

PROTEGGERE LA MEMORIA DELLE AZIENDE

GLI ARCHIVI RAPPRESENTANO IL SILENZIOSO DEPOSITO DELLE INFORMAZIONI SULLE QUALI È CRESCIUTA NEL TEMPO UN'IMPRESA E PER QUESTO INCARNANO, OLTRE AL SAPERE, LA GARANZIA DEL SUO VALORE. ALLA STRATIFICAZIONE DOCUMENTALE SI È AGGIUNTA IN TEMPI RECENTI LA CONSERVAZIONE DEI DATI DIGITALI, PIÙ LABILE E PLASTICA MA UTILE A PORRE LE BASI DELLA CRESCITA FUTURA. DUE MONDI APPARENTEMENTE DISTANTI, MA CHE RICHIEDONO LA STESSA ATTENZIONE PER LA LORO TUTELA

di Maria Moro

Il termine *archivio* evoca nell'immaginario un luogo polveroso, denso di schedari e scaffali pieni di cartelle di documenti, registri e volumi, accessibile a pochi iniziati che ne conoscono le regole e sono responsabili della sua tutela. A parte la fisicità del luogo e del contenuto, accessibilità, regole e tutela sono questioni comuni alle più moderne versioni digitalizzate e alle basi dati. Parlare di conservazione e di protezione degli archivi non è quindi anacronistico, anzi, si tratta di

un tema di piena attualità, una dottrina che si è evoluta passando dalla dimensione concretamente fisica alla maggiore complessità di quella digitale.

Quando si discute di sicurezza degli archivi, oggi il pensiero va immediatamente ai data base, ai server, ai data center e a forme di tutela relative soprattutto all'integrità dei dati informatici e alla cyber security.

È una visione corretta, ma orientata più a questioni operative che a un approccio strategico. La gestione del rischio,





anche quando si tratta di archivi, richiede una visione a tutto tondo del tema, perché solo un'osservazione completa e comprensiva di tutte le variabili può portare a soluzioni razionali e coerenti valide per tutto il sistema interessato. L'osservazione parte quindi dalla motivazione originaria che porta alla creazione di un archivio. L'archivio nasce con l'azienda, ne è memoria, perché deposito dello storico delle azioni e della loro evoluzione, e motore, in quanto ogni iniziativa trova le sue basi nelle attività in precedenza sviluppate. Qualunque sia lo scopo della conservazione delle informazioni, "la funzione documentaria e i principi e gli strumenti necessari a un'ideale organizzazione degli archivi all'interno di un'organizzazione aziendale, nascono dall'esigenza di conferire certezza all'attività giuridico-amministrativa e di conser-

varne stabilmente memoria", osserva **Alberino Battagliola**, risk manager e socio di **Anra**. Di conseguenza, aggiunge, "l'archivio deve corrispondere a esigenze di funzionalità e di reperibilità dei documenti, oltre ad assicurare condizioni corrette di conservazione che garantiscano l'integrità dei documenti, l'accesso e la tutela alla riservatezza". Queste caratteristiche di funzione, storicamente condivise per la documentazione cartacea, si sono negli ultimi anni allargate ai dati intangibili, che siano raccolti per via informatica, inclusa la messaggistica, o che siano trasposizione del cartaceo per la conservazione ed elaborazione digitale. Da alcuni anni l'ordinamento giuridico italiano e dell'Unione Europea "ha stabilito che i dati debbano essere oggetto di trattamento adeguato in termini di formazione e conservazione, assicurando la per-

sistenza di caratteristiche di integrità, autenticità e accuratezza, così come avviene per gli archivi tradizionali", sottolinea Battagliola.

CONSERVAZIONE E GARANZIA DI AUTENTICITÀ

Se lo scopo degli archivi è di conservare le informazioni per mantenerle integre nel tempo e per renderle fruibili e comprensibili, la gestione del rischio è una funzione che diventa necessario implementare.

In riferimento agli archivi documentali fisici, è noto che la carta è di per sé un supporto deperibile, e fragile nel momento in cui dovesse essere soggetta a elementi come acqua e fuoco. Le alluvioni (una su tutte quella di Firenze del 1966) e gli incendi (e in questo caso

a provocare danni irreparabili al nostro patrimonio di memoria storica sono stati i bombardamenti della Seconda Guerra mondiale) rappresentano due delle fonti di rischio che “hanno reso evidente già da tempo l'esigenza di adottare delle linee guida di salvaguardia e di mettere in pratica azioni di messa in sicurezza, partendo da un'analisi circostanziata dei rischi e da misure di prevenzione”.

L'archivio informatico è anch'esso soggetto ai rischi fisici ma, in quanto sistema complesso, è interessato a uno spettro più ampio di rischi. “L'avvento del digitale – osserva Battagliola – ha innescato un'evoluzione dei modi di formazione e gestione del documento e dello

stesso ruolo e concetto di archivio – osserva Battagliola – La razionalizzazione dei sistemi amministrativi e dell'organizzazione del lavoro, così come le nuove modalità di comunicazione, hanno introdotto una serie di vantaggi, a partire da una più efficace organizzazione della produzione documentaria e dal controllo della proliferazione di copie”. Sono però emersi anche nuovi rischi di manipolazione e perdite difficilmente verificabili a distanza di tempo, aspetti che rendono più complesse la progettazione e la gestione degli archivi e richiedono la collaborazione tra diverse specializzazioni e procedure interne condivise e rigorose.

Secondo Battagliola, quindi, sia che si tratti di archivi analogici o digitali, il risk management, diventa “elemento fondamentale in un'ottica di tutela, progettazione, gestione, utilizzo e conservazione degli archivi, al fine di

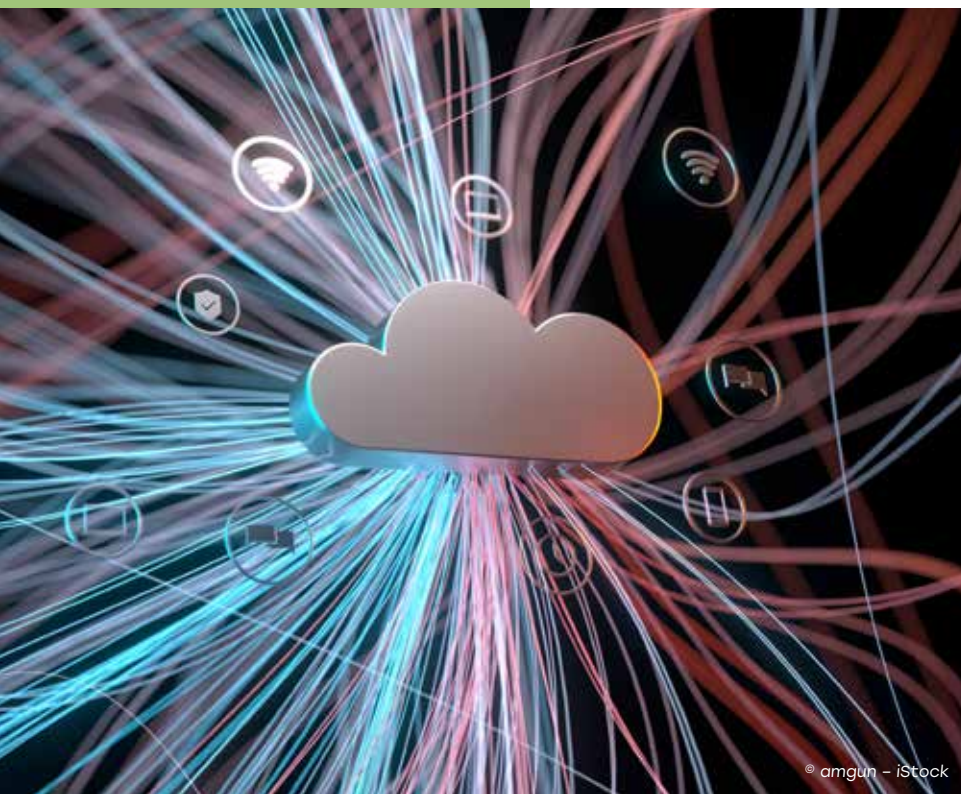
mantenere nel tempo la caratteristica dell'autenticità della produzione documentaria come prova di certezza giuridica e certezza di diritti che qualifica l'azione di trasparenza e affidabilità di ogni soggetto produttore”.

ANALOGICO E DIGITALE, I FATTORI DI RISCHIO CAMBIANO

Guardando ai fattori di rischio, c'è una distinzione fondamentale tra documenti analogici e digitali: se nel primo caso prevalgono le criticità legate alla conservazione, nel secondo caso va necessariamente considerato in primo luogo il loro ruolo all'interno dei processi di lavoro complessi di cui sono parte integrante.

Oltre ai danni fisici, a cui in parte si è già accennato e che includono in generale le minacce alle strutture e ai supporti, un aspetto critico tipico riguarda i rischi di sicurezza, che si concretizzano oggi soprattutto nella cyber security con modalità e strumenti di protezione dalle minacce informatiche, senza escludere però la necessità di proteggere l'accesso anche ai documenti analogici.

In maniera più ampia, Battagliola tiene a sottolineare la centralità dei rischi tecnologici, che “riguardano principalmente le violazioni dei dati, la perdita di informazioni sensibili, lo smaltimento inadeguato dei documenti, la non conformità alle normative, le procedure insufficienti di backup dei dati, l'obsolescenza digitale, gli accessi non controllati, la protezione dei dati sensibili e anche l'uso di social media e *cloud computing* per l'utilizzo, la lavorazione e la condivisione dei documenti aziendali. Diventa fondamentale garantire che i sistemi siano configurati corret-



tamente, così che i documenti digitali siano creati, gestiti e archiviati in modo sicuro e, quando serve, eliminati in maniera appropriata. L'eliminazione dei documenti digitali non equivale, infatti, alla loro distruzione”.

Un ulteriore contesto di rischio è quello relativo agli impatti finanziari e commerciali di una gestione non corretta degli archivi, a partire dalle sanzioni derivanti dalla mancanza di compliance rispetto al governo e al trattamento dei documenti e dei dati.

Infine, vanno considerati i rischi legati ai fattori sociali, culturali e politici, direttamente collegati alla comunicazione dell'informazione e all'utilizzo che ne viene fatto, “questo soprattutto in relazione all'uso dell'informazione nella società di oggi, in grado di cambiare la percezione del mondo circostante. La credibilità, qualità della fonte di provenienza, diventa fondamentale in un processo di costruzione dello spirito critico, in particolare in questo specifico contesto storico in cui le produzioni dell'intelligenza artificiale prendono sempre più campo”, riflette Battagliola.

UN CAMBIAMENTO CULTURALE NELLE IMPRESE

Anche nel caso degli archivi, una gestione del rischio strutturata necessita di un approccio integrato fra le competenze di settore, visione che già appartiene alla comunità archivistica e che ha trovato supporto con l'introduzione del digitale. “Nessun sistema di gestione documentale corretto può prescindere da uno scambio di conoscenze e competenze di dominio finalizzato alla costruzione di un sistema strutturale”, afferma Battagliola. In questo senso, le funzioni coinvolte afferiscono agli



aspetti gestionali e a quelli strategici, dove i primi si riferiscono ai meccanismi interni di funzionamento e allo sviluppo stesso dell'archivio, mentre i secondi comprendono la definizione e la gestione delle direttrici che includono tutti gli stakeholder esterni, dai canali di raccolta delle informazioni all'utenza.

La solidità del sistema nel suo complesso è anche propedeutica alle principali strategie di mitigazione dei rischi. “Un approccio *risk-based* nella gestione dei documenti e delle informazioni – sostiene Battagliola – ha il potenziale per offrire vantaggi che vanno dal miglioramento delle prestazioni di un'organizzazione al potenziamento dell'uso strategico delle informazioni”.

Fondamentali in questo senso sono la conoscenza delle norme, la formazione del personale aziendale e lo scambio di competenze e di informazioni.

Si tratta soprattutto di mettere in atto un cambiamento culturale nelle aziende, ossia “prendere consapevolezza che l'archivio è una ricchezza fondamentale per ogni organizzazione, perché è su di esso che si basano non solo la corretta gestione del lavoro, ma anche qualsiasi ripresa di attività dopo situazioni di emergenza”, conclude Battagliola, ribadendo il valore di custodia “della memoria, delle regole, del patrimonio di informazioni” degli archivi. ●