reati» presupposto, secondo «una concezione normativa della colpa».

[41] Cfr. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo*, cit., 648. Ancora, cfr. Cass., sez. VI, 11 novembre 2021, n. 23401, cit., nel senso che occorre «prendere in considerazione anche il c.d. "comportamento alternativo lecito"» anche «nel giudizio sull'idoneità dei modelli adottati», che deve snodarsi ad un tempo *in astratto* e *in concreto*.

re il giudizio di idoneità dei modelli organizzativi»[42] – potendo queste ultime senz'altro contribuire efficacemente a quell'abbassamento del rischio di commissione di reati, che costituisce ad un tempo lo scopo e l'indice di adeguatezza del modello organizzativo – sarà pur sempre necessario dimostrare che i (diversi) presidi adottati dall'ente non fossero comunque idonei a prevenire l'evento (il reato) che si è verificato; che l'alternativa digitale avesse per converso una concreta capacità impeditiva; che, infine, si trattasse di comportamento effettivamente *esigibile*, perché ad esempio riconducibile a uno *standard* di settore, oppure perché proporzionato alle dimensioni o alle risorse dell'ente o perfino "auto-prodotto" dall'ente secondo una metodologia non autoreferenziale in quanto, per l'appunto, *technology-based*[43]. Non pare, dunque, che la (pur crescente) possibilità di ricorrere a cautele organizzative digitali o automatizzate possa *di per sé* trasfigurare strutturalmente il giudizio di idoneità del modello organizzativo, a meno di non voler scadere in un'adesione eccessivamente entusiastica o comunque acritica alle potenzialità delle tecnologie digitali[44].

Per altro verso, si è anche rilevato come la progressiva digitalizzazione dei modelli organizzativi determinerebbe – quale effetto inevitabile della devoluzione a sistemi automatizzati dei compiti di valutazione e gestione del rischio – una maggiore *opacità* del loro funzionamento, essendo per i soggetti non specializzati comprensibile al più l'esito, ma non il processo che l'ha generato: da questo punto di vista, la *compliance* digitale potrebbe allora incidere non soltanto sulla determinazione dello *standard* cautelare, ma anche sulle moda-

---

[42] Cfr. NISCO, *Riflessi della* compliance *digitale in ambito 231*, cit., 10. Anche SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, cit., 121, nel senso che l'utilizzo di *software* di intelligenza artificiale «innalzerebbe senz'altro lo standard di idoneità preventiva del modello», anche perché impedirebbe al potenziale trasgressore una «mera frontale violazione» delle prescrizioni, ma anzi gli richiederebbe di aggirarle (vale a dire, di realizzare una «elusione fraudolenta»).

[43] Ancora MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo*, cit., 651.

[44] Sottolinea ad esempio SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 223, che anche in un sistema organizzativo a base tecnologica l'adeguatezza o l'idoneità potrebbe difettare ad esempio per un vizio di progettazione o di funzionamento. Analogamente, anche SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, cit., 122 considera l'ipotesi problematica della «omessa o erronea segnalazione da parte del *software*», che, come osserva l'A., potrebbe trasformare la colpa di organizzazione in una *culpa in eligendo*.

lità di valutazione (anche giudiziale) dell'idoneità del modello, attribuendo un ruolo ancora più centrale alle analisi di consulenti tecnici e periti, depositari del relativo sapere tecnico[45] in una prospettiva di necessaria *governance* della *compliance* digitale che risulti in linea con l'indispensabile *explainability* delle metodologie utilizzate e dei processi che hanno condotto a determinati *output*[46].

Addirittura, la prospettata tecnicizzazione dei presidi organizzativi e cautelari ha indotto alcuni Autori a ipotizzare la possibilità di ricorrere a una nuova regola di giudizio – che parrebbe applicabile anche ai modelli di *compliance* digitalizzata – definibile come «*technology judgement rule*»[47]: a fronte della doppia delega decisionale che contraddistinguerebbe i presidi a base tecnologica (non solo alle imprese private chiamate ad adottare le cautele, ma anche agli esperti delle tecnologie digitali chiamati a svilupparle), sarebbe precluso al giudice di entrare *nel merito* della scelta "cautelare" operata dal soggetto garante (in quanto connotata da un elevato grado di *tecnicità*), purché quest'ultima risulti ragionevole e assunta sulla base di un'adeguata valutazione del rischio e degli strumenti disponibili.

Già sul piano della progettazione del modello organizzativo e della valutazione della sua idoneità astratta, il paradigma della *compliance* digitale rivela dunque implicazioni sistematiche di primario rilievo, che si riverberano ad un tempo sull'oggetto, sul metodo e sui parametri ai quali s'informa lo scrutinio giudiziale dei presidi di auto-organizzazione adottati dall'ente.

2.1.1. *Postilla: Presidi digitali per rischi digitali.* Pare necessario, a questo punto dell'analisi, inserire un breve appunto, per riflettere su un altro piano dell'intersezione tra *compliance* e digitalizzazione, che si può apprezzare già al momento della *costruzione* del modello organizzativo. Come si è già anticipato in premessa – e come si è anche visto più in dettaglio nel paragrafo

[45] Cfr. SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 219, nel senso che la *e-compliance* trae linfa dalla posizione di «privilegio tecnologico» nella quale si trova chi abbia «il dominio del sapere tecnico».

[46] Cfr. NISCO, *Rilessi della compliance digitale in ambito 231*, cit., 11.

[47] Cfr. DENGA, *Die Technology Judgement Rule*, in *Intelligente Systeme – Intelligentes Recht*, a cura di Kusschel-Asmussen-Golla, Baden-Baden, 2021, 63 ss.

precedente – la nozione di *compliance* digitale posta a fondamento della presente ricerca allude all'utilizzo di nuove tecnologie informatiche e digitali (intelligenza artificiale, *big data analytics*, e così via) nell'ambito dei (tradizionali) processi aziendali di *compliance*: in altre parole, si riflette sulla digitalizzazione dei *presidi* e dei *controlli*, per la prevenzione degli "*ordinari*" rischi-reato.
Non va sottaciuto, tuttavia, come la digitalizzazione intersechi il tema della *compliance* aziendale (almeno) su un altro distinto piano, là dove cioè l'utilizzo di nuove tecnologie nell'ambito dell'impresa determina *nuovi* rischi e *nuove* esigenze di conformità normativa, "tipici" della società dell'informazione e relativi, ad esempio, all'uso di strumenti informatici, al trattamento automatizzato di dati personali o alla prestazione di servizi digitali[48].
Ad esempio, può ascriversi a questo diverso filone d'indagine l'inserimento dei delitti informatici tra i reati-presupposto della responsabilità dell'ente (ai sensi dell'art. 24-*bis* del d. lgs. 231/2001), che ha determinato il coinvolgimento degli attori privati nella tutela dei sistemi d'informazione[49] e che ha decretato la riconducibilità dei delitti informatici alla categoria criminologica della c.d. «criminalità del profitto»[50]. Ancora, può riportarsi a questa diversa nozione di "*compliance* digitale" l'impostazione preventiva che informa il *GDPR*

[48] Analizzano ad es. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 137 ss., la trasformazione della funzione di *compliance* determinata dal continuo sviluppo della tecnologia digitale e dalla pervasiva presenza di "segmenti" digitali in tutti i processi aziendali. Un altro esempio di tale prospettiva sull'intersezione tra *compliance* e digitalizzazione si può rinvenire in HILGENDORF, *Grundfragen strafrechtlicher Compliance am Beispiel der strafrechtlichen Produkthaftung für teilautonome technische Systeme*, in *Criminal Compliance vor den Aufgaben der Zukunft*, a cura di Rotsch, Baden-Baden, 2013, 19 ss.; MAZZACUVA, *The impact of AI on corporate criminal liability: algorithmic misconduct in the prism of derivative and holistic theories*, in *Revue Internationale de Droit Pénal*, 2021, 92, 1, 143-158, che si focalizza sul problema della «*purely algorithmic corporate misconduct*» e sui possibili modelli di imputazione e di prevenzione. In argomento, è altresì essenziale l'analisi di MOZZARELLI, *Digital Compliance: The Case for Algorithmic Transparency*, in *Corporate Compliance on a Global Scale*, cit., 259 ss., che si concentra sui nuovi rischi emergenti dalla «*digitalisation of everything*», distinguendo tra "vecchi" rischi che si presentano in nuove forme, e "nuovi" rischi.
[49] In argomento, cfr. ad es. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex d. lgs. n. 231/2001*, in *Trattato di diritto penale – Cybercrime*, diretto da Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 193 ss., nonché PICOTTI, *I delitti informatici previsti dal d.lgs. n. 231/2001*, in *Cybercrime e responsabilità da reato degli enti*, a cura di Monti, Milano, 2022, 23 ss.
[50] Al riguardo v. ad es. PAYNE, *White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?*, in *Criminology, Criminal Justice, Law & Society*, 2018, 19, 3, 16-32.

(Reg. UE 679/2016), con il quale il legislatore europeo, adottando un approccio *risk-based* nel settore della protezione dei dati personali[51], ha elaborato un complesso sistema di obblighi di *conformità* e di «tutela preventiva» dei dati, fondato «sulla strutturale e dinamica responsabilizzazione della filiera soggettiva coinvolta»[52].

Nella diversa prospettiva, poi, di tutelare i sistemi informatici da aggressioni esterne, gli attori privati sono altresì divenuti destinatari, in conseguenza della sempre maggiore «digitalizzazione dell'impresa e dei processi di *business*»[53], di precisi (e pervasivi) «doveri di protezione» e di obblighi di prevenzione e mitigazione dei rischi di *cyberattacks*, mediante l'adozione di misure di carattere tecnico e organizzativo, funzionali ad un tempo alla «protezione del patrimonio informativo» dell'ente, al governo dei processi di trattamento dei dati personali, nonché all'«assolvimento di specifici obblighi normativi» di sicurezza[54].

In un simile contesto, è allora evidente come la nozione di *compliance* digitale si presti a ricomprendere profili d'indagine anche molto vari: il che ha portato a preferire, nel presente scritto, la dicitura di *compliance* "digitalizzata", per circoscrivere in modo più preciso l'oggetto della ricerca. Non deve trascurarsi, tuttavia, la profonda correlazione tra i due diversi ambiti della *compliance* a base tecnologica e della *compliance* IT, spesso essendo i presidi *digitali* gli strumenti più indicati (benché non gli unici) per contrastare i rischi propriamente *digitali*. Così, ad esempio, per la prevenzione del crimine informatico proveniente *dall'interno* o *dall'esterno* di un ente, sono proprio le

---

[51] Osserva 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, 53, come il sistema di protezione dei dati personali delineato dal *GDPR* paia «ruotare attorno al concetto di rischio».

[52] Cfr. CALZOLAIO, *Protezione dei dati personali (dir. pubbl.)*, in *Dig. Disc. Pubbl.*, Agg., Torino, 2017, 594 ss. e in part. 614, nonché MONTI, *Il modello organizzativo 231 e la protezione dei dati personali*, in *Cybercrime e responsabilità da reato degli enti*, cit., 225 ss. Sottolinea un siffatto mutamento in senso preventivo anche FLOR, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet,* 2019, 3, 453-467 e in part. 466-467.

[53] Cfr. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in *Cybercrime e responsabilità da reato degli enti*, cit., 149 ss.

[54] Per i virgolettati, v. *ibid.*, 150. Cfr. anche MANCINI-PAGNOTTA, *Cyberattack: tecniche di prevenzione, rilevazione e mitigazione*, in *Cybercrime e responsabilità da reato degli enti*, cit., 1 ss., che forniscono anche esempi pratici delle misure tecniche di prevenzione che è possibile adottare per gestire il rischio di commissione di delitti informatici.

«contromisure tecnologiche»[55] a costituire l'ossatura essenziale del sistema di *governance* della sicurezza informatica; analogamente, nell'ambito della protezione delle infrastrutture critiche ai sensi del d.l. 105/2019 (in tema di perimetro nazionale di sicurezza cibernetica), tra le misure elencate dal legislatore per garantire la sicurezza delle reti, dei sistemi informativi e dei servizi informatici rientrano anche presidi di carattere *tecnologico*, volti ad assicurare, ad esempio, la "protezione fisica e logica" dei dati[56]. Le considerazioni esposte nel paragrafo precedente inducono, tuttavia, a non limitare l'analisi a tali profili, ma anzi a riguardare la *compliance* digitalizzata quale fenomeno trasversale, produttivo di implicazioni sistematiche sul modello dell'auto-normazione preventiva.

2.2. *L'uso di tecnologie digitali per l'efficace* attuazione *del modello organizzativo: dal potenziamento dei controlli alla prova in giudizio*. La fase nella quale l'uso di tecnologie digitali è considerato maggiormente "rivoluzionario" per le attività di *compliance* è soprattutto quella dell'*attuazione* del modello organizzativo, potendo i presidi digitali già brevemente richiamati – coerentemente con le caratteristiche intrinseche della digitalizzazione – assicurare un miglioramento nell'*effettività* e nell'*efficacia* dei *compliance programs*, rispetto alle tradizionali modalità ("umane", analogiche) di gestione e monitoraggio dei presidi organizzativi[57].

In tale prospettiva, la tecnologia digitale può allora contribuire alla prevenzione dei reati secondo (almeno) tre diverse modalità, in parte già anticipate nei paragrafi che precedono: in primo luogo, la tecnologia può infatti essere utilizzata quale strumento di monitoraggio, controllo e rilevazione in tempo reale di segnali d'allarme, anomalie e potenziali violazioni del modello; in secondo luogo, lo sviluppo di protocolli e procedure a base tecnologica consen-

[55] Cfr. MANCINI-PAGNOTTA, *Cyberattack: tecniche di prevenzione, rilevazione e mitigazione*, cit., 2. Osserva però DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, cit., 149-150, come «un effettivo sistema di gestione della sicurezza» informatica «non può essere solo fondato sulla tecnologia, ma deve necessariamente includere l'analisi del fattore umano e l'efficacia delle procedure».

[56] Che peraltro si affiancano a misure di carattere organizzativo, preposte dalla gestione della sicurezza informatica.

[57] Cfr. in questo senso BURCHARD, *Digital criminal compliance*, cit., 744.

te il continuo tracciamento (e, dunque, la continua registrazione) di tutte le operazioni, i flussi informativi e le segnalazioni e può, dunque, facilitare la dimostrazione e la prova in giudizio dell'effettiva attuazione del modello; infine, in una circolarità nella quale il compimento del processo di monitoraggio, definizione dei presidi, produzione di flussi informativi e interventi correttivi mirati può fornire le basi per individuare gli ambiti nei quali potrebbe essere probabile la realizzazione di futuri illeciti, la digitalizzazione può consentire una forma di prevenzione *diretta* dei reati, là dove i protocolli di gestione e di formazione delle decisioni adottati dall'ente siano informatizzati, nonché *a priori* programmati per poter operare soltanto entro determinati standard conformi alla rilevante disciplina.

Nella prima delle direzioni indicate, si è allora ipotizzato che le nuove *smart technologies* possano costituire uno strumento operativo da mettere a disposizione dell'Organismo di Vigilanza[58], per rilevare eventuali anomalie, ovvero per evidenziare i processi nei quali si riscontri un aumento del rischio[59], facilitando e potenziando la vigilanza sull'osservanza e sull'adeguatezza del modello, mediante la raccolta e l'analisi di dati[60].

In più, per tutti quei reati nei quali la *conformità* e la *non-conformità* normativa possano essere codificate o espresse in termini numerici (ad esempio: il rispetto di valori-soglia; la verifica di indici patrimoniali; la quantificazione di flussi finanziari), l'impiego delle nuove tecnologie digitali può altresì consentire forme di monitoraggio quantitativo in tempo reale e mettere a disposizione sistemi di *alert*: in quest'ottica è stata studiata, ad esempio, la possibilità di prevedere (e prevenire) il rischio di insolvenza mediante tecniche (anche molto semplici) di *machine learning*, capaci di pronosticare con un buon grado di accuratezza la crisi di un'impresa, sulla base di indici finanziari facilmente reperibili[61]. Del pari, anche nei settori della tutela ambientale, dell'antiriciclaggio, della prevenzione della corruzione, della tutela del regola-

[58] Cfr. RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 95; analogamente, VIANELLI-VALENTI, *RegTech e Modelli 231*, cit., 99 ss.

[59] Ancora RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 95.

[60] Cfr. SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 221.

[61] Cfr. SHETTY-MUSA-BRÉDART, *Bankruptcy Predicition Using Machine Learning Techniques*, in *Journal of Risk and Financial Management*, 2022, 15, 35, 1-10.

re funzionamento dei mercati finanziari, o ancora della prevenzione dei reati colposi, sono state analizzate le potenzialità e le virtualità applicative di sistemi di *compliance* digitalizzati, nell'ottica di supportare o di sostituire le tradizionali funzioni di controllo interno[62].

Più in generale, si è anche sottolineato come l'analisi capillare e in tempo reale resa possibile dalla «*smart data analytics*» conduca da un'impostazione «statico-reattiva» della *compliance* societaria a una modalità di funzionamento invece «dinamico-preventiva»[63]: capace, cioè, di intervenire *prima* dell'effettiva commissione di un reato.

Le ricadute di tale incremento nell'efficienza dei controlli sarebbero quindi più d'una anche sul piano della *efficace attuazione* del modello[64], che – al pari dell'idoneità – costituisce un aspetto sicuramente critico, in termini di valutazione e prova, nell'ambito dello scrutinio giudiziale degli sforzi di auto-organizzazione dell'ente e, anche in prospettiva *de iure condendo*, di premialità per l'investimento in innovazione organizzativa.

---

[62] Per le diverse possibili applicazioni dell'intelligenza artificiale per la prevenzione di reati, cfr. SABIA, *Artificial Intelligence And Environmental Criminal Compliance*, in *Revue Internationale de Droit Pénal*, 2020, 179-201; DI FLORIO, *Il diritto penale che verrà. Brevi considerazioni sul possibile impiego dell'IA per prevenire il rischio di disastri colposi*, cit.; BIRRITTERI, *Big Data Analytics* e *compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Dir. pen. cont.*, 2019, 2, 289-303; CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa titoli di credito*, 2018, 2, 195-234; HAN- HUANG-LIU-TOWEY, *Artificial intelligence for anti-money laundering: a review and extension*, in *Digital Finance*, 2020, 2, 211-239; LIN, *Compliance, technology, and modern finance*, in *Brooklyn Journal of Corporate, Financial and Commercial Law*, 2016, 11, 159-182.

[63] Cfr. BURCHARD, *Digital Criminal Compliance*, cit., 746. Segnala la centralità del passaggio «*from a reactive rules-based approach to proactive engagement with the business*» nei sistemi di *compliance* anche EY, *Integrity in the spotlight,* cit., 23.

[64] Cfr. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 139, evidenziano come il requisito dell'effettività-efficacia (*effectiveness*) sia invero parametro trasversale e costante nella valutazione del modello organizzativo, ricorrendo tanto nella giurisprudenza tedesca, quanto ad es. in quella statunitense. Nell'ordinamento italiano, cfr. ad es. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive*, cit., 68, nel senso che la componente della "efficace attuazione", pur rispondendo all'indubbia esigenza che il modello di organizzazione adottato non rimanga «meramente cartolare», «introduce tuttavia un elemento valutativo (ulteriormente) incerto in sede di apprezzamento ad opera del giudicante». Cfr. anche ARENA, *L'adozione e l'efficace attuazione di un idoneo modello organizzativo*, cit., 367, ove l'A. individua gli «otto requisiti» dell'efficace attuazione del modello organizzativo, elencandovi, ad esempio, l'effettiva applicazione delle procedure aziendali, l'efficace e continua azione dell'OdV, la completezza dei flussi informativi, la formazione del personale, la gestione delle segnalazioni o delle rilevazioni di situazioni di rischio.

Seguendo la seconda linea di sviluppo indicata in premessa, inoltre, un modello di *compliance* digitalizzato consentirebbe non soltanto di potenziare i controlli interni, ma permetterebbe altresì di documentare e tracciare con estremo grado di dettaglio il monitoraggio compiuto: quasi come se si trattasse, per così dire, di una sorta di "scatola nera" dell'attività e della *compliance* aziendale[65]. In tal senso, dunque, l'utilizzo di tecnologie informatiche potrebbe rappresentare un inedito strumento di gestione, sviluppo e tracciamento dei flussi informativi e di documentazione delle attività di *compliance*, anche in funzione della successiva – benché eventuale – prova da fornire in giudizio[66]. Si è già ricordato, ad esempio, come sia la stessa l. 179/2017 (che ha modificato l'art. 6 del d. lgs. 231/2001) ad aver prescritto il ricorso a modalità informatiche per la gestione delle segnalazioni provenienti da *whistleblower*, onde garantirne la segretezza e l'integrità[67]. Oltre a ciò, alcune tecnologie – in particolare, la *blockchain* – sono state individuate come la soluzione più efficace (in quanto automatica, criptata e non modificabile) per quegli «oneri documentali e probatori»[68] che il d. lgs. 231/2001 pone in capo all'ente, che vo-

[65] Cfr. anche LANGEVOORT, *Global Behavioral Compliance*, in *Corporate Compliance on a Global Scale*, cit., 217 ss., e in part. 227-228, nel senso che una *compliance* digitalizzata può facilitare lo sviluppo di nuove "metriche", utili non soltanto per monitorare in tempo reale l'attività aziendale, ma anche per "misurare" la stessa attività di *compliance*. Sottolinea BURCHARD, *Digital criminal compliance*, cit., 750, come la *compliance* digitalizzata non sia a sua volta immune da vizi o da possibili "elusioni fraudolente", potendo ad es. i soggetti intranei sfruttare le "debolezze" del sistema digitale (c.d. «*oracle attacks*»).

[66] Osserva RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 112, come, per provare in giudizio di aver adottato ed efficacemente attuato un modello di organizzazione idoneo a prevenire reati della specie di quello che si è verificato, nonché, nei casi dell'art. 6, che il reato sia stato la conseguenza di una elusione fraudolenta del modello, l'ente non possa limitarsi a dimostrare l'adozione formale del modello organizzativo, ma debba anche documentare l'effettivo rispetto, da parte dell'organizzazione, di regole e protocolli, unitamente all'effettivo e continuativo svolgimento di un'attività di controllo da parte dell'organismo di vigilanza.

[67] Secondo un paradigma destinato a divenire di applicazione generalizzata, con il recepimento della direttiva europea 2019/1937, come già illustrato, per cui cfr. *supra* nt. 8. Cfr. anche STAPPERS, *EU Whistleblower Protection Directive: Europe on Whistleblowing*, in *ERA Forum*, 2021, 2, 87-100, che riflette anche sulle prospettive di *outsourcing* dei canali digitali di *whistleblowing* a società esterne, che assicurino il rispetto della disciplina in tema di protezione dei dati personali, nonché l'analisi delle segnalazioni.

[68] Cfr. ancora RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 112: la tecnologia *blockchain* rappresenterebbe infatti un inedito sistema di custodia di informazioni in maniera sostanzialmente immutabile, [...] apponendo la marcatura temporale ai blocchi di dati ed utilizzando chiavi criptate per la scrittura da parte di ciascun nodo della catena». Cfr. anche VIANELLI-VALENTI, *RegTech e Modelli 231*, cit., 102.

glia dimostrare di aver ad un tempo *adottato ed efficacemente attuato* un modello organizzativo idoneo a prevenire reati della specie di quello che si è verificato.

Nuovamente, tuttavia, è essenziale che la riflessione non si arresti su un piano meramente operativo, ma cerchi di individuare le implicazioni sistematiche che la *compliance* digitalizzata porta con sé, anche nella fase dell'*attuazione* del modello organizzativo. Ebbene, le questioni di più ampio respiro che paiono (pro)porsi all'interprete sono, in questo ambito, per lo meno due: da un lato, deve considerarsi il mutamento strutturale del "rapporto normativo" tra il soggetto interno all'ente e la regola di comportamento, là dove questa sia tecnicamente incorporata nel sistema di gestione aziendale e così resa autoesecutiva e non più rimessa alla libera adesione da parte del destinatario del precetto (per cui v. *infra*, par. 2.2.1); dall'altro lato, non può trascurarsi come alcuni autori abbiano prospettato la possibilità di utilizzare gli strumenti di *compliance* digitalizzata per «tracciare le strutture di comportamento» e così potenzialmente prevenire in tempo reale eventuali violazioni[69], postulando non già soltanto il monitoraggio della realtà aziendale e dell'attività operativa (nei termini già descritti *supra*), bensì anche forme di sorveglianza sui singoli *soggetti* che nell'impresa si trovano a operare. Dato che quest'ultimo scenario pare invero piuttosto problematico – presupponendo il d. lgs. 231/2001, delle due, piuttosto la prima forma di vigilanza (sull'attività), non la seconda (sui dipendenti) – esso sarà analizzato direttamente nella seconda parte di questo scritto (v. *infra*, par. 3), appunto dedicata ai rischi della *compliance* digitale.

[69] Cfr. NEUFANG, *Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen*, cit., 251; SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 143. In generale, circa la necessaria presenza di una componente predittiva nell'ambito di ogni modello di *compliance*, tuttavia solitamente fondata su generalizzazioni empiriche od osservazioni delle strutture del comportamento umano, cfr. anche CENTONZE, *The Imperfect Science: Structural Limits of Corporate Compliance and Co-regulation*, in *Corporate Compliance on a Global Scale*, cit., 50, nel senso che «*the main problem facing organization rulemaking is the precariousness of the generalizations and conceptual frameworks necessary to predict deviant behavior by organizational members*»; LANGEVOORT, *Global Behavioral Compliance*, cit., 220-221 propone, quale alternativa per una più efficace predizione dei comportamenti, di ricorrere alla psicologia cognitiva e sociale, e in particolare alla c.d. «*behavioral ethics*», ovvero a un modello fondato sulla cultura (collettiva) della *compliance*.

2.2.1. *Il modello organizzativo "*self-enforcing*" al confine tra repressione e prevenzione*. Come si anticipava, la digitalizzazione del modello organizzativo nella fase della sua *attuazione* pare aggiungere anch'essa un tassello, sul piano della "teoria generale", alla progressiva e ormai nota trasfigurazione del tradizionale monopolio normativo statuale che dipende dal (e si esprime nel) paradigma dell'auto-normazione. Ciò, in particolare, non dipende tanto dal fatto che il modello dell'auto-regolazione (digitalizzata) altera le gerarchie della produzione normativa, demandando ad attori privati una funzione regolativa, secondo un modello di «normazione decentralizzata»[70]: a ben vedere, infatti, la digitalizzazione nulla aggiunge, sul versante della *produzione*, alle già esistenti dinamiche di intersezione tra potestà normativa statuale e normazione reticolare e *riflessiva* da parte degli attori privati, presupposte dal modello regolatorio trasfuso nel d. lgs. 231/2001.

La peculiarità "normativa" della digitalizzazione si apprezza, invece, sul piano dell'*applicazione* delle regole: la codificazione (in senso digitale) di una regola (giuridica)[71] e l'automazione della sua applicazione finiscono, per certi versi, per alterare il rapporto tra la realtà e il diritto, il quale degrada nella sua stessa effettività[72]. In altri termini, in un contesto di «diritto operativo» e "auto-esecutivo", qual è un modello organizzativo automatizzato, l'atto conforme a diritto diventa esso stesso *l'unica realtà possibile*[73], proprio in virtù della capacità del digitale di «internalizzare» le regole e di renderle al contempo *immediatamente* e *inevitabilmente* esecutive. A tal proposito, è stata coniata la dicitura di «*regulating technologies*»[74] (tecnologie *regolatrici*), proprio al fine di

[70] Cfr. TORRE, Compliance *penale e normativa tecnica*, in *Arch. pen.*, 2022, 1, in part. 7.

[71] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 722, nel senso che «*code shapes legal meaning through implementation of formal mandates*».

[72] Cfr. in questi termini GARAPON-LASSEGUE, *La giustizia digitale*, cit., 132. Cfr. anche LESSIG, *Code*, New York, 2006, in part. 81 ss., dedicate al tema della «*regulation by code*», ove si osserva come, in tale mutato contesto, «*the rule applied to an individual does not find its force from the threat of consequences enforced by the law—fines, jail, or even shame. Instead, the rule is applied to an individual through a kind of physics*», un «*physical constraint*».

[73] Cfr. ancora GARAPON-LASSEGUE, *La giustizia digitale*, cit., 196, nel senso di una «trasformazione interna della normatività», nonché 226 ss., ove gli Autori evidenziano la differenza (e la concorrenza) tra la simbolizzazione tramite il diritto (che si realizza attraverso «la scrittura alfabetica, la qualificazione giuridica e il rituale») e la digitalizzazione (vale a dire, la codificazione del reale tramite la «scrittura digitale»).

[74] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 723.

descrivere quei dispositivi tecnologici che incorporano «vincoli comportamentali e decisionali», determinati in modo conforme a diritto.

Se, come si anticipava, una simile forma di controllo coattivo (privato) dei comportamenti non pone questioni di legittimazione democratica – giacché le regole incorporate all'interno del modello organizzativo non corrispondono ad altro che all'attuazione degli obblighi derivanti dalla disciplina (statuale) vigente all'esterno dell'ente e alla quale l'ente stesso è tenuto a conformarsi[75] – si deve nondimeno evidenziare come la *compliance* digitale renda vieppiù sfumati i confini tra repressione e prevenzione[76], operando essa coercitivamente sul comportamento da ricondurre "a legalità" in un'ottica non più successiva, ma già preventiva. Il superamento della logica condizionale nella declinazione delle regole di condotta può allora prestare il fianco, anche in questo specifico ambito, ad alcune obiezioni: per un verso, infatti, un siffatto paradigma affievolisce quella conoscenza e quell'adesione consapevole ai precetti, da parte dei destinatari delle prescrizioni interne, che lo stesso d. lgs. 231/2001 (come si vedrà anche *infra*, par. 3.3) considera invece essenziale elemento della diffusione e dell'efficace attuazione del modello; per altro verso, un modello di regole "*self-enforcing*" può rivelarsi, ove non adeguatamente affiancato da un giudizio o un controllo umano, perniciosamente *inflessibile*, sino a diventare esso stesso fattore di rischio.

Con tali considerazioni non s'intende certo predicare l'impossibilità o l'inopportunità di attuare modelli di *compliance* a base tecnologica, *tutt'altro*: lo scopo è, invece, quello di definire le necessarie cautele, affinché la *compliance* digitale possa soddisfare quelle esigenze di trasparenza e di *accountability* che risultano essenziali nello sviluppo di qualsivoglia sistema algoritmico, dotato di poteri coercitivi e normativi sul comportamento dei soggetti che vi interagiscono e per questa ragione bisognoso di quell'*human oversight* che garantisce il rispetto dei principi generali del sistema pur in un contesto non più analogico ma, per l'appunto, digitale.

---

[75] *Ibid.*, 724.

[76] In argomento anche BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Rivista Italiana di Diritto e Procedura Penale*, 2019, 4, 1909-1942; ID., *Von der »Strafrechts«ordnung der Prädiktionsgesellschaft zur Strafrechts»ordnung« des liberalen Rechtsstaats*, in *Normative Ordnungen*, a cura di Forst-Günther, Berlino, 2021, 553 ss.

2.3. *Prime conclusioni provvisorie sulle potenzialità della compliance digitalizzata entro e oltre il d. lgs. 231/2001.* A conclusione di questa prima sezione, dedicata alle potenzialità della *compliance* digitale, pare si sia dimostrato come siano molteplici le ragioni – anzitutto in termini di efficienza pratica – che militino a favore dell'elaborazione di modelli organizzativi *data-driven* e *tech-based*; i quali potrebbero, peraltro, potenzialmente costituire un ulteriore *booster* rispetto all'(auspicata) standardizzazione tecnica dei c.d. *compliance programs*, in sinergia con il sistema delle certificazioni di qualità. A tale ultimo proposito, pur non potendo i due strumenti essere del tutto assimilati in ragione della profonda diversità di contenuti e finalità, la transizione digitale del processo della *compliance* potrebbe risultare utile ad attivare quei "minimi comuni denominatori" rispetto al sistema delle certificazioni di qualità che consentano all'ente di beneficiare, anche a fini 231, del riconoscimento del possesso di un sistema di organizzazione e controllo idoneo, in negativo, a prevenire la commissione di reati-presupposto e, in positivo, ad integrare la legalità nella *governance*, superando la tradizionale idea della "sovrastruttura burocratica" verso la richiamata prospettiva di una "*compliance embedded*".
A ciò si aggiunga poi come l'opportunità della digitalizzazione non si apprezzi soltanto con riguardo al d.lgs. 231/2001 e alla funzione di prevenzione dei reati nel contesto dell'impresa, ma paia potersi estendere in senso, per così dire, "olistico" a ogni altro sistema di *compliance*, adottato da parte di soggetti privati – si pensi, ad esempio, ai sistemi di gestione certificati – ma anche (ed è forse questo un profilo ancora piuttosto inesplorato) da parte di autorità pubbliche[77].

[77] A tale ultimo riguardo, si osservi, ad esempio, come il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, che istituisce il dispositivo per la ripresa e la resilienza, abbia previsto modalità di monitoraggio e controllo sull'utilizzo dei fondi, da parte delle amministrazioni degli Stati membri, essenzialmente digitalizzate: ad esempio, all'art. 22, in tema di tutela degli interessi finanziari dell'Unione, si prevede che, ai fini dell'audit e del controllo sull'impiego dei fondi *Next Generation UE*, i singoli Stati membri debbano raccogliere e fornire alla Commissione una serie di categorie standardizzate di dati; inoltre, si prevede che la Commissione metta a disposizione degli Stati membri «un sistema integrato e interoperabile di informazione e monitoraggio, comprendente un unico strumento di estrazione di dati e valutazione del rischio, al fine di accedere ai dati pertinenti e di analizzarli, in vista di un'applicazione generalizzata di tale sistema da parte di Stati membri», così prefigurando un modello di controllo senz'altro riconducibile al paradigma della *compliance* digitale.

Com'è stato osservato, infatti, la logica della *compliance* – che individua nel «fattore organizzativo» il «punto d'appoggio delle politiche di prevenzione»[78] – ispira tutti i più recenti paradigmi regolatori e si contraddistingue quale «tecnica di intervento e gestione dei rischi»[79] tipica dell'era contemporanea: sia essa «cogente», «incentivata» o «volontaristica», rigida o flessibile[80], essa si basa in ogni caso sull'adozione di sistemi di controllo interno che, per tutte le ragioni già analizzate, possono indubbiamente risentire dei benefici (in termini di *efficacia, efficienza, effettività*) della digitalizzazione.

Ma vi è di più, perché pare a chi scrive che la digitalizzazione della *compliance* possa intercettare con singolare efficacia – e, in tal senso, coadiuvare – le linee di sviluppo che ora si prefigurano per il paradigma stesso della *compliance*, vale a dire la c.d. "*compliance* integrata" e la "*cooperative compliance*". Non essendo questa la sede per soffermarsi con ampiezza di riferimenti su tali traiettorie evolutive, basterà soltanto sottolineare come la digitalizzazione possa, anzitutto, agevolare l'interazione sinergica tra i diversi sistemi di *compliance* adottati all'interno dell'ente, nonché tra questi e la funzione di *governance*: con l'effetto, dunque, di evitare i «problemi di coordinamento» e le «ridondanze» che derivano dalla propagazione e dalla sovrapposizione dei diversi sistemi di controllo interno che un medesimo ente può essere tenuto ad adottare[81]. Sul versante, invece, della *cooperative compliance*, si è parimenti rilevato come le tecnologie dell'informazione possano incentivare percorsi di riforma del modello della *compliance*, verso forme di regolazione dinamica (al contempo *top-down* e *bottom-up*), nelle quali le autorità pubbliche definiscano *standard* per la gestione del rischio e cooperino continuativamente con gli enti privati nelle attività di monitoraggio, secondo un paradigma di vigilanza collaborativa *data-driven*[82].

---

[78] In questi termini, cfr. MONGILLO, *Presente e futuro della* compliance *penale*, cit., 2.

[79] *Ibid.*, 6.

[80] *Ibid.*, 7, ove l'A. distingue tra *compliance* cogente», «incentivata» o «volontaristica», in dipendenza del «diverso grado di vincolatività» delle regole di *compliance*, e tra «rigida» e «flessibile» a seconda della maggiore o minore definizione normativa dei presidi da adottare; sulle diverse forme di autonormazione, cfr. anche BIANCHI, *Appunti per una teoria dell'autonormazione penale*, in *Riv. it. dir. proc. pen.*, 2019, 3, 1477-1526.

[81] Cfr. MONGILLO, *Presente e futuro della* compliance *penale*, cit., 9-10.

[82] Cfr. a tal proposito le *proposals of reform* delineate da BAMBERGER, *Technologies of Compliance*, cit., 729; TORRE, Compliance *penale e normativa tecnica*, cit., 23. In argomento, v. anche PERRONE, *La*

3. *I rischi della* compliance *digitalizzata*. Come anticipato, nella seconda parte dell'analisi risulta essenziale indagare quali siano i limiti e i rischi connessi al ricorso a sistemi di *compliance* digitalizzata all'interno dell'impresa, dovendosi sin d'ora anticipare come, per un verso, sia particolarmente avvertita l'esigenza di scongiurare il rischio che un modello organizzativo a base tecnologica possa tramutarsi in una sorta di sistema di *predictive policing* privato[83]; e come, per altro verso, ai modelli di *compliance* basati su *smart technologies* si estendano tal quali le medesime esigenze di tutela e di controllo che già contraddistinguono le più varie applicazioni dell'intelligenza artificiale e degli algoritmi basati sui dati.

Prima di entrare nel merito della riflessione, si vuole precisare come esuli, invece, dall'ambito del presente lavoro una disamina delle possibili implicazioni sociali ed economiche del ricorso a sistemi di *compliance* a base tecnologica: a tal proposito, può essere sufficiente segnalare come sia stata da taluni denunciata la «normalizzazione e internalizzazione di una modalità post-panottica di esercizio del potere e di limitazione della libertà»[84] che ne deriverebbe, così riconducendosi anche il modello della *compliance* digitalizzata a quel c.d. «capitalismo della sorveglianza» da più parti individuato quale nuovo modello di *business* tipico del futuro digitale[85]. Analogamente non si farà qui riferimento alle questioni connesse al *digital divide* che rende potenzialmente meno comprensibili i processi alla base della *compliance* digitale medesima, se non nei limiti di quanto attiene al requisito della *explainability*.

3.1. *Il predictive policing aziendale tra protezione dei dati e tutela dei lavoratori*. La principale preoccupazione manifestata dagli interpreti, rispetto

---

nuova vigilanza. RegTech e capitale umano, in *Banca borsa titoli di credito*, 2020, 4, 516-526 e in part. 526, ove l'A. prospetta per l'appunto «un'evoluzione del rapporto tra vigilanza e *RegTech* in senso marcatamente cooperativo».

[83] In ordine alle potenzialità predittive delle nuove tecnologie digitali, cfr. ZACCARIA, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, cit., *passim*.

[84] In questi termini BURCHARD, *Digital criminal compliance*, cit., 750-751, che ravvisa in questo fenomeno una «*Normalisierung und Internalisierung eines post-panoptischen Machtausübungs- und Freiheitsbegrenzungsmodus*».

[85] Il riferimento è ovviamente a ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

all'ipotesi della *compliance* digitalizzata, risiede generalmente nel timore che, per suo tramite, si introduca all'interno dell'ente un sistema di «algoritmi inquisitori»[86], che potrebbero sacrificare eccessivamente, sull'altare delle ragioni della conformità normativa interna, interessi contrapposti, quali ad esempio la protezione dei dati personali, il diritto alla riservatezza, la tutela della dignità dei lavoratori e il principio di non discriminazione[87].

A ben vedere, se riguardato in questa prospettiva, il tema della "legittimità" della *compliance* digitale si pone allora al crocevia tra diverse questioni già più familiari alla dottrina penalistica: si allude, segnatamente, alla definizione dei limiti del controllo a distanza dei lavoratori; all'individuazione, in difetto di un'apposita disciplina, delle disposizioni applicabili alle c.d. "investigazioni interne" all'impresa; nonché, da ultimo, all'uso di strumenti di c.d. *predictive policing*, ora da valutarsi non tanto rispetto ai poteri delle autorità statali[88], quanto invece nell'ambito delle prerogative di autotutela preventiva da parte di soggetti privati[89]. Simili profili di potenziale criticità si pongono, beninteso, soprattutto là dove gli strumenti di monitoraggio e i controlli interni digitalizzati si estendano *dall'ente a coloro che vi operano*[90]: un'eventualità che, tuttavia, non è meramente ipotetica, essendo anzi già diffusi – all'interno di alcuni *compliance programs* – strumenti di c.d. «*electronic performance monitoring*»[91], che consistono in forme di sorveglianza diretta e di esercizio di poteri di polizia predittiva sui dipendenti dell'ente[92].

---

[86] SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 222.

[87] Cfr. ancora BURCHARD, *Digital criminal compliance*, cit., 754, ove si evidenzia anche il conflitto di *ratio* tra le diverse discipline che la *compliance* digitalizzata chiama in causa: il diritto penale, il diritto del lavoro, il diritto societario, ad esempio.

[88] Sul tema, nell'ambito di una letteratura sconfinata, si può fare riferimento, ad es., ad ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. proc.*, 2021, 6, 724-734, nonché a FERGUSON, *Policing predictive policing*, in *Washington University Law Review*, 2017, 94, 5, 1109-1189.

[89] In argomento, cfr. ad es. KATYAL, *Private Accountability in the Age of Artificial Intelligence*, in *UCLA Law Review*, 2019, 66, 54-141.

[90] Osserva ad es. SEVERINO, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, cit., 123, che le questioni di tutela della *privacy* e dei diritti dei lavoratori non si pongono qualora oggetto di analisi algoritmica siano dati di carattere puramente oggettivo.

[91] Cfr. KALISCHKO-RIEDL, *Electronic Performance Monitoring in the Digital Workplace: Conceptualization, Review of Effects and Moderators, and Future Research Opportunities*, in *Frontiers in Psychology*, 2021, 12, 1-15, che descrivono le molteplici forme che l'*electronic performance monitoring* dei dipendenti può assumere, distinguendo anche a seconda dei livelli di monitoraggio (a livello di organizzazione, di dipartimento, fino al monitoraggio individuale), ovvero dell'oggetto (la *performance*, il lavoro o

È, dunque, indubbio che – a fronte della trasformazione del luogo di lavoro in un c.d. «*digital workplace*», nel quale ogni azione o transazione produce dati e risulta perciò tracciabile e monitorabile (dalla posta elettronica aziendale, fino agli stessi spostamenti del dipendente, in uno con la sempre più marcata sovrapposizione tra «strumento di lavoro e strumento di controllo»[93]) – si ponga l'esigenza di definire i limiti dei (più ampi) poteri d'indagine ora disponibili per il datore di lavoro, sul presupposto – come si anticipava – del necessario bilanciamento tra le ragioni della *compliance* e i diritti fondamentali dei soggetti coinvolti.

Nuovamente, la riflessione richiede una preliminare *actio finium regundorum*, non volendosi in questa sede analizzare, in una prospettiva onnicomprensiva, tutte le ipotesi nelle quali l'oggetto dell'investigazione interna sia in formato elettronico: uno scenario, quest'ultimo, che evoca il ben diverso tema della prova digitale e della c.d. *digital forensics*. Al contrario, nell'ambito della presente ricerca si vuole comprendere quali nuove e ulteriori esigenze di tutela derivino *specificamente* dalla digitalizzazione dei processi di *compliance*.

Per procedere con ordine, pare allora opportuno analizzare le diverse forme di controllo, ipotizzabili nell'ambito di un modello organizzativo a base tecnologica, seguendo un'ideale struttura a cerchi concentrici, nella quale il dipendente occupa il punto centrale e la distanza dal centro aiuta a rappresentare graficamente il grado di invasività dei controlli rispetto ai diritti della personalità dei soggetti destinatari.

---

l'individuo), o ancora delle tecnologie impiegate.

[92] Cfr. in particolare RUDKOWSI, *„Predictive policing" am Arbeitsplatz*, in *Neue Zeitschrift für Arbeitsrecht*, 2019, 72-77, che evidenzia come tali forme di sorveglianza non possano utilizzare dati anonimizzati senza subire una notevole limitazione in termini di efficacia, ritenendo che la prevenzione diretta e specifica dei possibili reati possa essere *effettiva* solo se e in quanto riferita ai *singoli* dipendenti. Cfr. anche TULLINI, *Controllo tecnologico nell'impresa e protezione dei dati personali dei lavoratori*, in *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia,* cit., 377 ss., che per l'appunto rileva come la crescente applicazione di tecnologie digitali nei processi produttivi comporti «un significativo rafforzamento della sorveglianza in azienda e dei controlli a distanza sui lavoratori» e imponga, pertanto, di richiamare la disciplina prevista dall'art. 4 Stat. Lav.

[93] Cfr. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *www.sistemapenale.it*, 20 dicembre 2021, 24. Anche TULLINI, *Controllo tecnologico nell'impresa e protezione dei dati personali dei lavoratori*, cit., 389 ss., sottolinea come, in contesti produttivi caratterizzati da una sempre maggiore digitalizzazione, ogni dispositivo tecnologico finisca per costituire ad un tempo strumento dell'attività lavorativa, ma anche mezzo di monitoraggio, sorveglianza o raccolta di dati.

Così, una prima forma di controllo cui si può alludere – e che si pone nell'anello più esterno, in termini di invasività – è quella avente ad oggetto le comunicazioni dei dipendenti, con finalità, ad esempio, di prevenzione del rischio-reato. La questione non pare, a ben vedere, del tutto inedita, potendosi fare riferimento al tema – invero già noto, nell'ambito della dottrina penalistica, e per certi versi antesignano delle crescenti capacità di monitoraggio derivanti dalla digitalizzazione – del controllo della posta elettronica del dipendente. A tal proposito, non pare infatti che la *compliance* digitale ponga questioni sostanzialmente nuove, essendo in ogni caso il controllo della *mail* e dei mezzi di comunicazione aziendale condizionato alla previa informativa e al previo consenso del dipendente: pena, in caso contrario, la violazione del "domicilio digitale" del lavoratore[94].

Senz'altro più invasiva – e da collocare, pertanto, in un anello più interno, nella descritta progressione a cerchi concentrici – è invece la possibilità di monitorare in tempo reale *direttamente* il singolo lavoratore, con analoghe finalità di prevenzione dei reati o di controllo dell'attività produttiva: una questione che, com'è stato condivisibilmente osservato, porta nuova linfa al tema "classico" della liceità del controllo a distanza dei lavoratori, disciplinato dall'art. 4 dello Statuto[95]. Anche in tal caso, tuttavia, la disciplina attualmente in vigore rende sufficienti – là dove il controllo rientri nelle finalità previste dalla norma (esigenze organizzative e produttive, sicurezza del lavoro e tutela

[94] Cfr. ROCCO, *Attività: ricerca e analisi documentale ed altre attività*, in *Investigazioni interne. Poteri, Diritti, Limiti, Responsabilità*, a cura di Di Fiorino-Fornari, Pisa, 2022, 35 ss. e in part. 38, nonché 44 ss., ove l'A. elenca le indicazioni fornite dal Garante per la protezione dei dati personali, in tema di accesso alla *mail* aziendale. Cfr. anche ad es. Cass., sez. V, 28 ottobre 2015, n. 13057, in *Cass. pen.*, 2017, 1, 144 ss., nel senso che l'accesso alla casella di posta elettronica del dipendente, protetta da una *password*, comporta una violazione del suo domicilio informatico, ed è pertanto comportamento illecito – in mancanza di consenso – anche là dove posto in essere dal superiore gerarchico. Cfr. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, cit., 190, che ipotizza anche il possibile controllo sull'utilizzo di internet da parte dei dipendenti, anche mediante l'interdizione della possibilità di navigare liberamente sul web mediante i pc aziendali. Sottolinea LANGEVOORT, *Global Behavioral Compliance*, cit., che sia frequente, specialmente nelle grandi *corporations*, l'effettuazione di un costante «*machine read*» di tutte le e-mail dei dipendenti per coglierne il "tono" e individuare possibili segnali di allarme (ansia, pressione, etc.).

[95] In argomento, cfr. essenzialmente NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, cit., nonché BIRRITTERI, *Controllo a distanza del lavoratore e rischio penale*, in *www.sistemapenale.it*, 16 febbraio 2021. Ancora, TULLINI, *Controllo tecnologico nell'impresa e protezione dei dati personali dei lavoratori*, cit., 378 ss.

del patrimonio aziendale, tra le quali non v'è dubbio che rientri anche la *compliance*[96]) – la previa informativa e l'acquisizione del consenso delle rappresentanze sindacali (ovvero dell'autorizzazione dell'Ispettorato del lavoro). Ciò, sebbene l'art. 88 GDPR (in tema di *Trattamento dei dati nell'ambito dei rapporti di lavoro*) preveda espressamente la possibilità, per gli Stati di membri, di introdurre *standard* di maggiore tutela dei dati dei lavoratori, includendo anche «i sistemi di monitoraggio sul posto di lavoro» tra le ipotesi particolari di trattamento che possono giustificare l'adozione di «misure appropriate e specifiche, a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati», sul presupposto per cui le mutate *modalità* di controllo (ora digitalizzate o automatizzate) possono rendere non più sufficiente un sistema autorizzativo che si basi sul solo consenso del dipendente interessato[97].

Da ultimo, l'anello più interno dell'ideale tassonomia dei controlli strutturata secondo cerchi concentrici, è senz'altro occupato dalla possibilità – prospettata da parte della dottrina[98] – che i sistemi di *compliance* digitalizzati possano comprendere una sorta di *predictive policing personale* che – sul modello del *predictive policing* utilizzato dalle autorità pubbliche per la prevenzione dei reati[99] – integri e potenzi il modello organizzativo con una valutazione preven-

[96] Cfr. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, cit., 25, nel senso che «l'adozione di un modello organizzativo attecchisca proprio nelle esigenze elencate dall'art. 4, comma 1 St. lav». Cfr. TULLINI, *Controllo tecnologico nell'impresa e protezione dei dati personali dei lavoratori*, cit., 385, ove l'A. riflette sulla nozione di «controlli difensivi» e sulla riconducibilità ad essa, ad esempio, dei controlli posti in essere dal datore di lavoro per la prevenzione degli illeciti (anche informatici) eventualmente commessi dai singoli dipendenti.

[97] Cfr. BURCHARD, *Digital criminal compliance*, cit., 743, che esclude altresì la possibilità di ritenere un tale consenso *liberamente espresso.* Va peraltro rilevato come anche l'art. 22 GDPR, in tema di processi decisionali automatizzati, pur riconoscendo il diritto dell'interessato di «non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona», esclude tuttavia che un siffatto divieto si applichi quando la decisione «si basi sul consenso esplicito dell'interessato».

[98] Cfr. in termini critici RUDKOWSI, *„Predictive policing" am Arbeitsplatz*, cit., *passim*; in termini maggiormente entusiastici invece cfr. ad es. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 143; NEUFANG, *Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen*, cit., 251.

[99] In relazione al quale cfr. da ultimo la *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in*

tiva e predittiva del rischio *individuale* di commissione di reati o di violazioni del modello, con riferimento a quanti si trovano a operare nell'ente[100]: il che sottende un salto concettuale che non deve passare inosservato, individuandosi in tale maniera il rischio da gestire non già soltanto nell'attività dell'ente, quanto invece e soprattutto *nel singolo lavoratore*, che verrebbe a costituire egli stesso un fattore di rischio[101]. Dal punto di vista delle esigenze di tutela dei soggetti coinvolti, del resto, non si tratta più soltanto di garantire l'integrità della corrispondenza o il diritto alla riservatezza, ma di assicurare la tutela della dignità umana e di scongiurare esiti discriminatori, nell'ambito di valutazioni predittive che – sia pur in contesto privato – sono idonee a produrre effetti concreti sull'individuo e, ad esempio, sul suo rapporto di lavoro[102]. Pur non potendosi in questa sede analizzare *funditus* il tema del *predictive policing* in ambito privato, pare tuttavia che ad esso possano opportunamente estendersi le riflessioni già elaborate con riguardo all'uso di algoritmi predittivi da parte di autorità pubbliche: non potendosi, infatti, dubitare del fatto che anche gli attori privati – sia pur in misura variabile, a seconda delle effettive conseguenze di un'eventuale prognosi negativa – debbano garantire la trasparenza e l'*accountability* degli strumenti predittivi adottati per la valutazione del rischio-reato di individui o gruppi, a garanzia di valori «non rinunciabili», quali il principio di non discriminazione e la tutela della dignità e libertà della persona[103].

3.2. *Il modello organizzativo digitalizzato quale oggetto di regolazione: spunti dall'AI Act.* Accanto alle descritte implicazioni per la tutela dei diritti fonda-

ambito penale (2020/2016(INI)), ove, pur riconoscendosi le «grandi opportunità» che l'intelligenza artificiale può offrire nel settore delle attività di contrasto della criminalità, si evidenziano tuttavia i «rischi significativi per i diritti fondamentali dei cittadini» che tale strumento comporta e si ritiene che «l'applicazione generalizzata dell'IA al fine della sorveglianza di massa sarebbe sproporzionata».

[100] Cfr. BURCHARD, *Digital criminal compliance*, cit., 748.

[101] Segnala questa eventualità ancora BURCHARD, *Digital criminal compliance*, cit., 751, che ravvisa in questo passaggio una "deviazione" verso il "paradigma della sfiducia" all'interno del contesto aziendale.

[102] Cfr. ancora la *Risoluzione del Parlamento europeo del 6 ottobre 2021*, cit., che individua nell'autonomia, nella dignità umana e nella non-discriminazione i valori essenziali cui assicurare tutela, rispetto all'utilizzo di sistemi predittivi di *scoring*.

[103] Cfr. ZACCARIA, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, cit., 44, con riferimento all'uso di algoritmi predittivi da parte di autorità pubbliche.

mentali, tra le "controindicazioni" della digitalizzazione della *compliance* sono stati anche annoverati alcuni dei rischi "tipici" dell'automazione: tra tutti, l'eccessivo (quanto inevitabile) affidamento che sarebbe necessario riporre negli esiti di un processo valutativo e deliberativo di gestione del rischio non facilmente comprensibile o verificabile "dall'esterno", in quanto automatizzato (c.d. effetto *black box*)[104].

In questo senso, se l'idea stessa della digitalizzazione nasce dall'esigenza di «salvare il giudizio [umano] dalla propria umanità», liberando i processi di percezione, controllo e deliberazione da ogni possibile pregiudizio, errore o «stortura cognitiva»[105], non può non rilevarsi come in ogni ambito – ed è emblematica, in tal senso, la stessa impostazione della Proposta di Regolamento europeo sull'intelligenza artificiale[106] – sia, tuttavia, vieppiù avvertita l'esigenza di corredare l'automazione di una necessaria forma di controllo umano (c.d. *human oversight*).

A tale proposito, risulta dunque rilevante, anche ai più limitati fini della presente riflessione, passare brevemente in rassegna i criteri cui la citata Proposta di Regolamento europeo (c.d. *AI Act*) ispira la disciplina dei sistemi di intelligenza artificiale ad alto rischio (nell'ambito dei quali possono farsi rientrare anche i sistemi di *compliance* "intelligenti"[107]): tra questi, ad esempio, la ne-

---

[104] Cfr. BAMBERGER, *Technologies of Compliance*, cit., 705 ss. Nel rinviare a PASQUALE, *The black box society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015, si vuole sottolineare come l'A. individui in effetti in una «*intelligible society*» l'obiettivo cui mirare, rispetto al futuro sviluppo di strumenti algoritmici e intelligenza artificiale. SABIA, *Artificial Intelligence And Environmental Criminal Compliance*, cit., 179 ss., ricollega all'uso dell'intelligenza artificiale per finalità di *compliance* un ulteriore profilo critico, tradizionalmente connesso all'automazione: nel caso in cui l'ente affidi la prevenzione dei reati a un *software* automatizzato e un reato venga comunque commesso, nell'interesse o a vantaggio dell'ente medesimo, potrebbe risultare complesso attribuire all'ente la responsabilità per il delitto che ha omesso di prevenire, qualora ciò sia dipeso da un malfunzionamento o da un errore dell'algoritmo "autonomo", utilizzato per le attività di *compliance*.

[105] Lo illustrano GARAPON-LASSEGUE, *La giustizia digitale*, cit., 112.

[106] Cfr. *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021.

[107] L'elencazione dei sistemi di IA ad alto rischio è contenuta nell'Allegato III, che vi annovera – per quanto ora rileva – ad esempio «l'IA destinata a essere utilizzata per [...] il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito [dei] rapporti di lavoro». In generale, la riconducibilità dei modelli di *compliance* digitale alla definizione di sistemi di IA ad alto rischio parrebbe anche confermata dal considerando n. 36, che comprende tra i sistemi ad alto rischio quelli capaci di produrre un impatto significativo «sul futuro delle persone controllate e dunque sui loro diritti

cessità che il sistema sia corredato di apposite misure di gestione del rischio; che il sistema consenta la registrazione automatica degli eventi durante il suo funzionamento; che il sistema sia progettato e sviluppato in modo tale da garantire che il suo funzionamento sia sufficientemente trasparente, così da consentire agli utenti di interpretare l'*output* del sistema e utilizzarlo adeguatamente; ancora, che i sistemi siano strutturati in modo tale da poter essere efficacemente supervisionati da persone fisiche quando sono in uso. Com'è evidente, la diffusione di modelli di *compliance* digitalizzata basati sull'intelligenza artificiale porrebbe allora l'esigenza di adottare alcuni presidi che tutelino l'ente da eventuali malfunzionamenti del suo stesso sistema di *compliance* e che ne garantiscano la trasparenza e la c.d. *explainability*.

Per altro verso, è stato altresì segnalato come i medesimi protocolli a base tecnologica dei quali si postula l'infallibilità si prestino nondimeno a elusioni e manipolazioni da parte di quanti ne conoscano il funzionamento (nonché, volendo, anche *dall'esterno* dell'ente). Coerentemente con gli standard di accuratezza, robustezza e *cybersecurity* previsti dall'*AI Act* (art. 15), pare allora essenziale che l'ente si impegni per *tutelare* attivamente il sistema di *compliance* digitale adottato, la cui adeguatezza dipenderà, pertanto, anche dal grado di protezione complessivamente assicurata ai dati, ai dispositivi e alle reti: si dovrà, ad esempio, assicurare che il sistema stesso sia *cyber*-resistente (potendo esso, appunto, resistere a eventuali attacchi informatici esterni, in quanto dotato di adeguati presidi difensivi), ma anche *cyber*-resiliente (vale a dire, capace di assicurare la continuità del proprio funzionamento).

In questi termini, dunque, pare che i requisiti (che saranno) dettati per disciplinare lo sviluppo di sistemi di intelligenza artificiale possano riflettersi sulla stessa valutazione di idoneità ed efficace attuazione del modello di *compliance*, che potrà dirsi adeguato in quanto, ad esempio, protetto da eventuali malfunzionamenti o *cyber*attacchi: quindi, prefigurando un'ulteriore ricaduta sistematica della digitalizzazione sui paradigmi di auto-normazione e sulla relativa valutazione giudiziale.

---

fondamentali», per cui cfr. anche NISCO, *Riflessi della compliance digitale in ambito 231*, cit., 8.

3.3. Compliance *digitalizzata e teoria delle organizzazioni; dalla metafora meccanicistica alla cultura dell'integrità.* Alcuni ulteriori spunti critici, rispetto alle potenzialità di forme di *compliance* (interamente) automatizzate, possono, infine, derivare dagli studi di teoria dell'organizzazione.

In particolare, riprendendo il fondamentale studio di Gareth Morgan sulle metafore dell'organizzazione[108], l'idea di una completa informatizzazione delle attività di *compliance* pare appiattirsi eccessivamente sull'immagine dell'organizzazione come "macchina"[109], che si esprime nella standardizzazione di ogni segmento dell'attività aziendale, mediante «una serie precisa di norme», il cui rispetto è successivamente oggetto di controllo e valutazione. Un simile approccio meccanicistico tende però «a farci sottovalutare gli aspetti umani dell'organizzazione»[110] e a trascurare la complessità del suo funzionamento, tanto che le potenzialità e i limiti che Morgan riconduce all'uso di una «metafora meccanicistica» per la descrizione di un sistema complesso, qual è una società o un altro ente collettivo[111], paiono attagliarsi precisamente anche alla *compliance* digitale: tra tutti, la deresponsabilizzazione dei singoli "ingranaggi" e la creazione di una tendenza alla conformità passiva (appunto, meccanica) alle regole di condotta *in ogni caso*, che non incoraggiano né i tentativi «di migliorare ciò che si sta facendo», né l'adattamento ai mutamenti o la flessibilità di reazione[112].

Simili conseguenze non risultano, peraltro, irrilevanti, a maggior ragione se considerate alla luce del contesto normativo già analizzato, ove è al contrario essenziale il coinvolgimento di tutte le componenti dell'organizzazione nelle attività di prevenzione del rischio-reato: basti pensare, ad esempio,

---

[108] Cfr. MORGAN, *Images. Le metafore dell'organizzazione*, Milano, 2002.

[109] Cfr. *ibid.*, 33, nel senso che le imprese tendenzialmente «sono state progettate per essere delle macchine ed i loro dipendenti devono comportarsi come se fossero dei componenti di tali macchine». Cfr. in senso analogo anche SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, cit., 222, nel senso che la *compliance* penale tecnologica porta con sé il rischio di trasformare l'impresa in un «ente meccanico», una «*clockwork corporation*».

[110] *Ibid.*, 49.

[111] *Ibid.*, 48 ss.

[112] Nella medesima prospettiva, anche GARAPON-LASSEGUE, *La giustizia digitale*, cit., 242, sottolineano come il «mito della delega alle macchine» ricomprenda un insieme di «idee guida» - «reti, flusso, calcolo, formalizzazione, automaticità, sistema» - che «tende a rappresentare il mondo sociale come un *sistema*».

all'importanza che le attività di formazione dei dipendenti e dirigenti rivestono tanto nel "sistema 231", quanto nei sottosettori della *compliance antitrust* o della prevenzione della corruzione in ambito pubblico.

Elemento comune ai diversi sistemi di *compliance*[113] – nonché requisito valorizzato anche dalla giurisprudenza di legittimità, nell'ambito della valutazione sull'efficace attuazione del modello organizzativo[114] –, la formazione dei dipendenti sul contenuto dei modelli organizzativi, in parallelo con la diffusione di una cultura dell'integrità nel contesto aziendale[115], restituisce al contrario l'immagine di un modello di *compliance* che – su un piano squisitamente giuridico – è tanto più efficace, quanto più diffuso e condiviso nell'ambito aziendale. Tale descrizione evoca, allora, una diversa metafora utilizzata per descrivere le organizzazioni complesse, e segnatamente quella concezione che vede nell'ente collettivo (anche) un «sistema culturale», che si contraddistingue per un maggior coinvolgimento dei singoli membri e che realizza, come spiega Morgan, la condivisione di una cultura aziendale e di codici di comportamento «che permettano di vivere quotidianamente i modelli organizzati-

---

[113] Al riguardo, ritiene condivisibilmente BURCHARD, *Digital criminal compliance*, cit., 744, che la *criminal compliance* si componga di «*Kontroll*» e «*Kultur*». Evidenziano anche SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 138, come la «*Unternehmesnkultur*» (orientata al rispetto di principi di comportamento e alla conformità alla legge) costituisca uno dei "pilastri" sui quali si regge la valutazione dell'efficacia ed effettività del modello organizzativo in diversi ordinamenti (nella specie, in quello tedesco e in quello statunitense). D'altra parte, come rammentano gli Autori, anche le *US Sentencing Guidelines* (reperibili in *www.guidelines.ussc.gov*) ricomprendono tra i parametri di valutazione elencati nel §8B2.1 (*Effective Compliance and Ethics Program*) anche la promozione di «*an organizational culture that encourages ethical conduct and a commitment to compliance with the law*» e l'impegno «*to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program*» a quanti operano all'interno dell'ente. Anche LANGEVOORT, *Global Behavioral Compliance*, cit., 222, sottolinea come «*much of compliance in* informational *in nature*» (enfasi nel testo), così individuando anche una essenziale "sfida pedagogica" nella *compliance*; *ibid.*, 228, ove l'A. rileva come, sia negli USA che in Europa, il modello di *compliance* ritenuto preferibile anche dai regolatori unisca una componente «*data-driven*» e una componente «*behavioral*».

[114] Cfr. ad es. Cass., sez. IV, 22 gennaio 2020, n.13575, in *www.ilpenalista.it,* 17 luglio 2020, nel senso che concorre all'omessa previsione di un modello organizzativo adeguato anche la mancata formazione dei dipendenti.

[115] In relazione alla rilevanza di *entrambe* tali attività di formazione, da intendersi come separate e distinte (nei contenuti e negli obiettivi) cfr. ad es. le *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231* pubblicate da Confindustria nel mese di giugno 2021, 53: «accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari. Esso deve illustrare le ragioni di opportunità - oltre che giuridiche - che ispirano le regole e la loro portata concreta».

vi che si vuole realizzare»[116]: una dimensione, quest'ultima, che parrebbe eccessivamente sacrificata, là dove si optasse per modelli di *compliance* quanto più possibile automatizzati.

Infine, a completamento di tale diversa prospettiva sul tema oggetto del presente lavoro, può anche richiamarsi la metafora dell'organizzazione come "strumento di potere"[117], la quale – individuando nelle imprese strumenti di dominio che promuovono interessi economici a discapito di altri – può ritenersi anch'essa co-ispiratrice del sistema delineato dal d. lgs. 231/2001, ove solo si consideri che quest'ultimo fa appunto leva su una serie di fattori (la razionalità d'azione o la ricerca del profitto) caratteristici dell'organizzazione come "strumento di potere" – nel senso che a tale espressione attribuisce Morgan – e li "aziona" allo scopo di utilizzare la stessa organizzazione quale strumento di cambiamento. Ebbene, anche tale ulteriore dimensione della c.d. "prevenzione organizzativa" del rischio-reato potrebbe risultare eccessivamente trascurata là dove si ponesse un esclusivo accento su modelli di *compliance* auto-esecutivi.

Tali cenni, sicuramente non esaustivi e piuttosto asistematici, paiono ad ogni modo sorprendentemente efficaci, per individuare gli spazi che possono (o debbono) essere riservati alla *compliance* digitale, riconoscendo come all'elemento "obiettivo" della conformità alla legge debba necessariamente intersecarsi la creazione e la promozione di una cultura "dell'integrità".

4. *Profili di sostenibilità nella transizione digitale della* compliance. In una prospettiva più ampia rispetto a quella adottata sinora si vogliono, infine, evidenziare e analizzare i diversi piani d'intersezione – anche a livello di politiche globali ed europee – tra la (cruciale) nozione di «sostenibilità»[118] e le prospettive della transizione digitale della *compliance*.

Anzitutto, deve osservarsi come, al livello delle politiche globali, la transizione digitale della *compliance* possa rivelarsi un essenziale "strumento" per il per-

[116] Ancora MORGAN, *Images. Le metafore dell'organizzazione*, cit., 190-191.
[117] *Ibid.*, 382 ss.
[118] Sulla nozione di sostenibilità e le sue molteplici accezioni, cfr. ad es. FABER-JORNA-VAN ENGELEN, *The sustainability of "sustainability" — a study into the conceptual foundations of the notion of "sustainability"*, in *Journal of Environmental Assessment Policy and Management*, 2005, 7, 1, 1-33.

seguimento degli obiettivi di sostenibilità: rientra, infatti, tra i "17 obiettivi di sviluppo sostenibile" (*Sustainable Development Goals, SDGs*) delineati nella c.d. «Agenda 2030 per lo Sviluppo Sostenibile», promossa dalle Nazioni Unite[119], anche l'obiettivo (n. 16) di «creare organismi efficienti, responsabili e inclusivi a tutti i livelli», promuovendo le ragioni della giustizia e agendo per la prevenzione della criminalità. In particolare, nell'ambito dell'obiettivo n. 16 dell'Agenda Onu 2030 rientrano i "*target*" di «ridurre in modo significativo i flussi finanziari [...] illeciti», di «combattere tutte le forme di criminalità organizzata», di «ridurre sostanzialmente la corruzione e la concussione in tutte le loro forme». È dunque evidente una sensibile identità di accenti, rispetto ai sistemi di *compliance* aziendale, il cui potenziamento, mediante la digitalizzazione, risulta allora un'innovazione strumentale (anche) al raggiungimento di detti obiettivi: secondo un modello di sostenibilità *mediante la compliance* normativa che consente di intendere la nozione stessa di sostenibilità quale direttrice del futuro sviluppo ispirata alla cultura della legalità[120].

Parallelamente, la transizione digitale della *compliance* pare altresì intercettare gli obiettivi e le linee di intervento delineate, a livello europeo, nel programma *NextGenerationUE* e, a livello interno, nel Piano Nazionale di Ripresa e Resilienza: nello specifico, la Componente 2 della Missione 1 ha l'obiettivo di «rafforzare la competitività del sistema produttivo rafforzandone il tasso di digitalizzazione, innovazione tecnologica e internazionalizzazione», con particolare riguardo alle piccole e medie realtà produttive[121]. Una linea di intervento, dunque, che si pone in consonanza con le descritte possibilità di

[119] Cfr. *Resolution adopted by the General Assembly on 25 September 2015, 70/1. Transforming our world: the 2030 Agenda for Sustainable Development*, reperibile in *www.un.org*. Al riguardo, cfr. anche ARECCO-CATELLANI, Compliance, *ambiente, sostenibilità*, in *Ambiente&Sviluppo*, 2021, 893-896, che sottolineano il ruolo centrale degli attori privati (e della *compliance* aziendale) nel perseguimento degli obiettivi di sostenibilità delineati nell'Agenda 2030.

[120] Cfr. ancora ARECCO-CATELLANI, Compliance, *ambiente, sostenibilità*, cit., 893. In argomento, è stata altresì segnalata l'esigenza di una "sostenibilità digitale", per cui cfr. BENANTI-MAFFETTONE, *Decisioni politiche e sostenibilità digitale*, in *Intelligenza artificiale: Politica, economia, diritto, tecnologia*, cit., 10 ss. (ed. ebook), e in part. 35 ss., che rilevano la necessità di orientare lo sviluppo tecnologico «verso il bene comune».

[121] Cfr. il *Piano Nazionale di Ripresa e Resilienza* italiano e in part. 97 ss. (M1C2: Digitalizzazione, innovazione e competitività nel sistema produttivo).

digitalizzazione dei sistemi di controllo interno, in una prospettiva di crescita sostenibile agevolata dall'innovazione tecnologica.

Più in generale, si è anche rilevato come la digitalizzazione delle procedure e dei controlli interni possa determinare una maggiore *sostenibilità* economica e pratica degli obblighi-oneri di *compliance* aziendale. Sul primo versante, infatti, la transizione digitale consentirebbe un'indubbia riduzione dei costi[122], anche mediante l'integrazione tra i diversi sistemi di *compliance*[123]: con la conseguenza allora che la maggiore accessibilità di presidi organizzativi efficaci ed efficienti, capaci di ottimizzare gli sforzi di conformità normativa da parte della singola impresa, comporterebbe anche una sorta di "democratizzazione" nell'adozione dei modelli di *compliance*, che non sarebbero più appannaggio delle grandi realtà organizzate, ma potrebbero anzi essere adottati su più ampia scala nel tessuto economico delle PMI[124]. In un'accezione ancora diversa, la digitalizzazione del modello organizzativo potrebbe infine contribuire alla *sostenibilità* "pratica" e normativa, in termini di legalità e di prevedibilità del precetto, del modello di auto-normazione previsto dal d. lgs. 231/2001 e degli altri modelli di *compliance*, a condizione che essa, in virtù del suo più elevato grado di tecnicizzazione, possa sopperire a quella mancanza di *standard* che tuttora impedisce ai singoli di orientarsi con un ragionevole grado di certezza nell'adempimento dei propri oneri di prevenzione del rischio-reato[125].

---

[122] Cfr. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, cit., 151.

[123] In questo senso, cfr. MC KINSEY & COMPANY, *Sustainable compliance: seven steps toward effectiveness and efficiency*, in *www.mckinsey.com*, 10 febbraio 2017, che evidenzia come la moltiplicazione dei controlli e degli obblighi di *compliance* abbia portato le singole imprese a mettere in discussione la sostenibilità, pratica ed economica, della complessiva architettura preventiva adottata.

[124] In questo senso, anche TORRE, Compliance *penale e normativa tecnica*, cit., 9 evidenzia il nesso tra standardizzazione tecnica dei modelli organizzativi e sostenibilità della *compliance* per le piccole o medie imprese. Più in generale, sottolineano GARAPON-LASSEGUE, *La giustizia digitale*, cit., 86-87, come la digitalizzazione, nello specifico ambito del c.d. *legaltech*, abbia un'innegabile capacità di *empowerment* facilitando l'accesso alla giustizia e così democratizzando il "sistema" del diritto.

[125] Osserva ad esempio MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo*, cit., 661, come «la "autonormazione guidata" possa ritrovare un corretto equilibrio con le istanze di prevedibilità e "calcolabilità del diritto", e di sostenibilità per il mondo delle imprese». Ritiene tuttavia PALIERO, *Sub Art. 7,* in *Il 231 nella dottrina e nella giurisprudenza*, cit., 261 ss. e in part. 273 che difficilmente il legislatore possa ragionevolmente tipizzare «una realtà così variegata», condizionata da variabili «*dipendenti dalla singola e specifica realtà*» (corsivo nel testo), risultando così preferibile all'ipotesi della «positivizzazione di matrice pubblicistica» invece la «standardizzazione» imprenditoriale del «*know-how*» precauzionale-impeditivo.

5. Riflessioni conclusive: dalla conformità alla conformazione tecnologica dei comportamenti? Verso l'intersezione tra auto-normazione e digitalizzazione.
La riflessione sviluppata nelle pagine precedenti consente, in conclusione, di delineare alcune considerazioni di sintesi sulle potenzialità della *compliance* digitalizzata, sui rischi connessi al suo sviluppo e infine sulle implicazioni "di sistema" che sono ad essa riconducibili.
Come si è visto, infatti, la digitalizzazione – quale tecnica di codifica e di elaborazione di dati – è particolarmente affine, da un punto di vista strutturale, a tutti quei modelli di regolazione e di gestione del rischio che si basano sulla *procedimentalizzazione* delle attività e dei presidi e, in quanto tale, può dunque determinarne un indubbio quanto intuitivo potenziamento, secondo le tre direttrici, già richiamate, dell'*efficienza*, dell'*efficacia* e dell'*effettività*; ancora, la transizione digitale della *compliance* si appalesa particolarmente promettente per il perseguimento di obiettivi di *sostenibilità* dei processi di auto-normazione, in tutte le diverse accezioni nelle quali quella stessa nozione può essere intesa.
Come si è anticipato, vi è però anche un rovescio della medaglia. Sulla scorta delle precedenti considerazioni, pare infatti essenziale che ai dispositivi digitali di *compliance* sia attribuita una (mera, benché essenziale) funzione di *supporto* (e non già di *sostituzione*) rispetto ai più tradizionali presidi organizzativi e controlli interni: e ciò sia nel senso di assicurare che sul funzionamento di questi ultimi rimanga comunque costante la supervisione umana, sia nel senso di garantire che la conformità obiettiva alle norme – quand'anche facilitata dalla digitalizzazione e dalla sua capacità di rendere la *compliance* "*embedded*", in quanto incorporata nei processi e conseguentemente idonea a "forzare" il rispetto delle regole di comportamento insite nel *mezzo* tecnologico – si accosti alla diffusione e allo sviluppo di programmi di alfabetizzazione digitale parallelamente al rafforzamento di una cultura della legalità e dell'integrità all'interno dell'ente. In sintesi, quella tra digitalizzazione e auto-normazione deve configurarsi come *un'intersezione dinamica, consapevole e governata*, affinché la prima sviluppi le potenzialità della seconda e non ne esacerbi invece i nodi tuttora irrisolti.

In una prospettiva più generale, deve infine rilevarsi come le descritte tendenze alla transizione digitale dei processi di *compliance* mettano in un luce – per vero – un nuovo modello di disciplina e controllo dei comportamenti umani, che sicuramente trascende il limitato ambito della *compliance*: nella misura in cui le tecnologie della società dell'informazione consentono un pervasivo monitoraggio sui singoli e l'impedimento *diretto* di attività ritenute illecite, mediante una "conformazione tecnologica" dei comportamenti, viene posto in discussione, in termini di efficacia e di legittimazione, lo stesso modello (sinora invalso) di prevenzione (indiretta) dei reati mediante la minaccia di una pena[126]. Come anticipato, la sostenibilità, *rectius* l'aderenza ai principi generali del sistema penale, della transizione digitale dei processi di *compliance* potrebbe consentire di mantenere la capacità preventiva della sanzione attraverso una maggiore consapevolezza di quelli che si sono in precedenza definiti i diversi segmenti della filiera della *compliance* digitale nella tendenziale prospettiva di un impegno comune a valorizzare le opportunità offerte dalla tecnologia in ambiti storicamente dominati dalla componente umana. Piuttosto che tratteggiare linee conclusive, dunque, la presente riflessione non può allora che aprire nuovi interrogativi sul *futuro* dello stesso diritto penale – quale strumento di controllo e orientamento sociale – nell'era della sorveglianza tecnologica.

[126] Al riguardo, ritiene BURCHARD, *Digital criminal compliance*, cit., 741, che tale torsione verso forme di prevenzione "*diretta*" dei reati o di costante sorveglianza dei consociati debba ascriversi a un cambiamento di paradigma (in senso securitario) nell'approccio statuale al c.d. "*crime control*". Così, anche SIEBER, *The New Architecture of Security Law. Crime Control in the Global Risk Society*, in *Alternative systems of crime control: national, transnational, and international dimensions*, a cura di Sieber-Mitsilegas-Mylonopoulos-Billis-Knust, Berlin, 2018, 3 ss. sottolinea come si assista a un «*fundamental paradigm shift in the field of crime control: the traditionally punitive (or repressive) criminal law is being entrusted with progressively more preventive tasks, and it is increasingly being supplemented or partially replaced with 'more effective' legal regimes*», i cui effetti sarebbero addirittura amplificati dalle nuove tecnologie della società dell'informazione.