DIRITTO COMMERCIALE INTERNO E INTERNAZIONALE

LINDA MIOTTO

ORGANIZZAZIONE DI IMPRESA E GESTIONE DEI DATI PERSONALI

Il rischio di non *compliance* nelle catene di fornitura

G. GIAPPICHELLI EDITORE – TORINO

PREMESSA
LINEE DI SISTEMA E DI LETTURA

SOMMARIO: 1. Il ramo giuscommercialistico della gestione del rischio per la sicurezza dei dati personali. – 2. La tutela dei dati tra mercato e discrezionalità di impresa: verso un primato dei presidi organizzativi? Una lettura congiunta con la disciplina dei pagamenti elettronici, per l'enucleazione di un modello di gestione organizzata del rischio. – 3. Nuove tecnologie e propagazione del rischio tra imprese. Da un modello organizzativo atomistico a uno relazionale, tra co-regolamentazione e protezioni standardizzate. – 4. Dall'*outsourcing* bancario alla (etero)gestione del rischio di non conformità in tutte le catene negoziali. Generalizzazione, con adattamenti, di un modello settoriale. – 5. Dalla catena dei rischi a quella delle responsabilità. Implicazioni sulla *business judgment rule*.

1. *Il ramo giuscommercialistico della gestione del rischio per la sicurezza dei dati personali*. – Le fonti che normano la protezione dei dati personali possono essere rappresentate visivamente richiamando la forma di una struttura ramificata, che a partire dal fusto si diparte in due assi primari, l'uno dal quale si sviluppa la disciplina delle basi giuridiche per effettuare il trattamento, l'altro relativo ai presidi organizzativi funzionali a eseguirlo correttamente. Il primo ramo a sua volta si articola in ulteriori propaggini, su ciascuna delle quali possono collocarsi le riflessioni della dottrina, per lo più giusprivatistica, sui diversi fondamenti di liceità del trattamento. Si pensi ai dibattiti sulle condizioni di validità del consenso del titolare dei dati, e sull'interesse legittimo a procedere al trattamento anche senza l'acquisizione della relativa volontà autorizzatoria; ovvero alle discussioni sulle fattispecie nelle quali i dati siano trattati in adempimento di obblighi contrattuali o legali, o per la tutela di interessi vitali della persona interessata o di terzi o pubblici, o ancora nell'esercizio di

pubblici poteri. Le considerazioni che si svolgono in questo scritto si concentrano piuttosto sull'altro dei due rami primari, sul quale poggiano elementi di disciplina che, seppure riferiti alla protezione tecnica e organizzativa dai rischi specifici cui sono esposti i dati, in un approccio teorico-sistematico coinvolgono temi generali di corretta gestione imprenditoriale e di adeguatezza degli assetti organizzativi.

Come rappresentato dall'immagine naturalistica evocata, i due versanti della materia sono peraltro articolazioni di un apparato normativo unitario seppure complesso, che necessita di essere letto alla luce delle interconnessioni tra le sue parti. L'importanza della predisposizione di presidi organizzativi adeguati, in particolare, si comprende appieno se si pone in relazione con le diverse basi giuridiche del trattamento. Le cautele organizzative sono infatti richieste a prescindere che il trattamento si radichi sul consenso o sull'interesse legittimo, ma con una portata differente. Nel primo caso può ritenersi infatti, semplificando, che esse integrino l'autotutela valutativa del titolare dei dati; nel secondo operano invece quali condizioni che permettono di superare la necessità del consenso. L'eterotutela basata sulla gestione organizzata e procedimentalizzata del rischio, quindi su architetture tipiche dell'impresa, assume in tal modo il primato sull'autotutela basata sul meccanismo della volontà dell'individuo e su un approccio alla disponibilità dei dati radicato su uno stato di c.d. sovranità sugli stessi.

Lo spostamento del baricentro della tutela dal consenso all'organizzazione è funzionale a un mercato che ha nell'accessibilità dei dati una delle sue forze motrici, ma sul piano teorico pone temi complessi quali, anzitutto, l'effettività della protezione dei dati in relazione all'adeguatezza dei presidi organizzativi e, di conseguenza, l'individuazione delle leve per conseguirla tenendo conto dell'altrettanto rilevante esigenza di preservare la discrezionalità di impresa pur responsabilizzando chi la esercita. Si profila, più precisamente, una prima contrapposizione tra l'esigenza di delimitare la discrezionalità, per incrementare in modo generalizzato il livello delle tutele, e quella di preservare la flessibilità e l'autonomia organizzativa di impresa, per favorire la competizione e per scongiurare l'obsolescenza delle norme rispetto ai progressi della tecnica. La responsabilizzazione per le decisioni sulle valutazioni del rischio e sulle misure adeguate a gestirlo, in tal modo, entra in apparente antitesi con l'istanza di preservare lo spazio inviolabile della discrezionalità d'impresa, in particolare rispetto alla sindacabilità giudiziaria delle solu-

zioni adottate. Vanno comprese in queste diverse prospettive le implicazioni di alcune impostazioni di fondo del Regolamento sulla protezione dei dati (Gdpr) che, come si dirà, pare voler coniugare flessibilità, autonomia e responsabilità attraverso l'induzione a prescegliere soluzioni standardizzate, in particolare valorizzando l'adesione a specifici codici di condotta o a schemi di certificazione come indici di adeguatezza delle misure di sicurezza adottate.

Il ramo tematico delle misure organizzative, attorno al quale ruotano tali questioni, a sua volta si biforca. I presidi organizzativi si dispiegano infatti anzitutto nella struttura interna dell'ente, potendo richiedere sia l'adozione di procedure tecniche quali la pseudonomizzazione e la minimizzazione dei dati e dei relativi accessi, sia un'articolazione specifica degli apparati, come evidente ad esempio nei casi di designazione obbligatoria di un responsabile della protezione dati con competenze qualificate. L'organizzazione può rilevare però anche in una seconda dimensione che potremmo definire "relazionale", in quanto relativa ad interconnessioni con altre imprese rilevanti sul piano della condivisione del rischio. Il Regolamento considera l'ipotesi in cui il titolare del trattamento attribuisca all'esterno compiti specifici direttamente concernenti la protezione dei dati, e prevede in dettaglio le caratteristiche dell'atto di designazione di un terzo quale responsabile del trattamento, nonché di eventuali subresponsabili, a partire dalle indicazioni tassative da inserire sulle categorie di dati coinvolti, su natura, durata e finalità del trattamento assegnato, nonché sulle misure tecniche e organizzative adeguate a consentire il rispetto delle norme e delle istruzioni impartite dal titolare.

La possibile dimensione relazionale dei presidi organizzativi non si esaurisce peraltro in queste ipotesi, in quanto la protezione dei dati può essere pregiudicata da interazioni con altre imprese che non hanno a oggetto immediato il trattamento dei dati, ma che possono interferire con esso. Si pensi alle tecnologie inserite nei beni connessi che raccolgono dati degli utilizzatori con funzioni di ascolto ed eventualmente di pagamento. Il Regolamento generale adombra al riguardo la necessità di stabilire appositi presidi organizzativi interni. In base al principio noto come "*data protection by default and by design*", esplicita invero la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili per una protezione adeguata. Si limita però a rimettere all'autonomia privata la definizione di regole idonee a garantire che i presidi or-

ganizzativi si perpetuino lungo la catena negoziale, lasciando al titolare del trattamento la relativa responsabilità. Sul piano della ricostruzione sistematica, i temi che di conseguenza si prefigurano concernono le procedure di trasferimento e di acquisizione di informazioni da un ente all'altro sui rischi e sulla loro gestione; la ricostruzione di ruoli e funzioni di controllo su tali flussi; le eventuali prerogative di impartire istruzioni in rapporto alla discrezionalità gestionale e all'indelegabilità delle responsabilità.

Tornando all'immagine delle fonti normative sulla protezione dei dati personali come una ramificazione complessa, si può rilevare come l'esame del Gdpr consenta di tratteggiarne gli elementi strutturali, ma non i dettagli. Lascia difatti aperto il tema dell'adeguatezza degli assetti in relazione al rischio per i dati che sia generato e traslato lungo le catene negoziali, ponendo la necessità di ricostruire a partire dal sistema quale sia il punto di equilibrio tra tutela dei dati e libertà di impresa nel rapporto tra enti dotati di reciproca autonomia soggettiva. Il *deficit* di regolamentazione che già emerge con riguardo agli assetti interni, è invero ancora più evidente per quelli relazionali, cosicché è su questa ramificazione della materia che si concentrerà in particolare l'indagine seguente. Al fine di ricostruirla con un grado superiore di dettaglio si proporrà un coordinamento del Gdpr con altre fonti, anzitutto con la direttiva Psd2, ove reca la disciplina dei pagamenti elettronici. Tale prospettiva combinata risulta di immediato interesse per la rilevanza che la tutela dei dati personali assume nell'ambito dei pagamenti, sia per l'individuo sia per il mercato, considerato che la fiducia nella sicurezza delle transazioni è il presupposto del progresso economico nel nuovo ambiente ad alto tasso tecnologico. Soprattutto, in una proiezione giuridica, le norme sui pagamenti elettronici rilevano per la loro idoneità a porsi quale punto di avvio dell'analisi, in quanto presentano la peculiarità, unica nel quadro normativo attuale, di fornire elementi di dettaglio sui presidi organizzativi non solo interni ma per l'appunto relazionali tra imprese.

Con riferimento a questa seconda dimensione dell'organizzazione, si può pervenire a un grado ulteriore di dettaglio se si combina la menzionata direttiva con altri due corpi di disciplina, l'uno specificamente dedicato al fenomeno dell'*outsourcing* nel settore bancario, che può comprendere anche l'esternalizzazione di attività indirettamente incidenti sulla protezione dei dati, nei pagamenti e non solo; l'altro, nel quale il primo è incluso, sulla cybersicurezza. Tornando alla nostra raffigurazione del tema,

possiamo dire che se il Gdpr vale a tracciare la sagoma della struttura normativa nelle sue ramificazioni, il coordinamento sistematico con le discipline appena dette è funzionale a pervenire a un'immagine di dettaglio. La lettura congiunta e sistematica consente, più precisamente, di enucleare due modelli per la gestione dei dati, il primo interno alla singola impresa, il secondo nelle catene negoziali.

L'interrogativo ulteriore che ci si pone è se i modelli così ricostruibili, e in particolare quello relazionale, possano essere generalizzati, e con quali adattamenti e modifiche possano applicarsi a un ambito più ampio non solo, sul versante oggettivo, rispetto ai pagamenti elettronici, ma anche, sul piano dei soggetti, rispetto alle imprese bancarie, per riferirsi a qualsivoglia attività delle società comuni che esponga a rischio dati personali. La tesi è che, una volta enucleato un modello settoriale di organizzazione, si possa procedere a configurarne uno generale relazionale, relativo al rischio per la protezione dei dati generato e traslato nelle catene negoziali. In quanto attinenti ai presidi organizzativi, le diverse previsioni speciali *supra* individuate si prestano in effetti a riempire di contenuti di dettaglio non solo le clausole generali del Gdpr, ma anche quelle sulla correttezza gestionale.

L'immagine che in questa prospettiva si intravede si arricchisce di un livello ulteriore, sorretto dalla struttura ramificata sin qui tratteggiata, e a sua volta articolato in più segmenti, attorno ai quali ruotano molteplici tematiche interpretative. Basti considerare che l'ipotesi di un'applicazione generalizzata di norme di organizzazione e gestione dettate per l'ambito bancario, per quanto circoscritta a un rischio specifico, non può che evocare l'ampio dibattito sulla specialità dell'impresa bancaria. Quando le relazioni lungo la catena negoziale presentino i tratti del controllo ovvero della direzione e coordinamento, si pone inoltre il problema di una lettura congiunta con le relative discipline. Le quali peraltro, a prescindere che trovino diretta applicazione nelle singole fattispecie, divengono referenti teorici necessari in un ragionamento che riguardi i flussi di informazioni ed eventualmente di istruzioni tra società distinte. Ed eguale rilevanza deve riconoscersi ai frammenti di disciplina e alle teoriche sulla *compliance* delle società monadi e dei gruppi, considerato che la protezione dei dati rientra nell'alveo degli obblighi di conformità normativa.

Mantenendo l'immagine, potremmo dire che la linfa che unisce tutte tali diverse articolazioni della struttura mostrata, nonché tutti gli elementi

di discussione che ulteriormente si sviluppano attorno a ciascuno dei rami descritti, è formata da più interessi: degli individui titolari dei dati, delle imprese interessate al trattamento e del mercato; delle società lungo la filiera e dei rispettivi amministratori; di questi e infine dei soci, nell'ottica dei quali l'aspirazione alla sicurezza compete con quella al lucro, quantomeno nel breve periodo.

2. *La tutela dei dati tra mercato e discrezionalità di impresa: verso un primato dei presidi organizzativi? Una lettura congiunta con la disciplina dei pagamenti elettronici, per l'enucleazione di un modello di gestione organizzata del rischio*. – L'approccio normativo europeo e internazionale alla gestione dei rischi implicati dalla digitalizzazione dell'economia rivela la ricerca di un contemperamento tra la tutela dei diritti individuali e la volontà di assecondare le nuove prospettive di una crescita competitiva del mercato. L'esigenza di aprire l'accesso ai dati a nuovi intermediari e imprese mediante supporti tecnologici in continua evoluzione compete, invero, con quella di alimentare la fiducia necessaria al successo delle innovazioni. Due corpi normativi, in particolare, palesano nei loro plurimi punti di intersezione la tensione tra questi interessi: il regolamento generale sulla protezione dei dati (Reg. UE 2016/679, GDPR), e la direttiva sui servizi di pagamento (Dir. UE 2015/2366, PSd2).

Se si pone mente al fenomeno empirico, la congiunzione tra gli ambiti disciplinati dalle due fonti si coglie con immediatezza. Invero, se applicate ai pagamenti le nuove tecnologie accentuano la loro idoneità a rendersi strumento e veicolo di rischi per i dati degli utenti, favorendo il moltiplicarsi di forme di accesso non autorizzato, indebito utilizzo ovvero sottrazione delle informazioni necessarie a effettuare le transazioni elettroniche. Difatti tra le innovazioni più significative della direttiva PSd2 compaiono quelle intese a rafforzare le salvaguardie tecniche per il contrasto delle frodi, in particolare tramite la procedura per convalidare l'identificazione degli utenti detta *Strong Customer Authentication*, basata sull'uso di due o più credenziali di autenticazione e propedeutica all'autorizzazione di pagamenti *on line*. L'intreccio con le tutele giuridiche crea però nodi che non è sempre facile sciogliere, la cui rilevanza non è circoscritta all'interpretazione di singoli disposti, essendo coinvolto l'equilibrio sul piano sistematico tra gli interessi accennati, individuali e di mercato.

Ci si può avvedere di questi due livelli di lettura portando la prima attenzione sulla nozione di consenso, termine impiegato in entrambe le discipline citate ma con accezioni non eguali. L'esame congiunto delle fonti è necessario per chiarire quale relazione sussista, ai fini applicativi, tra il consenso al trattamento dei dati e quello negoziale alla prestazione di un servizio di pagamento, ma rivela al contempo una questione più ampia di carattere sistematico. Emerge infatti come nell'ambito dei pagamenti elettronici basi giuridiche alternative sulle quali radicare il trattamento dei dati – il c.d. interesse legittimo, nello specifico – stiano assumendo un'importanza crescente, tale da suggerire una riflessione sul superamento della centralità del consenso al fine prestato dal singolo. Le ragioni di tale direttrice evolutiva sembrano riconducibili al riconoscimento dell'insufficienza e comunque per lo più della ineffettività della tutela offerta da un'espressione di volontà che, per giunta, spesso non è appieno consapevole. Vi è però anche (o, forse, soprattutto) l'intento di scongiurare che dissensi individuali impediscano trattamenti che, usando la terminologia del GDPR, si reputano oggetto di un interesse "legittimo", in specie quando siano coinvolte operazioni bancarie e finanziarie che, a loro volta, sono riferibili all'interesse maggiore delle economie di mercato. Quantomeno in tali settori, la declamata sovranità dell'individuo sui suoi dati sembra in parte retrocedere in favore di un regime di eterotutela affidato a coloro che devono trattare i dati stessi, e che sono chiamati a effettuare un bilanciamento degli interessi coinvolti tenendo conto dell'impatto in termini di rischi dell'attività che compiono e dell'idoneità a mitigarli delle misure organizzative che loro stessi implementano.

È per l'appunto il primato dell'organizzazione d'impresa nella prospettiva della salvaguardia dai rischi operativi il profilo che emerge e che si intende approfondire, dedicando in particolare il primo capitolo di questo scritto all'elaborazione di una proposta di un coordinamento interpretativo sistematico con i temi, in particolare, del governo delle società e delle connesse responsabilità.

In questa prospettiva, è immediato cogliere un collegamento con la centralità che la predisposizione di assetti organizzativi adeguati è andata assumendo nella teorica della corretta gestione di impresa. Rispetto a tale più ampio tema, l'ottica del rischio specifico per i dati induce a porre in correlazione il concetto di adeguatezza con l'obiettivo del conseguimento di un livello minimo di tutela, e a individuare nella conseguente respon-

sabilità una leva per mantenere un equilibrio tra diritti individuali e interessi di mercato. È peraltro evidente il pericolo di inidoneità e soprattutto di disomogeneità applicativa di un meccanismo per la salvaguardia di interessi esterni indisponibili che si basi su autovalutazioni degli stessi soggetti coinvolti. In questa chiave critica in effetti si leggeranno i plurimi interventi che, dispiegati su tutti i livelli delle fonti giuridiche, hanno in vario modo delimitato la nozione di adeguatezza organizzativa nella materia della sicurezza dei dati, per lo più stabilendo schemi procedimentali standard da seguire, talvolta giungendo a individuare possibili misure tecniche da implementare.

Nelle intenzioni – e, vedremo, anche sul piano delle conseguenze giuridiche – tali indicazioni organizzative operano quali limiti alla discrezionalità che, per effetto del moltiplicarsi di atti di normazione intesi a conseguire un livello minimo comune e omogeneo di tutela, risulta compressa entro un cerchio che sembra restringersi progressivamente. A consegnare questa immagine sono le plurime linee guida elaborate dall'Autorità garante della privacy e soprattutto dalle Autorità del settore bancario e finanziario, europeo e internazionale, nonché gli orientamenti delle Organizzazioni internazionali con i quali sono stati predisposti standard che fungono da supporti operativi per la gestione dei rischi che le tecnologie informatiche pongono nei comparti finanziari e in quelli collegati. È uno scenario, diremo, senz'altro dominato dalla tecnica, ma anche da logiche strettamente giuridiche di distribuzione dei poteri (di etero o autodisciplina dell'esercizio dell'impresa) e di collocazione gerarchica degli interessi (in particolare alla sicurezza rispetto a quello al contenimento dei relativi costi in funzione di una maggiore distribuzione di utili). Le diverse linee guida che costellano la materia, nonché le direttive e i regolamenti che le hanno in vario modo recepite o riconosciute, esprimono infatti una ponderazione dell'ordine delle tutele che implica una riduzione della discrezionalità sia del singolo titolare dei dati, sia dell'impresa che li tratta, in entrambi i casi per la salvaguardia di interessi superiori, per lo più di mercato. Pare delinearsi più precisamente un doppio passaggio: dal consenso individuale quale strumento di autotutela, all'organizzazione di impresa quale eterotutela approntata da chi tratta i dati; e poi dalla valutazione di adeguatezza effettuata da ciascun titolare del trattamento, alla standardizzazione su base globale delle condotte minime organizzative. La tutela individuale risulta così affidata a un giudizio in certo senso col-

lettivo, che argina l'arbitrio delle singole imprese affinché tutte apprestino tutele minime idonee.

La prevalutazione dell'ordine degli interessi non si traduce però in un catalogo rigido di condotte doverose, o almeno – si argomenterà – non pare che così debba essere interpretata. Sembra, piuttosto, che l'evoluzione tecnologica sospinga verso nuovi modelli di co-regolazione tra pubblico e privato che, oltre a preservare sul piano giuridico il libero esercizio dell'impresa, sono funzionali a garantire alla tecnologia quel contesto flessibile e in continua evoluzione che la può agevolare e al contempo guidare senza diventare obsoleto. Il deterrente utilizzato è la responsabilità, la cui connessione con l'adeguamento a standard è esplicitata dallo stesso GDPR, che premia l'adesione a codici di condotta, ovvero la sottoposizione di attività o prodotti a certificazioni di sicurezza, con un'agevolazione nella prova della *compliance* ai requisiti normativi.

3. *Nuove tecnologie e propagazione del rischio tra imprese. Da un modello organizzativo atomistico a uno relazionale, tra co-regolamentazione e protezioni standardizzate*. – Per il settore bancario e finanziario all'istanza di garantire misure minime omogenee si affianca peraltro quella di scongiurare l'opposto pericolo che in nome di un incremento delle tutele si restringa l'accesso al relativo mercato per nuove figure di prestatori di servizi. Per questo, a salvaguardia dell'esigenza di competitività, si vieta di impedire o rendere eccessivamente gravoso l'accesso alle piattaforme API (*Application Programming Interfaces*) ovvero l'acquisizione e il trattamento dei dati dei clienti per le nuove figure di intermediari non bancari (sinteticamente *Thirdy Party Providers* – TTP) abilitati dalla direttiva PSd2 a prestare servizi di disposizione di ordini di pagamento elettronici ovvero di informazione sui conti dei clienti. Il che, invertendo la prospettiva, significa che si impone di accettare – con l'impegno a governarlo – il rischio conseguente all'interazione con tali soggetti. La volontà di innovare sul duplice piano tecnologico e competitivo il mercato dei servizi finanziari ha, in altri termini, come effetto riflesso un'estensione del problema della salvaguardia dei dati dal piano del singolo intermediario a quello delle interazioni con gli ulteriori operatori che popolano il nuovo scenario dei servizi *on line*.

Quello così tracciato è nondimeno solo un frammento del quadro di

interazioni e interconnessioni soggettive che si sta delineando a seguito dell'avvento del fattore tecnologico nelle dinamiche di mercato. Diremo in particolare di come nella nuova dimensione della *Internet of Things* si apra sempre più la possibilità di interconnessioni miste, tra oggetti e soggetti, e di come al contempo la necessità di *know how* e competenze in costante evoluzione e sempre più difficili da conseguire sospinga le imprese verso modelli di integrazione orizzontali, sviluppati attraverso l'esternalizzazione di funzioni, servizi e segmenti della produzione. Sono proprio queste interconnessioni i nuovi fattori di rischio con i quali è imprescindibile misurarsi. E invero quello proveniente da terzi è una componente centrale del rischio che, in una dimensione globale, è collegato alle tecnologie, in particolare informatiche e delle comunicazioni; tant'è che la sua gestione è divenuta fondamentale nelle politiche europee sulle infrastrutture del mercato finanziario e, con un approccio sempre più lato, del comparto bancario. Il rischio operativo è del resto oramai difficilmente isolabile in un'unica impresa, non solo per l'estensione delle potenziali esternalità negative all'intero mercato, ma per l'appunto anche sotto il profilo delle fonti di produzione, in ragione di una capacità di trasmissione dei rischi che risulta senz'altro potenziata dalle nuove tecnologie informatiche. La gestione del rischio eterogenerato diventa pertanto un problema giuridico da affrontare a partire dal processo di produzione e in tutte le fasi successive, ovverosia *by design* e *by default*, secondo la formula che è sancita nel GDPR ma che sembra in realtà pervadere per intero la politica normativa sulla cybersicurezza.

Si coglie, in questa prospettiva, come la centralità dell'organizzazione assuma una dimensione ulteriore che possiamo chiamare intersoggettiva, nella quale la protezione dei dati si compie in due fasi caratterizzate da diverse modalità. La prima è diretta e affidata all'impresa che ha il contatto più immediato con la fonte del rischio in quanto gestisce i prodotti, processi o servizi che includono le tecnologie suscettibili di veicolare frodi; la seconda, indiretta e dispiegata lungo la catena negoziale, avviene attraverso una stratificazione di controlli che le imprese esposte a una traslazione di tale rischio effettuano sulle misure di salvaguardia adottate dalla prima impresa, e presuppone come evidente l'adozione di appropriate misure negoziali sulle cautele da adottare e sulle verifiche conseguenti. Le previsioni contrattuali in effetti assumono un'importanza crescente attestata anche dalle direzioni evolutive di recente impresse alla

legislazione europea. Basti pensare – ma anche su questo punto si tornerà nella trattazione – come a fronte di un paniere dei dati, personali e no, che si vuole sempre più ampio e condiviso, si tenti di promuovere la diffusione di contratti con clausole di salvaguardia standardizzate. Lo si coglie nel nuovo regolamento europeo relativo alla resilienza operativa digitale per il settore finanziario (*Digital Operational Resilience Act* – DORA), ma anche nella *Data Strategy* (che ha preso corpo nel *Digital Services Act*, nel *Digital Market Act*, nel *Data Governance Act* e nella proposta di *Data Act*) con la quale l'Europa mira a incrementare la sicurezza dello spazio digitale rispetto alla tutela dei diritti fondamentali degli utenti, stabilendo al contempo condizioni di parità per le imprese.

Che la sede nella quale dovrebbero trovare collocazione le protezioni dai rischi siano i contratti che originano e regolano le interconnessioni tra imprese emerge del resto dallo stesso GDPR, che rimette alla regolazione privata la funzione di circoscrivere la discrezionalità nella gestione della sicurezza nella catena negoziale attraverso il richiamo agli standard di settore. Questi divengono quindi punti di riferimento per la formulazione delle clausole negoziali, e in particolare per l'individuazione dei presidi di sicurezza da richiedere alle controparti e da verificare in costanza di rapporto. Le salvaguardie di natura tecnologica e giuridica si intrecciano anche su questo piano, in quanto le previsioni contrattuali divengono il tramite per la diffusione di supporti tecnici adeguati.

Si tratta di un'ulteriore espressione della co-regolamentazione prima detta, in relazione alla quale si delineano diversi piani di responsabilità. A un primo livello vi è la protezione dell'utente, che è affidata a norme imperative che pongono un obbligo di risarcimento del danno in capo al titolare del trattamento dei dati. Poiché tali previsioni prescindono dalle scelte organizzative, si evince come queste, non potendo comunque pregiudicare la salvaguardia degli interessi deboli riconosciuti dal legislatore, si caratterizzino per una neutralità sulla quale meriterà soffermarsi. L'ente in questione può peraltro a sua volta attivare i meccanismi del regresso per far valere le responsabilità – di secondo livello – delle imprese che lungo la catena negoziale abbiano operato senza presidi adeguati per la sicurezza; alla tutela risarcitoria esterna si affianca così quella ripristinatoria interna, che conduce a una ricollocazione del peso del risarcimento commisurata al contributo di ciascuna impresa nel produrre il danno. La condizione, però, è che nel contratto si sia avuto cura di esplicitare le regole di condotta

nella gestione del rischio, ponendo le basi per un ristoro e, a monte, per un controllo orizzontale tra le imprese stesse sull'adeguatezza degli assetti organizzativi da ciascuna predisposti. La prospettiva del riparto di responsabilità promuove per tale via la prevenzione del danno, affidata a meccanismi di controllo tra pari lungo la catena negoziale.

La vocazione preventiva si riconosce anche nell'ulteriore piano di responsabilità conseguente alla scelta di affidare al contratto la funzione descritta, in quanto la prospettiva di regresso può aversi, oltre che fra imprese, anche verso i rispettivi amministratori. L'esposizione di questi ultimi a pretese risarcitorie opera quale leva affinché siano in effetti implementate quelle adeguate misure organizzative che, come visto, sono divenute il nucleo sul quale si radica la salvaguardia dei terzi, e in particolare affinché nel contratto con i fornitori siano inclusi vincoli di sicurezza e connesse prerogative di controllo. Di qui la centralità del ruolo degli amministratori, nei rapporti impresa-utente come in quelli tra imprese, anche nell'utilizzo e nella diffusione di protezioni standardizzate.

Per l'appunto seguendo l'idea che la responsabilità gestionale possa essere baricentro anche rispetto ai nuovi rischi operativi connessi all'informatizzazione, diviene fondamentale comprendere quale grado di effettività essa abbia. La questione a sua volta richiede di chiarire preliminarmente quale discrezionalità residui, in particolare nelle scelte che attengono all'individuazione dei fornitori e alla formulazione di condizioni contrattuali sui livelli di sicurezza e sui relativi controlli, per stabilire poi – e di conseguenza, come diremo – se possa invocarsi la *business judgement rule*, nonostante le implicazioni organizzative delle decisioni sulla gestione della sicurezza. A seconda dell'interpretazione che si adotti, ci si trova in bilico tra due rischi: indebolire la capacità deterrente della responsabilità, e quindi lasciare esposti a pregiudizio diritti fondamentali tra i quali la riservatezza dei dati, innescando una catena negativa che dalla sfiducia dei singoli può condurre all'insuccesso dei nuovi modelli di mercato, viceversa fortemente voluti dall'Europa; o, all'opposto, contrarre la libertà di impresa al punto da generare un possibile conflitto con le norme codicistiche e costituzionali che la prevedono.

4. *Dall'*outsourcing *bancario alla (etero)gestione del rischio di non conformità in tutte le catene negoziali. Generalizzazione, con adattamenti,*

di un modello settoriale. – Sul piano preliminare della delimitazione degli spazi di discrezionalità il regolamento europeo sulla protezione dei dati (GDPR) non offre indicazioni specifiche sui modelli organizzativi da adottare per far fronte al rischio generato nella catena negoziale, salvo un riferimento nelle linee guida attuative alla selezione di controparti che aderiscano a standard o sottopongano i loro prodotti o servizi a certificazioni. Di per sé già tale indicazione merita un approfondimento per comprendere condizioni e conseguenze di una scelta gestionale che se ne discosti, anche considerato che le piccole e medie imprese che non hanno risorse per sottoporsi periodicamente alle revisioni esterne necessarie per ottenere formali certificazioni potrebbero vedersi (quantomeno) di fatto precluso l'accesso al mercato, come detto in notevole espansione, delle forniture connesse a tecnologie che implicano la gestione di dati. Di qui l'interesse ad allargare l'indagine a ulteriori fonti normative, per ricostruire sul piano sistematico la nozione di corretta gestione in rapporto al rischio eterogenerato.

Poiché si intende, più in dettaglio, mettere in correlazione assetti organizzativi e relazioni negoziali, le norme che paiono da assumere a riferimento – e che in effetti, come vedremo, si intrecciano in più punti con GDPR e PSD2 – sono quelle che regolano la prassi del c.d. *outsourcing*, che con frequenza crescente vede le imprese del settore bancario affidare all'esterno loro attività, per implementare *know how* e strumenti tecnologici che sarebbe più costoso acquisire e gestire direttamente. Anche su tale fronte occorre confrontarsi con previsioni disseminate in fonti di diverso rango, che a loro volta si intrecciano con la più ampia politica normativa sulla cybersicurezza. Sembra peraltro di poter ricostruire – e al relativo impegno sarà dedicato il secondo capitolo – un disegno unitario, nel quale il controllo del rischio è scandito in fasi di un procedimento che si ripete nei suoi passaggi essenziali nelle diverse fonti, delimitando in vario modo e misura la discrezionalità dei gestori.

Rispetto al primo stadio, concernente la scelta dei fornitori, le norme precisano l'istruttoria che dovrebbe essere svolta introducendo criteri di selezione che pongono come preminente l'affidabilità della prestazione in termini di sicurezza rispetto alla convenienza economica dell'offerta. In tal modo delimitano la discrezionalità sino a condizionare scelte di pura gestione, su un piano quindi che va oltre il presupposto sempre verificato nel sindacato sulla condotta gestionale, ovverosia la completezza dell'indagine condotta. Nella fase successiva, nella quale si procede alla sottoscrizione e

all'esecuzione del contratto, la correzione della discrezionalità pertiene a scelte organizzative quale in particolare la struttura dei controlli di ambedue le imprese coinvolte – richiedendosi la predisposizione di assetti e adempimenti interni a ognuna, nonché l'istituzione di flussi informativi reciproci – e conseguentemente si riflette sulla distribuzione delle risorse che devono essere per l'appunto destinate a copertura dei costi di tali controlli, e in generale a servizio di una gestione prudente del rischio. Tale duplice livello di contrazione della discrezionalità si ritrova anche nello stadio finale di reazione a eventuali inadempimenti nel preservare un livello concordato di sicurezza, in quanto un'ipotetica risoluzione del contratto non può che coinvolgere scelte gestionali e insieme organizzative, per l'istituzione diretta o l'esternalizzazione tempestiva ad altre imprese di idonei presidi per il rischio. La standardizzazione perseguita attiene pertanto al procedimento, e al contempo ai contenuti organizzativi e gestionali delle decisioni.

Ebbene, tali previsioni sull'*outsourcing* paiono in definitiva precisare per le imprese del settore bancario la nozione di corretta gestione del rischio tecnologico generato nella catena di fornitura, nelle sue implicazioni operative e giuridiche. Il tema ulteriore è comprendere se tali norme assumano interesse in una prospettiva soggettiva più ampia, di sistema.

Per il vero un'applicazione del complesso normativo in parola anche a imprese che non afferiscono al comparto bancario e finanziario è in parte testuale, in quanto la disciplina dell'esternalizzazione è stata estesa a tutti i rapporti con terze parti dai quali possa derivare una traslazione dei rischi operativi. Già in conseguenza di tale impostazione il rischio diventa un dato da apprezzare come preminente sulla natura dell'impresa esercitata al fine di stabilire la sfera di applicazione delle disposizioni sull'*outsourcing*, essendo la base sulla quale è stata ricercata sul piano normativo una uniformità quantomeno dei livelli minimi di tutela lungo le catene del valore. L'ulteriore passaggio che si intende indagare, dedicandovi il terzo capitolo, è se a partire dalla disciplina dell'esternalizzazione si possa ricostruire un paradigma generale per la gestione del rischio eterogenerato, a prescindere che nei rapporti lungo la catena negoziale compaiano imprese bancarie. A suggerire di interrogarsi su tali profili è anche la più recente *Data Strategy* dinanzi menzionata, intesa a innovare il quadro normativo in modo da agevolare l'accesso anche delle PMI a un sempre più ampio paniere di informazioni, alla ricerca di un riequilibrio competitivo in favore di tali imprese.

Ragionando di portata interpretativa di norme di organizzazione e ge-

stione dettate per il settore bancario non si può omettere il confronto con il più ampio dibattito sulla specialità delle imprese che vi operano, quale ostacolo a un'estensione delle relative regole di *governance*. Il tema sembra peraltro poter essere affrontato in una prospettiva peculiare, focalizzata non sulla natura dell'impresa complessiva bensì su quella del rischio, in ragione del fatto che determinate tecnologie possono generare nel settore finanziario e negli altri nei quali siano utilizzate problemi pressoché identici, in termini sia di pregiudizio alla sicurezza dei dati sia di modalità di trasmissione. L'indagine verterà quindi sulla configurabilità di un'estensione selettiva della disciplina sull'esternalizzazione, allo scopo di tracciare una distinzione tra le norme che la compongono a seconda che siano influenzate dalla natura delle imprese per le quali sono state formulate, e alle quali devono quindi rimanere circoscritte, o siano invece state elaborate in risposta alle specificità del rischio tecnologico, risultando in quanto tali suscettibili di essere elevate a principi per la sua corretta gestione, concretizzando le clausole generali codicistiche.

Occorrerà al contempo distinguere le disposizioni sugli assetti organizzativi e in particolare sui controlli, e quelle concernenti *iter* e clausole negoziali, sulle quali ultime si concentrano in particolare gli interrogativi sull'idoneità a dare contenuti di dettaglio alla clausola generale di corretta gestione del rischio. In tali riflessioni occorre tenere conto anche del principio di proporzionalità, precetto che è a sua volta centrale nell'elaborazione che ci si propone in quanto, ragionando di estensione di norme settoriali, non si può trascurare la minore capacità di sostenere i costi dell'organizzazione da parte delle società comuni, al netto di ogni valutazione su dimensioni e apertura al mercato che le possono singolarmente caratterizzare.

L'evoluzione tecnologica sembra quindi rinnovare il ruolo della disciplina del settore bancario quale ambito sperimentale per l'introduzione di regole destinate a estendersi, seppure per l'appunto con i necessari adattamenti, a tutte le imprese. L'applicazione delle tecnologie informatiche agli scambi finanziari in fondo mostra a livello macroeconomico la rilevanza dei rischi ai quali sono esposti individui e mercato, ma il problema può ritenersi ormai presente in tutti i livelli del tessuto imprenditoriale, tra l'altro proprio per effetto del processo congiunto di diffusione delle tecnologie e di integrazione dei servizi e sistemi di pagamento in attività di natura non bancaria. La trasversalità rispetto agli ambiti di attività è del resto una caratteristica strutturale della disciplina posta nel GDPR, che

recepisce sul piano giuridico la pervasività del rischio al quale i dati sono esposti in ogni settore economico, quale riflesso dell'applicazione egualmente generale delle tecnologie.

All'interno di questa più ampia cornice, la specialità settoriale sembra dover essere ripensata spostando come detto l'attenzione dall'impresa alle frazioni di rischio alle quali è esposta. Al contempo, peraltro, la traslazione del rischio nella catena negoziale può identificare una specialità trasversale sulla quale impostare nuovi criteri di interpretazione sistematici.

A tal fine il ruolo e la conformazione degli assetti organizzativi nella gestione del rischio che si origina e trasmette lungo la catena negoziale vanno analizzati considerando se gli obblighi gestori differiscano a seconda che le relazioni contrattuali in questione siano riconducibili, anziché no, alle nozioni di controllo ovvero di direzione e coordinamento, con la conseguente soggezione (anche) alle relative discipline. Avendo scelto la protezione dei dati quale chiave di analisi, occorrerà al contempo riflettere sulle intersezioni con le teorie giurisprudenziali e dottrinali sulla *compliance*, partendo da quella di gruppo per poi comprenderne i necessari adattamenti a tutte le relazioni negoziali che agevolino la traslazione del rischio per la sicurezza.

Il primo obiettivo è ricostruire le interconnessioni tra i doveri di fonte legale e quelli di fonte negoziale rispetto ai flussi informativi concernenti il rischio e le iniziative adottate per monitorarlo, mitigarlo e gestirlo. In tale prospettiva il tema teorico da affrontare è la salvaguardia della riservatezza, che può assumere particolare rilevanza per l'esigenza di tutela del *know how* sulle modalità per conseguire livelli elevati di sicurezza.

L'obiettivo successivo è individuare entro quali limiti possa riconoscersi, su base legale o negoziale, la prerogativa di dare indicazioni su come gestire il rischio. Al fine occorre ragionare sulla diversa collocazione teorico sistematica di clausole intese a stabilire il livello accettabile di rischio – attraverso le quali si può in effetti compiere il disegno virtuoso di una diffusione dei livelli più elevati di cautela nella gestione dei rischi descritti – e di clausole con le quali si pretenda invece di preindividuare strumenti o metodi da adottare in concreto per conseguire la sicurezza dovuta, che rischiano di annullare la discrezionalità gestionale lungo la catena negoziale, con effetti negativi anche su innovazione e competizione. Si riproduce in definitiva lungo la catena negoziale il problema dell'equilibrio tra delimitazione della discrezionalità e salvaguardia della

libertà di impresa. L'incidenza sulle modalità di esercizio dell'impresa, quindi su scelte che possono essere al contempo di organizzazione e di gestione in senso stretto, determina invero che nello svolgere l'analisi in chiave giuridica ci si debba misurare con il tema dell'autonomia gestionale, che nei rapporti tra imprese si collega a quello dell'autonomia soggettiva. Definire gli equilibri tra autonomia ed eteronomia diviene pertanto ineludibile anche rispetto agli assetti che concernono l'organizzazione dei rapporti con le imprese lungo la catena che, insieme al valore, produce il rischio. La peculiarità è che può generarsi un doppio fenomeno espropriativo, in quanto al processo di standardizzazione generale (collettiva) delle condotte, che come detto è intesa a sottrarre spazi di discrezionalità alle singole imprese, può sommarsi un'eguale elisione della libertà di decisione sul rischio, effettuata però su base negoziale da un'impresa sull'altra (o le altre) appartenenti alla medesima catena.

Gli interrogativi sulla discrezionalità degli amministratori si pongono così per la società che esternalizza e per quella fornitrice, e conducono alla più generale questione dell'esclusività della competenza gestionale, nei rapporti interni ed esterni alle società. Il punto diventa se e come i termini del relativo dibattito mutino alla luce della peculiarità ravvisabile nella traslazione da un'impresa all'altra di un rischio che le stesse non possono accettare in quanto concerne il diritto individuale su dati personali, quindi una posizione esterna intangibile la cui tutela è imperativa. La sicurezza diviene una priorità e la strumentalità a realizzarla diviene – argomenteremo – ragione giustificatrice e al contempo limite teorico sia dell'accesso alle informazioni e della prerogativa di verificarle, sia delle misure di gestione del rischio adottate e richieste lungo la catena negoziale, secondo una lettura funzionale di poteri e doveri reciproci.

La ricostruzione sistematica di un vincolo alla prudenza nel trattamento del rischio tecnologico giustifica al contempo la destinazione delle risorse (anziché alla distribuzione) alla copertura dei costi necessari per conseguire il livello minimo di sicurezza appropriato rispetto alle caratteristiche del rischio, con un doppio effetto, sulle dinamiche relazionali esterne stabilite su base negoziale con le imprese fornitrici, ma anche su quelle interne, tra amministratori e soci, che si avvicinano anche sotto questo profilo a quelle corrispondenti proprie delle imprese bancarie.

In ragione di tali peculiarità, la fonte esterna di un rischio inaccettabile sembra candidarsi a essere un nuovo criterio interpretativo sistematico utile

a enucleare un modello organizzativo unitario per tutti i rischi di *compliance* la cui origine e trasmissione si collochino lungo la catena negoziale. L'approccio ultrasettoriale è del resto coerente con la vocazione trasversale che è propria sia delle tecnologie sia, sul piano giuridico, delle esigenze di tutela di diritti individuali quali quelli implicati dalla salvaguardia dei dati.

Al contempo, il modello di assetti organizzativi adeguati che può così disegnarsi è peculiare per le imprese che operano in contesti coinvolti dalle nuove tecnologie basate sull'interconnessione e interoperabilità descritte, con una identità che può reputarsi autonoma in un triplice senso. È invero peculiare anzitutto rispetto al modello organizzativo più generale che può ricostruirsi per la *compliance* rispetto a rischi isolabili, sotto il profilo della genesi e degli strumenti di gestione, in capo a singole società, visto che nelle fattispecie considerate la conformazione della catena di fornitura diviene invece, come detto, la componente centrale delle valutazioni di conformità. È inoltre peculiare rispetto al modello organizzativo della *compliance* di gruppo, se non altro in quanto non ricorre quella coesistenza tra pluralità di soggetti e unicità di impresa sulla quale fa perno la disciplina della direzione e coordinamento, avendosi una più limitata condivisione di frazioni di rischi operativi e giuridici. È infine peculiare rispetto al modello delineato dalla disciplina settoriale dell'esternalizzazione, che va acquisito come uno schema di principio, da epurare dalle componenti influenzate dalla specificità dell'impresa bancaria anziché da quelle del rischio, e da coniugare poi con le regole organizzative adeguate alle dimensioni della singola impresa di diritto comune, tenendo in conto l'entità del rischio secondo il principio della proporzionalità.

Sembra allora tracciabile un *continuum* teorico nel quale la crisi del consenso del titolare dei dati quale strumento di tutela si unisce alla riduzione della discrezionalità di impresa in una strategia unitaria di sviluppo di un mercato europeo basato sulle nuove tecnologie, che a sua volta si inserisce in una più ampia riconsiderazione degli assetti organizzativi. Acquistano rilevanza infatti non solo gli assetti interni ma anche quelli relazionali, nel senso non solo di un'accresciuta rilevanza ma anche di una minore libera determinabilità.

5. *Dalla catena dei rischi a quella delle responsabilità. Implicazioni sulla* business judgment rule. – Su tali premesse ci si ricollega al tema

della responsabilità gestionale, il cui ruolo centrale di leva (non tanto per la riparazione quanto) per la prevenzione del danno diviene ancora più percepibile.

La correttezza della condotta gestoria va verificata anzitutto in relazione alla stesura dei contratti che regolano i rapporti di fornitura all'origine del rischio descritto, in quanto come detto si richiede non solo di precisare i livelli attesi di sicurezza, ma anche di porre le basi per le verifiche sulle misure di protezione attuate. Sotto questo profilo la responsabilità completa, rafforzandolo, il disegno di una tutela innestata nell'organizzazione societaria e resa obbligatoria lungo le catene di fornitura da apposite previsioni negoziali. Nei rapporti che ne conseguono la gestione del rischio, anziché essere diretta, assume i contenuti prevalenti del controllo sulla gestione altrui, e pertanto della prevenzione. La regola del controllo reciproco tra membri dello stesso organo si estende così – secondo il modello (diremo) in parte modificato delle relazioni di gruppo – al rapporto tra gestori (e sindaci) delle società che condividono il medesimo rischio, veicolato e diffuso dai supporti tecnologici utilizzati.

La lettura sistematica delle discipline rivela una sovrapposizione di relazioni e di responsabilità. Dal rapporto tra titolare dei dati e titolare del relativo trattamento si passa a quello tra imprese alle quali sono riferibili le frazioni della condotta finale sulla quale si basa il trattamento; dal giudizio individuale di adeguata gestione del rischio si passa a quello collettivo formalizzato negli standard settoriali. Parallelamente, nella prospettiva degli amministratori si passa dalle relazioni interne agli organi a quelle tra organi delle imprese che compongono la catena di fornitura; e di conseguenza si passa da una responsabilità gestionale circoscritta – quantomeno nella concreta applicazione – ai rapporti tra soci e amministratori, a una attivabile *ab externo* sul presupposto dei danni diretti che l'omissione delle cautele concordate può generare per gli utenti e per le imprese tenute, in via diretta o in sede di regresso, al risarcimento.

Orbene, poiché l'effettività della responsabilità gestionale è connessa alla verifica giudiziaria delle condotte assunte, sembra di interesse riconsiderare – e invero vi si dedicherà il quarto capitolo – il tema della *business judgment rule* alla luce delle fonti normative sin qui menzionate, e in particolare degli elementi ulteriori che dalle stesse possono trarsi in relazione al punto, come noto critico, della coestensione tra discrezionalità e insindacabilità.

Già i primi elementi che si sono anticipati come caratterizzanti la disciplina del rischio trasmissibile nella catena di fornitura paiono avere implicazioni organizzative frammiste ad altre gestionali. Si pensi agli assetti di controllo, che come detto devono essere adeguati al monitoraggio del rischio tanto per la società che ha ne ha la gestione immediata, tanto per quella che esternalizza, che deve essere in condizione di acquisire informazioni affidabili sulla condotta della prima, di fare le opportune verifiche e di assumere le decisioni conseguenti. L'afferenza alla gestione è d'altro canto evidente nelle regole sulla scelta dei fornitori, ma a ben vedere permea l'intera materia, se solo si considera quanto l'imposizione della prudenza incida sui vincoli di destinazione delle risorse, comportando che le esigenze di sicurezza siano antergate alle aspettative (di risparmio di spesa e) di lucro.

Tale intersezione tra i due piani induce una riflessione sull'utilità, quantomeno nelle fattispecie in esame, di stabilire l'estensione della *business judgment rule* sulla base della distinzione tra decisioni organizzative e di gestione. L'indicazione che si trae è piuttosto di rimeditare lo spazio per il sindacato giudiziario alla luce delle norme tecniche sull'*outsourcing*, assumendo quale punto di partenza i contenuti con i quali è stata concretizzata la nozione di gestione corretta del rischio eterogenerato. Sulla base dei limiti che gli stessi pongono alla discrezionalità degli amministratori si possono infatti ricostruire anche i confini che, di riflesso, sono posti pure alla citata *rule*.

Tornando all'immagine di una discrezionalità nel fare impresa racchiusa in un cerchio che si restringe sempre di più, la sindacabilità giudiziaria è raffigurabile come il presidio che serve a ottenere il rispetto del limite così definito. È però un confine che non può essere alterato neppure dai giudici che, vincolati a loro volta a non superare le linee tracciate dalle norme, non possono entrare nello spazio che per le accennate ragioni di flessibilità e competitività è lasciato all'autonomia decisionale, ad esempio nelle scelte tra metodi – di organizzazione o di gestione operativa – che in astratto sono al pari idonei a conseguire la sicurezza minima necessaria.

Il processo di standardizzazione sembra giungere per tale via sino alle decisioni giudiziarie, a salvaguardia di un'ulteriore certezza che ricalca quella che si persegue per l'operato delle autorità garanti del settore bancario e finanziario, alle quali in effetti le norme sull'esternalizzazione pure

sono espressamente rivolte. È una tendenza evolutiva che si presenta allora eguale nel metodo, in quanto radicata nel riconoscimento di un ruolo di crescente importanza agli standard, anche se in apparenza di segno opposto sul piano della distribuzione dei poteri, in quanto alla diminuzione dell'area della discrezionalità di impresa corrisponde un'estensione di quella del sindacato giudiziario delle relative scelte, incluse quelle sui costi e sulla composizione delle catene di fornitura, e questo anche ritenendo applicabile la *business judgment rule* alle decisioni organizzative.

All'autonoma identità del modello organizzativo per la gestione del rischio eterogenerato, sembra corrispondere un autonomo modello di *business judgment rule*.