LE LEGGI NON SCRITTE DELLA BUSINESS CONTINUITY

GLORIA COLANTONI*

La congiuntura economica negativa degli ultimi anni ha evidenziato un problema sottostimato al punto da essere quasi ignorato anche dal legislatore: la Business Continuity. Questi è infatti intervenuto solo tardivamente ed in modo frammentario per affrontare tematiche quali la gestione del rischio d'impresa e la tutela della continuità operativa. La disciplina della privacy ed il Codice dell'Amministrazione Digitale (CAD) regolamentano la materia fornendone un inquadramento minimale. Più circostanziata la normativa di Banca d'Italia che sembra allinearsi agli standard di settore ed alle indicazioni espresse dall'Unione Europea. Quali che siano le motivazioni dell'attuale vulnus legislativo, è il momento di realizzare un unico quadro normativo di riferimento.

Le rilevazioni Istat confermano segnali di ripresa per l'economia italiana che ha vissuto un lungo periodo di congiuntura negativa, la quale ha portato alla luce tutta una serie di problematiche finora ignorate.

Poco esplorata da dottrina e giurisprudenza ma ben nota al mondo aziendale è la *Business Continuity* (BC), ossia l'insieme delle attività volte a minimizzare gli effetti distruttivi e dannosi di un evento che può colpire un'azienda o parte di essa, garantendone la continuità. Il concetto di BC è chiarito da standard internazionali (ISO 22301) ed accomuna settori tra di loro molto distanti (dal privato al pubblico, dal tecnologico al bancario) ma che hanno o possono esercitare un forte impatto sull'economia nazio-

* Banca di Credito Cooperativo di Roma - gloriacolantoni@alice.it

nale e locale.

Connesso alla *Business Continuity* è il piano di continuità operativa, meglio noto come *Business Continuity Plan* (BCP), documento risultante da un processo complesso, coerente ed articolato, volto ad individuare le minacce a cui è potenzialmente esposta un'impresa e a definire le azioni necessarie ad assicurare la resilienza della struttura aziendale al verificarsi di condizioni avverse o di incidenti, ad assicurarne la continuità operativa ed a preservarne la capacità produttiva.

Il buon imprenditore od il manager accorto devono saper soppesare le componenti di rischio legate allo svolgimento dell'esercizio d'impresa, cogliendo altresì quei fattori, eventi, contingenze ambientali che per natura e definizione sfuggono al controllo del processo organizzativo aziendale.

La *Business Continuity* è da molti ritenuta subordinata al *Risk Management* al quale è usualmente associato, nonostante ne sia concettualmente distinto e non sovrapponibile. Secondo gli Standard Internazionali ISO 31000 il "Rischio" è l'effetto conseguente al manifestarsi di un evento incerto, sia tale effetto positivo che negativo. La gestione del rischio attraverso la funzione di *Risk Management* si sostanzia con l'identificazione e la classificazione dei rischi, delimitandone le conseguenze al fine di predisporre azioni e procedure atte a minimizzare l'impatto negativo di eventi sfortunati ovvero massimizzarne il profitto in caso di eventi favorevoli.

La *Business Continuity* può dunque essere vista quale parte integrante del più ampio *Risk Management*, ovvero quale attività da esso separata e collaterale. Il corretto posizionamento della funzione di BC sta nella scelta discrezionale e consapevole delle singole organizzazioni ed è determinata nello svolgimento della propria attività.

Una precisa definizione delle due funzioni è uno sforzo di sintesi che potrebbe comunque condurre ad una interpretazione controversa, ma a ben guardare la soluzione a questo quesito appare semplice purché circoscritta al perimetro "ruolo - responsabilità".

La *Business Continuity* predispone e mantiene le condizioni minime necessarie a garantire l'esercizio dell'attività di impresa, il *Risk Management* identifica le potenziali minacce e le migliori opportunità di intervento che si possano manifestare nella conduzione dell'esercizio d'impresa, ed a

completamento ed integrazione, il *Crisis Management* dispone procedure, risorse e competenze per la gestione dei periodi di crisi susseguente ad evento dirompente, straordinario ed inaspettato.

Se per i motivi suesposti è pacifica l'importanza ed il ruolo rivestito dalla presenza di un piano di *Business Continuity* all'interno dell'organizzazione aziendale, meno certa e di non immediata intuizione è la posizione assunta dal Legislatore italiano nel disciplinare tale materia. Questi parrebbe infatti aver preferito non dare un inquadramento normativo complessivo, organico ed omogeneo in cui tale materia si possa inserire. È quanto meno singolare che non vi sia stata discussione sull'opportunità di imporre norme cogenti a tutela del bene pubblico, eventualmente ipotizzabili anche avverso quelle aziende private che abbiano un rilevante impatto pubblico. La valutazione dei costi-benefici riconducibili alla previsione di un BCP, indurrebbe senz'altro il Legislatore ad imporre vincoli normativi alle imprese, in particolare a quelle che hanno un forte impatto sul mercato.

Una conferma in tal senso arriva dal settore bancario: gli aggiornamenti del luglio 2013 alle "Disposizioni di Vigilanza" di Banca d'Italia (circolare n.263/2006) e le "Linee guida in materia di continuità operativa delle infrastrutture di mercato" del maggio 2014, disciplinano compiutamente la materia accogliendo in modo organico ed aggiornato i principi e le indicazioni di settore definite in sede internazionale e comunitaria.

Nuovi complessi ed evoluti scenari di rischio macroeconomico, un'accresciuta complessità organizzativa e normativa, maggiore dipendenza da sistemi e protocolli informatizzati, libertà di accesso ai mercati finanziari e la conseguente offerta di strumenti sofisticati e diversificati ad un pubblico non qualificato e vasto, hanno imposto la realizzazione di un quadro unico e dettagliato in materia di continuità operativa per le banche.

Le disposizioni di Banca d'Italia si articolano nella definizione di concetti basilari quali "crisi", "escalation", "emergenza", "gestione della continuità operativa", "piano di continuità operativa", "piano di disaster recovery", "tempo di ripristino di un processo" ed altri. Definiscono inoltre responsabilità, requisiti e scenari che si sostanziano nella previsione di obblighi di fare.

In particolare Banca d'italia definisce la "gestione della continuità opera-

tiva" come l' "*insieme delle iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti o catastrofi che colpiscono direttamente o indirettamente un operatore*", distinguendola dal "piano di continuità operativa" definito come il "*documento che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse, per la gestione della continuità operativa dei processi aziendali critici e a rilevanza sistemica*".

Gli ultimi interventi di Banca d'Italia in materia di continuità operativa hanno inteso chiarire e puntualizzare alcuni aspetti trattati forse superficialmente fino a quel momento.

In particolare il Titolo V, capitolo 9 delle Disposizioni di Vigilanza del 2013 statuisce che organo di controllo della continuità operativa è l'*Internal Audit*, addetto a monitorare il piano aziendale dei fornitori di servizi e dei fornitori critici. Qualora si tratti poi di funzioni esternalizzate, nei contratti tra Banca e fornitore dei servizi devono essere formalizzati e chiaramente definiti i livelli di servizio assicurati in caso di emergenza e le soluzioni di continuità adottate, coerenti con le esigenze aziendali e con le prescrizioni dell'Autorità di Vigilanza. La Banca acquisisce i piani di continuità operativa del fornitore al fine di valutare la qualità delle misure previste e provvederne l'integrazione con soluzioni interne.

È lecito domandarsi se gli ultimi aggiornamenti abbiano dotato il sistema bancario non solo di una normativa specifica, quant'anche di una normativa uniforme ed armonizzata. Sul punto si è espressa "Pantaray", società di consulenza specializzata in formazione sulla BC, la quale ha considerato le Disposizioni di Vigilanza lacunose per terminologia e definizioni utilizzate e per l'eccessiva enfasi posta sul Piano di *Business Continuity*, distogliendo l'attenzione dalla necessità di disciplinare il più complesso Sistema di Gestione del Rischio.

Al di fuori del settore bancario non sembrano rinvenirsi riferimenti normativi di dettaglio ed anzi, paradossalmente, è stato abrogato ciò che prima sembrava compiutamente disciplinare la materia.

Si fa riferimento all'articolo 50 *bis* del Codice dell'Amministrazione Digitale (CAD), il quale stabiliva l'obbligo per le pubbliche amministrazioni di redigere il piano di Continuità Operativa ed il piano di *Disaster Recovery*, nel rispetto di strette e vincolanti prescrizioni tecniche, ed impegnava

il *Ministro per la pubblica amministrazione e l'innovazione* ad assicurare l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni.

Il tempo imperfetto non è errore né scelta stilistica, ma semplicemente frutto delle significative modifiche apportate con D.lgs 176/2016, resesi necessarie per armonizzare il CAD al nuovo Regolamento Europeo eIDAS, che hanno portato il Legislatore italiano all'abrogazione integrale dell'articolo.

Di nostro specifico interesse è l'argomentazione circa le possibili conseguenze derivanti in termini di diritto e di fatto da tale scelta. L'obbligo di redigere un BCP per la Pubblica Amministrazione è stato quindi definitivamente eliminato, ovvero è possibile individuare in altre disposizioni di legge un appiglio testuale garante di tale previsione?

Sul punto le diverse associazioni di settore, attive partecipanti alla discussione *a latere* dell'iter normativo, hanno espresso la propria perplessità circa l'abrogazione dell'art 50 *bis*, in quanto strumento fondamentale per garantire la continuità informatica nella pubblica amministrazione e conseguentemente la continuità operativa del servizio pubblico.

Con l'abrogazione dell'articolo si è diffusa la convinzione, plausibilmente non corretta, dello stralcio dell'obbligo per le amministrazioni pubbliche di redigere un piano di *Business Continuity* e prevedere attività di *Disaster Recovery*. Di fatto, riferimenti contenuti nello stesso Codice dell'Amministrazione Digitale ma anche in altri dettati normativi, confutano questa presunzione.

In primo luogo l'art 51 del CAD, nel disporre di *"...soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture..."* e nel ribadire che "*... I documenti informativi delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta"*, continua a preservare l'obbligo di continuità operativa. Inoltre con le modifiche apportate al CAD all'articolo 43 comma 1 *bis* laddove il "*documento informatico sia conservato per legge da uno dei soggetti di cui all'articolo 2, comma 2, cessa l'obbligo di conservazione a carico dei cittadini e delle imprese che*

possono in ogni momento richiedere accesso al documento stesso" e ciò sembra suggerire se non l'obbligatorietà, la necessità di prevedere quantomeno l'attività di *Disaster Recovery*.

Un altro richiamo normativo significativo è contenuto nel Regolamento UE 2016/679 in materia di protezione dei dati personali, regolamento entrato in vigore a maggio 2016 e che sarà definitivamente applicabile e vincolante a partire dal 25 maggio 2018. Il regolamento di cui sopra, all'art 32 par.1 stabilisce che il titolare ed il responsabile del trattamento dei dati personali devono mettere in atto misure tecniche ed organizzative adeguate, per garantire un livello di sicurezza adeguato al rischio, comprendenti la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati personali.

La lettura del D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) conforta circa l'obbligatorietà anche per la PA di istituire e mantenere in essere procedure atte a garantire il *Disaster Recovery* come pure a prevedere un adeguato piano di B*usiness Continuity*, in quanto tali obblighi sono ben chiaramente esplicitati ed in quanto non sono previste inopportune deroghe a favore della PA stessa. Il Decreto, *ex* articoli 7 (Diritto di accesso ai dati personali ed altri diritti), 31 (Obblighi di sicurezza), 34 (Trattamenti con strumenti elettronici), 35 (Trattamenti senza l'ausilio di strumenti elettronici), vincola alla previsione di attività volte a garantire la conservazione e l'integrità dei dati sensibili e personali, economici, giudiziari, sanitari, ed inoltre a garantire la conservazione e l'inalterabilità dei *log* di accesso a tali dati.

L'obbligatorietà per la Pubblica Amministrazione di redigere un piano di *Business Continuity* e prevedere attività di *Disaster Recovery*, pur essendo intrinsecamente preservata dalle vigenti norme di carattere generale, non è normata da regole tecniche ed adempimenti puntuali. Con tutta probabilità l'intento del Legislatore è stato condizionato dalla proverbiale propensione ad agire secondo le regole del buon padre di famiglia. La realtà della PA è di fatto composta ed articolata in una molteplicità di amministrazioni pubbliche dello Stato, Enti locali, Autorità Amministrative Indipendenti, altri Enti pubblici, Nazionali e Locali, ossia una vastità di attori che ben difficilmente avrebbero potuto realizzare, con proprie competenze e risorse, gli ambiziosi obiettivi prefissi dalla Legge.

Lo stesso *Ministro per la pubblica amministrazione e l'innovazione* avrebbe fallito nel rispetto del comma n.2 dell'abrogato art. 50 *bis*, volto ad assicurare l'omogeneità delle soluzioni di continuità operativa.

Le carenze, i ritardi ed i vuoti normativi della disciplina italiana appena evidenziati sono, con tutta probabilità, mal comune a molti dei Paesi membri dell'Unione Europea.

Esiste indubbiamente un problema di mancata uniformità del quadro normativo. Alcune materie per l'importanza che rivestono, causa il proprio impatto sulla qualità della vita dei cittadini, dovrebbero condurre il Legislatore Europeo ad adottare nei confronti dei Paesi membri quegli sforzi e provvedimenti necessari ad armonizzare tali materie.

L'importanza della *Business Continuity* e del *Risk Management* è tale da richiedere un simile intervento.

All'indomani del rinnovato impegno dei Trattati di Roma, l'Italia ed i singoli Paesi membri hanno espresso la volontà di perseguire una maggiore integrazione. A questo proclama farà eco un'integrazione normativa/legislativa?