

Antiriciclaggio, effetto privacy

ARTURO BELCULFINÈ E GIUSEPPE SCIARRETTA

La questione della raccolta dati svolta attraverso l' adeguata verifica della clientela Norme applicabili in parte: mancano le regole tecniche Norme antiriciclaggio applicabili solo in parte anche a causa della mancata attuazione delle regole tecniche degli organismi di autoregolamentazione nonché dei provvedimenti delle autorità di controllo. Le criticità sono aumentate dallo scorso maggio, con l' entrata in vigore del decreto legislativo n. 51 del 2018, il cosiddetto decreto privacy, emanato in attuazione della direttiva (UE) 2016/680 del Parlamento e del Consiglio europeo, il quale è andato ad impattare sul trattamento dei dati antiriciclaggio raccolti nell' adempimento delle prescrizioni normative. Uno dei presidi fondamentali su cui si muove tutto il sistema di prevenzione al riciclaggio è proprio la raccolta dei dati svolta



attraverso l' adeguata verifica della clientela. Oggi, però, risulta rilevante, ai fini di una corretta applicazione della norma sulla privacy, come questi documenti vengono conservati. Lo stesso dlgs n. 90/2017, all' art. 31 prevede il perfezionamento di tale obbligo attraverso la conservazione, per dieci anni, di tutti i documenti, i dati e le informazioni «utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento di analisi effettuate, nell' ambito delle rispettive attribuzioni, dalla Uif o da altra autorità competente». Le modalità di conservazione, disciplinate dall' art. 32 del dlgs n. 231/2007, impongono ai soggetti obbligati l' adozione di sistemi di conservazione dei documenti, dei dati e delle informazioni, idonei a garantire il rispetto delle norme dettate dalla normativa in vigore in materia di protezione dei dati personali; resta inteso che il trattamento dei medesimi dati avvenga esclusivamente per le finalità di cui alla normativa antiriciclaggio. Attualmente quindi, alla luce delle nuove disposizioni i soggetti obbligati alla normativa antiriciclaggio dovranno: fornire ai clienti idonea informativa nella quale venga specificato che il trattamento dei dati avverrà anche per le finalità previste dalla

normativa antiriciclaggio; individuare i soggetti incaricati del trattamento dei dati con le modalità previste dall' art.30 del dlgs196/2003; prevedere che le operazioni vengano effettuate solo dagli incaricati che operano sotto la diretta autorità del titolare o del responsabile della società o studio professionale, effettuando la designazione per iscritto e individuando in maniera puntuale l' ambito del trattamento consentito. Sempre in riferimento all' art. 32 del dlgs n. 231/2007 diventa ancora più importante per i soggetti obbligati andare ad osservare tutte le misure di sicurezza previste dalla normativa, attraverso il ricorso a credenziali di autenticazione per l' accesso ai dati conservati elettronicamente, avendo cura di limitare l' accesso in funzione dell' attività concretamente e prevedendo, inoltre, istruzioni dettagliate per gli incaricati. Particolare attenzione, infine, va posta sul rischio di perdita delle informazioni raccolte. I soggetti obbligati dovranno infatti ridurre al minimo i rischi di distruzione o perdita dei dati, anche accidentale, garantendo nel contempo che non venga effettuato un accesso alle informazioni da parte di soggetti non autorizzati. Le autorità di vigilanza e gli organismi di autoregolamentazione Un ruolo determinante, in tale contesto, è certamente svolto dalle autorità di vigilanza (per gli intermediari finanziari) e dai «neo» organismi di autoregolamentazione (per le categorie dei professionisti). L' art. 9 del dlgs 90/2017 (disposizioni finali) recita che le autorità di vigilanza di settore, entro 12 mesi dalla data di entrata in vigore del novellato decreto antiriciclaggio (che si ricorda essere stata il 4 luglio 2017), avrebbero dovuto emanare le disposizioni attuative dell' art. 16 comma 2 del dlgs n. 231/2007 per mitigare il rischio di riciclaggio e di finanziamento del terrorismo. In effetti, in aderenza a quanto chiesto dal legislatore, seppur in tempi e modi differenti, entrambe le autorità hanno divulgato le proprie disposizioni: «regole tecniche» emanate dai organismi di autoregolamentazione, in attuazione dell' art. 11 comma 2 del dlgs 231/2007, trattando appunto anche le modalità di conservazione dei dati e delle informazioni; un provvedimento da parte di Banca d' Italia, del 31 luglio 2018, con cui sono state appunto date disposizioni specifiche per la conservazione e l' utilizzo dei dati e delle informazioni ai fini antiriciclaggio e di contrasto al finanziamento al terrorismo. Da evidenziare però come il provvedimento in questione non è entrato in vigore in quanto si tratta, al momento, di una consultazione pubblica, con il fine di raccogliere suggerimenti, osservazioni o proposte, prima dell' entrata in vigore prevista per il 1° gennaio 2019. Entrambi gli elaborati però non chiariscono alcunché. Non vi sono infatti rimandi specifici al novellato decreto privacy, lasciando quindi presupporre che nulla sia cambiato rispetto alle precedenti disposizioni e/o prassi utilizzate per la conservazione dei documenti raccolti nell' ambito dell' attività di adeguata verifica. Cosa si può fare nel frattempo al fine di scongiurare sanzioni? Sarebbe forse opportuno progettare un modello di compliance integrato che riduca il rischio di violazioni a entrambe le discipline adottando strumenti organizzativi, standardizzati e informatici in grado di gestire aspetti diversi (l' antiriciclaggio e la privacy) nel modo più efficace possibile, affiancando una formazione del personale sempre più pregnante. © Riproduzione riservata.