

Per la conservazione dei dati antiriciclaggio dieci anni sono troppi

Parere favorevole, ma condizionato, del Garante della privacy sullo schema di DLgs. di recepimento della Direttiva 2015/849/UE

/ Maurizio MEOLI

Il Garante della privacy ha espresso **parere favorevole**, ma **condizionato**, sullo schema di DLgs. volto a recepire la Direttiva 2015/849/UE, relativa alla prevenzione dell'uso del sistema finanziario a fini di **riciclaggio** o finanziamento del terrorismo, in attuazione dell'art. 15 della L. 170/2016 ("legge di delegazione europea 2015"). Si ricorda, in primo luogo, come la Direttiva 2015/849/UE ponga espressamente la necessità di assicurare la **protezione dei dati** e stabilisca che la raccolta ed il successivo trattamento di dati personali da parte dei soggetti obbligati debbano essere limitati a quanto necessario per conformarsi alle prescrizioni della Direttiva, senza un ulteriore trattamento dei dati personali che sia incompatibile con gli scopi suddetti. Inoltre, è previsto il categorico divieto di ulteriore trattamento dei dati personali a fini commerciali.

Si evidenzia, quindi, come la previsione secondo la quale i soggetti destinatari delle disposizioni antiriciclaggio debbano applicare gli obblighi di **adeguata verifica** della clientela, fra l'altro, quando vi sia "il sospetto di riciclaggio o di finanziamento del terrorismo" (nuovo art. 17 comma 2 lett. a) del DLgs. 231/2007), lasci un elevato margine di discrezionalità. Risulta quindi necessario individuare, già nel decreto, alcuni criteri, quantomeno generali, da applicare per valutare la sussistenza di tale "sospetto"; ciò analogamente, o anche mediante rinvio, a quanto previsto per la valutazione del "rischio" di riciclaggio e per l'individuazione delle **operazioni sospette**.

Quanto alle condizioni poste, si richiede, tra l'altro, di introdurre nelle disposizioni che regolano i **flussi dei dati** verso la **UIF** – e che quindi determinano la costituzione presso tale soggetto della banca dati delle segnalazioni di operazioni sospette – una norma che preveda tra gli obblighi della UIF anche l'individuazione di misure idonee a garantire la protezione dei dati personali e sulla tenuta e gli accessi alla banca dati, da adottare sentito il Garante.

Il nuovo art. 19, comma 1, lett. b) prima parte del DLgs. 231/2007 contempla l'ipotesi in cui emergano perplessità circa la **veridicità dei dati identificativi** forniti dal cliente per adempiere agli obblighi di adeguata verifica. In tal caso si prevede che il riscontro della veridicità degli stessi venga effettuato tramite la consultazione del sistema pubblico per la prevenzione del furto di identità di cui al DLgs. n. 64/2011 (c.d. SCIPAFI).

Si richiede di prevedere una nuova disposizione che rimandi ad un decreto modificativo della disciplina attuale di **accesso al sistema** (prevista dal DM 19 maggio

2014 n. 95) che, previo parere del Garante, individui i presupposti, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti.

Nel secondo periodo dell'art. 19, comma 1, lett. b) si prevede: "La verifica dell'identità può essere effettuata anche attraverso il ricorso ad **altre fonti attendibili** ed indipendenti tra le quali rientrano le basi di dati ad accesso pubblico o condizionato al rilascio di credenziali di autenticazione, riferibili a una pubblica amministrazione". La disposizione è reputata troppo generica, non permettendo di individuare le banche dati pubbliche che dovrebbero essere consultate. Pertanto si ritiene opportuno inserire un rinvio ad un successivo atto regolamentare che le individui, o in mancanza espungere tale periodo dal testo. Ciò in quanto l'accesso a SCIPAFI già consente la verifica dei dati attraverso la consultazione delle banche dati pubbliche, anche ad accesso riservato, idonee a verificare l'identità.

Si ribadisce, poi, la contrarietà ad un termine di **conservazione** dei dati **sostanzialmente indefinito**, quale quello che deriva dall'impiego dell'espressione "almeno dieci anni". Posta la necessità della previsione di un chiaro termine finale di conservazione, si osserva come l'art. 40 della Direttiva 2015/849/UE si limiti, al riguardo, a stabilire un termine di **"almeno cinque anni"** dalla fine del rapporto d'affari o dall'esecuzione dell'operazione. Rispetto ad esso non risulta alcuna necessità di prevedere un termine almeno decennale.

Il nuovo art. 32 comma 3 del DLgs. 231/2007, infine, consente ai soggetti obbligati di avvalersi di un **autonomo centro di servizi**, ovvero di un soggetto esterno, per la conservazione di documenti, dati e informazioni, purché sia assicurato ai soggetti obbligati l'accesso diretto e immediato al sistema di conservazione. Con riferimento al ruolo assunto dal centro di servizi, rispetto al trattamento dei dati personali, occorre prescrivere che: tale soggetto sia preventivamente designato quale responsabile del trattamento, che deve offrire idonee garanzie in relazione a quanto previsto dall'art. 29 del Codice in materia di protezione dei dati personali (DLgs. 196/2003); siano fornite a tale soggetto adeguate istruzioni; il titolare vigili sul trattamento da effettuare, con particolare riguardo alle ipotesi in cui tale soggetto sia designato responsabile da più operatori, al fine di garantire misure di carattere tecnico organizzativo volte ad assicurare la segregazione dei flussi con ciascun operatore.