CONSIGLIO NAZIONALE DEL NOTARIATO

COMMISSIONE ANTIRICICLAGGIO

STUDIO 2_2020 B

L'IDENTIFICAZIONE NON IN PRESENZA FISICA NEL CONTRASTO AL RICICLAGGIO ED AL TERRORISMO INTERNAZIONALE

di Gea Arcella, Laura Piffaretti e Michele Manente

Approvato dalla Commissione Antiriciclaggio il 22.05.2020
Approvato dal Consiglio Nazionale del Notariato il 26.06.2020

ABSTRACT

Il presente studio prende le mosse da un attento esame della Guida all'identità digitale, emanata dal GAFI, nello scorso mese di marzo 2020. L'esigenza dell'emanazione della Guida nasce dal particolare momento storico caratterizzato dalla necessità del distanziamento sociale volto a contenere l'epidemia scatenata dal virus Sars-CoV-2; tale distanziamento ha condotto ad un utilizzo massivo di strumenti di colloquio a distanza, causando anche la possibilità di frodi o di utilizzo improprio di detti strumenti. In questo contesto la Guida ha inteso fornire proprio un orientamento sull'utilizzo di forme di identificazione digitale, secondo criteri di sicurezza e rispetto della protezione dei dati personali, al fine di eseguire transazioni finanziarie o di altro tipo senza la necessaria compresenza degli interessati (cliente e soggetto obbligato). Nell'esame della Guida, tra le altre cose, si precisa che per stabilire se l'uso di un sistema di identificazione digitale sia coerente con la Raccomandazione 10, i governi, gli istituti finanziari e le altre parti interessate sono tenuti a svolgere valutazioni circa i livelli di garanzia forniti dal sistema di identificazione digitale in base alla sua tecnologia, architettura e governance per determinarne l'affidabilità/indipendenza nonché, sulla base dei predetti livelli di garanzia, a stabilire - con un approccio basato sul rischio - se il sistema di identificazione digitale è adeguatamente affidabile, alla luce dei potenziali rischi di riciclaggio del denaro, frode e altri finanziamenti illeciti, tenendo comunque conto che i sistemi di identificazione digitale possono presentare un livello standard di rischio e possono persino essere a rischio più basso se vengono implementati livelli di garanzia più elevati e/o appropriate misure di controllo del rischio antiriciclaggio.

Lo studio prosegue con un cenno al concetto di identificazione, nella sua più ampia accezione e nelle declinazioni che storicamente ha assunto in ambito giuridico, e quello di identificazione digitale, con la precisazione che, recentemente, l'accezione "ID digitale" è passata ad indicare l'uso della tecnologia per affermare e dimostrare la propria identità personale, così come essa risulta dai dati anagrafici pubblici relativi al soggetto interessato, avente la stessa valenza identificativa di un documento di identità tradizionale.
Viene, quindi, esaminata la legislazione italiana antiriciclaggio sull'identificazione senza la presenza fisica, analizzando, in primis, le differenze che intercorrono tra l'identificazione

prevista dalla legislazione notarile e quella della normativa speciale. In particolare all'art. 19, comma 1, lett. a), del D.Lgs. n. 231/2007 vengono disciplinate alcune ipotesi in cui sia possibile svolgere l'identificazione non in presenza del cliente. Essa può essere effettuata sulla base di numerosi presupposti (di tipo documentale, di tipo informatico, conoscenza pregressa) che, nell'ambito dello studio, sono oggetto di una puntuale trattazione.

Attraverso una ricostruzione sistematica delle disposizioni sul punto, si passa poi ad analizzare nel dettaglio l'identificazione a fini antiriciclaggio non in presenza fisica del cliente anche nell'ipotesi in cui esso agisca a mezzo di un esecutore.
Vengono quindi illustrate le possibili modalità di interazione tra il cliente e un operatore che, collegato da remoto, supervisioni l'identificazione e verifica del cliente; si richiama e si illustra, in particolare, come sia possibile ottemperare alle operazioni di adeguata verifica del cliente, che, come noto, non si esaurisce nella sua mera identificazione, anche quando questi non sia fisicamente presente presso il notaio.

Nello studio, infine, si affrontano i profili relativi alla sottoscrizione delle eventuali dichiarazioni rese dal cliente, ai sensi dell'art. 22 del D.Lgs. n. 231/2007, senza la sua presenza fisica anche utilizzando modalità di firma elettronica, purché queste ultime assicurino l'integrazione del requisito della forma scritta in base alla normativa vigente.

A - <u>Il documento GAFI</u>[1]

L'attuale momento storico caratterizzato dalla necessità di un distanziamento sociale, al fine di contenere l'epidemia scatenata dal virus Sars-CoV-2, ha portato ad un utilizzo massivo di strumenti di colloquio a distanza che, se correttamente utilizzati, consentono di agevolare l'esecuzione di molte operazioni senza ricorrere alla presenza fisica e quindi contribuendo alla sicurezza sanitaria sia degli operatori che degli utenti.
Crescono, d'altronde, anche le possibilità di frodi o di utilizzo improprio di detti strumenti pertanto il GAFI con la sua Guida all'identità digitale[2] ha inteso fornire una bussola circa l'utilizzo proprio di queste forme di identificazione digitale, secondo criteri di sicurezza e rispetto della protezione dei dati personali, al fine di eseguire transazioni finanziarie o di altro

1 La Task Force di azione finanziaria (antiriciclaggio), o Financial action task force - FAFT- , nota anche con il nome francese Groupe d'action financière (GAFI), è un'organizzazione intergovernativa fondata nel 1989 su iniziativa del G7 con lo scopo di ideare e promuovere strategie di contrasto al riciclaggio dei capitali di origine illecita e, dal 2001, anche di prevenzione del finanziamento al terrorismo. Nel 2008, il mandato del GAFI è stato esteso anche al contrasto del finanziamento della proliferazione di armi di distruzione di massa.
Gli obiettivi del GAFI sono stabilire standard e promuovere un'efficace attuazione delle misure legali, regolamentari e operative per combattere il riciclaggio di denaro, il finanziamento del terrorismo e altre minacce connesse all'integrità del sistema finanziario internazionale. Pertanto il GAFI elabora raccomandazioni riconosciute a livello internazionale per il contrasto delle attività finanziarie illecite, analizza le tecniche e l'evoluzione di questi fenomeni, valuta e monitora i sistemi nazionali. Individua, inoltre, i Paesi con lacune strategiche nei loro sistemi di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, così da fornire al settore finanziario elementi utili per le analisi del rischio da esso condotte.
Del GAFI fanno parte 37 membri in rappresentanza di stati e organizzazioni regionali, nonché, come osservatori, rilevanti organismi finanziari internazionali e del settore (tra i quali Nazioni Unite, Fondo monetario internazionale, Banca mondiale, Banca Centrale Europea, Europol, Egmont).

2 Il GAFI, prendendo le mosse dall'attuale situazione di emergenza epidemiologica da COVID-19, nel mese di marzo 2020, ha elaborato una Guida all'identità digitale, volta ad agevolare l'individuazione e l'utilizzo delle più moderne ed evolute forme di identificazione, comprese quelle digitali. Consultabile al seguente link https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html e pubblicata con una breve nota di presentazione di M.C. Cignarella nel CNN Notizie del 28 aprile 2020, n. 80.

tipo senza la necessaria compresenza degli interessati (cliente e soggetto obbligato); infatti, l'identificazione del cliente e le transazioni c.d. "non faccia a faccia" basate su sistemi di identificazione digitale affidabili, indipendenti e che mettano in atto adeguate misure di mitigazione del rischio di riciclaggio, possono presentare un livello di tale rischio standard o, persino, più basso che nelle normali operazioni svolte in presenza.
L'obiettivo delle indicazioni contenute nella Guida è quello di rendere più facile l'erogazione del credito predisposto dagli Stati in occasione della pandemia, senza rinunciare ai presidi antiriciclaggio, ma anche di aumentare la c.d. "inclusione finanziaria" per tutta quella platea di soggetti che non ha accesso ai servizi bancari e finanziari ordinari poiché priva di documenti di identità tradizionali e che, invece, – proprio grazie alle nuove tecniche di identificazione digitale – potrebbe essere identificata con la medesima affidabilità, prescindendo da riscontri documentali non sempre possibili.

Il GAFI utilizza i termini, "faccia a faccia" e "non faccia a faccia" per classificare le relazioni d'affari (incluso l'*onboarding, id est* l'assunzione dell'incarico) e le transazioni economiche in generale. Ai fini della Guida GAFI, si considerano interazioni "faccia a faccia" quelle che si svolgono "di persona", da intendersi nel senso che le parti dell'interazione/transazione si trovano nella stessa collocazione fisica e conducono le loro attività attraverso un'interazione in presenza. Per interazioni "non faccia a faccia" sono, invece, intese quelle che avvengono a distanza, da intendersi nel senso che le parti non si trovano nella stessa posizione fisica e svolgono attività con mezzi digitali o altri strumenti remoti, come la posta o il telefono.
Nella Guida in esame, si osserva che la nota interpretativa della raccomandazione 10 del GAFI include i "rapporti o transazioni commerciali non faccia a faccia" tra gli esempi di una situazione potenzialmente a rischio più elevato nella *due diligence* del cliente. Tuttavia ciò non significa che le autorità competenti e le entità regolamentate, ovvero - secondo le definizioni adottate dal legislatore italiano - i soggetti obbligati, debbano classificare sempre i rapporti commerciali o le transazioni finanziarie "non faccia a faccia" come a rischio più elevato ai fini antiriciclaggio[3].
La Guida stessa, infatti, precisa che "*data l'evoluzione della tecnologia, (...), è importante chiarire che le identificazioni e le transazioni dei clienti svolte 'non faccia a faccia' che si basano su affidabili ed indipendenti sistemi di identificazione digitale, dotati di adeguate misure di mitigazione del rischio, possono presentare un livello standard di rischio e possono persino essere a rischio più basso se vengono implementati livelli di garanzia più elevati e/o appropriate misure di controllo del rischio antiriciclaggio (...).*"[4]

Ed ancora osserva che "*i sistemi di identificazione digitale possono consentire l'identificazione/verifica da remoto dei clienti e supportare transazioni finanziarie remote con livelli di rischio standard o persino bassi. Gli standard tecnici consentono la verifica e l'attribuzione a distanza dell'identità, anche a livelli di garanzia più elevati*"[5].

Per determinare se l'uso di un sistema di identificazione digitale sia coerente con i requisiti della Raccomandazione 10, i governi, gli istituti finanziari e le altre parti interessate vengono esortati dal GAFI a condurre le seguenti valutazioni:

3 Così testualmente nella Guida all'identità digitale del GAFI, marzo 2020, pag. 30

4 GAFI, Guida all'identità digitale, marzo 2020, pag. 30

5 GAFI, Guida all'identità digitale, marzo 2020, pag. 57

A. Comprendere i livelli di garanzia forniti dal sistema di identificazione digitale in base alla sua tecnologia, architettura e governance per determinarne l'affidabilità/indipendenza; e
B. Sulla base dei predetti livelli di garanzia, stabilire - con un approccio basato sul rischio - se il sistema di identificazione digitale è adeguatamente affidabile, alla luce dei potenziali rischi di riciclaggio del denaro, frode e altri finanziamenti illeciti.

Nella Guida GAFI viene fatto riferimento a diverse tecnologie e sistemi impiegati in tutto il mondo come strumenti di identificazione digitale. Questi sistemi possono usare le tecnologie digitali in vari modi, a titolo esemplificativo, ma non esaustivo:

- Database elettronici, inclusi registri distribuiti, per ottenere, confermare, archiviare e/o gestire le prove dell'identità.
- Credenziali digitali per autenticare l'identità per l'accesso a dispositivi mobili, applicazioni online e offline.
- Interfacce per programmi applicativi digitali (API), piattaforme e protocolli che facilitano identificazione / verifica online e autenticazione dell'identità.
- Biometria per aiutare a identificare e / o autenticare le persone.

I casi di studio indicati nell'Appendice B della Guida, inoltre, forniscono un esempio di alcuni dei sistemi esistenti in India, Perù e Nigeria, in Svezia, Singapore ed Estonia.
Nell'Appendice E[6], inoltre, si fa una panoramica sui livelli di garanzia digitale e sugli standard tecnici adottati negli Stati Uniti ed nell'Unione Europea.
In particolare nelle NIST (National Institute of Standards and Technology) Digital ID Standards, il concetto di verifica dell'identità "di persona" include le c.d. interazioni remote "supervisionate" con il richiedente, esattamente al pari delle interazioni in cui il richiedente e il fornitore di servizi di identità sono fisicamente presenti nella stessa posizione.

Secondo tali standard statunitensi, il controllo ed il rilascio di identità "di persona" possono essere effettuati da:

* un'interazione fisica con il richiedente, supervisionata da un operatore; o
* un'interazione remota con il richiedente, sotto la supervisione di un operatore, basata su requisiti specifici per il controllo dell'identità personale in remoto, che raggiunga livelli comparabili di affidabilità e sicurezza rispetto al controllo tramite interazione fisica.

Per entrambi i tipi di accertamento di identità in persona, le norme tecniche richiedono che:

1) l'operatore debba ispezionare almeno una fonte biometrica (ad esempio impronte, volto) (...);

2) l'operatore raccolga tale fonte con modalità tali da garantire che essa sia raccolta direttamente dal richiedente e non da un altro soggetto e che vengano rispettati tutti i requisiti dell'evidenza biometrica stabiliti nelle norme.

Per stabilire poi l'equiparabilità tra una verifica e attribuzione di una identità effettuata in remoto sotto la supervisione di un operatore e l'analoga operazione effettuata in presenza fisica, devono essere soddisfatti i seguenti requisiti (...),

il Provider deve:

6 GAFI, Guida all'identità digitale, marzo 2020, pag. 93 e ss.

* monitorare l'intera sessione di verifica dell'identità (ad es. mediante una trasmissione video ad alta risoluzione continua del richiedente);
* far partecipare un operatore dal vivo, connesso a distanza con il richiedente per l'intera sessione di verifica d'identità. Gli operatori devono aver svolto un programma di formazione per essere in grado di rilevare potenziali frodi e per eseguire correttamente una sessione di prove virtuali;
* far eseguire tutte le verifiche digitali possibili (ad es. tramite chip o tecnologie wireless) mediante scanner e sensori integrati;[7]
* assicurarsi che tutte le comunicazioni avvengano su un canale protetto, reciprocamente autenticato;
* approntare sistemi di rilevamento di possibili manomissioni fisiche ai sistemi, approntati sulla base delle caratteristiche del luogo ove si svolge la verifica dell'identità (ad esempio, un chiosco situato in un'area riservata o monitorato da un individuo di fiducia richiede un rilevamento di manomissione fisico inferiore rispetto a uno situato in un'area semi-pubblica, ad esempio l'atrio di un centro commerciale).

Il richiedente deve rimanere continuamente (non può discostarsi) all'interno della sessione monitorata di verifica dell'identità e tutte le azioni intraprese dal richiedente durante la sessione di verifica dell'identità devono essere chiaramente visibili all'operatore remoto.[8]

B - Cenni sull'identificazione e sull'identità digitale

Non è questa la sede per svolgere un'analisi completa ed esaustiva sul tema dell'identità personale e su quanto attualmente si intenda per identità digitale, non di meno vanno premessi alcuni cenni su tali concetti per meglio comprendere le osservazioni che verranno svolte in tema di identificazione a distanza nell'ambito della normativa contro il riciclaggio ed il finanziamento del terrorismo.
L'identità personale è una formula che, in ambito giuridico, assume più valenze semantiche[9]. Tralasciando in questo scritto il tema amplissimo ed affascinante del diritto all'identità personale, frutto dell'elaborazione della dottrina e della giurisprudenza più recente sulla scorta dei testi normativi dedicati alla protezione dei dati personali, ed identificato come il *"diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo"*[10], l'accezione più diffusa di identità personale designa il *"complesso delle risultanze anagrafiche, che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati*"[11]. Tali risultanze normalmente confluisco in un documento di identità il cui rilascio

7 Ad esempio come i lettori NFC, acronimo che sta per Near field communication.

8 Si fa presente che le attuali procedure da remoto autorizzate dall'AgiID per il rilascio di certificati qualificati associati alle firme qualificate (*id est* firme digitali) da parte dei Certificatori Qualificati ricalcano esattamente gli standard americani sopra descritti.

9 Sul punto si vedano le riflessioni svolte da G. Renna, Identità personale ed identità digitale, in IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA, Anno XXIII Fasc. 3 – 2007, Milano Giuffré Editore.

10 Così definisce il diritto all'identità personale la sentenza di Corte Costituzionale 3 febbraio 1994, n. 13, in Foro it., 1994, I, 1668.

11 Così G. Renna cit. il quale cita a sua volta G. FALCO, voce Identità personale, in Nuovo dig. it., VI, Torino, 1938, pag. 649: *«La identità personale è costituita dallo insieme dei caratteri (connotati e contrassegni personali) e dal nome*

è, in Italia, una prerogativa statale o comunque affidata a soggetti pubblici[12] o vigilati. In questo senso l'espressione "identità personale" compare in diversi testi normativi, tra cui la stessa legge notarile[13] e il R.D. 773/1931 in tema di pubblica sicurezza[14], va comunque precisato che se il mero possesso del documento di identità non sempre esaurisce il complesso procedimento attraverso il quale viene accertata l'identità di un soggetto; l'accertamento dell'identità, infatti, può essere visto come la risultante di un processo di identificazione e autenticazione soggettiva, da parte del pubblico ufficiale che si trova ad attestarla e a farsene garante, basato su una serie di circostanze sia fattuali che documentali.

Rispetto al concetto classico di identità personale, l'evoluzione in materia ha portato ad un riconoscimento più ampio dell'identità che, inizialmente limitata all'identificazione anagrafica ed alla sua valenza pubblicistica, si è poi estesa a ricomprendere altre manifestazioni della personalità ben delineate dal passaggio della sentenza della Corte Costituzionale citata, in ambito digitale, invece, il processo è stato per certi versi inverso[15]. Inizialmente l'espressione "identità digitale" non ricorreva in alcuna disposizione normativa, ma veniva utilizzata – sempre in ambito giuridico - come sinonimo di identità "in rete" o "virtuale", per lo più collegandola ad alcune espressioni della personalità (come ad esempio agli account social), al fine, essenzialmente, di poter approntare una tutela reputazionale della persona anche in ambito virtuale[16]. Poiché l'utilizzo di una risorsa informatica presuppone quasi sempre un sistema di riconoscimento dell'utente affinché questi vi possa accedere, in un'altra e più tecnica accezione l'identità digitale è stata definita come "l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore", collegando in tal modo le modalità di autenticazione informatica[17] all'identificazione a mezzo di strumenti informatici del soggetto utilizzatore.

Più recentemente, l'accezione "ID digitale" è passata ad indicare l'uso della tecnologia per affermare e dimostrare la propria identità personale[18], così come essa risulta dai dati anagrafici pubblici relativi al soggetto interessato, avente la stessa valenza identificativa di un documento di identità tradizionale.

(generalità). I documenti di identità contengono i caratteri e il nome. Fissare in un documento caratteri e nome di una persona vuol dire fissare la identità».

12 Si ricorda che anche i notai, nell'esercizio della loro funzione pubblica, possono rilasciare fotografie autenticate in cui l'effige del richiedente viene collegata a determinate risultanze anagrafiche, di cui il pubblico ufficiale si fa garante.

13 V. l'art. 49 della Legge n.89/1913: «Il notaio deve essere certo dell'identità personale delle parti e può raggiungere tale certezza, anche al momento dell'attestazione, valutando tutti gli elementi atti a formare il suo convincimento».

14 Cfr. art. 144 R.D. cit.: "L'autorità di pubblica sicurezza ha facoltà di invitare, in ogni tempo, lo straniero ad esibire i documenti di identificazione di cui è provvisto, e a dare contezza di sé. Qualora vi sia motivo di dubitare della identità personale dello straniero, questi può essere sottoposto a rilievi segnaletici".

15 Per una disamina divulgativa sul concetto di identità digitale cfr. M. Nastri, *L'evoluzione digitale del notaio e la sicurezza giuridica in rete*, 2020, Formato Kindle, cap.11, pag. 107 e ss..

16 In questa accezione veniva tutelata anche la possibilità di utilizzare pseudonimi o in generale di creare una proiezione del sé non collegata ai propri dati anagrafici, ma anzi volutamente diversa da quella reale (cfr. G. Renna, cit.).

17 Tradizionalmente gli strumenti di autenticazione informatica vengono classificati secondo la seguente tripartizione:
1. qualcosa che sai: parola chiave (password);
2. qualcosa che sei: caratteristiche biometriche (iride, impronta digitale, impronta vocale, riconoscimento del volto, ecc.);
3. qualcosa che hai: un particolare oggetto (tessera magnetica, smart card, ecc.).

Attualmente l'autenticazione elettronica è definita dal Regolamento UE 910/2014 come: "un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica".

18 La Guida GAFI in commento così definisce l'ID digitale.

Se guardiamo ai testi normativi attuali, nel Regolamento UE 910/2014 - c.d. Regolamento eIDAS- non viene definita l'identità digitale quanto piuttosto il risultato del suo utilizzo, in quanto l'art. 3, n. 1, indica come *«identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica*, mentre nel considerando n. 16 si chiarisce che: *"...i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata"*.
La nostra legislazione nazionale, invece, nel D. Lgs. 82/2005 o CAD all'art. 1, comma 1, lett u-quater) definisce esplicitamente il concetto di identità digitale come: "*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64".*
Sia la legislazione di matrice comunitaria che quella interna conoscono diversi livelli di sicurezza nell'identificazione elettronica e nell'attribuzione dell'identità digitale, tanto che, come vedremo, la legislazione Antiriciclaggio (AR) vigente consente l'utilizzo solo di alcuni di questi strumenti, in particolare di quelli che assicurano il più elevato livello di sicurezza possibile.

C - La legislazione italiana sull'identificazione a distanza in ambito AR

Preliminarmente non è inutile sottolineare che l'identificazione prevista dalla legislazione antiriciclaggio è profondamente diversa da quella notarile: abbiamo visto nel paragrafo precedente come l'accertamento dell'identità disciplinato dalla legge notarile è un complesso ed articolato procedimento che conduce il pubblico ufficiale a maturare una specifica convinzione circa l'identità di un soggetto, facendosene garante nei confronti dell'ordinamento mediante una attestazione fidefaciente; diversamente, a fini antiriciclaggio, ciò che rileva è un mero accertamento documentale, basato sull'acquisizione dei dati identificativi indicati dall'art.1, comma 2, lett. n) D. Lgs. 231/2007[19], che può essere svolto, per altro, a mezzo dei propri dipendenti e/o collaboratori (v. art. 19, lett. a, D. Lgs. 231 cit.).
Nel sistema AR tale forma di identificazione del cliente è operazione sempre dovuta (ad es. anche per la mera consulenza[20]) e preliminare all'accettazione dell'incarico[21], mentre l'accertamento dell'identità personale notarile è finalizzata al ricevimento dell'atto; quest'ultima, inoltre, essendo temporalmente successiva all'identificazione AR, può

19 Decreto Legislativo n.231/2007, così come modificato dal Decreto Legislativo n.90/2017 (Decreto di Recepimento della IV Direttiva UE), che ne ha completamente sostituito l'articolato e, da ultimo, dal Decreto Legislativo n.125/2019 (Decreto di recepimento della V Direttiva UE).

20 Cfr art. 18, comma 4 D. Lgs. 231 cit.: "*Fermi gli obblighi di identificazione, i professionisti, limitatamente ai casi in cui esaminano la posizione giuridica del loro cliente o espletano compiti di difesa o di rappresentanza del cliente in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, sono esonerati dall'obbligo di verifica dell'identità del cliente e del titolare effettivo fino al momento del conferimento dell'incarico".*

21 Cfr. Art. 18, comma 2 D. Lgs. 231 cit.. Si precisa che ai sensi dell'art. 18, comma 3 infra citato alla nota 30: "*In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo può essere posticipata ad un momento successivo all'instaurazione del rapporto o al conferimento dell'incarico per lo svolgimento di una prestazione professionale, qualora ciò sia necessario a consentire l'ordinaria gestione dell'attività oggetto del rapporto ...omissis"* previsione da coordinare con il disposto della Regola Tecnica n. 8 .

eventualmente sanare qualche insufficiente acquisizione documentale verificatasi durante la fase istruttoria.
La diversità di presupposti su cui si basano le due forme di identificazione comporta, poi, delle evidenti aporie: si faccia l'esempio di una prestazione notarile richiesta da un soggetto, noto ed identificato da tempo da parte del notaio per conoscenza personale, che o sia privo di un documento di identità o semplicemente abbia un documento scaduto. In questa situazione nessun problema può porsi ai fini dell'accertamento dell'identità personale notarile; nondimeno ai sensi delle norme del D. Lgs. 231 citate il soggetto obbligato dovrebbe rifiutare la prestazione o peggio ancora procedere ad eseguire una Segnalazione di Operazione Sospetta; onde porre rimedio a questo difetto di coordinamento tra le due normative è stata emanata la Regola Tecnica n. 7, approvata dal CNN nelle sedute del 27 luglio 2017 e 27 ottobre 2017 e munita di parere favorevole del CSF al cui contenuto qui si rimanda. Resta il fatto che in alcuni atti – considerati senza parti per la legge notarile[22] – la presenza di un richiedente della prestazione professionale e quindi di un cliente, comporta comunque lo svolgimento di tutte le attività di identificazione dello stesso dovute dalla normativa antiriciclaggio sopra richiamata.
Inoltre, in presenza di un esecutore (*id est* di un procuratore), l'identificazione notarile è dovuta solo ed esclusivamente nei suoi confronti in quanto comparente all'atto, mentre quella richiesta dalla normativa AR si estende ai soggetti rappresentati, fisici o non fisici che siano, secondo le specifiche regole dell'identificazione in presenza o a distanza dettate dall'art. 19, D. Lgs. 231 cit. che si sta esaminando.
L'attuale legislazione italiana in materia di antiriciclaggio ha, infatti, già previsto alcune ipotesi in cui sia possibile svolgere l'identificazione non in presenza del cliente; se ne occupa l'art. 19, comma 1, lett. a) cit., che testualmente recita:
"(...) L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, nei seguenti casi:
1) per i clienti i cui dati identificativi risultino da atti pubblici, da scritture private autenticate o da certificati qualificati utilizzati per la generazione di una firma digitale associata a documenti informatici, ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82;
2) per i clienti in possesso di un'identità digitale, di livello massimo di sicurezza, nell'ambito del Sistema di cui all'articolo 64 del predetto decreto legislativo n. 82 del 2005 e successive modificazioni, e della relativa normativa regolamentare di attuazione, nonché di un'identità digitale di livello massimo di sicurezza o di un certificato per la generazione di firma digitale, rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014 o identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale;
3) per i clienti i cui dati identificativi risultino da dichiarazione della rappresentanza e dell'autorità consolare italiana, come indicata nell'articolo 6 del decreto legislativo 26 maggio 1997, n. 153;
4) per i clienti che siano già stati identificati dal soggetto obbligato in relazione ad un altro rapporto o prestazione professionale in essere, purché le informazioni esistenti siano aggiornate e adeguate rispetto allo specifico profilo di rischio del cliente;
5) per i clienti i cui dati identificativi siano acquisiti attraverso idonee forme e modalità, individuate dalle Autorità di vigilanza di settore, nell'esercizio delle attribuzioni di cui

22 Si pensi, ad esempio, a talune forme di verbali (come quelli di aggiudicazione nell'ambito di procedure di dismissioni o societari), sottoscritti dal solo notaio relativamente ai quali gli accertamenti e le menzioni sull'identità personale previsti dalla legge notarile sono attualmente oggetto di discussione.

all'articolo 7, comma 1, lettera a), tenendo conto dell'evoluzione delle tecniche di identificazione a distanza;".
Nonostante la possibilità della non presenza fisica del cliente al momento dell'identificazione sia stata prevista, seppure con una diversa formulazione, sin dal testo originario del D. Lgs. n.231 cit.[23], è solo ultimamente che tali prescrizioni sono diventate di particolare attualità, sia per lo sviluppo tecnologico che ha investito il campo dell'identità digitale, che per le già ricordate misure di distanziamento sociale conseguenti alla pandemia di Covid-19.

Da questo punto di vista, l'attuale dettato normativo già rispecchia molte delle raccomandazioni presenti nella Guida GAFI per le Autorità Governative in quanto, relativamente all'ID digitale, identifica compiutamente una serie di strumenti tecnologici, affidabili ed indipendenti, idonei ad attestare l'identità di un soggetto anche in ambito digitale.

D - Gli strumenti di identificazione a distanza

In termini generali, dalla norma in commento si può evincere che l'identificazione a distanza può essere effettuata in presenza di numerosi presupposti, non tutti necessariamente legati all'informatica, vediamoli nel dettaglio.

Presupposti di tipo documentale

1. atti pubblici o scritture private autenticate;
2. documenti informatici firmati con firma qualificata/digitale;
3. dichiarazioni della rappresentanza e dell'autorità consolare italiana.

Ogni qual volta i dati identificativi risultino da atti notarili, scritture private firmate digitalmente o dichiarazioni dell'Autorità consolare, i predetti dati risultano validati e si può effettuare una identificazione senza la presenza fisica del cliente; questa modalità risulterà particolarmente utile quando, dovendo identificare entrambe le parti di una qualsiasi compravendita, i dati del venditore, che più difficilmente si reca personalmente presso lo studio del notaio prima della stipula, siano ricavabili dall'atto di provenienza di matrice notarile, oppure qualora una delle parti si avvalga di un esecutore e pertanto i dati del "cliente" (parte sostanziale dell'atto) risultino da un procura notarile o consolare. Anche la produzione di un precedente documento informatico firmato digitalmente può utilmente essere utilizzato a questi fini: si faccia l'esempio di una precedente cessione di quote di srl perfezionata senza l'intervento notarile, ma con la sottoscrizione digitale ex art. 24 D. Lgs. 82/2005 (o *CAD*).

Presupposti di tipo informatico

23 V. l'art. 28, comma 3 del testo originario del D. Lgs. 231 cit.: *"Gli obblighi di identificazione e adeguata verifica della clientela si considerano comunque assolti, anche senza la presenza fisica del cliente, nei seguenti casi: a) qualora il cliente sia già identificato in relazione a un rapporto in essere, purché le informazioni esistenti siano aggiornate; b) per le operazioni effettuate con sistemi di cassa continua o di sportelli automatici, per corrispondenza o attraverso soggetti che svolgono attività di trasporto di valori o mediante carte di pagamento; tali operazioni sono imputate al soggetto titolare del rapporto al quale ineriscono; c) per i clienti i cui dati identificativi e le altre informazioni da acquisire risultino da atti pubblici, da scritture private autenticate o da certificati qualificati utilizzati per la generazione di una firma digitale associata a documenti informatici ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82; d) per i clienti i cui dati identificativi e le altre informazioni da acquisire risultino da dichiarazione della rappresentanza e dell'autorità consolare italiana, così come indicata nell'articolo 6 del decreto legislativo 26 maggio 1997, n. 153."*

La legge indica quattro diverse possibilità:

1. identità digitale ex art. 64 CAD, ovvero lo SPID di massimo livello (c.d. livello 3, che richiede un token fisico – smart card, chiavetta usb ecc.- per attestare l'identità digitale)[24];
2. identità digitale di massima sicurezza rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014, ad es. la CIE[25] o il passaporto elettronico;
3. certificato qualificato associato ad una firma elettronica qualificata (firma digitale) emesso da Autorità di Certificazione Qualificate a norma dell'articolo 9 del regolamento UE n. 910/2014;
4. procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale[26].

Con particolare riferimento alla CIE si ricorda che essa è stata notificata alla Commissione Europea e agli altri Stati membri secondo la procedura di cui all'art. 9 del Regolamento 910 cit.

24 Per quanto concerne il cd. SPID di terzo livello attualmente (https://forum.italia.it/t/spid-terzo-livello/9432/7) esistono alcune limitate applicazioni (ad es. https://www.regione.toscana.it/con-credenziali-spid) per altro ancora in via sperimentale. Il sistema, nonostante sia normativamente previsto, risulta implementato solo da due gestori - Poste e Aruba - che lo rilasciano secondo le istruzioni rinvenibili a questo link: https://www.spid.gov.it/richiedi-spid;

25 La Carta d'Identità Elettronica (o CIE) è l'evoluzione della carta di identità in versione cartacea. Ha le dimensioni di un bancomat ed è costituita da: un supporto di materiale plastico in policarbonato, su cui sono stampati a laser la foto e i dati del cittadino, protetti con elementi e tecniche di anticontraffazione, come ologrammi e inchiostri speciali; un microchip contactless che contiene: i dati personali, la foto e le impronte del titolare, protetti da meccanismi che ne prevengono la contraffazione e la lettura impropria; le informazioni per consentire l'autenticazione in rete da parte del cittadino a servizi erogati in rete da pubbliche amministrazioni e imprese; ulteriori dati per la fruizione di servizi a valore aggiunto, in Italia e in Europa. Su ciascuna CIE è riportato un numero di serie stampato sul fronte in alto a destra ed avente il seguente formato: 2 lettere – 5 numeri – 2 lettere (ad esempio CA00000AA). Tale numero è il Numero Unico Nazionale. I dati stampati sul documento o memorizzati all'interno del microchip sono:

Comune emettitore
Nome
Cognome
Luogo e data di nascita
Sesso
Statura
Cittadinanza
Immagine della firma del titolare
Validità per l'espatrio
Fotografia
Immagini di 2 impronte digitali (un dito della mano destra e un dito della mano sinistra)
Nome e cognome del padre e della madre (nel caso di un minore)
Codice fiscale nei formati alfanumerico e codice a barre
Estremi dell'atto di nascita
Indirizzo di residenza
Comune di iscrizione AIRE (per i cittadini residenti all'estero);

essa è leggibile con i tutti i lettori contactless o con la maggior parte dei tablet/smartphone dotati di interfaccia NFC.

26 In questa previsione normativa dovrebbero rientrare altri strumenti di identificazione on line come ad es. la Carta Nazionale dei Servizi, in particolare quella rilasciata dalla Regioni e nata dall'integrazione della TS – Tessera sanitaria con il codice fiscale. In generale la CNS è uno strumento che permette di identificare con certezza il cittadino online ed accedere ai servizi messi a disposizione dalla pubblica amministrazione in internet. Si tratta di una chiavetta USB oppure di una smart card, dotata di microchip e anche di tecnologia contactless, che consente di identificare l'utente attraverso i dati in esso contenuti. Nel caso della smart card rilasciata dalle Regioni, essa sostituisce ed elimina la tessera sanitaria e il tesserino del codice fiscale: infatti dal 2011 la CNS/TS viene inviata direttamente dal MEF – Ministero dell'economia e delle finanze -, ne sono destinatari i cittadini che godono dell'assistenza del Servizio sanitario nazionale (o SSN) ed attualmente è valida per sei anni. Inizialmente la tessera sanitaria non era dotata di microchip, ma dopo l'integrazione con la CNS esso è stato inserito e tramite apposito lettore, essa ora consente di utilizzare i servizi online della pubblica amministrazione.

e con la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea C 309 del 13 settembre 2019 è divenuta pienamente operativa come strumento per attestare l'identità digitale di massima sicurezza in tutti gli Stati dell'Unione Europea, infatti è stata integrata con il nodo eIDAS, in conformità con l'omonimo Regolamento (UE) n. 910 cit.[27].
Tutti i mezzi di identificazione elettronica sopra elencati, se letti e memorizzati con gli strumenti informatici adeguati, consentono di conservare anche gli elementi di autenticità informatica di cui sono dotati: ad esempio un certificato qualificato associato ad una firma digitale contiene tutte le informazioni circa la CA Qualificata che lo ha rilasciato e le chiavi di sottoscrizione delle CA medesima, a riprova della sua autenticità e della sua mancata contraffazione; così come per la CIE ed il passaporto elettronico la memorizzazione informatica, tramite ad es. un lettore NFC, dei dati anagrafici in essi contenuti, va di pari passo con la memorizzazione degli ulteriori elementi di sicurezza associati ai predetti documenti che ne comprovano l'autenticità e non falsificazione, con un risultato in termini di affidabilità e sicurezza assolutamente non paragonabile alla loro mera fotocopiatura.
La possibilità di leggere l'ID digitale nel formato nativo in cui è stata generata è tanto più essenziale tenuto conto che, se l'obbligo principale è quello dell'identificazione, la legislazione AR richiede in talune ipotesi anche la verifica dell'identità del cliente, dell'esecutore e dell'eventuale titolare effettivo[28].
Normalmente la verifica delle informazioni ricevute dal cliente è solo eventuale e va compiuta quando emergano dubbi o incongruenze sui dati forniti; in particolare la verifica dell'identità del cliente è una attività talvolta non dovuta[29], o da svolgere quando[30], in presenza di un basso

27 L'iter era stato avviato a gennaio 2019 da AgID, e con la predetta pubblicazione nella Gazzetta Ufficiale Europea, è attualmente consentito utilizzare, oltre il Sistema Pubblico di Identità Digitale (SPID), anche la CIE per accedere ai servizi digitali delle pubbliche amministrazioni degli Stati dell'Unione Europea.
L'Italia, con la notifica europea del sistema SPID e quella della CIE, è il primo paese in Europa ad aver ultimato l'iter per la notifica europea di due diversi sistemi di identità digitali. Anche Belgio, Croazia, Repubblica Ceca, Estonia, Germania, Lussemburgo, Portogallo, Spagna, Olanda e Regno Unito hanno provveduto a notificare i propri sistemi di autenticazione ai servizi online.
La Carta d'Identità Elettronica (CIE), grazie al rilascio da parte del Poligrafico e Zecca dello Stato insieme al Ministero dell'Interno di una nuova modalità di identificazione online, a partire dal 6 aprile 2020 è diventata la chiave di accesso che permette l'autenticazione con i massimi livelli di sicurezza ai servizi online degli enti che ne consentono l'utilizzo, Pubbliche Amministrazioni e soggetti privati, infatti, tutti i cittadini italiani in possesso della Carta d'Identità Elettronica 3.0 possono accedere direttamente da remoto ai servizi digitali della P.A., tra cui quelli previdenziali dell'Inps, o sanitari ed anagrafici di Regioni e Comuni che già permettono l'accesso con la CIE, per citare solo alcuni.

28 Se ne occupa nel dettaglio l'art. 19, comma 1 lett. b): *la verifica dell'identità del cliente, del titolare effettivo e dell'esecutore richiede il riscontro della veridicità dei dati identificativi contenuti nei documenti e delle informazioni acquisiti all'atto dell'identificazione, laddove, in relazione ad essi, sussistano dubbi, incertezze o incongruenze. Il riscontro può essere effettuato attraverso la consultazione del sistema pubblico per la prevenzione del furto di identità di cui decreto legislativo 11 aprile 2011, n. 64. La verifica dell'identità può essere effettuata anche attraverso il ricorso ad altre fonti attendibili e indipendenti tra le quali rientrano le basi di dati, ad accesso pubblico o condizionato al rilascio di credenziali di autenticazione, riferibili ad una pubblica amministrazione nonché quelle riferibili a soggetti privati autorizzati al rilascio di identità digitali nell'ambito del sistema previsto dall'articolo 64 del decreto legislativo n. 82 del 2005 ovvero di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento EU n. 910/2014. (...)*."

29 Crf. Art.18, comma 4 : *"Fermi gli obblighi di identificazione, i professionisti, limitatamente ai casi in cui esaminano la posizione giuridica del loro cliente o espletano compiti di difesa o di rappresentanza del cliente in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o piu' avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo,* ***sono esonerati dall'obbligo di verifica dell'identità del cliente*** *e del titolare effettivo fino al momento del conferimento dell'incarico."*

30 V. art. 18, comma 3 D.Lgs. 231 cit.: "*In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo può essere posticipata ad un momento successivo all'instaurazione del rapporto o al conferimento dell'incarico per lo svolgimento di una prestazione professionale, qualora ciò sia necessario a consentire l'ordinaria gestione dell'attività oggetto del rapporto. In tale ipotesi, i soggetti obbligati, provvedono comunque all'acquisizione dei dati identificativi del cliente, dell'esecutore e del titolare effettivo e dei dati*

rischio di riciclaggio, in un primo momento si sia proceduto all'acquisizione dei dati identificativi del cliente e dell'esecutore senza l'esibizione di alcun documento di identità o la presenza fisica del cliente e in assenza dei presupposti sopra evidenziati per l'identificazione a distanza - e solo successivamente si sia provveduto a completare le procedure di verifica dell'identità dei medesimi, nel rispetto del termine di trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico; ovvero da compiere solo quando sussistono dubbi, incongruenze e incertezze in ordine alla veridicità dei dati e dei documenti acquisiti all'atto della identificazione.
A questo ultimo proposito l'art. 19, comma 1 lett. b) individua alcune modalità di riscontro dei dati che, per le identità digitali sopra esaminate, possono avvenire solo in modalità elettronica; infatti, tali strumenti di identificazione sono dotati di alcuni elementi di autenticità che in una trasposizione cartacea si perderebbero irrimediabilmente e che, invece, possono essere verificati e memorizzati proprio attraverso meccanismi informatici.

Da quanto sopra si ricava che in tutte le ipotesi in cui il cliente possa essere identificato o tramite una identità digitale tra quelle sopra elencate (SPID di massimo livello, documento di identità elettronico, certificato qualificato collegato ad una firma qualificata o comunque tramite procedure di identificazione regolamentate tramite AgID), è altresì possibile procedere ad una identificazione a distanza ed eventualmente ad una verifica dei dati connessi a quell'identità digitale.
Inoltre la possibilità che l'obbligo di identificazione, senza la presenza fisica del cliente, possa essere assolto non solo per il tramite dell'acquisizione informatica dell'identità digitale (ad es. mediante la memorizzazione di tutti i dati contenuti nel documento di identità elettronico), ma anche attraverso una verifica della stessa nell'arco di una sessione continua di video conferenza con l'ausilio di un operatore remoto, assicura quel grado ulteriore di sicurezza e di mitigazione del rischio raccomandato dalla Guida GAFI.

Va, infatti, sottolineato che non sempre l'utilizzo di uno strumento di identificazione digitale, per quanto di massimo livello di sicurezza e *compliant* con la normativa AR sopra richiamata, si accompagna all'interazione, seppure da remoto, con un operatore umano; a questo proposito si faccia l'esempio del procedimento per la costituzione on line delle start up innovative senza notaio: in questo processo l'utente arriva a comporre il suo atto costitutivo e lo statuto della start up non solo on line, ma soprattutto senza che alcuno sottoponga a verifica la sua identità digitale (attestata dal certificato qualificato utilizzato sia per la sottoscrizione che per la sua identificazione) attraverso lo svolgimento di un video collegamento in contestualità al suo concreto utilizzo.

Ed a ben vedere, sulla base delle linee guida del GAFI in commento, utilizzi "non presidiati" da alcun operatore delle identità digitali sarebbero addirittura visti come possibili fonti di aumento del rischio, posto che il GAFI stesso richiama l'attenzione degli Stati non solo (e non tanto) al momento del rilascio della identità digitale, quanto soprattutto al momento del suo concreto utilizzo.

relativi alla tipologia e all'importo dell'operazione e completano le procedure di verifica dell'identità dei medesimi al più presto e, comunque, entro trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico. Decorso tale termine, qualora riscontrino l'impossibilità oggettiva di completare la verifica dell'identità del cliente, i soggetti obbligati, si astengono ai sensi dell'articolo 42 e valutano, sussistendone i presupposti, se effettuare una segnalazione di operazione sospetta ai sensi dell'articolo 35." Cfr. sul punto anche la Regola Tecnica n. 7.

Infatti, mentre le organizzazioni criminali in passato potevano avvalersi di prestanomi fisici, ora esse possono utilizzare i c.d. "muli digitali" (*rectius* corrieri digitali) per compiere operazioni addirittura con o senza la consapevolezza del prestanome stesso, proprietario dell'identità digitale. Le organizzazioni criminali, in altre parole, "*possono acquistare credenziali di identificazione digitale da individui che consentono loro di accedere ai conti delle persone presso entità regolamentate, trasformandoli in effetti in muli digitali per l'organizzazione*"[31].
A tale proposito, è utile osservare che nelle "Quaranta raccomandazioni del GAFI" (datate luglio 1990), la Raccomandazione 12 imponeva alle entità regolamentate di identificare i propri clienti "sulla base di un documento di identificazione ufficiale o di altro tipo affidabile". Questa dizione è stata mantenuta invariata anche attraverso le revisioni di giugno 1996 e giugno 2003 delle Raccomandazioni, ed è rimasta in vigore fino all'adozione della versione attuale delle Raccomandazioni nel febbraio 2012. In tale ultima versione, il GAFI ha aggiunto il requisito della "**verifica dell'identità**" e l'ulteriore requisito secondo cui le prove dell'identità devono essere anche "**indipendenti**" oltre a "affidabili".
Ebbene, il GAFI precisa che nel contesto dell'ID digitale, il requisito secondo cui i "documenti, dati o informazioni" digitali devono essere "affidabili e indipendenti" significa che il sistema di identificazione digitale utilizzato per condurre le transazioni deve essere basto su tecnologia e *governance* adeguata, nonché su **processi e procedure** che forniscono un livello adeguato di sicurezza che il sistema produca risultati il più possibile accurati.

Ora, se da un lato, il GAFI precisa che per le entità regolamentate, una frequente autenticazione digitale di un cliente ai propri sistemi informatici appare idonea a fornire una "*ragionevole garanzia basata sul rischio (vale a dire, l'affidamento) che la persona che afferma l'identità oggi sia la stessa persona che ha precedentemente aperto il conto o altri servizi finanziari, ed è in realtà la stessa persona che è stata sottoposta a identificazione e verifica "affidabile, ed indipendente" al momento del rilascio dell'identità digitale*"[32], in quanto una autenticazione digitale **continuata nel tempo**, risulta capace di collegare tale identità con la relativa attività finanziaria, facilitando la capacità di condurre una significativa *due diligence* e monitoraggio del soggetto; risulta altrettanto evidente che una singola ed **isolata** autenticazione informatica non potrà al contrario essere considerata adeguata - sulla base di un approccio basato sul rischio – nell'ipotesi di una operazione "spot". In tal caso, infatti, dovranno essere approntati processi e procedure di controllo ulteriori.

Conoscenza pregressa

Se il cliente è stato preventivamente identificato in relazione ad un pregresso rapporto, purché esso sia tutt'ora in essere, si può sempre procedere ad una identificazione a distanza, con l'unica accortezza di verificare che le informazioni siano aggiornate (ad esempio in questi casi va verificato che il documento di identità non sia scaduto).

E - <u>Identificazione a distanza di cliente ed esecutore</u>

31 GAFI, Guida all'identità digitale, marzo 2020, pag. 41

32 GAFI, Guida all'identità digitale, marzo 2020, pag. 31

Come abbiamo visto l'attuale formulazione del Decreto Antiriciclaggio prevede, quale regola generale, che l'identificazione del cliente e del titolare effettivo deve essere svolta in presenza del medesimo cliente ovvero dell'esecutore (articolo 19, comma 1, lettera a).
La stessa norma, tuttavia, prevede anche delle eccezioni a questo principio. Più precisamente, prevede che l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, in una serie di specifici casi, analizzati nel paragrafo precedente.
La lettera a) del primo comma dell'articolo 19 prevede, poi, una ulteriore, ultima, ipotesi in cui l'obbligo di identificazione si può considerare assolto anche senza la presenza del cliente: si tratta dell'ipotesi prevista dal n.5, che testualmente recita: "*5) per i clienti i cui dati identificativi siano acquisiti attraverso idonee forme e modalità, individuate dalle Autorità di vigilanza di settore, nell'esercizio delle attribuzioni di cui all'articolo 7, comma 1, lettera a), tenendo conto dell'evoluzione delle tecniche di identificazione a distanza;*". Tale ultima previsione si ritiene non applicabile ai professionisti, il cui soggetto regolamentare di riferimento è il c.d. "organismo di autoregolamentazione" [33], che non viene menzionato nel punto 5 sopra riportato. Questa mancanza non può ascriversi ad una "dimenticanza" del legislatore, quanto piuttosto ad una precisa scelta del legislatore stesso che, dove ha inteso attribuire determinati poteri e facoltà sia agli organismi di autoregolamentazione che alle Autorità di vigilanza di settore [34], lo ha previsto espressamente (per entrambi) [35]. Richiesto di esprimersi sul punto, il Comitato di Sicurezza Finanziaria ha confermato l'esclusione, confermando che *"spetta esclusivamente alle Autorità di vigilanza di settore individuare forme e modalità di identificazione a distanza, svolta senza la presenza fisica del cliente, che tengano conto dell'evoluzione delle tecniche di identificazione a distanza, perché l'ordinamento a oggi vigente non attribuisce la medesima competenza agli organismi di autoregolamentazione"* [36]. Per completezza, si precisa che Banca d'Italia, con provvedimento del 30 luglio 2019, pubblicato su GU n.189 del 13 agosto 2019, ha previsto specifiche disposizioni in materia di operatività a distanza (rivolte ai soggetti vigilati) e che, conformemente all'interpretazione sopra esposta in relazione al disposto del punto n.5, nessun organismo di autoregolamentazione ha fatto altrettanto.
Assodato che nell'ambito dell'attività notarile non è possibile svolgere l'identificazione a distanza nell'ipotesi residuale prevista al più volte citato punto 5 della lettera a) del primo comma dell'articolo 19 del D. Lgs. 231/2007, è pur vero, invece, che l'identificazione non in presenza può essere svolta ricorrendo le condizioni testualmente previste nei primi quattro punti della lettera a) del primo comma.
Viene da chiedersi se quanto sin qui detto circa l'adeguata verifica non in presenza valga anche per l'esecutore: l'articolo 19, infatti, non menziona mai (sotto questo aspetto) l'esecutore, prevedendo l'identificazione a distanza solo in relazione al cliente.

33 L'organismo di autoregolamentazione è l'ente esponenziale, rappresentativo di una categoria professionale, cui l'ordinamento attribuisce, tra l'altro, poteri di regolamentazione e di controllo della categoria (art.1, comma 2, lettera aa) del D. Lgs. 231/2007).

34 Autorità di vigilanza di settore sono le autorità preposte alla vigilanza e al controllo, tra gli altri, degli intermediari bancari e finanziari, ad esempio la Banca d'Italia, la CONSOB e l'IVASS (art.1, comma 2, lettera c) del D. Lgs. 231/2007).

35 Si vedano, ad esempio, le previsioni di cui agli articoli 15, comma 1 (in materia di valutazione del rischio) e 23, comma 3 (in materia di misure semplificate di adeguata verifica della clientela) del D. Lgs. 231/2007, a differenza di quanto, ad esempio, previsto dall'articolo 15, comma 3 (in materia di individuazione dei soggetti che presentano un rischio di riciclaggio irrilevante), in cui è nominata solo l'Autorità di vigilanza di settore.

36 Cfr. "Nell'emergenza possibile l'identificazione del cliente via videoconferenza", S. de Rosa e A. De Vivo, su: www.eutekne.info/Sezioni/Art_779956_nell_emergenza_possibile_l_identificazione_del_cliente_via_videonconferenza.aspx.

L'identificazione dell'esecutore è regolata dall'art. 18[37], con norma che sembra essere stata scritta, originariamente, solo per l'ipotesi di identificazione in presenza fisica. Esistono però indici, sia sistematici che normativi (anche in conseguenza di modifiche susseguitesi nel tempo), che portano a ritenere possibile l'identificazione a distanza anche dell'esecutore.
A livello di sistema si rileva che esecutore può essere non solo un rappresentante volontario, ma anche un soggetto che agisce per **rappresentanza organica** di una società o di un altro ente non personificato: in tale ultimo caso, il rapporto organico fa sì che non vi sia altra persona fisica che rappresenti il cliente ed è quindi, necessariamente, all'esecutore che vanno riferite le norme che consentono l'identificazione a distanza.
A livello normativo si richiama l'attuale formulazione dell'articolo 31[38], che pone a carico del soggetto obbligato l'onere di conservare i dati e i documenti acquisiti in occasione dell'adeguata verifica, in modo che si possano ricostruire univocamente *"i dati identificativi, ivi compresi, ove disponibili, i dati ottenuti mediante i mezzi di identificazione elettronica e i pertinenti servizi fiduciari di cui al regolamento UE n. 910/2014 o mediante procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale, del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione"*[39]. Questa norma, pur occupandosi di conservazione, facendo riferimento ai "*dati ottenuti mediante i mezzi di identificazione elettronica e i pertinenti servizi fiduciari di cui al regolamento UE n. 910/2014 o mediante procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale*" sia in relazione al cliente, che al titolare effettivo, che all'esecutore (testualmente previsto), implicitamente ammette l'identificazione non in presenza anche per l'esecutore.
Sembra evidente che l'originario compilatore degli articoli 18 e 19 non immaginasse la possibilità dell'identificazione a distanza per l'esecutore, possibilità che invece sembra presupposto dell'attuale testo dell'articolo 31 cit.. Appare, quindi, conforme ad un'interpretazione sistematica ed evolutiva ritenere che l'articolo 18 consenta, in via generale, l'identificazione a distanza anche dell'esecutore, sia perché altrimenti si creerebbe una contraddizione normativa per il caso di immedesimazione organica, sia perché non si comprenderebbe il dettato dell'articolo 31 novellato.
Questa ricostruzione appare confermata anche dal provvedimento della Banca d'Italia sopra citato, che, come detto, contiene disposizioni attuative del punto 5 della lettera a) del primo comma dell'articolo 19 (che fa riferimento al solo cliente): ebbene, tale provvedimento, alla Sezione III, rubricata "*L'identificazione del cliente e dell'esecutore*", rimanda alla Sezione VIII, che individua le modalità per l'operatività a distanza. In tale ultima Sezione viene definita quale "*operatività a distanza*" quella "*svolta senza la compresenza fisica (...) del cliente*" e si precisa che "*quando il cliente è un soggetto diverso da una persona fisica, esso si considera presente quando lo è l'esecutore*" e che il destinatario (cioè il soggetto vigilato) deve porre particolare attenzione all'operatività a distanza, in considerazione dell'assenza di un contatto

37 Art. 18: 1. Gli obblighi di adeguata verifica della clientela si attuano attraverso:
a) l'identificazione del cliente e la verifica della sua identità attraverso riscontro di un documento d'identità o di altro documento di riconoscimento equipollente ai sensi della normativa vigente nonché sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Le medesime misure si attuano nei confronti dell'esecutore, anche in relazione alla verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente.

38 Nella versione attualmente vigente, a seguito delle modifiche di cui al D. Lgs. 125/2019.

39 Anche dal punto di vista della conservazione si evidenzia come il corretto trattamento dei documenti digitali sia improcrastinabile in quanto la loro lettura e memorizzazione informatica, in tutte le loro componenti ivi incluse soprattutto quelle che ne attestano l'autenticità, sia già prevista per legge.

diretto "*con il cliente o con l'esecutore*". Da ciò si può senz'altro concludere che la Banca d'Italia ha inteso riferire la possibilità dell'identificazione a distanza anche all'esecutore.

Da ultimo occorre rilevare che la citata Sezione VIII del provvedimento della Banca d'Italia in data 30 luglio 2019, rubricata "*Disposizioni specifiche in materia di operatività a distanza*", sembra riferirsi solo a quei soggetti per cui l'unica modalità di identificazione possibile è quella attraverso **un documento cartaceo**. Questo, a ben vedere, è coerente con quanto sopra affermato, e cioè che per tutti coloro la cui identificazione possa essere effettuata secondo i requisiti di cui ai primi quattro punti della lettera a) del primo comma dell'articolo 19, non era necessario dettare ulteriori e diverse modalità di identificazione a distanza, previste al n.5) e riferibili, pertanto, solo ad ipotesi in cui sia completamente mancante un ID digitale o il riscontro di una documentazione autentica, di matrice notarile o consolare.

F - Le modalità di colloquio con il cliente e l'interazione con un operatore che supervisioni l'identificazione/verifica dell'identità del cliente collegato in remoto

L'adeguata verifica del cliente non si esaurisce nella mera identificazione dello stesso, ma ricomprende un complesso di operazioni che – senza scendere del dettaglio – possiamo schematizzare in quattro elementi da modulare differentemente in funzione del rischio:

a) l'identificazione del cliente e la verifica della sua identità;
b) l'identificazione del titolare effettivo e la verifica della sua identità;
c) l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale;
d) il controllo costante del rapporto con il cliente.

Va poi accertato se il cliente ricopra o meno la qualifica di Persona Politicamente Esposta (PEP). Alcune delle attività in cui si sostanza l'Adeguata Verifica (AV) presuppongono accertamenti di tipo documentale: si pensi, ad esempio, alla verifica del potere di rappresentanza, o all'acquisizione dei mezzi di pagamento; altre, invece, inevitabilmente, si sostanziano in una richiesta di informazioni (ad es. quella relativa al Titolare Effettivo o quella riguardante la condizione di PEP) che il cliente, se richiesto, ha l'obbligo ex art. 22, D. Lgs. 231 cit. di fornire per iscritto.
Nulla dice il Decreto Legislativo sulle modalità del colloquio tra il soggetto obbligato ed il cliente, né tanto meno sulla modalità con cui raccogliere tali dati ed informazioni, che pertanto sarà a forma libera e potrà svolgersi sia in presenza che a distanza; laddove si volesse ricorrere alla dichiarazione ex art. 22 cit. è evidente che la forma scritta dovrà essere valutata – in caso di colloquio a distanza mediante strumenti informatici – sulla base della normativa vigente portata dal Regolamento UE 910/2019 e dal D. Lgs. 82/2005.
Nella richiesta di dati ed informazioni sarà ammissibile sia il mero colloquio telefonico, ma anche forme più moderne ed interattive (quali il video collegamento) accompagnate, se del caso, dall'invio di moduli per la raccolta dei predetti dati ed informazioni da restituire o firmati in maniera autografa su supporto cartaceo o elettronicamente su supporto informatico, purché detta sottoscrizione elettronica integri il requisito della forma scritta.
Qualora l'identificazione a distanza fosse basata su un'ID digitale, come abbiamo visto, tornano utili le indicazioni della Guida GAFI sui requisiti di comparabilità per la verifica e l'attribuzione di identità di una persona in remoto supervisionate, che collegano allo svolgimento di una video

conferenza la possibilità di aumentare il livello di sicurezza della predetta identificazione a distanza. In particolare, nelle NIST (National Institute of Standards and Technology) Digital ID Standards statunitensi si richiamano alcuni requisiti per stabilire la comparabilità tra la verifica e l'attribuzione di una identità effettuata in remoto sotto la supervisione di un operatore e l'analoga operazione effettuata in presenza fisica, i quali potrebbero essere di non difficile implementazione e che, di fatto[40], sono attualmente utilizzati dai Certificatori Qualificati nelle procedure autorizzate dall'AgiID per il rilascio di firme digitali.
Da ciò si ricava che il contemporaneo svolgimento di una identificazione da remoto dei clienti in possesso di una identità digitale tra quelle sopra elencate e di un colloquio costante in videoconferenza con il medesimo cliente, raggiungerebbe il duplice scopo di rafforzare l'identificazione effettuata per il tramite dell'identità digitale e consentirebbe il corretto svolgimento dell'adeguata verifica quanto meno relativamente ad una prima richiesta di dati ed informazioni.

G - Il problema della sottoscrizione delle dichiarazioni ex art. 22

Lo svolgimento dell'adeguata verifica richiede, come abbiamo visto, l'acquisizione di una serie di dichiarazioni da parte del cliente, il quale, se richiesto, ha l'obbligo di fornirle, ex art. 22, D. Lgs. 231 cit., per iscritto. Se su carta l'integrazione della forma scritta è riscontrabile *ictu oculi* mediante la redazione di un testo sottoscritto in modo autografo dall'interessato, nel campo dei documenti informatici l'integrazione del medesimo requisito è legato a numerose caratteristiche di integrità, non modificabilità e sicurezza, sia del documento informatico in sé, che della sottoscrizione elettronica utilizzata per l'assunzione di paternità dello stesso.
Le tipologie di sottoscrizione utilizzabili ai sensi della normativa vigente per rendere per iscritto le dichiarazioni ex art. 22 cit. attraverso un documento informatico, ovvero le modalità di sottoscrizione elettronica avente valore di forma scritta che non sia liberamente valutabile in giudizio, sono così riassumibili:

- firma qualificata/digitale (v. Regolamento (UE) n.910/2014 - eIDAS, secondo cui *"Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri"*);
- firma avanzata (v. art. 20 comma 1bis: 1-bis[41] e art. 21 2-bis [42] CAD);

40 V. nota 8.

41 Testo dell'art. 20, comma 1bis CAD: "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalita' tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida."*

42 Testo dell'art. 21 2-bis CAD: "*Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13) del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalita' di cui all'articolo 20, comma 1-bis, primo periodo*".

- firma di processo (v. artt. 20 e 21 cit. nonché le linee guida AgID portanti Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD del 21 aprile 2020).

Conclusioni:

In una possibile procedura di identificazione a distanza con sottoscrizione dei documenti relativi all'adeguata verifica è possibile prevedere l'utilizzo alternativo o cumulativo dei seguenti strumenti:

- conoscenza pregressa + sottoscrizione delle dichiarazioni ex art. 22 in tutte le modalità consentite dall'ordinamento giuridico, sia cartacee che elettroniche, purché queste ultime integrino il requisito della forma scritta;
- produzione di documenti autentici (atti notarili, documenti firmati digitalmente, dichiarazioni dell'autorità consolari) + sottoscrizione delle dichiarazioni ex art. 22 in tutte le modalità consentite dall'ordinamento giuridico, sia cartacee che elettroniche, purché queste ultime integrino il requisito della forma scritta;
- identificazione a distanza tramite il certificato qualificato + sottoscrizione delle dichiarazioni ex art. 22 in modalità sia cartacea che elettronica con il medesimo certificato qualificato (astrattamente sarebbe possibile utilizzare altre forme di sottoscrizione elettronica ammessa dall'ordinamento, ma ciò risulterebbe quanto meno incongruo visto che il cliente è dotato di un certificato di firma qualificato);
- identificazione a distanza tramite i documenti di identità elettronici (CIE o passaporto elettronico) o tramite SPID di massimo livello (livello 3 con token fisico) e sottoscrizione delle dichiarazioni ex art. 22 in tutte le modalità consentite dall'ordinamento giuridico, sia cartacee che elettroniche, purché queste ultime integrino il requisito della forma scritta.

Gea Arcella - Laura Piffaretti - Michele Manente