



Massime, tecniche e tassazione notarile

RIVISTE WOLTERS KLUWER

Notai, regole antiriciclaggio e ausili informatici

giovedì 11 marzo 2021

di Razzante Ranieri Professore a contratto in Intermediazione finanziaria e Legislazione antiriciclaggio presso l'Università di Bologna

Di seguito l'articolo del Prof. Razzante, pubblicato su *Notariato* n. 1/2021, Ipsoa, Milano.

Il decreto legge 76/2020 (c.d. decreto semplificazioni) ha introdotto alcune misure per favorire la diffusione dell'accesso ai servizi informatizzati tramite l'utilizzo dell'identità digitale. Tra queste figura uno snellimento delle procedure di adeguata verifica da remoto, con la possibilità di utilizzare lo SPID con livello di sicurezza almeno significativo.

Premessa

La professione notarile è tutta stata investita dalla "pandemia digitale", come è stato sottolineato già da altri in questo numero della Rivista. Con modifiche poderose al quotidiano dispiegarsi degli atti tipici dell'attività costitutiva dei notai. Le novità introdotte dal decreto semplificazioni (D.L. 16 luglio 2020, n. 76, conv. L. 11 settembre 2020, n. 120), come noto, hanno inciso sugli adempimenti antiriciclaggio per l'adeguata verifica da remoto, contenute nel D.Lgs. n. 231/2007 (c.d. Decreto antiriciclaggio). Il decreto 76, infatti, visto il perdurare delle misure di contenimento del virus Covid-19, nel tentativo di favorire la diffusione dell'accesso ai servizi informatizzati tramite l'utilizzo dell'identità digitale, ha snellito le procedure di identificazione della clientela non in presenza.

Alcune brevi premesse sul D.Lgs. n. 231/2007, contenente le disposizioni oggetto di revisione. Esso introduce l'obbligo della adeguata verifica della clientela. Il principio ispiratore è connesso alla gestione delle asimmetrie informative: i destinatari della normativa antiriciclaggio non devono limitarsi a registrare le informazioni, ma sono tenuti ad avere una conoscenza approfondita del profilo complessivo di un cliente, per essere in grado di cogliere rapidamente eventuali anomalie nel corso del rapporto professionale.

Il principio cui deve ispirarsi l'adeguata verifica della clientela è quello del Know Your Customer (KYC). Detto principio richiede, da un lato, il passaggio dal semplice obbligo di identificazione (consistente sostanzialmente nell'acquisizione di informazioni sull'identità) ad un ampio dovere di verifica, che si sostanzia in un processo composto dal succedersi di molteplici misure. In altre parole, viene esteso il compito della conoscenza del cliente, muovendo dalla mera identificazione verso un continuum nel quale l'applicazione dei presidi antiriciclaggio (raccolta di informazioni, valutazione dell'attività esercitata, rilevazione di fenomeni anomali) accompagna tutto il corso dello svolgimento della prestazione professionale. Dall'altro, la valutazione del rischio di riciclaggio è adottata quale parametro essenziale per determinare in profondità ed in estensione i compiti di verifica della clientela.

L'obbligo di adeguata verifica consiste, lo si sottolinea, nelle attività riportate nell'art. 18, D.Lgs. n. 231/2007:

- a) identificazione del cliente e verifica dell'identità sulla base di documenti, dati o informazioni ottenute da una fonte affidabile e indipendente;
- b) identificazione dell'eventuale titolare effettivo e verifica dell'identità;
- c) reperimento di informazioni sullo scopo e sulla natura prevista del rapporto continuativo;
- d) monitoraggio costante nel corso del rapporto continuativo.

Gli strumenti di identificazione elettronica per l'adeguata verifica

L'identificazione è la prima attività del processo di adeguata verifica della clientela. Più in generale, il controllo della identità del soggetto operante e degli eventuali poteri di rappresentanza sono da ritenersi sempre doverosi, a comprova della corretta operatività del professionista.

Le modifiche introdotte dal decreto semplificazioni incidono proprio su questa prima fase. In particolare, l'art. 27, D.L. n. 76/2020 racchiude tutti gli emendamenti al decreto antiriciclaggio. Il primo riguarda la definizione di "dati identificativi", di cui all'art. 1, comma 2, lett. n), D.Lgs. n. 231/2007, con l'eliminazione delle parole "gli estremi del documento di identificazione". Come noto, nell'ambito degli adempimenti connessi all'adeguata verifica in presenza, il soggetto obbligato deve raccogliere una serie di informazioni riguardanti il cliente, per identificarlo e definirne il profilo di rischio. Secondo il nuovo testo emendato, laddove all'art. 18, D.Lgs. n. 231/2007 si chiede di raccogliere i "dati identificativi", sarebbero da annotare nella scheda AML solo il nome e il cognome, o la denominazione, il luogo e la data di nascita, la residenza anagrafica e il domicilio, se diverso dalla residenza anagrafica, o la sede legale, il codice fiscale. Non più quindi, seguendo alla lettera la norma, gli estremi del documento. È stato inoltre cambiato, in parte, il riferimento al riscontro dell'identità del cliente sulla base del documento d'identità o altro documento di riconoscimento equipollente, che ora dovrebbe avvenire confrontando documenti, dati o informazioni ottenuti da una "fonte affidabile e indipendente". Mancano, però, ad oggi, chiarimenti "ufficiali" sia sulla natura di tali documenti, sia delle caratteristiche delle fonti. Le Linee Guida antiriciclaggio dei commercialisti, pubblicate prima delle modifiche intervenute (23 maggio 2019), a scanso di equivoci,

prevedevano che l'obbligo dovesse ritenersi assolto attraverso l'acquisizione di copia del documento di identità/riconoscimento. E si ritiene che, finché non vi saranno indicazioni da Autorità di vigilanza o Organismi di autoregolamentazione, questo suggerimento prudenziale debba rimanere valido. Per far chiarezza, e riferendoci all'attività del notaio, nel caso di adeguata verifica in presenza, sarebbe opportuno lasciare invariate tutte le procedure di identificazione e di conservazione dei dati all'interno del fascicolo del cliente. Non sarà quindi necessario aggiornare le schede AML utilizzate dallo studio, ma si potranno mantenere le stesse. Così come si consiglia vivamente di conservare sempre le copie delle carte d'identità, o dei documenti equipollenti.

Modifiche più puntuali, invece, sono intervenute sull'adeguata verifica a distanza. Il decreto semplificazioni, infatti, prevede che, nel caso di identificazione di clienti in possesso di un'identità digitale (art. 19, comma 1, n. 2, lett. a), D.Lgs. n. 231/2007), per ritenere idoneo l'utilizzo di quest'ultima, basterà che la stessa abbia un livello di garanzia "almeno significativo", secondo i parametri del Codice dell'amministrazione digitale (CAD, D.Lgs. n. 82/2005), o del Reg. UE/910/2014 sull'identità digitale (c.d. Regolamento eIDAS - electronic IDentification Authentication and Signature). Il testo previgente del decreto 231 richiedeva, invece, un livello "massimo" (ossia elevato). I livelli, secondo l'art. 8, Reg. eIDAS, sono tre: basso, significativo ed elevato. Quest'ultimo solo prevede un procedimento di rilascio che contempli il riconoscimento tramite fotografia o caratteristiche biometriche del titolare. Inoltre, il decreto semplificazioni è intervenuto anche a introdurre il comma 2-duodecies all'art. 64 CAD (Codice dell'Amministrazione Digitale), con il risultato di equiparare l'esibizione del documento d'identità (proprio dell'identificazione de visu) al ricorso a sistemi informatici di verifica di media sicurezza. A tal proposito, pare opportuno rinviare agli approfondimenti presenti nello studio del Notariato sull'identità digitale (2BIS_2020 B), pubblicato nel novembre 2020, che rappresenta una sorta di vademecum per il professionista di fronte alle nuove opportunità offerte dalle innovazioni tecnologiche. In questa sede ci si consenta però di evidenziare che, secondo la nuova normativa, sarà quindi consentita un'adeguata verifica a distanza con modalità meno rigorose rispetto a quella in presenza. Infatti, nel caso si ricorra a sistemi di identificazione elettronica, per via degli emendamenti introdotti, l'esibizione del documento d'identità da parte del cliente non sarà più obbligatoria. In aggiunta, i sistemi consentiti, con livello di sicurezza "almeno significativo", prevedono procedure di istruzione e rilascio che non garantiscono il titolare da possibili sottrazioni fraudolente in seguito ad attacchi hacker, contrariamente ai sistemi di elevata sicurezza. Le procedure di rilascio per l'identità digitale attualmente lecite in Italia, si ricorda, sono lo SPID, modulabile nei tre livelli (basso, significativo ed elevato), e la CIE (Carta d'identità elettronica, solo per quello elevato).

Occorre, comunque chiarire quale sia il campo di applicazione delle disposizioni riguardanti l'adeguata verifica a distanza della clientela, tramite l'utilizzo di tali sistemi, nell'ambito delle attività svolte dal notaio. Come noto, infatti, la legge notarile impone (art. 47 l. not.) la presenza delle parti per la ricezione dell'atto. Tale presenza è necessaria anche per l'accertamento dell'identità personale del cliente. Pertanto, non sarà possibile eseguire la prestazione professionale esclusivamente "da remoto", ma semmai solo la compilazione, in via anticipata, della scheda AML. Quando gli adempimenti antiriciclaggio devono invece eseguirsi contestualmente alla stipula dell'atto, il ricorso a sistemi di identificazione informatici può ritenersi

idoneo solo per il supporto nell'attività di accertamento dell'identità del cliente, comunque sempre con la sua presenza in studio, ad esempio, attraverso la verifica della CIE, utilizzando le tecnologie NFC (Near field communication), disponibili anche su smartphone e tablet.

In alternativa all'identità digitale si potrà accettare un certificato per la generazione di firma elettronica qualificata. In questo contesto, occorre premettere che la disciplina del documento informatico e della firma digitale è contenuta nel CAD, come modificato dal D.Lgs. 13 dicembre 2017, n. 217. In particolare, secondo la definizione contenuta in detto decreto, la firma elettronica qualificata è "un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma". La generazione di questa tipologia di firma avviene attraverso un certificato qualificato rilasciato da una Autorità di certificazione (c.d. Certification Authority). Questa procedura, come anticipato, è idonea ad assolvere all'obbligo di identificazione, come previsto dal decreto antiriciclaggio.

Premesso che il notaio rimane, comunque, l'unico soggetto obbligato agli adempimenti antiriciclaggio, in questi casi egli dovrà accertare che il dispositivo di firma sia stato rilasciato da un soggetto certificatore dotato di una disciplina in materia di identificazione conforme alle disposizioni de quibus, nonché verificare, in sede di conferimento dell'incarico professionale, la validità della firma elettronica stessa. Il possesso da parte del cliente della firma elettronica qualificata, poi, risulta particolarmente utile anche per la sottoscrizione delle eventuali dichiarazioni rese dal cliente in sede di compilazione della scheda AML. Il decreto antiriciclaggio, all'art. 22 impone, infatti, un preciso obbligo per i clienti di fornire per iscritto e sotto la propria responsabilità (con sanzioni penali in caso di falso), tutte le informazioni necessarie e aggiornate per consentire ai soggetti obbligati di adempiere agli obblighi di adeguata verifica. Uno strumento modulabile, quello della firma qualificata, che può agevolare e velocizzare gli adempimenti di legge, specie nel caso si voglia procedere in momenti distinti alla sottoscrizione della dichiarazione ex art. 22 e alla stipula dell'atto.

Occorre comunque evidenziare che il ricorso a questi innovativi strumenti è idoneo ad esaurire solo la fase di identificazione del cliente. Permangono pertanto in capo al professionista gli altri adempimenti connessi all'adeguata verifica della clientela, e segnatamente la valutazione sullo scopo e sulla natura del rapporto, ed il suo controllo costante (laddove il cliente richieda altre prestazioni professionali). Ne consegue che, anche nel caso di instaurazione di un nuovo rapporto con un cliente precedentemente identificato, il notaio sarà tenuto a mettere in campo delle misure tali per cui esso, di volta in volta, possa verificare la coerenza della nuova operazione richiesta con il "complesso delle operazioni compiute in costanza del rapporto o di altri rapporti precedentemente intrattenuti" (art. 19, comma 1, lett. c), D.Lgs. n. 231/2007). Inoltre, egli dovrà garantire "il controllo costante nel corso del rapporto continuativo o della prestazione professionale [...] attraverso l'analisi delle operazioni effettuate e delle attività svolte o individuate durante tutta la durata del rapporto, in modo da verificare che esse siano coerenti con la conoscenza che il soggetto obbligato ha del cliente e del suo profilo di rischio, anche riguardo, se necessario, all'origine dei fondi" (art. 19, comma 1, lett. d), D.Lgs. n. 231/2007).

Resta inteso che, nel caso di variazioni nel profilo soggettivo del cliente, si dovrà eseguire una nuova identificazione. In particolare, per la circostanza di mutamento dell'assetto proprietario della società in nome e per conto della quale si stipula il contratto (cambiamento delle quote di controllo societario e, conseguentemente, del/i titolare/i effettivo/i), si dovrà procedere a nuova adeguata verifica.

Pertanto, per essere adempiente agli obblighi antiriciclaggio, il professionista deve previamente contemplare nelle proprie procedure interne antiriciclaggio, per ciascuna opzione per l'identificazione della quale il medesimo cliente intenda valersi per l'esecuzione della prestazione, le modalità di implementazione delle restanti fasi di adeguata verifica (oltre quella di identificazione tramite identità digitale o utilizzo del certificato di firma elettronica), nonché predisporre strumenti per la conservazione e consultazione tempestiva dei dati e acquisire, ove necessario, informazioni supplementari dal cliente ovvero da altre fonti.

Per quanto concerne, giustappunto, la conservazione dei dati, anche qui la tecnologia muove in favore di una semplificazione de facto dell'adempimento de quo. È ammessa, infatti, come noto (art. 32, D.Lgs. n. 231/2007) la possibilità di archivi informatici, in affiancamento al repertorio, che si vogliano utilizzare per mantenere più ordinatamente le evidenze derivanti dalla Know Your Customer.

Infine, ultimo ma non ultimo, l'adempimento della segnalazione di operazioni sospette. Qui la tecnologia, al di là del dovuto metodo di collegamento/invio con l'Autorità ricevente (UIF), si presta a fornire banche dati per la profilatura del cliente, arricchite da liste PEPS e terroristi. Ciò oltre agli eventuali studi reputazionali, mediante la collazione di informazioni open source, che talune società di settore forniscono.

Pensare a questi adempimenti, oggi, senza l'associazione con le funzioni tecnologiche avanzate, non risulta possibile a chi scrive.

Copyright © - Riproduzione riservata