

ATTUALITÀ 

# IL LATO PROFITTEVOLE DEL GDPR

di MARIA MORO

LA CONFORMITÀ AL REGOLAMENTO UE SUL TRATTAMENTO DEI DATI PERSONALI È UN'OCCASIONE DI CAMBIAMENTO NELL'OPERATIVITÀ.

UN PASSAGGIO NECESSARIO PER ADEGUARE LA PROPRIA PROFESSIONALITÀ A UN ECOSISTEMA DI MERCATO CHE RICHIEDE DI ESSERE ALLINEATI SUI TEMI DI SICUREZZA, PRIVACY E RISCHIO CYBER. L'INTERMEDIARIO SI METTE IN GIOCO COME IMPRENDITORE RESPONSABILE E COME CONSULENTE. QUESTE ALCUNE EVIDENZE EMERSE NEL CORSO DI UN RECENTE CONVEGNO DI ACB

Il modo di lavorare di domani sarà completamente diverso da quello a cui facciamo riferimento oggi: lo si afferma ormai da tempo, ma ancora non è pienamente evidente cosa significherà dover fare i conti con le nuove tecnologie, e con le normative che cercano di trasformare il flusso *disruptive* in una placida corrente. La prima evidenza, come spesso è accaduto nella storia delle innovazioni, è stata la scoperta dei vantaggi commerciali dei nuovi strumenti, poi delle opportunità per efficientare l'operatività aziendale e, in rincorsa, la normativa che si preoccupa di regolamentare l'uso di mezzi dalle enormi potenzialità.

E a questo punto si ricomincia: perché una volta evidenziati i problemi e posti dei limiti, quanto è già stato fatto deve essere riportato nell'alveo della compliance, con nuovi vincoli e anche nuove opportunità. Tutto ciò avrà riflessi consistenti sul modo di lavorare delle imprese, cambiandone completamente i paradigmi operativi e commerciali. Vale per tutti i soggetti sociali ed economici, e vale ancor di più per un settore particolarmente normato come quello assicurativo. Su questo tema, il 12 aprile scorso **Acb** ha organizzato per i broker associati il convegno *Privacy e cyber risk. Sinergie della protezione e della gestione dei dati alla luce del nuovo Gdpr*, a cui hanno partecipato **Stella Aiello**, dirigente responsabile del servizio distribuzione di **Ania**; **Chiara Ceriolo**, legal & compliance manager di **Chubb Italia**; **Patrizia Contaldo**, docente presso l'Università Bocconi di Milano; **Paolo Cupola**, esperto di privacy e antiriciclaggio; **Alessandro Leone**, partner Grant Thornton financial advisory services, **Antonio Longo**, avvocato e docente presso l'Università della Tuscia di Viterbo; **Andrea Maura**, partner dello studio Legal Grounds; **Maria Teresa Paroli**, amministratore delegato di **Hit**; **Orazio Rossi**, country president di Chubb Italia.



## AGILE NON SIGNIFICA PRIVO DI CONTROLLO

Non è banale che gli esempi più evidenti dei rischi legati alla diffusione delle nuove tecnologie abbiano come protagonisti recenti proprio grandi player che hanno anticipato i tempi costruendo la propria fortuna sull'agilità del web e sul valore del dato. Alessandro Leone ha elencato le conseguenze su reputazione e titoli azionari dei casi più clamorosi in termini di sicurezza e privacy dell'ultimo periodo: *Wannacry*, che ha reso evidente la vulnerabilità di industrie strategiche come **Boeing**, l'inadeguato livello di sicurezza causa del massiccio furto di dati subito da **Uber**, la superficiale gestione della privacy in casa **Facebook**. Sono macro esempi che dimostrano la necessità di lavorare su cultura e sensibilità alla sicurezza a tutti i livelli. Gli intermediari devono considerare gli aspetti della sicurezza sia come tema da trattare in qualità di consulenti sia come detentori di dati sensibili dei propri clienti. Il

ATTUALITÀ **A**

consiglio che Leone offre è di applicare un modello di piano di sicurezza che deve essere basato su tre passi. “Prima di tutto – ha spiegato – disegnare la *security strategy* aziendale, che include la valutazione del rischio e la definizione di un *business continuity plan* e di un *recovery plan*; poi la gestione regolare e quotidiana della security; e, infine, il monitoraggio continuo delle potenziali minacce”.

**LA GESTIONE INTEGRATA DELLA NORMA**

Ci sono alcuni aspetti nel Gdpr che richiamano responsabilità a cui sono tenuti anche gli intermediari. Antonio Longo ha spiegato che la decadenza delle prescrizioni del codice della Privacy lascia al gestore dei dati una libertà di azione che nasconde una maggiore responsabilità: “La norma fa riferimento ai principi di legittimità, necessità, proporzionalità e trasparenza. Significa che il trattamento dei dati deve essere coerente all’attività specifica dell’impresa in termini di pertinenza, necessità e durata”, una valutazione che è demandata ora al responsabile dei dati. Paolo Cupola ha cercato di dare maggiore concretezza ai principi della norma. “Gestire la privacy *by design e by default* – ha osservato – significa considerare gli aspetti di sicurezza e riservatezza in parallelo a ogni azione che viene compiuta dagli intermediari. L’adozione di un

nuovo modulo di raccolta di informazioni del cliente, ad esempio, va prevista in conformità al Gdpr, così come ogni azione che riguardi i collaboratori”. Altre prescrizioni possono avere un impatto particolare sull’attività degli intermediari, e tra queste il diritto di portabilità dei dati e il diritto all’oblio. Il primo caso afferma il diritto del cliente di chiedere il trasferimento dei dati raccolti su di lui a un nuovo consulente; il diritto all’oblio prevede invece che chi ha avuto qualche tipo di relazione con l’intermediario (un cliente, ma anche un ex dipendente o un fornitore) possa richiedere la cancellazione di tutte le informazioni che lo riguardano, atto che implica la verifica della presenza di tali informazioni non solo presso la propria sede, ma anche presso qualsiasi terzo con cui si possa aver condiviso i dati per ragioni professionali.

**DOVE SI NASCONDE L’OPPORTUNITÀ**

È necessario, come ha sottolineato Stella Aiello, “un salto di qualità che prima di essere organizzativo è culturale, ma anche un approccio proattivo per passare dalla compliance fine a se stessa all’adesione a reali comportamenti di sicurezza, sia nelle agenzie, sia nell’adempiere al ruolo sociale verso gli assicurati”. Un passaggio che è molto vicino a cogliere il lato profittevole delle implicazioni normative: secondo Patrizia Contaldo, “la competenza in materia di rischi cyber e privacy e la capacità di gestire i dati possono impattare positivamente sul modello di business se inserite in un processo consapevole”. Su un piatto della bilancia vanno messi gli inevitabili costi di adeguamento tecnologico e normativo, dall’altro i risparmi sui costi operativi, la maggiore efficienza dei processi e la crescita delle competenze dei collaboratori. Ma in più va considerata la valenza economica della capacità di gestire i dati, che si esplica in una migliore relazione con il cliente basata su trasparenza e competenze, e in una gestione più consapevole delle informazioni in archivio, da utilizzare per azioni di marketing sempre più raffinate, per proposte effettivamente personalizzate e per la definizione più precisa dei target di mercato: il tutto con l’attenzione a non scivolare nelle insidie del Gdpr. **1**

