Maggio 2020

Il GAFI apre all'identità digitale

Antonio Martino, Of Counsel, DLA Piper; Ernesto Carile, Tenente Colonnello, Guardia di finanza

Il rapido diffondersi delle tecnologie informatiche connesse allo sviluppo dei pagamenti digitali rende fondamentale l'adeguamento e l'evoluzione degli strumenti normativi di contrasto al riciclaggio e al finanziamento del terrorismo al fine di garantire che qualsiasi transazione finanziaria sottenda il fondamentale requisito di conoscenza del cliente e di garanzia che i fondi coinvolti non abbiano provenienza illecita.

A livello globale e nazionale vi è un estremo interesse da parte degli operatori coinvolti all'applicazione della normativa AML/CFT nell'impatto che le nuove tecnologie ed il FinTech in generale potranno avere sotto il profilo del contrasto al riciclaggio e al finanziamento del terrorismo.

In una recente indagine conoscitiva della Banca d'Italia pubblicata nel dicembre del 2019[1] è stato delineato un quadro degli investimenti in FinTech del sistema finanziario italiano nel periodo 2017-2020. La ricerca ha fatto emergere come gli intermediari finanziari campionati abbiano polarizzato una parte degli investimenti nel settore AML/CFT alla luce del recepimento della IV[2] e V[3] Direttiva Antiriciclaggio, oltre che delle disposizioni della Banca d'Italia in materia di adeguata verifica della clientela, emanate il 30 luglio 2019 ed in vigore da gennaio di quest'anno[4]. È emerso un particolare interesse da parte

[1] Indagine Fintech nel sistema finanziario italiano del 20 dicembre 2019 - https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Allegato_2_Indagine_Fintech.pdf.

[2] Decreto Legislativo 25 maggio 2017, n. 90, in attuazione della Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

[3] Decreto Legislativo 4 ottobre 2019, n. 125, modifiche ed integrazioni al Decreto Legislativo 25 maggio 2017, n. 90 nonché attuazione della Direttiva (UE) 2018/843.

[4] In particolare: disciplinano in maniera analitica la procedura di video-identificazione con caratteristiche di sicurezza idonee a mitigare i rischi connessi all'assenza fisica del cliente; confermano la possibilità di condurre l'adeguata verifica a distanza sulla base di una procedura flessibile, in base alla quale gli

degli intermediari con riferimento specifico alle nuove modalità per l'identificazione a distanza relativamente all'incremento di prodotti e servizi che non richiedono la presenza fisica del cliente. Infatti gli intermediari stanno sviluppando gradualmente e con prudenza nuove modalità per identificare e verificare i dati della clientela a distanza. Dalle risposte fornite, è emerso che si sta procedendo in direzione di un orientamento prevalentemente focalizzato sull'utilizzazione di certificati per la generazione di firma digitale rilasciati da enti accreditati presso l'Agenzia per l'Italia Digitale (AGID). Comunque si rileva un'ampia diffusione della possibilità di firmare a distanza la contrattualistica attraverso firme digitali regolamentate, l'acquisizione del certificato viene generalmente considerato uno strumento ulteriore rispetto alle già previste modalità per la verifica dell'identità senza la presenza fisica del cliente. Una minima parte del campione intervistato ha dichiarato di utilizzare il riconoscimento a distanza che prevede l'iniziale trasmissione da parte del cliente di una propria foto o di un video dove si mostra in possesso di un documento d'identità di cui ha trasmesso copia oppure, nel caso del video, pronuncia una parola suggerita dal sistema; successivamente è prevista la verifica manuale delle informazioni trasmesse.

Dalla ricerca emerge anche che gli intermediari sono orientati strategicamente nello sviluppo di progetti basati su nuove tecnologie tendenti all'utilizzo delle banche dati per ricostruire il profilo di rischio del cliente oltre che per il monitoraggio delle transazioni sempre al fine di migliorare la Customer Due Diligence (CDD). L'indagine ha evidenziato l'esistenza di alcune sperimentazioni che prevedono l'impiego di Big Data e Intelligenza Artificiale (Machine Learning e reti neurali) nelle fasi specifiche di adeguata verifica del cliente e monitoraggio delle transazioni, tendenti all'individuazione automatica di soggetti ad alto rischio e delle operazioni potenzialmente sospette.

Nel quadro regolamentare nazionale, attualmente in vigore, oltre agli orientamenti degli intermediari relativi all'utilizzo di strumenti FinTech nel sistema di identificazione digitale, si innesta la Guidance on Digital Identity[5] pubblicata dal GAFI-FATF, il 6 marzo 2020, al fine di orientare i Governi, i soggetti obbligati e le altre entità interessate (fornitori di servizi di identità digitale) ad un migliore utilizzo dell'identificazione digitale relativamente all'adeguata verifica della clientela ai sensi delle Raccomandazioni GAFI con particolare riferimento alla numero 10[6]. Il GAFI quantifica i pagamenti digitali in una

---

intermediari possono individuare autonomamente i controlli migliori per mitigare tali rischi (riscontri basati su forme di riconoscimento biometrico); consentono agli intermediari di automatizzare alcune fasi dei processi AML/CFT, prevedendo algoritmi per la profilatura del rischio e procedure automatiche per monitorare l'operatività della clientela e individuare le operazioni anomale.

[5] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

[6] Raccomandazione GAFI nr. 10. Adeguata identificazione e verifica del cliente**.**

Deve essere fatto divieto alle istituzioni finanziarie di tenere conti anonimi o conti intestati a nominativi manifestamente fittizi.

Le istituzioni finanziarie devono essere obbligate ad adottare misure di adeguata verifica del cliente allorché:

1. instaurano un rapporto d'affari;

percentuale del 12,7% dell'ammontare globale delle transazioni e stima che, entro la fine del 2022, il 60% del PIL mondiale sarà digitalizzato. A fronte di questo incremento ha ritenuto determinante emanare delle indicazioni per individuare degli standard adeguati che consentano di utilizzare sistemi di identificazione digitale rispondenti ai requisiti AML/CFT. Il GAFI riconosce le potenzialità dell'ID digitale che, se affidabile e sicura, può semplificare l'identificazione dei clienti oltre che facilitare i requisiti di monitoraggio delle transazioni finanziarie minimizzando tra l'altro le possibili carenze nelle procedure di controllo umano. La Guida prende in esame i diversi tipi di tecnologie utilizzate per identificare digitalmente la clientela ed evidenzia come non vi sia attualmente un accordo globale e concordato che delinei degli standards per lo sviluppo e l'applicazione di

---

2. eseguono operazioni occasionali: (i) superiori alla soglia designata applicabile (USD/EUR 15.000); o (ii) sotto forma di bonifico nelle circostanze descritte nella Nota Interpretativa alla Raccomandazione 16;
3. vi è sospetto di riciclaggio di denaro o di finanziamento del terrorismo; o
4. l'istituzione finanziaria ha dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione del cliente.

Il principio secondo cui le istituzioni finanziarie sono tenute agli obblighi di adeguata verifica del cliente deve essere prescritto dalla legge. Ciascun Paese può determinare le modalità di adempimento degli specifici obblighi di adeguata verifica del cliente tramite leggi o atti vincolanti.

Gli adempimenti di adeguata verifica del cliente consistono nelle seguenti attività:

(a) Identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da fonte affidabile e indipendente.

(b) Identificare il titolare effettivo e adottare misure ragionevoli per verificarne l'identità, affinché l'istituzione finanziaria possa essere certa di sapere chi è il titolare effettivo. Per le persone giuridiche e i negozi giuridici di natura fiduciaria, ciò deve implicare che le istituzioni finanziarie conoscano la proprietà e la struttura di controllo del cliente.

(c) Comprendere e, se del caso, ottenere informazioni sullo scopo e sulla natura del rapporto d'affari.

(d) Svolgere un controllo costante del rapporto d'affari ed un'analisi accurata delle transazioni eseguite nel corso dell'intera durata di tale rapporto, al fine di garantire che le transazioni in fase d'esecuzione siano compatibili con le informazioni in possesso dell'istituzione finanziaria circa il proprio cliente, le sue attività e il profilo di rischio, ivi inclusa, ove necessario, l'origine dei fondi.

Le istituzioni finanziarie devono essere obbligate ad osservare ciascuna delle misure di adeguata verifica del cliente di cui alle lettere (a)-(d), ma devono stabilire l'estensione di tali misure sulla base della valutazione del rischio specifico conformemente alle Note Interpretative di questa Raccomandazione e della Raccomandazione 1.

Le istituzioni finanziarie devono essere obbligate a verificare l'identità del cliente e del titolare effettivo prima o al momento dell'instaurazione di rapporti d'affari o 14 dell'esecuzione di transazioni nel caso di clienti occasionali. I Paesi possono autorizzare le istituzioni finanziarie a completare tali verifiche non appena ragionevolmente possibile dal momento dell'instaurazione del rapporto d'affari, sempre che i rischi di riciclaggio di denaro e finanziamento del terrorismo siano efficacemente gestiti e nell'ipotesi che ciò sia essenziale per non interrompere il regolare svolgimento dell'attività.

Ove non sia in grado di adempiere agli obblighi di cui alle summenzionate lettere (a)-(d) (la cui estensione è suscettibile di opportune modifiche in maniera proporzionale al rischio specifico associato), l'istituzione finanziaria deve essere obbligata a: non accendere il conto; non instaurare il rapporto d'affari o non eseguire l'operazione; oppure deve essere obbligata a: porre termine al rapporto d'affari; e valutare la necessità di effettuare una segnalazione di operazione sospetta in relazione al cliente.

Tali obblighi devono essere applicati a tutti i nuovi clienti, sebbene le istituzioni finanziarie debbano altresì applicare questa Raccomandazione ai clienti preesistenti in base alla rilevanza e al rischio, e devono adempiere agli obblighi di adeguata verifica del cliente nell'ambito dei rapporti preesistenti al momento opportuno.

identità digitali. Essa analizza una serie di quadri di garanzia e requisiti tecnici sviluppati in diverse giurisdizioni relativi all'identità, alla sicurezza delle tecnologie informatiche ed alla privacy. In particolare si fa riferimento agli standard normativi di garanzia statunitensi sull'identità digitale dell'US National Institute of Standards and Technology (NIST)[7] e al Regolamento (UE) nr. 910/2014[8]. La Guida precisa che comunque devono essere rispettati i requisiti di identificazione e verifica dell'identità del cliente utilizzando documenti, dati o informazioni "affidabili e indipendenti" (Raccomandazione nr. 10) al fine di poter condurre l'adeguata verifica della clientela sulla base di processi e procedure che forniscano livelli adeguati di fiducia consentendo di produrre risultati accurati al fine di mitigare al massimo i rischi di riciclaggio o finanziamento del terrorismo.

Naturalmente il FATF rileva come i sistemi di identificazione digitale, relativi al controllo dell'identità e/o l'autenticazione del cliente, possano comportare dei rischi soprattutto nel momento in cui venga utilizzata una rete di comunicazione "aperta" (internet) in relazione a potenziali attacchi informatici o a furti di identità. Inoltre, viene evidenziato come un utilizzo distorto di false identità digitali possa consentire, al pari della movimentazione di denaro contante, lo spostamento di fondi senza poter risalire all'effettivo beneficiario economico. L'esempio è quello di organizzazioni criminali che possono acquisire le credenziali di identificazione digitali di soggetti compiacenti che di fatto si trasformerebbero in una sorta di "spalloni digitali". Nell'affrontare i rischi connessi all'uso della ID digitale, la Guida non intende scoraggiarne l'uso, ma lo vincola all'utilizzo di strumenti affidabili, indipendenti e che comunque soddisfino livelli di garanzia adeguati per non consentire di abusare del nuovo veicolo tecnologico.

Accanto a tali pericoli viene rilevato come sistemi d'identificazione digitale sicuri potrebbero facilitare l'identificazione e la verifica del cliente al momento dell'instaurazione del rapporto o della prestazione professionale, supportando la Customer Due Diligence e facilitando le misure di adeguata verifica della clientela, nonché la gestione del rischio e la limitazione di potenziali attività illecite. Il GAFI rappresenta come un robusto sistema di ID digitale possa supportare l'inclusione finanziaria per consentire di ricondurre nel settore finanziario regolamentato tutte quelle persone attualmente escluse da un'ampia gamma di servizi finanziari, consentendo quindi di far confluire nell'ambito del generale ecosistema AML/CFT una vastissima categoria di soggetti che attualmente non ha accesso al circuito delle entità regolamentate. Il FATF quantifica in 1,7 miliardi le persone che nel mondo sono escluse dal circuito degli intermediari e di questi il 26% non ne ha la possibilità proprio per mancanza di adeguata

[7] The NIST 800-63 Digital Identity Guidelines consists of a suite of documents: NIST SP 800- 63-3 Digital Identity Guidelines (Overview); NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing; NIST SP 800-63B Digital Identity Guidelines: Authentication and Life Cycle Management; and NIST SP 800-63C, Digital Identity Guidelines: Federation and Assertions.

[8] Regolamento (UE) nr. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

documentazione che potrebbe essere opportunamente bypassata proprio grazie ad un solido ed affidabile sistema di ID digitale.

La Guida, nella Sezione V, fornisce indicazioni su come applicare un approccio basato sul rischio in relazione all'uso di sistemi di identificazione digitale e di Customer Due Diligence in linea con la Raccomandazione nr. 10 del FATF. L'approccio raccomandato è neutro dal punto di vista tecnologico e cioè gli standard suggeriti non favoriscono nessuna tecnologia o requisiti in particolare per l'utilizzo dell'identità digitale a scopi AML/CFT; l'Organismo Intergovernativo prevede due elementi generali cui fare riferimento: livelli di garanzia delle componenti principali del sistema di identificazione digitale che siano determinati da fonti di informazioni affidabili e indipendenti; sistemi di identificazione che forniscano un livello di affidabilità e indipendenza adeguato rispetto ai rischi di riciclaggio, finanziamento del terrorismo ed altri illeciti finanziari.

La Guida, raccomanda alle Autorità Governative di sviluppare delle linee guida e dei regolamenti che consentano di utilizzare i sistemi di ID digitale utilizzando dotazioni tecnologiche che si adattino ai requisiti già esistenti di adeguata verifica della clientela e Customer Due Diligence oltre a quelli previsti per la conservazione dei dati e delle informazioni. Inoltre le Autorità di controllo dovranno valutare l'impatto degli strumenti di ID digitale rispetto alle normative e all'ecosistema dei regolamenti esistenti anche alla luce della rapidità con cui si evolvono le metodologie di identificazione digitale. Le leggi, i regolamenti e le procedure dovranno consentire alle Autorità di controllo di sviluppare un efficace approccio basato sul rischio che sfrutti i flussi di dati e consenta, tramite una visione "multi-stakeolder", di sfruttare le opportunità e mitigare i potenziali rischi connessi all'identificazione digitale. Il GAFI poi richiama la Raccomandazione nr. 2[9] auspicando la cooperazione e il coordinamento con le Autorità competenti al fine di agevolare un approccio globale e coordinato per garantire la compatibilità dei requisiti AML/CFT ai sistemi di identificazione digitale anche con la protezione dei dati e le regole sulla privacy. Le Autorità di controllo dovranno supportare lo sviluppo e l'implementazione di strutture di ID digitale affidabili ed indipendenti controllandole e certificandole, cercando di armonizzarle sulla base di garanzie che consentano di

[9] Raccomandazione GAFI nr. 2. Cooperazione e coordinamento nazionali.
I Paesi devono disporre di politiche nazionali antiriciclaggio e di contrasto al finanziamento del terrorismo che tengano conto dei rischi individuati e siano periodicamente riviste. I Paesi devono altresì istituire un'autorità, avere un coordinamento o un altro meccanismo similare che si assuma la responsabilità di tali politiche.
I Paesi devono garantire che i responsabili dell'elaborazione di tali politiche, l'Unità d'Informazione Finanziaria (UIF), le forze dell'ordine, le autorità di vigilanza e le altre autorità competenti interessate, sia a livello di elaborazione delle politiche sia a livello operativo, dispongano di meccanismi efficaci che consentano loro di cooperare e, ove necessario, di coordinarsi e scambiarsi informazioni a livello nazionale per lo sviluppo e l'implementazione di politiche e attività volte a contrastare il riciclaggio, il finanziamento del terrorismo e il finanziamento della proliferazione di armi di distruzione di massa.
Ciò deve includere la cooperazione e il coordinamento tra le autorità competenti per assicurare la compatibilità dei requisiti antiriciclaggio e di contrasto al finanziamento del terrorismo con le norme sulla protezione dei dati e la privacy ed altre disposizioni in materia (ad es. sicurezza/localizzazione dei dati).

costituire criteri di identificazione digitale attendibili e indipendenti. Infine è necessario monitorare lo sviluppo della ID digitale per condividere best practices a livello nazionale ed internazionale e promuovere standard sempre più efficienti e funzionali in relazione al contesto AML/CFT.

Il GAFI poi approfondisce le Raccomandazioni indirizzate ai soggetti obbligati che dovranno adottare metodologie tendenti alla Customer Due Diligence che includano: una esatta comprensione dei livelli di garanzia del sistema di ID digitale finalizzati alla verifica e alla autenticazione dell'identità del cliente; assicurare che i livelli di garanzia del sistema siano rispondenti ai rischi AML/CFT associati al cliente, al prodotto, alla giurisdizione e all'area geografica. Le *Reguladed Entities* potranno valutare di adottare un'adeguata verifica della clientela a più livelli sfruttando proprio i sistemi di identificazione digitale magari utilizzando una due diligence semplificata nel caso di basso rischio di riciclaggio o finanziamento del terrorismo. Inoltre, grazie all'infrastruttura tecnologica derivante dall'applicazione dell'identificazione digitale, sarà possibile utilizzare processi di Cyber Security e antifrode per supportare la verifica o l'autenticazione dell'identità del cliente, oltre al controllo delle transazioni nell'ottica di rendere più efficiente l'attività di due diligence anche per monitorare e rilevare eventuali operazioni sospette. Infine è raccomandato ai soggetti obbligati di interagire con le Autorità di controllo per consentire di accedere a tutte le informazioni relative all'ID digitale con l'obiettivo di verificare l'identità del cliente.

Sebbene gli standard della Guida siano applicabili solo ai soggetti obbligati questa dovrà essere un punto di riferimento anche per i fornitori di servizi di identificazione digitale *(Digital ID Service Providers)* proprio perché questi ultimi forniscono i propri sistemi alle entità regolamentate. In tale ottica, è richiesto a detti soggetti di adeguarsi ai requisiti di Customer Due Diligence previsti dalle normative antiriciclaggio al fine di garantire idonei livelli di garanzia per la verifica dell'identità e l'autenticazione del cliente.

Lo sviluppo di applicativi rispondenti alle nuove linee guida dettate dal GAFI si rivelerà una straordinaria opportunità strategica per i soggetti obbligati e, in particolare, per gli intermediari finanziari: i sistemi di identificazione digitale consentiranno di migliorare l'efficienza, l'efficacia, l'affidabilità e la sicurezza, anche in termini di tutela della privacy. In particolare, strumenti affidabili di ID digitali indipendenti offriranno sicuri vantaggi per minimizzare il rischio di "errore umano" ed ottimizzare il funzionamento dei presidi di identificazione e verifica dell'identità del cliente, oltre che per il monitoraggio delle relative movimentazioni finanziarie in un'ottica di rendere sempre più performante la Customer Due Diligence e la compliance antiriciclaggio nel suo complesso.