Dialoghi di Diritto dell'Economia

Marzo 2023

ARTICOLI

L'adeguata verifica a distanza tra Linee guida EBA, profili di governance, cybersecurity e di protezione dei dati

Marcello Condemi

Professore Straordinario di Diritto dell'Economia
Università degli Studi Guglielmo Marconi

DB

Dialoghi di Diritto dell'Economia

Criteri di Revisione

I contributi proposti alla Rivista per la pubblicazione sono sottoposti a una previa valutazione interna da parte della Direzione o di uno dei Direttori d'Area; il quale provvede ad assegnare il contributo a un revisore esterno alla Rivista, selezionato, rationes materiae, fra professori, ricercatori o assegnisti di ricerca.

La rivista adotta il procedimento di revisione tra pari a singolo cieco (single blind peer review) per assicurarsi che il materiale inviato rimanga strettamente confidenziale durante il procedimento di revisione.

Qualora il valutatore esprima un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche, aggiunte o correzioni, la Direzione si riserva di negare la pubblicazione dell'articolo. Nel caso in cui la Direzione decida per la pubblicazione, deve verificare previamente che l'Autore abbia apportato le modifiche richieste dal Revisore.

Qualora il revisore abbia espresso un giudizio negativo, il contributo può essere rifiutato oppure inviato, su parere favorevole della maggioranza dei Direttori dell'area competente rationes materiae, a un nuovo revisore esterno per un ulteriore giudizio. In caso di nuovo giudizio negativo, il contributo viene senz'altro rifiutato.

L'adeguata verifica a distanza tra Linee guida EBA, profili di governance, cybersecurity e di protezione dei dati

Marcello Condemi

Sommario: *Premessa di contesto;* 1. *L'impianto AML/CFT ed i suoi capisaldi: l'"adeguata verifica" e la "segnalazione di operazione sospetta"; 1.1. Segue: L'Adeguata verifica a distanza: una prospettiva generale; 1.1.1. Segue: Contesto eurounitario; 1.1.2. Segue: Le nuove Linee Guida EBA; 1.1.2 a) Segue: L'adozione di politiche e procedure interne; 1.1.2 b) Segue: Valutazione preliminare e successive integrazioni della soluzione di remote onboarding nel sistema dei controlli interni; 1.1.2 c) Segue: Identificazione, acquisizione delle informazioni e verifica dell'identità e dell'integrità dei documenti; 1.1.2 d) Segue: Affidamento dell'adeguata verifica a terzi ed esternalizzazione; 2. Applicazione dell'adeguata verifica a distanza nel contesto nazionale: il Provvedimento Banca d'Italia del 30 luglio 2019 e il Regolamento IVASS n. 44 del 12 febbraio 2019; 3. Cybersecurity e Protezione dei Dati; 4. Conclusioni*

Premessa di contesto

Il rapido diffondersi delle tecnologie informatiche ed il contestuale celere sviluppo dei pagamenti digitali evidenziano la necessità di provvedere, nel continuo, all'adeguamento, tra gli altri[01], degli strumenti normativi ed operativi di *Anti Money Laundering* (AML) e *Combating Financing of Terrorism* (CFT); e ciò al fine di garantire che qualsivoglia transazione finanziaria, anche vieppiù informatizzata e digitale, sottenda il basilare requisito della conoscenza del cliente e della ragionevole garanzia che i fondi utilizzati non abbiano origine illecita.

Si rileva in proposito, a livello globale, un *trend* caratterizzato da una sempre maggior attenzione da parte degli operatori verso lo sviluppo di metodologie e procedure, anche tecniche, e del correlato adeguamento della normativa AML/CFT, con specifico riferimento all'impatto che le nuove tecnologie potrebbero avere tanto nel quadro delle attività di contrasto dei fenomeni di riciclaggio e finanziamento del terrorismo quanto sulle attività finanziarie riconducibili più in generale, per via di tali impatti, al c.d. *FinTech* (*Financial Technology*)[02].

01 Cfr., sulle tematiche introdotte dalle nuove tecnologie, M. CONDEMI, *Nuove tecnologie ed attività finanziarie: spunti per un rinnovato approccio regolamentare*, in *Diritto Bancario*, luglio 2021, nel quale ci si interroga sulle possibili, attuali e future, implicazioni derivanti dall'utilizzo delle nuove tecnologie nel contesto della regolazione delle attività finanziarie, auspicando, in particolare, un approccio coordinato a livello europeo volta ad evitare i rilevanti rischi di una prospettiva, che tuttora permane, che non tenga in sufficiente considerazione le esigenze dei nuovi, numerosi *players* del mercato.

02 Si veda, a proposito della nozione di *Fintech* e delle sue ampie articolazioni, M. CONDEMI, *Nuove tecnologie ed attività finanziarie: spunti per un rinnovato approccio regolamentare*, cit..

Nella consapevolezza del rilievo via via assunto da tali tematiche nell'area delle attività bancarie e finanziarie, nel dicembre 2019 la Banca d'Italia ha pubblicato gli esiti di un'"*Indagine FinTech nel sistema finanziario italiano*", nella cui premessa si dà conto, da un lato, (i) del perimetro dei soggetti indagati, riguardando essi «(...) *165 intermediari, tra cui 50 gruppi bancari, anche di matrice estera, 70 banche non appartenenti a gruppi, 5 filiali di banche estere, 3 intermediari in libera prestazione di servizi e 37 intermediari non bancari; sono state inoltre contattate 15 tra le maggiori imprese fornitrici di servizi tecnologici. Gli intermediari sono stati selezionati in base agli attivi e ai volumi di operatività; alcuni di essi, nonostante la limitata scala, sono stati inclusi nel campione in funzione dei particolari modelli di business adottati e della loro propensione ad innovare. Il tasso di partecipazione è stato dell'82 per cento; considerando le sole banche, la copertura in termini di attivo è stata pari a circa il 90 per cento del totale di sistema. Il tasso di risposta tra i service providers è stato invece significativamente più basso e pari ad un terzo delle imprese contattate; per questo segmento di mercato, dunque, i fenomeni emersi, parziali e non necessariamente indicativi delle tendenze in atto, non vengono riportati*» (ii), dall'altro, e per quanto qui specificamente di interesse, della circostanza che «(u)*na sezione ad hoc* (di tale indagine) *è dedicata alle modalità con cui vengono impiegate soluzioni innovative per contrastare il riciclaggio e il finanziamento del terrorismo*».

La ricerca ha evidenziato, a conferma della menzionata preoccupazione, come gli intermediari finanziari campionati, nel quadro degli investimenti volti a fronteggiare lo sviluppo delle nuove tecnologie, abbiano incentrato una parte delle risorse disponibili nel settore AML/CFT, in ragione delle Direttive UE 2015/849 (c.d. Quarta Direttiva Antiriciclaggio) e 2018/843 (c.d. Quinta Direttiva Antiriciclaggio) e dei rispettivi atti di recepimento, quali il d.lgs. 25 maggio 2017, n. 90, recante *"Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo* (...)" e il d.lgs. 4 ottobre 2019, n. 125, riguardante *"Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonche' attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849* (...)", oltreché delle disposizioni contenute nel Provvedimento della Banca d'Italia del 30 luglio 2019, contenente *"Disposizioni in materia di adeguata verifica a distanza della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo"*, di cui si avrà modo di trattare più approfonditamente *infra*.

Con specifico riferimento ai progetti destinati al contrasto dei fenomeni di ML/FT, l'indagine di Banca d'Italia rileva, più precisamente, come «(g)*li intermediari st*(iano) *sviluppando con cautela progetti basati su nuove tecnologie (specialmente quelle connesse all'AI) nelle aree suscettibili dei maggiori guadagni in*

termini di efficienza e di efficacia dei processi AML/CFT, in particolare in quelle connesse alla profilatura del rischio della clientela e all'individuazione delle operazioni anomale. Tali progetti sono sviluppati principalmente in house, ma anche in collaborazione con società di consulenza, enti di ricerca e università. In base alle evidenze emerse dall'indagine, nel biennio 2017-2018 la funzione antiriciclaggio degli intermediari è stata coinvolta in 33 iniziative FinTech con ricadute sui presidi antiriciclaggio (circa il 12 per cento delle iniziative censite). Parallelamente allo sviluppo di questi progetti, gli intermediari stanno incrementando il livello di automazione dei processi AML/CFT e l'utilizzo di banche dati per l'adeguata verifica della clientela; su impulso della nuova normativa antiriciclaggio, stanno inoltre sviluppando nuove soluzioni per l'identificazione a distanza della clientela. Si illustrano di seguito nel dettaglio i risultati dell'indagine con riferimento alle principali soluzioni innovative adottate in ambito AML/CFT».

Dall'indagine emerge, altresì, l'orientamento degli intermediari a ricorrere allo sviluppo, a fronte di un sempre maggior numero di prodotti e servizi bancari e finanziari a distanza, di nuove modalità per l'identificazione e la verifica dei dati identificativi acquisiti a distanza, di cui si dirà meglio i*nfra.*

Per il momento si ritiene d'interesse evidenziare come, in base alle risultanze dell'indagine di che trattasi, gli intermediari, nel 2019, si stessero approcciando alla tematica dell'identificazione a distanza in maniera prudente e graduale, emergendo «*dalle risposte fornite da 64 intermediari* (...) *che:*

- *Sei intermediari utilizzano i certificati per la generazione di firma digitale, rilasciati da enti accreditati presso l'AGID, per l'identificazione della clientela. Benché si rilevi 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 ordinarie modalità per la verifica dell'identità a distanza (ad esempio il bonifico a valere su un conto corrente del cliente);*

- *Soltanto 4 intermediari impiegano procedure alternative di riconoscimento a distanza, che prevedono: i) l'iniziale trasmissione da parte del cliente di una propria foto o di un proprio video, nella quale il cliente si mostra in possesso del documento d'identità di cui ha trasmesso copia o, nel caso del video, pronuncia una parola suggerita dal sistema; ii) la successiva verifica manuale delle informazioni trasmesse.*

- *Nessuno intermediario, infine, si avvale di modalità di identificazione basate su identità digitali regolamentate (ad esempio la SPID) né impiega sistemi automatizzati di riconoscimento biometrico per iden-*

tificare la clientela a fini antiriciclaggio»[03].

Come si avrà modo di osservare in seguito, nel periodo a venire si è assistito ad un'accelerazione esponenziale dei fenomeni di digitalizzazione.

Avuto riguardo al quadro normativo relativo ai fenomeni suindicati, spunti di rilievo si colgono nella *"Guida all'identità digitale"* pubblicata dal GAFI-FATF[04] il 6 marzo 2020 con lo scopo di orientare, nel-

03 Va segnalata, a fini comparativi, quanto riportato nello svolgimento del Webinar "*Adeguata verifica a distanza: nuove Linee guida EBA"* (organizzato dalla rivista "*DB Non solo Diritto Bancario*"), svoltosi lo scorso 7 febbraio 2023, in modalità telematica, da M. STELLIN, *Partner, Governance Risk & Compliance* di KPMG *Advisory* S.p.A., circa un'indagine, condotta dalla medesima KPMG S.p.a., relativamente ai *benchmark* rilevati sulle principali soluzioni di *remote onboarding* con riguardo ad un campione di 8 *Player* di cui: a) sei banche (tre "*significant*" e tre "*less significant*"); b) un'Assicurazione; c) un Istituto di Pagamento. Segnatamente viene riportato come: a) due dei *Player* prevedano *«1. Accesso Portale web/Area riservata; 2. Identificazione tramite SPID/CIE; 3. Sottoscrizione documentazione con firma digitale tramite OTP. Per i soli clienti privi di identità digitale o Firma Elettronica Qualificata (FEQ): 1. Accesso Portale web/Area riservata; 2. Acquisizione del documento di identità e del video-selfie online; 3. Verifica identità tramite Liveness check (verifica biometrica del volto del cliente rispetto alla foto presente sul documento caricato dallo stesso); 4. Sottoscrizione documentazione con firma digitale tramite OTP»*; b) altri due *Player «1. Accesso Portale web/Area riservata; 2. Acquisizione documentazione online; 3. Sottoscrizione documentazione con firma digitale tramite OTP»*; c) un *Player «1. Accesso Portale web/Area riservata; 2. Acquisizione documento di identità online e verifica degli stessi attraverso strumenti OCR; 3. Acquisizione di un selfie e scansione di un QR Code da parte del cliente; 4. Verifica numero di telefono (con supporto codice OTP) e richiesta di una transazione bancaria; 5. Sottoscrizione documentazione con firma digitale tramite OTP»*; d) un *Player «1. Accesso Portale Web o contatto tramite Phone banking; 2. Acquisizione informazioni rilevanti; 3. Sottoscrizione documenti tramite firma digitale; 4. Invio documentazione all'intermediario tramite posta elettronica certificata (PEC). Per i soli clienti privi di firma digitale: 1. Accesso Portale Web e compilazione del Form online; 2. Invio della documentazione tramite posta elettronica certificata (PEC); 3. Identificazione tramite videochiamata; 4. Sottoscrizione documentazione con firma digitale tramite OTP»*; e) un *Player «1. Accesso Portale Web o contatto tramite Phone banking; 2. Acquisizione informazioni rilevanti; 3. Sottoscrizione documenti tramite firma digitale; 4. Invio documentazione all'intermediario tramite posta elettronica certificata (PEC)»*; f) un *Player «1. Accesso al Portale Web; 2. Acquisizione documentazione online; 3. Esecuzione di un bonifico bancario o video identificazione; 4. Sottoscrizione della documentazione con firma digitale tramite OTP»*. In aggiunta, nella presente indagine, si osserva anche come «*Dalle analisi di benchmark si rileva la tendenza degli intermediari a valutare l'implementazione nei processi di adeguata verifica a distanza di: a) servizi fiduciari e servizi di identificazione nazionale (SPID e CIE); b) sistemi di video identificazione anche tramite l'utilizzo di video selfie»*.

04 Si rammenta che il GAFI/FATF (*Groupe d'action financière/Financial action task force*) – quale organizzazione intergovernativa fondata nel 1989 su iniziativa del G7 con il precipuo scopo di elaborare e promuovere strategie di contrasto al riciclaggio dei capitali di origine illecita e, a seguito degli attacchi dell'11/09/2001, anche di prevenzione del finanziamento al terrorismo nonché, dal 2008, di contrasto del finanziamento della proliferazione di armi di distruzione di massa – ha, quali compiti principali, di: a) stabilire standard e promuovere un'efficace attuazione delle misure legali, regolamentari e operative per combattere il riciclaggio di denaro, il finanziamento del terrorismo, nonché altre minacce connesse all'integrità del sistema finanziario internazionale; b) elaborare raccomandazioni riconosciute a livello internazionale per l'efficace contrasto delle attività finanziarie illecite; c) analizzare le tecniche e l'evoluzione dei fenomeni in esame; d) valutare e monitorare i sistemi nazionali; e) individuare i Paesi con lacune strategiche nei loro sistemi di AML/CFT (*Anti Money Laundering* e *Combating*

lo scenario dei principi contenuti nelle 40 Raccomandazioni e in particolare nella Raccomandazione n. 10[05], i Governi, i soggetti obbligati e le altre entità interessate, tra cui anche i fornitori di servizi di identità digitale, nella direzione di un migliore e più consapevole utilizzo dell'identificazione digitale nell'ambito dello svolgimento delle procedure di adeguata verifica della clientela[06].

Financing of Terrorism) e fornire al settore finanziario elementi utili per le analisi del rischio da esso condotte. Attesa la rilevanza, nel panorama internazionale, globalmente riconosciuta al GAFI/FATF - costituito da 37 membri, rappresentanti di stati ed organizzazioni regionali, nonché, seppure con la sola qualifica di osservatori, da rilevanti organismi finanziari internazionali e del settore (tra i quali ONU, FMI, Banca mondiale, BCE, Europol, Egmont, Moneyval) - gli stessi Ministri del GAFI/ FATF, in data 12 aprile 2019, hanno, a Washington D.C., approvato il nuovo mandato dell'Organizzazione, estendendone l'applicabilità con durata indeterminata, con l'obiettivo di intensificare gli sforzi volti a tutelare l'integrità e la trasparenza del sistema finanziario internazionale.

05 Le Raccomandazioni emanate dal GAFI/FATF rientrano, come noto, nella categoria degli atti di c.d. *Soft Law*, i quali, seppur privi di efficacia vincolante (*id est*: di immediata cogenza) nei confronti dei destinatari con conseguente assenza di sanzione in caso di loro violazione, presentano tuttavia [per via dell'autorevolezza della Fonte e degli incisivi (quanto "persuasivi") strumenti di "pubblicizzazione" delle proprie determinazioni e dei risultati di indagine ed ispettivi) carattere di forte *moral suasion* e *soft obligation* nei confronti dei destinatari: in altre parole le Raccomandazioni, anche se privi di una vera e propria vincolatività giuridica *strictu sensu*, generano comunque una condizione di subordinazione, tale da condurre i legislatori a tradurle in tradizionali strumenti legislativi/regolamentare di *hard law*.

06 Il GAFI, infatti, sottolinea al riguardo quanto segue. «*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: (i) instaurano un rapporto d'affari; (ii) 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; (iii) vi è sospetto di riciclaggio di denaro o di finanziamento del terrorismo; o (iv) 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*

All'interno della "*Guida*", il GAFI/FATF, a dimostrazione della significatività di tali nuovi fenomeni, quantifica i pagamenti digitali in una percentuale del 12,7% dell'ammontare globale delle transazioni e stima che, entro la fine del 2022, il 60% del PIL mondiale sarà digitalizzato.

Di qui l'indicazione, da parte del predetto Organismo, di individuare *standard* adeguati che consentano di utilizzare sistemi di identificazione digitale in linea tanto con gli *standard* normativi di garanzia statunitensi sull'identità digitale emanati dallo *US National Institute of Standards and Technology* (NIST)[07], quanto con gli *standard* di cui al Regolamento UE 2014/910 *"in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE"*.

Il GAFI/FATF, nella circostanza, rileva, tuttavia, come l'utilizzo di sistemi di identificazione digitale finalizzati al controllo dell'identità e/o all'autenticazione del cliente possano esporre l'intermediario a plurimi profili di rischio, quali quelli derivanti da potenziali attacchi informatico-cibernetici o da furti di identità, in tale ultimo caso al fine di poter trasferire fondi celando l'effettivo beneficiario economico, rendendo, in tal modo, l'utilizzo dei pagamenti elettronici, in termini di tracciabilità, del tutto analogo a quello del contante.

Il GAFI/FATF raccomanda, quindi, l'uso di sistemi d'identificazione digitale sicuri, tali, per un verso, da assicurare l'identificazione e la verifica del cliente nel momento dell'instaurazione del rapporto o della prestazione professionale, essenziali per supportare efficacemente le procedure di *Customer Due Diligence* (CDD), per altro verso, da favorire l'inclusione finanziaria, sì da consentire l'accesso al settore finanziario regolamentato di coloro che, attualmente, risultano esclusi da una molteplicità di servizi finanziari: secondo le stime contenute nel Documento infatti, circa 1,7 miliardi di persone sono oggi escluse dall'accesso a tali servizi ed il 26% di esse non ha la possibilità di accedervi proprio in ragione dell'ostacolo rappresentato dalla mancanza di adeguata documentazione.

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».

07 *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*

Di qui la necessità, segnalata dalla "*Guida*", affinché le autorità governative procedano all'elaborazione di linee guida e regolamenti che permettano l'utilizzo di sistemi di identificazione digitale rispondenti ai requisiti già esistenti e richiesti nell'ambito dell'adeguata verifica della clientela nonché dalla *Customer Due Diligence* e l'auspicio, altresì, che alla luce della Raccomandazione n. 2[08], possa darsi luogo a forme di cooperazione e coordinamento con altre autorità competenti in modo da assicurare che i sistemi di identificazione digitale siano compatibili con l'altrettanta avvertita necessità di protezione dei dati e con le regole sulla privacy[09].

Il GAFI/FAFT infine è dell'opinione che, nonostante gli *standard* indicati nella "*Guida*" vincolino esclusi-

08 Precisa a tale riguardo la Guida: «*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 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*».

09 A tal riguardo, anticipando quanto si dirà più approfonditamente *infra* sub par. 3, si ritiene d'interesse segnalare quanto dichiarato da Ginevra Cerrina Feroni, vice Presidente del Garante per la protezione dei dati personali, a "*Key4biz*" il 14 febbraio 2023, in relazione al rapporto intercorrente tra le tecniche di Intelligenza Artificiale - di cui, *lato sensu*, fanno parte anche i sistemi di rilevazione dati a distanza (es. algoritmi di acquisizione ed elaborazione di dati biometrici) - e la tutela dei dati personali. La vice Presidente afferma, a tale riguardo, che (i) «(s)*in dai primi tentativi di applicazione delle tecnologie d'intelligenza artificiale ai trattamenti di dati personali, il Garante ha compreso il rischio rappresentato dall'esposizione delle persone fisiche (e delle loro vite) a processi di decisione automatizzata basati sulla lettura e l'elaborazione algoritmica di dati, ma anche di meta-dati. Già nella vigenza del Codice pre-novella del 2018 il Garante si era espresso su trattamenti di analisi comportamentale degli utenti di siti commerciali in base alle loro modalità di navigazione online, così come aveva bocciato un sistema di rating reputazionale che, attraverso un processo di data scraping in Rete, attribuiva punteggi e stilava classifiche dei soggetti interessati. Come pure aveva vietato un sistema di lettura biometrica che, montato su totem pubblicitari, registrava sesso, range di età, distanza dal monitor e tempo di permanenza dinanzi ad esso dei passanti che s'imbattevano o s'intrattenevano a guardare uno degli spot proiettati, in modo da calcolare la fascia d'età, il sesso, il grado di attenzione e persino la stima dell'espressione facciale mostrata da differenti target commerciali rispetto ai vari prodotti pubblicizzati. Di fatto il Garante stava già consacrando il principio che di lì a poco sarebbe stato enunciato a chiare lettere dall'art. 22 del GDPR, ovvero il diritto dell'interessato a non essere soggetto ad una decisione basata unicamente su di un trattamento automatizzato, compresa la profilazione, che abbia il potere di produrre effetti giuridicamente rilevanti o, comunque, parimenti significativi sulla sua sfera di vita (si pensi alla concessione di un mutuo, alla definizione di una polizza assicurativa, ad una diagnosi clinica)*» (ii) e che «(n)*el 2021, dopo la Risoluzione del Parlamento europeo sull'intelligenza artificiale, con la presentazione del Regolamento sull'Intelligenza artificiale si è compiuto un passaggio decisivo. L'innovatività non sta solo nell'essere la prima normativa a livello sovraregionale a disciplinare in modo organico l'IA, ma nel sottendere una scelta importante sia in termini regolatori, sia politici che assiologici. La bozza di Regolamento, infatti, implica il tentativo di rimodulare il perimetro del tecnicamente possibile sulla base di quello che si ritiene giuridicamente ed eticamente accettabile*».

vamente i soggetti obbligati, essi, comunque, dovranno rappresentare un punto di riferimento anche per i fornitori di servizi di identificazione digitale *(Digital ID Service Providers)*, posto che essi, nel fornire i propri sistemi alle entità regolamentate, dovranno, inevitabilmente, essere tenuti ad 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.

1. L'impianto AML/CFT ed i suoi capisaldi: l'"adeguata verifica" e la "segnalazione di operazione sospetta"

Nell'ordinamento italiano l'impianto AML/CFT, recependo principi e regole sanciti in ambito internazionale, trova il suo documento cardine nel d.lgs. 21 novembre 2007, n. 231 recante "*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*", nel quale si chiarisce, attraverso le disposizioni di cui all'art. 2, commi 2 e 3, la stretta relazione esistente tra l'attività di prevenzione (e contrasto) di matrice amministrativo-finanziaria [per la quale, nello stesso decreto, vengono dettate «*misure volte a tutelare l'integrità del sistema economico e finanziario e la correttezza dei comportamenti degli operatori tenuti alla loro osservanza*» (art. 2, comma 2)] e l'attività, di matrice investigativo-giudiziaria, di *«repressione dei reati di riciclaggio*[10],

10 Occorre ricordare come l'impianto poliedrico di prevenzione e contrasto e di repressione trovi la propria fonte, sul piano nazionale, in due distinte - sebbene in parte complementari e anche sovrapponibili - definizioni del termine "riciclaggio", l'una, molto articolata, enunciata nell'art. 2, comma 4, del d.lgs. in esame, volta ad avere rilievo sul piano dell'attività di prevenzione (e contrasto) di cui al decreto medesimo, presidiata (quasi interamente) da sanzioni amministrative pecuniarie, l'altra (in senso ampio), anch'essa articolata, prevista dagli artt. 648-*bis* ("*Riciclaggio*"), 648-*ter* ("*Impiego di denaro, beni o utilità di provenienza illecita*"), e 648-*ter 1* ("*Autoriciclaggio*"), secondo le quali, rispettivamente:
in ambito amministrativo
a) «*Ai fini di cui al comma 1, s'intende per riciclaggio: a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attivita' criminosa o da una partecipazione a tale attivita', allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attivita' a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprieta' dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attivita' criminosa o da una partecipazione a tale attivita'; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attivita' criminosa o da una partecipazione a tale attivita'; d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione*»; a cui deve aggiungersi la previsione, contenuta nel successivo art. 2, comma 5, in cui si precisa che il "riciclaggio" «*e' considerato tale anche se le attivita' che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali. La conoscenza, l'intenzione o la finalita', che debbono costituire un elemento delle azioni di cui al comma 4, possono essere dedotte da circostanze di fatto obiettive*»;
in ambito penale

di quelli ad esso presupposti e dei reati di finanziamento del terrorismo[11]».

b) «*Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito* (...)»;
c) «*Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito* (...)»
d) «(...) *chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*».
Va sottolineato come, in nome di una più efficace lotta in materia di ML/FT, sia stato ampliato, ai sensi dell'art. 1, comma 1, lett. d) n. 1 e f) n. 1 del d.lgs. 8 novembre 2021, n. 195, recante "*Attuazione della direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale*", il novero dei reati presupposto, al fine di espandere lo spettro di configurabilità delle ipotesi delittuose contemplate dagli artt. 648-*bis* e 648-*ter* 1 c.p.; ciò è accaduto attraverso la soppressione delle disposizioni che prevedevano la necessità, quale reato presupposto, di un delitto esclusivamente doloso (*rectius "non colposo"*), lasciando così spazio all'introduzione anche di ipotesi di riciclaggio ed autoriciclaggio derivanti da delitti di natura colposa.
Sempre in tale contesto, si segnala come lo stesso d.lgs. 195/2021, ai sensi dell'art. 1, comma 1, lett. d) n. 2 ed f) n. 2, abbia integrato gli artt. 648-*bis* e 648-*ter* 1, introducendo ad entrambi un comma 2 che prevede la configurabilità di tali illeciti penali anche ove il reato presupposto non sia un delitto, bensì una contravvenzione.
Giova evidenziare come le citate fattispecie astratte, sia amministrative sia penali, lungi dal semplificare l'applicazione degli istituti contemplati dal d.lgs. n. 231/2007, finiscano invece, per un verso, per duplicare il quadro normativo a cui fare riferimento ai fini della nozione di riciclaggio, per altro verso, a non avere soltanto rilievo puramente definitorio-terminologico, posto che la nozione di riciclaggio di cui al d.lgs 231/2007, quale immediato parametro per l'applicazione delle previsioni in materia di segnalazione di operazione sospetta, va ad inserirsi all'interno della cornice normativa sanzionatoria pecuniaria di cui alla legge 689/1981, mentre quella di cui al codice penale va ad inserirsi nell'omologo sistema sanzionatorio, per ciascuno dei quali, come noto, vigono regole diverse, specie in ordine alla qualificazione dell'elemento soggettivo dell'autore, necessario ai fini della configurazione delle due diverse ipotesi di responsabilità. Se da un lato, infatti, ai sensi dell'art. 3 l. 689/1981, è sufficiente l'elemento soggettivo rappresentato almeno dalla colpa, affinché sia astrattamente configurabile l'illecito amministrativo, dall'altro, rientrando il reato di riciclaggio nella categoria dei "delitti", è necessario, per la sua configurabilità, che si ravvisi in capo all'autore del fatto l'elemento soggettivo del dolo. A tale ultimo riguardo, si sottolinea come, nonostante alcune locuzioni delle summenzionate fattispecie penalistiche possano indurre, *prima facie*, a ritenere che debba rinvenirsi, ai fini della configurazione dell'illecito penale, l'elemento soggettivo del dolo specifico, la Suprema Corte ha, invece, in più occasioni affermato che, per la giuridica esistenza del reato di riciclaggio, debba ritenersi sufficiente la mera presenza del dolo generico (cfr., *ex multis,* Cass., Sez. IV Pen., 30.1. 2007, n. 6350; Cass., Sez. VI Pen., 18.12. 2007, n. 16980; Cass., Sez. VI Pen., 4.4.2018, n. 38607). In merito alla rilevanza della distinzione tra le due fattispecie di riciclaggio, amministrativa e penale, si segnala quanto sancito dalla Corte di Giustizia, Grande Sezione, con la sentenza del 20.3. 2018 (cause riunite C-596/16 e C-597/16), la quale, in applicazione del principio del *ne bis in idem* di cui all'art. 50 della Carta dei Diritti fondamentali dell'Unione Europea, ha ritenuto che un procedimento sanzionatorio amministrativo pecuniario avente ad oggetto una sanzione di natura "sostanzialmente penale" non possa essere proseguito ove intervenga, con riguardo alla medesima fattispecie fattuale, una sentenza penale definitiva di condanna o di assoluzione.

11 La condotta - riprendendo pedissequamente quanto contenuto nell'art 1, comma 1, lett. d), del d.lgs. 22 giugno 2007, n. 109, recante "*Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attivita' dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE*"- viene definita dall'art. 2, comma 6, del d.lgs. 231/2007, ai sensi del quale «*Ai fini di cui al comma 1, s'intende per finanziamento del terrorismo qualsiasi attivita' diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente*

L'ampia gamma funzionale di siffatte attività [*id est*: di prevenzione e (contrasto) e, altresì, di repressione], unitamente all'ampiezza planetaria dei fenomeni in questione (*id est*: di riciclaggio, finanziamento del terrorismo e dei programmi di proliferazione di armi di distruzione di massa), impongono, a fini di efficacia, la presenza, anzitutto, di una solida ed articolata architettura di vigilanza, che, in collaborazione e cooperazione con le autorità investigativo-giudiziarie, garantisca, al di là degli schemi nazionali, un'efficace azione di prevenzione/contrasto/repressione sui diversi piani internazionale, sovranazionale e nazionale caratterizzata, in uno, da continuità ed omogeneità normativa e operativa.

Di qui la creazione di sistemi e reti (aventi matrice amministrativo-finanziario) di Autorità, di vigilanza e non, sia a livello internazionale (quali, a titolo esemplificativo, il già citato GAFI/FATF, il *Gruppo Egmont*[12]

o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o piu' condotte, con finalita' di terrorismo secondo quanto previsto dalle leggi penali cio' indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette».

12 Il *Gruppo Egmont* - quale organismo globale delle *Financial Intelligence Unit* (FIU) costituito nel 1995 con lo scopo di supportare le prassi operative e la collaborazione a livello internazionale - conta più di 150 FIU aderenti; esso: a) gestisce e sviluppa la rete protetta denominata *Egmont Secure Web* (ESW) utilizzata dalle FIU per lo scambio di informazioni operative; b) promuove lo sviluppo delle FIU; c) ne stimola la collaborazione e il reciproco scambio di informazioni e conoscenze relative a casi di riciclaggio e di finanziamento del terrorismo; d) elabora *standard* e pratiche comuni; e) favorisce la creazione di nuove FIU in paesi che ne sono privi fornendo anche il necessario supporto di natura tecnica. Il *Gruppo Egmont* nel corso del 2015, al fine di meglio far fronte alla minaccia terroristica globale, ha avviato lo sviluppo di un progetto finalizzato ad approfondire le modalità di finanziamento dell'autoproclamato Stato Islamico (ISIS/ISIL) e dei comportamenti finanziari associati ai *foreign terrorist fighters*, a tracciare i profili dell'attività finanziaria dei *foreign terrorist fighters* e ad individuare le reti di supporto ad attività riconducibili all'ISIS/ISIL.

o *Moneyval*[13]), sia a livello sovranazionale (quali, tra le altre, le AEV[14] e la costituenda AMLA[15]) sia, ancora,

13 Il Moneyval (*Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures*) - istituito nel 1997 nell'ambito dello *European Committee on Crime Problems* del Consiglio d'Europa quale organo preposto alle politiche antiriciclaggio nell'ambito del Consiglio d'Europa - svolge attività di *mutual evaluation* dei Paesi membri del Consiglio d'Europa, applicando, in tale quadro, gli standard e la Metodologia del GAFI/FATF.

14 Con tale acronimo si fa riferimento alle Autorità Europee di Vigilanza, nel cui novero si collocano la *European banking authority* (EBA), la *European Insurance and Occupational Pensions Authority* (EIOPA) e la *European Securities and Markets Authority* (ESMA); esse, a livello europeo, assolvono al compito, di fondamentale importanza, di redigere e pubblicare Orientamenti e Linee guida, aventi il fine di fornire indicazioni, nelle aree tematiche di rispettiva competenza, tanto alle Autorità di vigilanza nazionali, quanto ai singoli istituti creditizi o finanziari. Per quanto riguarda l'EBA, ma ciò riguarda anche le altre autorità, il potere di emanare Orientamenti viene riconosciuto espressamente dall'art. 8, paragrafo 2, lett. c), del Reg. Ue 2010/1093, a tenore del quale l'EBA ha il potere *di «c) emanare orientamenti e formulare raccomandazioni secondo le modalità previste all'articolo 16»*. Il perimetro ed i contenuti di tale prerogativa si rinvengono, in particolare, nel paragrafo 1 dello stesso articolo, il quale afferma che l'EBA *«a) contribuisce all'elaborazione di norme e prassi comuni di regolamentazione e vigilanza di elevata qualità, in particolare fornendo pareri alle istituzioni dell'Unione ed elaborando orientamenti, raccomandazioni e progetti di norme tecniche di regolamentazione e di attuazione basati sugli atti legislativi; b) contribuisce all'applicazione uniforme degli atti giuridicamente vincolanti dell'Unione* (sottolineatura nostra)*, in particolare contribuendo ad una cultura comune della vigilanza, assicurando l'applicazione uniforme, efficiente ed efficace degli atti di cui all'articolo 1, paragrafo 2, impedendo l'arbitraggio regolamentare, mediando e risolvendo controversie tra autorità competenti, assicurando una vigilanza efficace e coerente sugli istituti finanziari, garantendo il funzionamento uniforme dei collegi delle autorità di vigilanza e prendendo provvedimenti, anche in situazioni di emergenza»*. Per quanto concerne la vincolatività di tali atti giuridici, essi risultano avere natura di *softt law*; di qui - diversamente da quanto avviene per gli strumenti di *hard law* emanati dall' EBA, quali, ad esempio, la fissazione di *standard* tecnici di regolamentazione e attuazione vincolanti di cui all'art. 10 del già menzionato Reg. Ue 2010/1093 (cfr. D. VESE, *A Game of Thrones: ruolo e poteri dell'autorità bancaria europea alla luce degli orientamenti della Corte di Giustizia,* in *Rivista di Diritto Bancario,* Gennaio-Marzo 2023, pag. 36 ss.) – l'applicazione di quanto sancito dall'art. 16, paragrafo 3, del Reg. 2010/1093, secondo cui «*Le autorità e gli istituti finanziari competenti compiono ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni. Entro due mesi dall'emanazione di un orientamento o di una raccomandazione, ciascuna autorità nazionale di vigilanza competente conferma se è conforme o intende conformarsi all'orientamento o alla raccomandazione in questione. Nel caso in cui un'autorità competente non sia conforme o non intenda conformarsi, ne informa l'Autorità motivando la decisione. L'Autorità pubblica l'informazione secondo cui l'autorità competente non è conforme o non intende conformarsi agli orientamenti o alla raccomandazione. L'Autorità può anche decidere, caso per caso, di pubblicare le ragioni fornite da un'autorità competente riguardo alla mancata conformità all'orientamento o alla raccomandazione in questione. L'autorità competente riceve preliminarmente comunicazione di tale pubblicazione. Ove richiesto dall'orientamento o dalla raccomandazione in questione, gli istituti finanziari riferiscono, in maniera chiara e dettagliata, se si conformano all'orientamento o alla raccomandazione in parola»*. Gli orientamenti pertanto - pur apparendo (almeno formalmente) privi del carattere di cogenza, atteso che le autorità possono, secondo il dettato normativo appena richiamato, decidere, "*motivando la decisione*", di "*non conformarsi*" – acquistano, per prassi istituzionale, il requisito della cogenza, sebbene successivamente allo loro adozione, a seguito, come richiesto, del loro recepimento da parte di specifico atto emanato dall'Autorità nazionale competente.

15 E' l'acronimo della *Anti Money Laundering Authority* (AMLA) che, a breve, rappresenterà il vertice, in chiave europea, di un sistema integrato di controllo costituito da una rete di autorità di vigilanza nazionali AML/CFT in regime di cooperazione e scambio di informazioni. Nel dettaglio, la costituenda Autorità europea dovrà: a) emanare modelli vincolanti per la segnalazione di operazioni sospette; b) gestire la rete di comunicazione sicura tra le UIF (*Fiu.net*) e l'EBA; c) vigilare, secondo il già collaudato sistema di vigilanza europeo adottato in materia di

a livello nazionale[16] e, correlativamente, di Autorità Investigative (a cui si affiancano quelle Giudiziarie)

vigilanza prudenziale per le banche, su un determinato numero di soggetti valutati tanto a seconda del numero di Stati membri in cui operano (almeno sette per gli enti creditizi e almeno dieci per gli altri enti finanziari), quanto in relazione al profilo di rischio intrinseco dell'ente nei diversi Stati, ed il cui elenco varierà ogni 3 anni, a partire dal 2025; d) irrogare sanzioni nei confronti dei soggetti vigilati che risultino essere inadempienti; e) monitorare le autorità di vigilanza nazionale e coordinare le azioni di controllo, attraverso l'istituzione della succitata rete di relazioni, di cui è vertice. L'AMLA, di cui si prevede la creazione nel 2023, entrerà a pieno regime nel 2026 ed avrà un presidente e un direttore esecutivo responsabile della gestione. Il presidente rappresenterà l'Autorità e dirigerà i due organi direttivi collegiali: a) il Comitato Esecutivo, composto dal presidente dell'Autorità e da cinque membri indipendenti permanenti; b) il Consiglio Generale, che avrà due composizioni alternative: una di vigilanza con i direttori delle Autorità pubbliche responsabili della supervisione AML e una con i direttori delle UIF degli Stati membri. Proprio in ragione del peculiare ruolo ricoperto dall'AMLA, non solo i suoi dipendenti dovranno possedere i requisiti di capacità, conoscenze e competenze, ma anche e soprattutto quelli di onorabilità, onestà ed integrità, i quali andranno valutati per svolgere efficacemente le proprie funzioni. La nuova Autorità eserciterà un duplice ruolo: a) di "Supervisione antiriciclaggio" quale "*fulcro di un sistema integrato (…) composto dall'Autorità stessa e dalle autorità nazionali*"; b) di supporto alle analisi e alla cooperazione delle FIU quale "Meccanismo" di coordinamento sovranazionale. Mentre nell'azione di Supervisione la nuova Autorità eserciterà anche competenze dirette ora attribuite alle autorità nazionali, viceversa, nell'attività di cooperazione delle FIU in ambito europeo, i compiti operativi resteranno radicati a livello nazionale; tale ultima circostanza mira, in particolare, a rafforzare l'efficacia delle Unità (FIU) dei singoli Paesi, dando impulso allo svolgimento di analisi congiunte, nei casi di particolare complessità, attraverso la definizione di contenuti, metodi e procedure di lavoro verso cui le FIU dovrebbero convergere.

16 Il d.lgs. 231/2007 descrive l'architettura normativo-istituzionale istituzionale in materia antiriciclaggio e di contrasto al finanziamento del terrorismo, salvaguardando, in particolare, "(…) *la separazione tra funzione politica e autorità tecniche e valorizzando la cooperazione istituzionale sia a livello domestico, sia internazionale. Il Ministro dell'economia e delle finanze è responsabile delle politiche di prevenzione del riciclaggio e del finanziamento del terrorismo. Al fine di dare attuazione a tali politiche, il Ministero dell'economia e finanze promuove la collaborazione tra la UIF, le Autorità di vigilanza di settore, gli ordini professionali e le forze di polizia, nonché tra soggetti pubblici e settore privato.* (…)" Tra le autorità tecniche, a fianco della Banca d'Italia, della Consob dell'IVASS (quali Autorità di vigilanza di settore: cfr. art. 7), un ruolo centrale è assegnato all'Unità di Informazione Finanziaria per l'Italia (UIF), collocata presso la Banca d'Italia in posizione di autonomia e indipendenza (art. 6). «*La UIF riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, principalmente attraverso le segnalazioni di operazioni sospette trasmesse da intermediari, professionisti e operatori non finanziari; effettua l'analisi finanziaria di dette informazioni, utilizzando l'insieme delle fonti e dei poteri di cui dispone e ne valuta la rilevanza ai fini della trasmissione al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza-NSPV e alla Direzione Investigativa Antimafia-DIA, organi competenti per gli accertamenti investigativi* (…) *Le Autorità di vigilanza di settore (Banca d'Italia, Ivass, Consob) provvedono all'emanazione della regolamentazione di rispettiva competenza sui diversi aspetti della materia (adeguata verifica della clientela, conservazione dei dati, organizzazione, procedure e controlli interni) e sovraintendono al rispetto degli obblighi sanciti dalla normativa da parte dei soggetti vigilati, esercitando i connessi poteri sanzionatori. Le amministrazioni e gli organismi interessati presiedono alla verifica sul rispetto degli obblighi da parte dei soggetti non sottoposti al controllo delle autorità di vigilanza di settore*» (cfr., sul punto, il sito web della UIF).

sia internazionali (quale, tra le altre, l'Interpol[17]) sia sovranazionali (quale, tra le le altre, l'Europol[18]) sia

17 *«L›Organizzazione Internazionale di Polizia Criminale (OIPC - Interpol) assume l›attuale configurazione nel 1956, a seguito della formalizzazione della precedente Commissione Internazionale di Polizia Criminale che si riuniva in sessioni annuali, con il compito di: a) assicurare e sviluppare la più ampia assistenza reciproca tra le Autorità di polizia criminale, nel quadro delle leggi esistenti nei diversi Paesi e nello spirito della Dichiarazione Universale dei Diritti dell›Uomo; b) costituire e sviluppare ogni tipo di organismo in grado di contribuire efficacemente alla prevenzione ed alla repressione dei reati di diritto comune. Il funzionamento dell›Organizzazione è regolato dallo Statuto, contenente le norme basilari dell›OIPC, nonché dal Regolamento generale, che riguarda l›applicazione delle disposizioni statutarie. Interpol sviluppa una cooperazione internazionale che si basa su cinque principi fondamentali: a) della sovranità nazionale (art. 2 dello Statuto), secondo il quale ogni attività eseguita su richiesta di un Paese deve essere svolta nel rispetto della legislazione nazionale dello Stato richiesto. Ciò significa che la Polizia di uno Stato può non aderire alla richiesta se l›atto non previsto dalla normativa nazionale; b) del diritto comune (artt. 2 e 3 dello Statuto), in base al quale viene esclusa la cooperazione per quei reati che sono previsti esclusivamente in un ordinamento giuridico nazionale, ovvero abbiano carattere politico, religioso, razziale o militare; c) della universalità, per il quale la cooperazione viene attivata per il solo fatto che i due Stati aderiscono a OIPC; d) del carattere funzionale della cooperazione, che consente di dare luogo alla cooperazione a prescindere dalla collocazione amministrativa dell›organo richiedente; e) della strutturazione senza formalismi, per effetto del quale Interpol agisce senza la necessità di adottare provvedimenti o di redigere atti formali. Come si vede, lo Statuto intende conferire all›attività dell›OIPC la maggiore flessibilità ed estensione possibile, improntando tale tipo di cooperazione alla massima snellezza burocratica funzionalità rispetto all›obiettivo che essa si prefigge, cioè quello di agevolare l›attività al di fuori dei confini nazionali degli organismi che svolgono servizio di polizia. Interpol si articola su una struttura centrale con sede a Lione (Francia) ed una struttura periferica. Quest'ultima è rappresentata dagli Uffici Centrali Nazionali. In Italia tale unità è collocata in seno al Servizio per la Cooperazione Internazionale di Polizia, posto alle dipendenze della Direzione Centrale della Polizia Criminale. La 2^ e la 3^ Divisione del citato servizio sono appunto le strutture italiane di Interpol. Queste ultime, come l›intero Servizio, sono a composizione interforze, per cui l›Arma vi destina propri Ufficiali»* (cfr., sul punto, il sito web del Ministero della Difesa).

18 *«Il trattato sull'Unione europea (Maastricht, 7 febbraio 1992) dedica il Titolo VI alle "Disposizioni relative alla cooperazione nei settori della Giustizia e degli Affari Interni - G.A.I.", prevedendo all'art. 29 che la cooperazione di polizia, finalizzata alla prevenzione ed al contrasto contro il terrorismo ed il traffico di droga dovesse essere sviluppata da parte degli Stati membri attraverso lo scambio di informazioni in seno ad un Ufficio europeo di polizia (Europol). Sulla base di tale disposizione il Consiglio dell'Unione europea, nell'ambito delle competenze fissate dal Trattato di Maastricht relativamente alle materie del Titolo VI, in data 2 giugno 1993 fissava le linee guida dell'European Drugs Unit (EDU) e in data 10 marzo 1995 adottava l'Azione Comune 95/73/GAI, che attribuiva ad EDU compiti di scambio di informazioni tra gli organismi di polizia degli Stati membri e di analisi dei fenomeni criminali di cui all'art. 29 del Trattato, nonché in materia di traffico di materiale radioattivo e di autoveicoli, di immigrazione clandestina e di riciclaggio connesso con le citate attività illecite. Il 26 luglio 1995, gli Stati membri firmavano la Convenzione Europol che istituiva l'Ufficio europeo di polizia, entrata definitivamente in vigore nel luglio del 1999, a seguito della ratifica da parte di tutti i Paesi aderenti. Le funzioni di Europol, infine, sono state rafforzate dal nuovo testo del Trattato sull'Unione Europea (Amsterdam, 2 ottobre 1997) che, nel modificare il Titolo VI, conferisce al Consiglio il potere di promuovere la cooperazione internazionale attraverso l'Ufficio europeo di polizia»* (cfr., sul punto, quanto riportato nel sito web del Ministero della Difesa).

nazionali (quali il Nucleo Speciale di Polizia Valutaria[19] e le Direzioni Investigative Antimafia[20]).

19 Ai sensi dell'art. 9, commi 1-6, del d.lgs. 231/2007, «(i)*l Nucleo speciale di polizia valutaria della Guardia di finanza, nel quadro degli obiettivi e priorita' strategiche individuati annualmente dal Ministro dell'economia e delle finanze con la Direttiva generale per l'azione amministrativa e la gestione, esegue i controlli sull'osservanza delle disposizioni di cui al*
presente decreto da parte dei soggetti obbligati non vigilati dalle Autorita' di vigilanza di settore nonche' gli ulteriori controlli effettuati, in collaborazione con la UIF che ne richieda l'intervento a supporto dell'esercizio delle funzioni di propria competenza. 2. Al fine di garantire economicita' ed efficienza dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, il
Nucleo speciale di polizia valutaria della Guardia di finanza puo' eseguire, previa intesa con le autorita' di vigilanza di settore rispettivamente competenti, i controlli sui seguenti soggetti: a) istituti di pagamento, istituti di moneta elettronica e relative succursali; b) punti di contatto centrale di cui all'articolo 1, comma 2,lettera ii); c) societa' fiduciarie e intermediari di cui all'albo previsto dall' articolo 106 TUB; d) soggetti eroganti micro-credito ai sensi dell'articolo 111 TUB e i confidi e gli altri soggetti di cui all'articolo 112 TUB; e) succursali insediate sul territorio della Repubblica di intermediari bancari e finanziari e di imprese assicurative aventi sede legale e amministrazione centrale in un altro Stato membro o in uno Stato terzo; f) intermediari assicurativi di cui all'articolo 109, comma 2, lettere a), b) e d), CAP, che operano nei rami di attivita' di cui all'articolo 2, comma 1, CAP; g) revisori legali e societa' di revisione legale con incarichi di revisione legale su enti di interesse pubblico o su enti sottoposti a regimi intermedio; h) soggetti che esercitano l'attivita' di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'articolo 134 TULPS, salve le competenze in materia di pubblica sicurezza attribuite dal medesimo Testo Unico. 3. Il Nucleo speciale di polizia valutaria della Guardia di finanza definisce la frequenza e l'intensita' dei controlli e delle ispezioni in funzione del profilo di rischio, della natura e delle dimensioni dei soggetti obbligati e dei rischi nazionali e transfrontalieri di riciclaggio e di finanziamento del terrorismo. 4. Per le finalita' di cui al presente articolo, il Nucleo speciale di polizia valutaria della Guardia di finanza: a) effettua ispezioni e controlli anche con i poteri attribuiti al Corpo dalla normativa valutaria. I medesimi poteri sono attribuiti ai militari appartenenti ai reparti della Guardia di finanza ai quali il Nucleo speciale di polizia valutaria delega le ispezioni e i controlli; ((a-bis) acquisisce, anche attraverso le ispezioni e i controlli di cui ai commi 1 e 2, dati e informazioni presso i soggetti obbligati;)) ((b) con i medesimi poteri di cui alla lettera a), svolge gli approfondimenti investigativi delle informazioni ricevute ai sensi dell'articolo 13 e delle segnalazioni di operazioni sospette trasmesse dalla UIF ai sensi dell'articolo 40.)) 5. Ferme restando le competenze del Nucleo speciale di polizia valutaria di cui al comma 4, la Guardia di finanza: a) accerta e contesta, con le modalita' e nei termini di cui alla legge 24 novembre 1981, n. 689, ovvero trasmette alle autorita' di vigilanza di settore le violazioni degli obblighi di cui al presente decreto riscontrate nell'esercizio dei suoi poteri di controllo; b) espleta le funzioni e i poteri di controllo sull'osservanza delle disposizioni di cui al presente decreto da parte dei soggetti convenzionati e agenti di cui all'articolo 1, comma 2, lettera nn), nonche' da parte dei distributori ed esercenti di gioco, ivi compresi quelli di prestatori di servizi di gioco con sede legale e amministrazione centrale in altro Stato comunitario, che operano sul territorio della Repubblica italiana. 6. Per l'esercizio delle attribuzioni di cui al presente articolo, il Nucleo speciale di polizia valutaria ha accesso: a) ai dati contenuti nella sezione dell'anagrafe tributaria di cui all'articolo 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, 605, come modificato dall'articolo 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248; b) alle informazioni sul titolare effettivo di persone giuridiche e trust espressi, contenute in apposita sezione del registro delle imprese, ai sensi dell'articolo 21 del presente decreto. ((b-bis) ai dati e alle informazioni contenute nell'anagrafe immobiliare integrata di cui all'articolo 19 del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122)».

20 Ai sensi dell'art. 8, comma 1, del d.lgs. 231/2007, «(n)*ell'esercizio delle competenze e nello svolgimento delle funzioni di coordinamento delle indagini e di impulso investigativo ad essa attribuite dalla normativa vigente, la Direzione nazionale antimafia ed antiterrorismo: a) riceve tempestivamente dalla UIF per il tramite del Nucleo speciale di polizia valutaria della Guardia di Finanza ovvero, per quanto attinente alle segnalazioni relative alla criminalita' organizzata, per il tramite della Direzione investigativa antimafia, i dati attinenti alle segnalazioni di*

L'impianto nazionale antiriciclaggio ed antiterrorismo, alla luce del principio dell'"approccio basato sul rischio", si articola, sostanzialmente, nelle due macroaree – costituenti le facce di una stessa medaglia - rappresentate:

1. dalle procedure di "adeguata verifica" della clientela;

2. dal sistema delle "segnalazioni di operazione sospetta" (SOS).

È evidente, d'altra parte, come la prima di dette macroaree sia prodromica al corretto ed efficace svolgimento della seconda, la quale, in assenza di puntuali ed approfondite procedure di adeguata verifica, incontrerebbe serie difficoltà di adeguato svolgimento.

Per quanto qui di interesse, l'adeguata verifica della clientela - da svolgersi, ai sensi dell'art. 17, comma 1, del d.lgs. 231/2007, nelle circostanze ivi indicate e relativamente «*ai rapporti ed alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale* (...)» – prevede, in particolare, ai sensi del successivo art. 18, comma 1, «(...):

(a) l'identificazione del cliente e la verifica della sua identita' sulla base di documenti, dati o informazioni

---

operazioni sospette e relativi ai dati anagrafici dei soggetti segnalati o collegati, necessari per la verifica della loro eventuale attinenza a procedimenti giudiziari in corso, e puo' richiedere ogni altro elemento informativo e di analisi che ritenga di proprio interesse, anche ai fini della potesta' di impulso attribuita al Procuratore Nazionale. A tal fine la Direzione nazionale antimafia e antiterrorismo stipula con la UIF, la Guardia di finanza e la Direzione investigativa antimafia appositi protocolli tecnici, volti a stabilire le modalita' e la tempistica dello scambio di informazioni di cui alla presente lettera, assicurando l'adozione di ogni accorgimento idoneo a tutelare il trattamento in forma anonima dei dati anagrafici, necessari per la verifica della loro eventuale attinenza a procedimenti giudiziari in corso e la riservatezza dell'identita' del segnalante; b) riceve dall'Agenzia delle dogane e dei monopoli tutti i dati e le informazioni necessari all'individuazione di possibili correlazioni tra flussi merceologici a rischio e flussi finanziari sospetti, sulla base di protocolli tecnici, stipulati con la medesima Agenzia, volti a stabilire le modalita' e la tempistica dello scambio di informazioni; c) ferme le disposizioni vigenti in materia di tutela del segreto investigativo, fornisce alla UIF e all'Agenzia delle dogane e dei monopoli tempestivo riscontro in ordine all'utilita' delle informazioni ricevute; d) puo' richiedere alla UIF l'analisi dei flussi finanziari ovvero analisi e studi su singole anomalie, riferibili a ipotesi di utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' della criminalita' organizzata o di finanziamento del terrorismo, su specifici settori dell'economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realta' economiche territoriali; e) ha accesso alle informazioni sul titolare effettivo di persone giuridiche e trust espressi, contenute in apposita sezione del registro delle imprese, ai sensi dell'articolo 21 del presente decreto; f) fornisce al Comitato di sicurezza finanziaria, nel rispetto del segreto di indagine, i dati in suo possesso, utili all'elaborazione dell'analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo di cui all'articolo 14 e le proprie valutazioni sui risultati dell'attivita' di contrasto del riciclaggio e del finanziamento del terrorismo, al fine della elaborazione della relazione di cui all'articolo 5, comma 7; g) puo' richiedere, ai sensi dell'articolo ((371-bis del codice di procedura penale)) alle autorita' di vigilanza di settore ogni altra informazione utile all'esercizio delle proprie attribuzioni».

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;

b) l'identificazione del titolare effettivo e la verifica della sua identita' attraverso l'adozione di misure proporzionate al rischio ivi comprese, con specifico riferimento alla titolarita' effettiva di persone giuridiche, trust e altri istituti e soggetti giuridici affini, le misure che consentano di ricostruire, con ragionevole attendibilita', l'assetto proprietario e di controllo del cliente;

c) l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale, per tali intendendosi, quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative all'attivita' lavorativa, salva la possibilita' di acquisire, in funzione del rischio, ulteriori informazioni, ivi comprese quelle relative alla situazione economico-patrimoniale del cliente, acquisite o possedute in ragione dell'esercizio dell'attivita'. In presenza di un elevato rischio di riciclaggio e di finanziamento del terrorismo, i soggetti obbligati applicano la procedura di acquisizione e valutazione delle predette informazioni anche alle prestazioni o operazioni occasionali; (...)».

In ragione, poi, del livello di rischio connesso al cliente, la procedura di adeguata verifica può essere:

a) semplificata, di cui all'art. 23 del d.lgs. 231/2007[21];

21 «*In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, i soggetti obbligati possono applicare misure di adeguata verifica della clientela semplificate sotto il profilo dell'estensione e della frequenza degli adempimenti prescritti dall'articolo 18. 2. Ai fini dell'applicazione di misure semplificate di adeguata verifica della clientela e fermo l'obbligo di commisurarne l'estensione al rischio in concreto rilevato, i soggetti obbligati tengono conto, tra l'altro, dei seguenti indici di basso rischio: a) indici di rischio relativi a tipologie di clienti quali: 1) societa' ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarita' effettiva; 2) pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea; 3) clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c); b) indici di rischio relativi a tipologie di prodotti, servizi, operazioni o canali di distribuzione quali: 1) contratti di assicurazione vita rientranti nei rami di cui all'articolo 2, comma 1, del CAP, nel caso in cui il premio annuale non ecceda i 1.000 euro o il cui premio unico non sia di importo superiore a 2.500 euro; 2) forme pensionistiche complementari disciplinate dal decreto legislativo 5 dicembre 2005, n. 252, a condizione che esse non prevedano clausole di riscatto diverse da quelle di cui all'articolo 14 del medesimo decreto e che non possano servire da garanzia per un prestito al di fuori delle ipotesi previste dalla legge; 3) regimi di previdenza o sistemi analoghi che versano prestazioni pensionistiche ai dipendenti, in cui i contributi sono versati tramite detrazione dalla retribuzione e che non permettono ai beneficiari di trasferire i propri diritti; 4) prodotti o servizi finanziari che offrono servizi opportunamente definiti e circoscritti a determinate tipologie di clientela, volti a favorire l'inclusione finanziaria; 5) prodotti in cui i rischi di riciclaggio o di finanziamento*

b) rafforzata, di cui al successivo articolo 24[22].

del terrorismo sono mitigati da fattori, quali limiti di spesa o trasparenza della titolarita'; c) ((indici di rischio geografico relativi alla registrazione, alla residenza o allo stabilimento in)): 1) Stati membri; 2) Paesi terzi dotati di efficaci sistemi di prevenzione del riciclaggio e del finanziamento del terrorismo; 3) Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un basso livello di corruzione o di permeabilita' ad altre attivita' criminose; 4) Paesi terzi che, sulla base di fonti attendibili e indipendenti, quali valutazioni reciproche ovvero rapporti di valutazione dettagliata pubblicati, prevedano e diano effettiva applicazione a presidi di prevenzione del riciclaggio e di finanziamento del terrorismo, coerenti con le raccomandazioni del GAFI. 3. Le autorita' di vigilanza di settore, nell'esercizio delle attribuzioni di cui ((all'articolo 7, comma 1, lettera a))), e gli organismi di autoregolamentazione, in conformita' delle regole tecniche di cui all'articolo 11, comma 2, possono individuare ulteriori fattori di rischio da prendere in considerazione al fine di integrare o modificare l'elenco di cui al precedente comma e stabiliscono misure semplificate di adeguata verifica della clientela da adottare in situazioni di basso rischio. Nell'esercizio delle medesime attribuzioni, le autorita' di vigilanza di settore ((possono individuare)) la tipologia delle misure di adeguata verifica semplificata che le banche e gli istituti di moneta elettronica sono autorizzati ad applicare in relazione a prodotti di moneta elettronica, ricorrendo, cumulativamente, le seguenti condizioni: a) lo strumento di pagamento non e' ricaricabile ovvero e' previsto un limite mensile massimo di utilizzo di ((150 euro)) che puo' essere speso solo nel territorio della Repubblica; b) l'importo massimo memorizzato sul dispositivo non supera i ((150 euro)); c) lo strumento di pagamento e' utilizzato esclusivamente per l'acquisto di beni o servizi; d) lo strumento di pagamento non e' alimentato con moneta elettronica anonima; e) l'emittente effettua un controllo sulle operazioni effettuate idoneo a consentire la rilevazione di operazioni anomale o sospette; f) qualora l'importo memorizzato sul dispositivo sia superiore a ((50 euro,)) tale importo non sia rimborsato o ritirato in contanti. ((f-bis) lo strumento di pagamento non e' utilizzato per operazioni di pagamento a distanza, come definite dall'articolo 4, paragrafo 7, della direttiva (UE) 2015/2366, del Parlamento europeo e del Consiglio, del 25 novembre 2015, qualora l'importo dell'operazione e' superiore a 50 euro.)) 4. L'applicazione di obblighi semplificati di adeguata verifica della clientela e' comunque esclusa quando vi e' sospetto diriciclaggio o di finanziamento del terrorismo».

22 «*I soggetti obbligati in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo applicano misure rafforzate di adeguata verifica della clientela. 2. Nell'applicazione di misure rafforzate di adeguata verifica della clientela, i soggetti obbligati tengono conto, almeno dei seguenti fattori: a) fattori di rischio relativi al cliente quali: 1) rapporti continuativi o prestazioni professionali instaurati ovvero eseguiti in circostanze anomale; 2) clienti residenti o aventi sede in aree geografiche ad alto rischio secondo i criteri di cui alla lettera c); 3) strutture qualificabili come veicoli di interposizione patrimoniale; 4) societa' che hanno emesso azioni al portatore o siano partecipate da fiduciari; 5) tipo di attivita' economiche caratterizzate da elevato utilizzo di contante; 6) assetto proprietario della societa' cliente anomalo o eccessivamente complesso data la natura dell'attivita' svolta; b) fattori di rischio relativi a prodotti, servizi, operazioni o canali di distribuzione quali: 1) servizi con un elevato grado di personalizzazione, offerti a una clientela dotata di un patrimonio di rilevante ammontare; 2) prodotti od operazioni che potrebbero favorire l'anonimato; ((3) rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza, non assistiti da procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale;)); 4) pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attivita'; 5) prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso ditecnologie innovative o in evoluzione per prodotti nuovi o preesistenti; ((5-bis) operazioni relative a petrolio, armi, metalli preziosi, prodotti del tabacco, manufatti culturali e altri beni mobili di importanza archeologica, storica, culturale e religiosa di raro valore scientifico, nonche' avorio e specie protette)); c) fattori di rischio geografici quali quelli relativi a: 1) Paesi terzi che, sulla base di fonti attendibili e indipendenti quali valutazioni reciproche ovvero rapporti pubblici di valutazione dettagliata, siano ritenuti carenti di efficaci presidi di prevenzione del riciclaggio e del finanziamento del terrorismo coerenti con le raccomandazioni del GAFI; 2) Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un elevato livello di corruzione o di permeabilita' ad altre attivita' criminose; 3) Paesi soggetti a sanzioni, embargo o misure analoghe emanata dai competenti organismi nazionali e internazionali; 4) Paesi che finanziano o sostengono attivita' terroristiche o nei quali operano organizzazioni*

Nel quadro delle procedure di adeguata verifica assumono, altresì, particolare rilevanza:

a) l'accertamento della "*titolarità effettiva dei clienti diversi dalle persone fisiche*", locuzione questa con la quale si intende, ai sensi dell'art. 20, comma 1, del d.lgs. 21 novembre 2007, n. 231 «*la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo*». Appare superfluo ribadire come l'accertamento della "titolarità effettiva" sia di fondamentale importanza nel quadro delle attività di prevenzione e contrasto AML/CFT, atteso che non sempre, ma anzi, la persona fisica o giuridica che assume la formale qualifica di cliente corrisponde al soggetto nel cui interesse l'operazione e/o le operazioni sono effettuate. È ragionevole infatti ritenere che chi intenda compiere attività di *Money Laundering* o di *Terrorism Financing* ha la necessità di utilizzare un prestanome o ad agire tramite società, o, ancora, attraverso catene societarie nazionali e/o estere; di qui la disposizione di cui all'art. 21 del d.lgs. 231/2007, con cui si recepisce nell'ordinamento nazionale la rilevante statuizione introdotta, nel quadro di un'efficace azione AML/CFT, dalla Direttiva UE 2015/849, consistente nell'obbligo per gli Stati membri di acquisire, in relazione alle operazioni poste in essere dai soggetti obbligati, una serie di informazioni sui titolari effettivi e, anche, di riportarle

terroristiche. 3. Ai fini dell'applicazione di obblighi di adeguata verifica rafforzata della clientela i soggetti obbligati esaminano contesto e finalita' di operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalita' cui le medesime sono, in concreto, preordinate e, in ogni caso, rafforzano il grado e la natura delle verifiche atte adeterminare se le operazioni siano sospette. 4. Le autorita' di vigilanza di settore, nell'esercizio delle attribuzioni di cui ((all'articolo 7, comma 1, lettera a))), e gli organismi di autoregolamentazione, in conformita' delle regole tecniche di cui all'articolo 11, comma 2, possono individuare ulteriori fattori di rischio da prendere in considerazione al fine di integrare o modificare l'elenco di cui al comma 2 e possono stabilire misure rafforzate di adeguata verifica della clientela, ulteriori rispetto a quelle di cui all'articolo 25, da adottare in situazioni di elevato rischio. 5. I soggetti obbligati applicano sempre misure di adeguata verifica rafforzata della clientela in caso di: ((a) rapporti continuativi, prestazioni professionali ed operazioni che coinvolgono paesi terzi ad alto rischio;)) b) rapporti di corrispondenza transfrontalieri ((, che comportano l'esecuzione di pagamenti,)) con un ente creditizio o istituto finanziario corrispondente di un Paese terzo; c) rapporti continuativi, prestazioni professionali o operazioni con clienti e relativi titolari effettivi che siano persone politicamente esposte ((, salve le ipotesi in cui le predette persone politicamente esposte agiscono in veste di organi delle pubbliche amministrazioni. In dette ipotesi, i soggetti obbligati adottano misure di adeguata verifica della clientela commisurate al rischio in concreto rilevato, anche tenuto conto di quanto previsto dall'articolo 23, comma 2, lettera a), n. 2)). 6. I soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo applicano misure di adeguata verifica rafforzata di clienti che, originariamente individuati come persone politicamente esposte, abbiano cessato di rivestire le relative cariche pubbliche da piu' di un anno. La medesima disposizione si applica anche nelle ipotesi in cui il beneficiario della prestazione assicurativa o il titolare effettivo del beneficiario siano state persone politicamente esposte. ((6-bis. I soggetti obbligati valutano, in base al rischio, se applicare misure rafforzate di adeguata verifica nei confronti di succursali o filiazioni, aventi sede in paesi terzi ad alto rischio, controllate da soggetti obbligati aventi sede nel territorio della Repubblica o di altro Stato membro, qualora tali succursali o filiazioni si conformino alle politiche e alle procedure di gruppo, a norma dell'articolo 45 della direttiva.))».

in un registro centrale. Ed è così che nasce la sezione speciale del Registro delle imprese e di quello delle persone giuridiche private, nota come "*registro dei titolari effettivi*", al cui interno è previsto che debbano confluire le informazioni relative alla propria titolarità effettiva[23];

23 L'accesso a questa sezione speciale è consentito non solo alle Autorità pubbliche indicate nel decreto, ma anche a tutti quei soggetti obbligati allo svolgimento dell'adeguata verifica della clientela, purché previo accreditamento e pagamento di diritti di segreteria. Tuttavia la possibilità di conoscere dette informazioni non si arresta ai soggetti appena citati, in quanto, in presenza di condizioni e presupposti, sia pure significativamente stringenti, la conoscenza di alcune delle informazioni contenute nei registri dei titolari effettivi è consentita anche ai soggetti privati, compresi quelli portatori di interessi diffusi, purché non ricorrano le cause di esclusione previste dallo stesso decreto all' art. 21, comma 4, lett. d) bis, vale a dire quando «*l'accesso esponga il titolare effettivo a un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione ovvero qualora il titolare effettivo sia una persona incapace o minore d'età*». L'Unione Europea, con il Regolamento UE 369/2021, ha istituito, a partire dal 22 marzo 2021, il sistema "BORIS" (*Beneficial ownership registers interconnection system*), a cui è affidato, attraverso la piattaforma centrale europea, il servizio centrale di ricerca, avente il compito di interconnettere tra loro i registri centrali nazionali dei titolari effettivi e il portale europeo della giustizia elettronica. Il tema dell'accessibilità a questa sezione speciale, tuttavia, potrebbe presentare, in talune circostanze, profili di criticità, quali quelle evidenziate, da ultimo, dalla Corte di Giustizia dell'Unione Europea (CGUE), la quale, con sentenza della Grande Sezione del 22 novembre 2022, si è soffermata sulla nuova formulazione dell'art. 30, paragrafo 5, della Direttiva UE 2015/849 (così come modificato dall'art. 1, punto 15, lett. c), della Direttiva UE 2018/843), ai sensi del quale «*Gli Stati membri provvedono affinché le informazioni sulla titolarità effettiva siano accessibili in ogni caso: a) alle autorità competenti e alle FIU, senza alcuna restrizione; b) ai soggetti obbligati, nel quadro dell'adeguata verifica della clientela a norma del capo II; c) al pubblico. Le persone di cui alla lettera c) hanno accesso almeno al nome, al mese e anno di nascita, al paese di residenza e alla cittadinanza del titolare effettivo così come alla natura ed entità dell'interesse beneficiario detenuto. Gli Stati membri possono, alle condizioni stabilite dal diritto nazionale, garantire l'accesso a informazioni aggiuntive che consentano l'identificazione del titolare effettivo. Tali informazioni aggiuntive includono almeno la data di nascita o le informazioni di contatto, conformemente alle norme sulla protezione dei dati*». Ad avviso della CGUE, tale disposizione lascia un ampio margine discretivo alla normativa nazionale circa la quantità e la qualità delle informazioni da poter rendere accessibili al pubblico, non ponendo altri limiti se non quelli previsti dalla stessa legislazione nazionale. Secondo la Corte presenta criticità il diritto lussemburghese in quanto l'art. 3, paragrafo 1, della l. 13 gennaio 2019, che istituisce il Registro dei Titolari effettivi, afferma che «*Devono essere iscritte e conservate nel Registro dei titolari effettivi le seguenti informazioni relative ai titolari effettivi degli enti registrati: 1° il cognome; 2° il(i) nome (i); 3° la (o le) cittadinanza (e); 4° la data di nascita; 5° il mese di nascita; 6° l'anno di nascita; 7° il luogo di nascita; 8° il paese di residenza; 9° l'indirizzo privato preciso o l'indirizzo professionale preciso ;10° per gli iscritti nell'anagrafe delle persone fisiche: il numero di identificazione (…); 11° per i non residenti non iscritti nell'anagrafe delle persone fisiche: un numero di identificazione estero; 12° la natura dell'interesse beneficiario detenuto; 13° l'entità dell'interesse beneficiario detenuto*»). Disposizione, questa, ad avviso dei Giudici europei, da ritenersi invalida, in quanto lesiva dell'art. 7 della "Carta di Nizza" secondo cui «(o)*gni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*», da interpretarsi alla luce dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, a tenore del quale «*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*». La legislazione italiana, poiché permette al pubblico di accedere ad un più limitato ambito di informazioni e dati personali, potrebbe, a differenza di quanto accaduto con riguardo al diritto lussemburghese, non dare adito a particolari preoccupazioni in termini di validità delle relative disposizioni. Le riflessioni in argomento sono tuttavia

b) la disposizione di cui all'art. 42 del d.lgs. n. 231/2007, rubricato come "astensione", ai sensi del quale «*1. I soggetti obbligati che si trovano nell'impossibilita' oggettiva di effettuare l'adeguata verifica della clientela, ai sensi delle disposizioni di cui all'articolo 19, comma 1, lettere a), b) e c), si astengono dall'instaurare, eseguire ovvero proseguire il rapporto, la prestazione professionale e le operazioni e valutano se effettuare una segnalazione di operazione sospetta alla UIF a norma dell'articolo 35. 2. I soggetti obbligati si astengono dall'instaurare il rapporto continuativo, eseguire operazioni o prestazioni professionali e pongono fine al rapporto continuativo o alla prestazione professionale gia' in essere di cui siano, direttamente o indirettamente, parte societa' fiduciarie, trust, societa' anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio. Tali misure si applicano anche nei confronti delle ulteriori entita' giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non e' possibile identificare il titolare effettivo ne' verificarne l'identita'. 3. I professionisti sono esonerati dall'obbligo di cui al comma 1, 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'autorita' giudiziaria o in relazione a tale procedimento, compresa la consulenza sull'eventualita' di intentarlo o evitarlo. 4. E' fatta in ogni caso salva l'applicazione dell'articolo 35, comma 2, nei casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto».*

1.1 *Segue: L'Adeguata verifica a distanza: una prospettiva generale*

Con la locuzione "Adeguata verifica a distanza" - potendo essa svolgersi «*senza la compresenza fisica, presso il destinatario, del cliente, dei dipendenti del destinatario o di altro personale incaricato dal destinatario*»[24] - si fa riferimento alle procedure di *Customer Due Diligence* (CDD) che si innestano nei protocolli di c.d "*remote onboarding*", vale a dire a tutte le tipologie di pratiche che permettono (in via generale) l'acquisizione di nuova clientela da parte di enti creditizi e finanziari mediante modalità telematiche.

La possibilità di ricorrere a detta tipologia acquisitiva di clientela, attesi i molteplici vantaggi da essa offerti, era stata, in verità, già prevista dall'art. 1, paragrafo 1, n. 8, lett.a) della Direttiva UE 2018/843 (modificativo dell'art. 13, paragrafo 1, lett. a) della Direttiva Ue 2015/849). Nell'ambito delle attività di

ancora in corso.

24 Cfr., sul punto, Banca d'Italia, Provvedimento 30 luglio 2019 *"Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo"*.

adeguata verifica della clientela è possibile, infatti, «*identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte attendibile e indipendente, compresi, se disponibili, i mezzi di identificazione elettronica o i pertinenti servizi fiduciari di cui al regolamento (UE) n. 910/2014*[25] *del Parlamento europeo e del Consiglio o altre procedure di identificazione a distanza o elettronica sicure, regolamentate, riconosciute, approvate o accettate dalle autorità nazionali competenti*». La Pandemia da Covid-19, segnalando la "*necessità di un distanziamento sociale*", ha, poi, incrementato esponenzialmente l'utilizzo degli strumenti di che trattasi, richiedendo «(...) *un utilizzo massivo di strumenti di colloquio a distanza che, se correttamente utilizzati, consent*(issero) *di agevolare l'esecuzione di molte operazioni senza ricorrere alla presenza fisica e quindi contribuendo alla sicurezza sanitaria sia degli operatori che degli utenti*»[26].

Detti strumenti, nonostante la molteplicità di aspetti positivi, non sono tuttavia esente da rischi, in particolar modo connessi all'aumento in progressione geometrica dei tentativi di frode, potenzialmente idonei, già *ex se*, a compromettere, attesa la rilevanza del processo identificativo, i sistemi di *Anti Money Laundering* (AML) e *Combating the Financing of Terrorism* (CFT).

Di qui la *ratio* che ha spinto UE, Stati Membri ed Autorità indipendenti ad adottare provvedimenti che, lungi dallo scoraggiare il ricorso a tali pratiche, ne cogliessero invece, in uno, i potenziali vantaggi e ne mitigassero i rischi, atteso che, «*data l›evoluzione della tecnologia* (...)», «(...) *le transazioni dei clienti svolte "non faccia a faccia"*[27] *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*»[28].

1.1.2. *Segue: Contesto eurounitario*

Negli ultimi anni si è assistito ad un'imponente produzione documentale finalizzata a garantire il sem-

25 Si fa riferimento, a titolo esemplificativo, a firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, *etc.*.

26 Cfr., sul punto, G. ARCELLA, L. PIFFARETTI e M. MANENTE, *Studio 2bis-2020/b: L'identificazione non in presenza fisica nel contrasto al riciclaggio ed al terrorismo internazionale dopo il d.l. "Semplificazioni" n.76/2020 convertito con legge n. 120/2020*, in *www.consiglionazionaledelnotariato.it*, del 18.11. 2020.

27 Detta locuzione viene utilizzata per definire quelle attività che avvengono a distanza e si svolgono attraverso mezzi digitali o altri strumenti remoti, come la posta o il telefono.

28 Cfr. GAFI, *Guida all'identità digitale*, marzo 2020, pag. 30.

pre migliore sfruttamento dei sistemi di *remote onboarding*, ricercando, al contempo, di incrementarne maggiormente gli elementi di vantaggio e di marginalizzarne i profili di vulnerabilità.

A tale riguardo, un primo ed importante documento da prendere in considerazione è la *"Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa a una strategia in materia di finanza digitale per l'UE"*, datata 24.9.2020, con la quale si dichiara apertamente:

1. che «*Il futuro della finanza è digitale: i consumatori e le imprese hanno sempre più accesso a servizi finanziari in modalità digitale, partecipanti al mercato innovativi mettono in campo nuove tecnologie e i modelli di business già esistenti stanno cambiando*»;

2. che «*una porzione crescente di pagamenti presso i punti vendita è ora effettuata tramite tecnologie digitali e senza contatto fisico, e gli acquisti online (e-commerce) hanno registrato un forte aumento*».

Prosegue, poi, la Comunicazione rilevando come «(s)*oluzioni di tecnologia finanziaria (FinTech)* (abbiano) *contribuito ad ampliare e accelerare l'accesso ai prestiti, compresi quelli finanziati dal governo in risposta alla crisi di COVID19. Anche garantire l'operatività sicura e affidabile delle infrastrutture digitali ha acquisito più importanza, alla luce dell'aumento dell'accesso ai servizi finanziari online e del fatto che i dipendenti del settore finanziario lavorano essi stessi a distanza*». La Commissione - dimostrando piena consapevolezza dei notevoli vantaggi derivanti da un'ordinata, fors'anche non totale, transizione digitale, di cui fa espressa menzione[29] - segnala l'opportunità che,

29 «*Le nostre consultazioni con i portatori di interessi in tutta Europa hanno rilevato un ampio e forte sostegno per tale obiettivo, sulla base di molteplici motivazioni:*
- *scegliere la via della finanza digitale stimolerebbe l'innovazione e creerebbe opportunità per lo sviluppo di prodotti finanziari migliori per i consumatori, compresi i cittadini attualmente impossibilitati ad accedere a servizi finanziari. Ciò dischiude nuove modalità per veicolare i finanziamenti alle imprese dell'UE, in particolare alle PMI;*
- *promuovere la finanza digitale pertanto sosterrebbe la strategia di ripresa dell'economia europea e favorirebbe una più ampia trasformazione economica. Aprirebbe nuovi canali alla mobilitazione di fondi a sostegno del Green Deal e della nuova strategia industriale per l'Europa;*
- *alla luce del suo carattere transfrontaliero, la finanza digitale ha anche il potenziale per incrementare l'integrazione del mercato finanziario nell'Unione bancaria e nell'Unione dei mercati dei capitali 11 e dunque per rafforzare l'Unione economica e monetaria europea;*
- *infine, un solido e vibrante settore finanziario digitale a livello europeo rafforzerebbe la capacità dell'Europa di mantenere e consolidare la nostra autonomia strategica aperta nell'ambito dei servizi finanziari e, di conseguenza, la nostra capacità di disciplinare il sistema finanziario e vigilare su di esso al fine di preservare la stabilità finanziaria dell'Europa e i nostri valori*».

entro il 2024, «(...) *l'UE attui un solido quadro normativo che permetta l'utilizzo di soluzioni interoperabili per l'identità digitale, così da consentire ai nuovi clienti di accedere ai servizi finanziari in modo rapido e semplice ("onboarding"). È opportuno che tale quadro sia basato su norme in materia di antiriciclaggio (AML) e di contrasto del finanziamento del terrorismo (CFT) più armonizzate*».

Posta la fondamentale importanza che siffatta transizione digitale ricopre, quale obiettivo strategico dell'UE, considerata altresì la centralità del ruolo che, in quest'ottica, riveste l'armonizzazione delle procedure di adeguata verifica a distanza in ambito AML/CFT, non stupisce affatto che la Commissione abbia, poi, invitata «*l›Autorità bancaria europea (ABE) a elaborare orientamenti in stretto coordinamento con le altre autorità europee di vigilanza entro il terzo trimestre del 2021* (...)»; e ciò al fine di garantire «(...) *una maggiore convergenza sugli elementi relativi all'identificazione e alla verifica necessari per l'onboarding, nonché sulle modalità e i limiti nell'ambito dei quali i fornitori di servizi finanziari sono autorizzati ad affidare i processi di adeguata verifica della clientela a terzi, inclusi altri fornitori di servizi finanziari*».

L'invito della Commissione all'EBA risulta, d'altronde, facilmente comprensibile, atteso che la Direttiva, poiché oggetto di successivo recepimento negli ordinamenti nazionali, avrebbe inevitabilmente dato adito ad eterogeneità normativa, con ogni intuibile conseguenza in termini di efficacia del presidio ritenuto, dalla stessa Commissione, di estrema rilevanza (anche per via dei profili tecnici correlati).

Le Linee Guida, tuttavia - muovendosi (come si vedrà) nell'ottica della c.d. "neutralità tecnologica" e, perciò, non dettando specifiche istruzioni in ambito di *software*, piattaforme, programmi *etc.*, ma limitandosi, in quanto Linee Guida, ad indicare, anche a beneficio delle Autorità nazionali, regole di condotta, più o meno puntuali, in tema di CDD connessa al *remote onboarding* – necessiteranno, ad iniziativa di queste ultime, di ulteriori disposizioni di dettaglio.

1.1.3. *Segue: Le nuove Linee Guida EBA*

In data 22 novembre 2022, l'Autorità Bancaria Europea ha, infine, pubblicato le proprie "*Linee Guida sull'utilizzo delle soluzioni di remote onboarding dei clienti ai sensi dell'art. 13, paragrafo 1, della Direttiva UE 2015/849*", la cui entrata in vigore è prevista decorsi 6 mesi dall'avvenuta traduzione delle stesse in tutte le lingue ufficiali dell'Unione; la prevista traduzione è, allo stato, ancora da completarsi.

Le Linee Guida, come già segnalato (cfr. *sub* nota n. 14), non rappresentano, ad onta del *nomen*, delle mere indicazioni da osservarsi discrezionalmente da parte degli Stati dell'Unione; esse, all'incontro, sono dotate, nei termini già rappresentati, di efficacia negli ordinamenti nazionali, sancendo infatti

l'art. 16, paragrafo 3, del Reg. UE n. 2010/1093, che «(l)*e autorità e gli istituti finanziari competenti compiono ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni*».

Le Linee Guida, inoltre, poiché finalizzate a determinare un più profittevole utilizzo degli strumenti di *remote onboarding,* sfruttandone al massimo i vantaggi e marginalizzandone il più possibile i rischi, vanno ad integrare altri (già emanati) Documenti quali:

1. gli "*Orientamenti sulla governance interna*" (EBA/GL/2017/11);
2. gli *"Orientamenti in materia di esternalizzazione"* (EBA/GL/2019/02);
3. gli *"Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza*" (EBA/GL/2019/04)
4. gli "*Orientamenti ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 849/2015 sulle misure di adeguata verifica della clientela e sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo associati ai singoli rapporti continuativi e alle operazioni occasionali («Orientamenti relativi ai fattori di rischio di ML/TF»), che abrogano e sostituiscono gli orientamenti JC/2017/37 (EBA/GL/2021/02)*".

1.1.3 a) *Segue: L'adozione di politiche e procedure interne*

In conformità con quanto sancito dall'art. 13, paragrafo 1, lett. a) e c), della Direttiva 2015/849, come modificato dalla Direttiva 2018/843, le Linee Guida precisano che l'ente finanziario o creditizio è tenuto ad adottare politiche e procedure interne al fine di marginalizzare i rischi connessi all'utilizzo delle soluzioni di *remote onboarding*. Tali soggetti, in particolare, devono:

1. descrivere le soluzioni di *remote onboarding* poste in essere dall'ente, ponendo particolare attenzione a specificare le modalità di acquisizione e trattamento dei dati personali del cliente, tanto nel processo di *remote onboarding,* quanto in quello di CDD; in tale quadro vanno, altresì, dichiarate le procedure di valutazione del rischio, specificando i fattori da prendere maggiormente in considerazione;
2. dichiarare quali fasi siano automatizzate e quali richiedano interventi manuali;

3. dichiarare i controlli di CDD adottati;

4. dichiarare i previsti programmi di introduzione e formazione costante del personale al fine di rendere più efficaci le attività di CDD[30].

Le Linee Guida, di fatto, si pongono, in attesa delle ulteriori disposizioni di attuazione da parte delle Autorità nazionali, quale strumento di puntualizzazione di quanto – quale mera cornica normativa e perciò senz' alcuna pretesa di dettaglio – è già contenuto, in tema di identificazione a distanza, nella Quinta Direttiva Antiriciclaggio, secondo cui, come già ricordato, occorre «*identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte attendibile e indipendente, compresi, se disponibili, i mezzi di identificazione elettronica o i pertinenti servizi fiduciari di cui al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio o altre procedure di identificazione a distanza o elettronica sicure, regolamentate, riconosciute, approvate o accettate dalle autorità nazionali competenti*».

1.1.3 b) *Segue: Valutazione preliminare e successive integrazioni della soluzione di remote onboarding nel sistema dei controlli interni*

Data la già menzionata pluralità di vantaggi offerti dall'utilizzo delle soluzioni di *remote onboarding* della clientela, è prevedibile, oltre che auspicabile, che, nel corso dei mesi a venire, si possa assistere ad un sempre più frequente utilizzo, da parte degli istituti bancari e finanziari, di tali soluzioni.

A tale proposito le Linee Guida specificano che, ove l'ente bancario e/o finanziario decidesse di utilizzare dette procedure, esso dovrebbe anzitutto valutare, prim'ancora di avvalersene, la loro adeguatezza, affidabilità e idoneità a garantire un efficace e sicuro svolgimento dell'attività in discorso.

L'istituto a questo proposito, precisano le Linee Guida, dovrebbe:

1. valutare l'adeguatezza della soluzione, specie in relazione alla completezza ed all'accuratezza dei dati oggetto di raccolta, con specifico *focus* sulle fonti da cui si trarrebbero alcune informazioni (quali, come meglio si dirà *infra*, l'utilizzo di banche dati);

30 I programmi di formazione, oltre ai profili normativi inerenti alle procedure di che trattasi, dovranno, più specificamente, orientarsi verso le soluzioni tecniche adottate, in modo da permetterne un'adeguata, efficace e sicura conduzione.

2. valutare l'impatto della scelta sulla rischiosità interna, specie di AML e di CFT;

3. effettuare *Stress-test*, in particolar modo incentrati sulle possibili vulnerabilità delle *Information and Communication Technologies* (ICT) utilizzate e prevedere le conseguenti, idonee misure mitigative. Sul punto si suggerisce agli enti bancari e finanziari l'utilizzo di regimi di identificazione elettronica, di cui si fa menzione anche all'art. 9 del Regolamento UE 2014/910, oppure di servizi fiduciari che, in base all'art. 24, paragrafo 1, lett. b), del medesimo Regolamento, si svolgano «*a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato* (sia) *stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisf*(i)*no i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia "significativo" o "elevato"*».

In aggiunta, gli enti citati, dovrebbero, non solo essere in grado di dimostrare dette risultanze positive alle Autorità di vigilanza competenti – formalizzazione, questa, da osservarsi in via generale da parte dell'ente, quale misura atta a dimostrare (quanto meno) l'adeguatezza del processo di valutazione condotto, con riguardo a qualsivoglia altra procedura aziendale - ma dovrebbero anche essere consapevoli di poter procedere all'utilizzo della soluzione di *remote onboarding* esclusivamente ove risultino possibili ulteriori aggiornamenti ed implementazioni della soluzione stessa. Gli enti, anche in ragione della costante ed incessante evoluzione delle soluzioni tecniche disponibili, dovrebbero infatti monitorare costantemente la soluzione di *remote onboarding*, ivi compresi i suoi profili tecnici, ed integrarla laddove risulti via via necessario, al fine di garantire un'effettiva e puntuale mitigazione dei rischi.

Segnatamente, essi dovrebbero almeno:

1. descrivere le misure, le modalità e la portata delle operazioni di revisione ed aggiornamento periodiche;

2. aggiornare la soluzione qualora si presentassero, per esempio:

   - Modifiche di esposizione al rischio di ML o FT;
   - Carenze nel funzionamento della soluzione;
   - Modifiche del quadro normativo in esame;
   - Aumento dei tentativi percepiti di frode.

In aggiunta, in un contesto come quello appena descritto, sarà necessario, da parte dell'ente, definire le procedure di integrazione e modifica, specie nei casi in cui dovesse emergere una vulnerabilità del sistema, che si traduca, a titolo esemplificativo, in una minore efficienza dell'attività di CDD.

Al fine di prevenire il verificarsi di tali ipotesi, le Linee Guida suggeriscono anche di eseguire test di garanzia della qualità oppure rapporti periodici sull'efficienza dei servizi informatici, ovvero ancora test a campione sulla tenuta dei sistemi[31].

1.1.3 c) *Segue: Identificazione, acquisizione delle informazioni e verifica dell'identità e dell'integrità dei documenti e dell'identità dei clienti*

Come facilmente intuibile, il rigore procedurale riguardante la verifica della clientela in regime di *remote onboarding* risulta essere, rispetto alla verifica in presenza, di gran lunga maggiore, tant'è che l'istituto, a titolo esemplificativo, deve interrompere la procedura nel caso in cui venissero identificate carenze tecniche o interruzioni della connessione.

Le Linee Guida prescrivono, in proposito, che l'istituto debba indicare le procedure e le politiche adottate nell'attività di acquisizione delle informazioni necessarie per l'identificazione del cliente e debba, altresì, garantire sia il soddisfacimento degli *standard* legali della CDD sia la qualità delle immagini e dei suoni (*id est*: la loro idoneità a riconoscere in modo inequivocabile il cliente). Indice di idoneità dell'attività a standard e Best Practice è rappresentato dall'utilizzo, da parte dell'ente, di regimi di identificazione elettronica di cui si fa anche menzione all'art. 9 del Regolamento UE 2014/910 o anche di servizi fiduciari che, in base all'art. 24, paragrafo 1, lett. b), del Regolamento medesimo, si svolgano «*a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato (sia) stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisf*(i)*no i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia "significativo" o "elevato"*».

Tutte le informazioni acquisite, inoltre, devono soddisfare le *Best Practice* in materia di *data protection*.

Le procedure di identificazione sono naturalmente differenti a seconda che il cliente sia una persona

31 Per un più puntuale esame della tematica relativa a valutazione pre-implementazione della soluzione di *remote onboarding*, nonché della valutazione costante *in itinere*, cfr. E. MORLINI, Slide presentate nel corso del Webinar "*Adeguata verifica a distanza: nuove Linee guida EBA*", organizzato, in modalità telematica, dalla rivista *"DB Non solo Diritto Bancario"* in data 7 febbraio 2023.

fisica o giuridica: se si tratta di persona fisica, l'istituto può procedere sulla base della documentazione fornita e rapportarla alle informazioni visibili[32], mentre se si tratta di persona giuridica, l'istituto deve, ove possibile, effettuare riscontri presso pubblici registri, al fine di verificare che la persona fisica preposta sia legittimata a rappresentare e ad assumere obbligazioni in nome e conto della persona giuridica.

Analizzando più nel dettaglio le due fattispecie, a mente delle Linee Guida, gli enti creditizi e finanziari, per ciò che concerne le persone fisiche, debbono dichiarare quali informazioni:

1. saranno oggetto di inserimento manuale da parte del cliente;
2. saranno acquisite in modalità automatica sulla base della documentazione messa a disposizione dal cliente;
3. saranno acquisite a seguito dell'esame di altre fonti esterne o interne.

Quanto, invece, al *remote onboarding* di persone giuridiche, gli istituti creditizi o finanziari devono assicurarsi che la soluzione adottata disponga di specifiche funzioni di raccolta di:

1. dati e documentazione pertinenti per identificare e verificare la persona giuridica;
2. dati e documentazione pertinenti per verificare che la persona fisica, che agisce in nome e per conto della persona giuridica, sia legalmente autorizzata a farlo;
3. informazioni connesse all'identificazione dei titolari effettivi[33].

Oltre a tali modalità, è permesso agli enti di procedere, ai fini del riconoscimento, anche attraverso captazione di dati biometrici; gli enti, tuttavia, devono assicurarsi che i dati richiesti a fini identificativi siano sufficientemente univoci ed inequivocabilmente collegati ad un'unica persona e che, inoltre, vengano utilizzati programmi in grado di captare (nella maniera più accurata possibile) i summenzionati dati. Ove ciò non fosse possibile, è allora necessario proseguire l'attività di verifica con ulteriori modalità di controllo, probabilisticamente incentrati su una verifica in presenza (*rectius*: "faccia a faccia"

32 A titolo esemplificativo, se il soggetto dovesse allegare un documento d'identità corredato di immagine identificativa, l'ente potrebbe confrontare la foto riportata sul documento con le immagini acquisite nel corso della procedura di *remote onboarding*.

33 Cfr., in ordine a tale nozione, sub note n. 6 e 23.

secondo la terminologia utilizzata dal GAFI/FATF nella già citata "*Guida all'identità digitale*").

Le procedure di *remote onboarding* possono classificarsi differentemente, come "presidiate" e "non presidiate", a seconda che il cliente vada a relazionarsi e ad interagire o meno con un dipendente dell'ente: ove il rapporto s'instauri con un dipendente si parla di "*remote onboarding presidiato*" mentre si parla di "*remote onboarding non presidiato*" nel caso opposto.

Con riguardo all'ipotesi di "*remote onboarding presidiato*", le Linee Guida prevedono che l'ente debba almeno:

1. richiedere che la qualità dell'immagine o dell'audio sia sufficiente a consentire una corretta verifica dell'identità del cliente;

2. assicurarsi che il dipendente sia in possesso di sufficienti conoscenze in tema di normativa AML e di aspetti di sicurezza nella verifica a distanza;

3. prevedere la predisposizione di una guida al colloquio utile per rilevare eventuali comportamenti sospetti.

Per quanto riguarda, invece, la soluzione di "*remote onboarding non presidiato*", l'ente deve, almeno:

a) richiedere che video e foto siano girati o scattate al momento della verifica ed effettuati con la dovuta illuminazione, sì da garantire una più semplice identificazione del soggetto;

b) eseguire verifiche di rilevamento della presenza in modo da assicurarsi che il cliente sia presente nel corso della sessione di comunicazione.

Le Linee Guida, in aggiunta, nella prospettiva di rendere le attività di verifica e controllo quanto più stringenti possibile, suggeriscono agli istituti di utilizzare procedure di *remote onboarding* che, di volta in volta, inseriscano casualmente le azioni da compiere, di modo che sia più complesso favorire fenomeni di coercizione o di utilizzo di identità sintetiche. Esse consigliano, altresì, l'attribuzione in capo ai dipendenti responsabili di funzioni casuali variabili, sì da rendere più difficili eventuali fenomeni collusivi.

Nella quasi totalità dei casi, come intuibile, l'istituto - trovandosi nell'impossibilità di consultare documentazione originale, bensì esclusivamente riproduzioni di quest'ultima - deve verificare l'autenticità

dei documenti, al fine di accertare se la riproduzione sia o meno fedele. L'ente dunque dovrebbe, quantomeno:

1. utilizzare, se possibile, il confronto con specifiche banche dati;

2. essere in grado di comprendere se dati o immagine sono stati manomessi.

Qualora poi venissero adoperati specifici sistemi atti a leggere in modo automatico le informazioni, quali, ad esempio, algoritmi di riconoscimento ottico dei caratteri (OCR) o verifiche delle zone a lettura automatica (MRZ), è necessario che l'ente adotti ogni idonea attività e/o misura disponibile affinché detti sistemi catturino le informazioni in modo accurato e coerente.

1.1.3 d) *Segue: Affidamento dell'adeguata verifica a terzi ed esternalizzazione*

Si tratta dell'ipotesi in cui il procedimento di adeguata verifica a distanza sia affidato dall'istituto a soggetti terzi ovvero sia esternalizzato.

Per quanto concerne l'affidamento a terzi della CDD, le Linee Guida prescrivono la contestuale necessità di:

a) accertarsi che i processi e le procedure di CDD da parte di costoro siano in linea con quanto prescritto nelle Linee Guida;

b) garantire la continuità dei rapporti commerciali tra cliente ed istituto di credito o finanziario.

Quanto, invece, all'esternalizzazione della CDD, l'intermediario deve adottare tutte le misure idonee a:

a) garantire che il fornitore applichi le politiche e le procedure di acquisizione dei dati relativi al *remote onboarding* sancite dall'intermediario e previste nell'accordo di esternalizzazione;

b) effettuare le necessarie valutazioni al fine di garantire che il fornitore sia in grado di eseguire il processo di *remote onboarding*, attraverso, ad esempio, test di vulnerabilità dei sistemi usati dal fornitore o valutazioni sulla formazione dei dipendenti o della *governance* dello stesso;

c) garantire che il fornitore informi l'ente creditizio o finanziario in caso di proposte di modifiche al processo di *remote onboarding* o di modifiche dello stesso ad opera del fornitore.

Al contempo l'ente, deve assicurarsi, ove il fornitore dovesse trovarsi nella condizione di memorizzare

i dati dei clienti, che:

a) vengano raccolti e conservati solo i dati in linea con un sistema chiaramente definito;

b) l'accesso ai dati sia strettamente limitato e registrato;

c) siano implementate le misure di *data protection.*

Si segnala infine che, in caso di esternalizzazione, tanto l'intermediario quanto il fornitore dovranno far riferimento non solo a quanto disposto nelle Linee Guida, ma anche a quanto contenuto nelle già menzionate Linee Guida EBA sugli accordi di esternalizzazione (EBA/GL/2019/04).

2. Applicazione dell'adeguata verifica a distanza nel contesto nazionale: il Provvedimento della Banca d'Italia 30 luglio 2019 e il Regolamento IVASS n. 44 del 12 febbraio 2019

In attesa che le nuove Linee Guida EBA in tema di adeguata verifica a distanza entrino formalmente in vigore, si ritiene utile soffermarsi, con riguardo alla medesima materia, su quanto contenuto:

- nel Provvedimento della Banca d'Italia del 30 luglio 2019[34], emanato ai sensi dell'art. 19, comma 1, lettera a), n. 5 del d.lgs. 21 novembre 2007, n. 231 (come modificato ai sensi dell'art. 2, comma 1, del decreto legislativo 25 maggio 2017, n. 90), in cui è precisato che l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, per coloro «(...) *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)*[35], *tenendo conto dell'evoluzione delle tecniche di identificazione a distanza*»;

- nel Regolamento IVASS n. 44 del 12 febbraio 2019 "*recante disposizioni attuative volte a prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, ai sensi dell'articolo 7, comma 1, lettera a) del decreto legislativo 21 novembre 2007, n. 231.*"

34 "*Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*".

35 «*Adottano nei confronti dei soggetti rispettivamente vigilati, disposizioni di attuazione del presente decreto in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela*».

In ordine al Provvedimento della Banca d'Italia del 30 luglio 2019

Come si è avuto modo di chiarire in precedenza, la verifica a distanza vede come elemento essenziale l'assenza di alcuna presenza fisica, presso il destinatario, del cliente, dei dipendenti del destinatario o di altro personale incaricato dal destinatario, svolgendosi attraverso le *Information and Communication Technologies (*ICT), sul cui ruolo e sulla cui necessaria protezione in tema di *Cybersecurity* si dirà *infra*.

La Banca d'Italia nel citato Provvedimento precisa, in particolare, che «(n)*ei casi di operatività a distanza, i destinatari:*

1. *acquisiscono i dati identificativi del cliente e dell'esecutore e ne effettuano il riscontro su una copia – ottenuta tramite fax, posta, in formato elettronico o con modalità analoghe – di un valido documento di identità, ai sensi della normativa vigente;*

2. *effettuano riscontri ulteriori rispetto a quelli previsti dalla Sezione V sui dati acquisiti, secondo le modalità più opportune in relazione al rischio specifico. A titolo esemplificativo, si indicano le seguenti modalità: contatto telefonico su utenza fissa (welcome call); invio di comunicazioni a un domicilio fisico con ricevuta di ritorno; bonifico effettuato dal cliente attraverso un intermediario bancario e finanziario con sede in Italia o in un paese comunitario; richiesta di invio di documentazione controfirmata; verifica su residenza, domicilio, attività svolta, tramite richieste di informazioni ai competenti uffici ovvero mediante incontri in loco, effettuati avvalendosi di personale proprio o di terzi. Nel rispetto dell'approccio basato sul rischio, i destinatari possono utilizzare meccanismi di riscontro basati su soluzioni tecnologiche innovative e affidabili (es., quelle che prevedono forme di riconoscimento biometrico), purché assistite da robusti presidi di sicurezza* (enfasi nostra)*;*

3. *individuano, nel documento di policy antiriciclaggio, gli specifici meccanismi di cui intendono avvalersi per effettuare le attività di riscontro sub b) ed illustrano le valutazioni condotte dalla funzione antiriciclaggio sui profili di rischio che caratterizzano ciascuno di questi strumenti e sui relativi presidi di sicurezza*» (enfasi nostra).

Precisazione che si ritiene di fondamentale rilevanza è che quanto appena riportato deve intendersi non un tassativo elenco di pratiche procedurali ed applicazioni tecnologiche prefissate, quanto una soglia minima al di sotto della quale non può (e non deve) collocarsi il livello di sicurezza delle soluzioni di CDD connesse al *remote onboarding*. Ne discende che devono ritenersi consentiti (ed anzi suspica-

ti) rafforzamenti nell'impianto, sia organizzativo sia tecnico, di adeguata verifica a distanza, specie in considerazione della costante e tumultuosa evoluzione dei mezzi informatici[36], al fine di costantemente assicurare l'affidabilità e la sicurezza delle stesse procedure.

L'Autorità di Vigilanza permette, in aggiunta, che, «(i)*n alternativa a quanto previsto sub a), b), c), l'identificazione del cliente-persona fisica* (possa) *essere effettuata dai destinatari in digitale da remoto secondo la procedura di registrazione audio/video disciplinata nell'Allegato 3*», nella quale è dettagliata la "Procedura di video-identificazione", relativamente alla quale è previsto che i destinatari realizzino un sistema che garantisca, preliminarmente all'instaurazione della sessione audio o video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati; l'Allegato richiede, altresì, al fine di facilitare l'utilizzo e l'accessibilità da parte del cliente, che la procedura ivi prevista garantisca l'utilizzo di applicativi orientati all'intuitività.

E' richiesto, altresì, che l'identificazione da remoto, effettuata dall'operatore addetto alla video-identificazione, «*rispetti le seguenti condizioni:*

1. *le immagini video sono a colori e consentono una visualizzazione chiara dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;*

2. *l'audio è chiaramente udibile, privo di distorsioni o disturbi evidenti;*

3. *la sessione audio/video, che ha ad oggetto le immagini video e l'audio del cliente e dell'operatore, è effettuata in ambienti privi di particolari elementi di disturbo*».

I destinatari sono tenuti ad assicurare che l'operatore preposto all'attività si astenga dall'avviare il processo di identificazione o lo sospenda quando la qualità audio/video è scarsa o ritenuta non adeguata a consentire l'identificazione del cliente.

36 Si pensi all'uso, da parte della clientela, delle VPN (*Virtual Private Network*), consistente in una rete privata virtuale che - per mezzo di un canale di comunicazione riservato (c.d. tunnel VPN), creato in sovrapposizione ad un'infrastruttura di rete pubblica, nonché di specifiche procedure di autenticazione e di una articolata crittografia - garantisce privacy, anonimato e sicurezza. Detta soluzione tecnologica potrebbe, tuttavia, rappresentare un vero e proprio elemento di rischio per l'integrità e l'efficacia dei sistemi e degli algoritmi utilizzati dagli enti finanziari e creditizi nell'ambito dell'adeguata verifica a distanza, in quanto, *ex multis*, idonea a celare l'indirizzo IP (*Internet Protocol Address*), con conseguente impossibilità di individuare l'effettivo luogo di connessione del cliente o aspirante tale (un soggetto, ad esempio, potrebbe falsamente dichiarare, supportato dalla localizzazione dell'indirizzo IP, di trovarsi in un determinato luogo, in tal modo celando la sua vera collocazione geografica, con ogni conseguente considerazione in termini di potenziale rischiosità dell'avvenuta identificazione).

Nell'Allegato si prevede, poi, che «*l'operatore che effettua l'identificazione:*

1. *acquisisc*(a) *i dati identificativi forniti dal cliente;*
2. *richied*(a) *l'esibizione di un documento d'identità valido, munito di fotografia recente e riconoscibile e di firma autografa del richiedente, rilasciato da un'amministrazione pubblica;*
3. *verific*(hi) *il codice fiscale tramite la tessera sanitaria in corso di validità. Del documento viene acquisita copia in formato elettronico*».

A fini di sicurezza, l'Allegato prevede, non solo che l'operatore che effettua l'identificazione possa escludere (o interrompere se avviata) l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal cliente, ma anche che la sessione audio/video sia interamente registrata e conservata. In aggiunta, è anche prevista la conservazione della documentazione relativa alle informazioni e ai documenti raccolti nel corso dell'attività di registrazione, posto che gli enti sono tenuti infatti a conservare, con modalità conformi alle previsioni previste dal decreto antiriciclaggio[37], i dati di registrazione nonché l'esplicita volontà manifestata dal cliente di

37 Si fa riferimento agli artt. da 31 a 34 del d.lgs 231/2007, i quali, rispettivamente, dispongono che:
Art. 31 «*I soggetti obbligati conservano i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attivita' di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dalla UIF o da altra Autorita' competente. 2. Per le finalita' di cui al comma 1, i soggetti obbligati conservano copia dei documenti acquisiti in occasione dell'adeguata verifica della clientela e l'originale ovvero copia avente efficacia probatoria ai sensi della normativa vigente, delle scritture e registrazioni inerenti le operazioni. La documentazione conservata deve consentire, quanto meno, di ricostruire univocamente: a) la data di instaurazione del rapporto continuativo o del conferimento dell'incarico; b) 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;((b-bis) la consultazione, ove effettuata, dei registri di cui all'articolo 21, con le modalita' ivi previste)); c) la data, l'importo e la causale dell'operazione; d) i mezzi di pagamento utilizzati. 3. I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale*»;
Art. 32 «*((1. I soggetti obbligati adottano sistemi di conservazione dei documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonche' il trattamento dei medesimi esclusivamente per le finalita' di cui al presente decreto. 2. Le modalita' di conservazione adottate devono prevenire qualsiasi perdita dei dati e delle informazioni ed essere idonee a garantire la ricostruzione dell'operativita' o attivita' del cliente nonche' l'indicazione esplicita dei soggetti legittimati ad alimentare il sistema di conservazione e accedere ai dati e alle informazioni ivi conservati. Le predette modalita' devono, altresi', assicurare: a) l'accessibilita' completa e tempestiva ai dati e alle informazioni da parte delle autorita' di cui all'articolo 21, comma 4, lettera a); b) la tempestiva acquisizione, da parte del soggetto obbligato, dei documenti, dei dati e delle informazioni, con indicazione della relativa data. E' considerata tempestiva l'acquisizione conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione*

instaurare il rapporto continuativo, memorizzati in file audio-video, immagini e metadati strutturati in formato elettronico.

Gli enti sono tenuti a richiedere il consenso al trattamento dei dati personali contenuti nelle riprese audio-video, ponendo attenzione, a tale proposito, alla completezza dell'informativa da rendere all'interessato, prevista dalle disposizioni in materia di protezione dei dati personali.

L'Allegato evidenzia, altresì, la necessità che «*la sessione audio*/video (sia) *condotta seguendo una procedura scritta e formalizzata dai destinatari* (enfasi nostra)", la quale preveda (almeno) che:

1. *l'operatore acquisisc*(a) *il consenso alla videoregistrazione e alla sua conservazione e* inform(i) *che la videoregistrazione sarà conservata in modalità protetta;*

2. *l'operatore dichiar*(i) *le proprie generalità;*

3. *il cliente* conferm(i) *i propri dati identificativi;*

---

professionale, dall'esecuzione dell'operazione o della prestazione professionale, dalla variazione e dalla chiusura del rapporto continuativo o della prestazione professionale; c) l'integrita' dei dati e delle informazioni e la non alterabilita' dei medesimi successivamente alla loro acquisizione; d) la trasparenza, la completezza e la chiarezza dei dati e delle informazioni nonche' il mantenimento della storicita' dei medesimi. 3. I soggetti obbligati possono avvalersi, per la conservazione dei documenti, dei dati e delle informazioni, di un autonomo centro di servizi, ferma restando la responsabilita' del soggetto obbligato e purche' sia assicurato a quest'ultimo l'accesso diretto e immediato al sistema di conservazione.))»;
Art. 33 « *Gli intermediari bancari e finanziari, ad esclusione di quelli di cui all'articolo 3, comma 2, ((lettere i), o), p), q) e v))), nonche' le societa' fiduciarie di cui all'articolo 3, comma 3, lettera a), trasmettono alla UIF dati aggregati concernenti la propria operativita', al fine di consentire l'effettuazione di analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali. 2. La UIF individua le tipologie di dati da trasmettere, le modalita' e la cadenza della loro trasmissione e verifica il rispetto dell'obbligo di cui al presente articolo, anche mediante accesso diretto ai dati e alle informazioni conservate dall'intermediario bancario o finanziario o dalla societa' fiduciaria»;*
Art. 34 «*(1. Nel rispetto del vigente quadro di attribuzioni e competenze,i dati e le informazioni conservate secondo le norme di cui al presente Capo sono utilizzabili a fini fiscali. 2. Il fascicolo del cliente, conforme a quanto prescritto dagli articoli 31 e 32, e la custodia dei documenti, delle attestazioni e degli atti presso il notaio nonche' la tenuta dei repertori notarili, a norma della legge 16 febbraio 1913, n. 89, del regolamento di cui al regio decreto 10 settembre 1914, n. 1326, e successive modificazioni, e la descrizione dei mezzi di pagamento ai sensi dell'articolo 35, comma 22, decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248 costituiscono idonea modalita' di conservazione dei dati e delle informazioni. 3. Fermo quanto stabilito dalle disposizioni di cui al presente decreto per le finalita' di prevenzione del riciclaggio e di finanziamento del terrorismo, nel rispetto dei principi di semplificazione, economicita' ed efficienza, le Autorita' di vigilanza di settore, a supporto delle rispettive funzioni, possono adottare disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni relativi ai clienti, contenuti in archivi informatizzati, ivi compresi quelli gia' istituiti presso i soggetti rispettivamente vigilati, alla data di entrata in vigore del presente articolo.))».*

4. *il cliente conferm*(i) *la data e l'ora della registrazione;*

5. *il cliente* conferm(i) *di voler instaurare il rapporto continuativo e conferm*(i) *i dati identificativi e gli altri dati inseriti nella modulistica on-line in fase di pre-registrazione;*

6. *il cliente* conferm(i) *il proprio numero di telefonia mobile e l'indi,rizzo mail;*

7. *l'operatore invi*(i) *un messaggio che il cliente espone al dispositivo di ripresa o il cui contenuto è comunicato all'operatore e una mail all'indirizzo di posta elettronica dichiarato dal cliente, con un link ad una URL appositamente predisposta per la verifica;*

8. *l'operatore* chied(a) *al cliente di inquadrare, fronte e retro, il documento di riconoscimento utilizzato, e si assicur*(i) *che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni ivi contenute (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante). Del documento viene acquisita copia elettronica;*

9. *l'operatore chied*(a) *di mostrare, fronte e retro, la tessera sanitaria su cui è riportato il codice fiscale del cliente;*

10. *l'operatore chied*(a) *al cliente di compiere una o più azioni casuali per rafforzare l'autenticità della interlocuzione;*

11. *l'operatore riassum*(a) *sinteticamente la volontà espressa dal cliente di voler instaurare il rapporto continuativo e ne raccoglie conferma».*

Qualora dovessero emergere dubbi, incertezze o incongruenze nell'identificazione del cliente, i destinatari debbono effettuare ulteriori riscontri, quali, a titolo esemplificativo, la consultazione del sistema pubblico per la prevenzione del furto di identità, disciplinato dal d.lgs. 11 aprile 2011, n. 64 (recante *"Ulteriori modifiche ed integrazioni al decreto legislativo 13 agosto 2010, n. 141, per l' istituzione di un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identita'"*).

Il Provvedimento della Banca d'Italia del 30 luglio 2019 fin qui illustrato, pur presentandosi sufficientemente esaustivo alla luce delle previsioni di rango sovranazionale e nazionale attualmente in vigore, dovrà, a breve, essere rivisto, dovendosi armonizzare, con riguardo ad alcuni profili integrativi e/o inno-

vativi, con le sopra illustrate Linee Guida EBA[38].

In ordine al Regolamento IVASS n. 44 del 12 febbraio 2019

La tematica in esame, molto più sinteticamente rispetto all'illustrato Provvedimento della Banca d'Italia del 30 luglio 2019, viene affrontata nell'art. 39 del predetto Regolamento rubricato come "*Operatività a distanza*". Tale disposizione, dopo aver chiarito, al comma 1, che «*Per operatività a distanza si intende quella svolta dal cliente o dal beneficiario, anche attraverso i sistemi di comunicazione telefonica o informatica, senza la presenza fisica di questi ultimi presso le imprese o gli intermediari assicurativi o gli intermediari assicurativi stabiliti senza succursale (...)*», affronta, più in dettaglio, le modalità di conduzione della procedura, concentrandosi, al contempo, tanto sugli obblighi in capo all'impresa, considerata nella sua accezione strutturale, quanto sulle linee di condotta a cui il personale della stessa deve attenersi nel corso della procedura.

I commi 2-5 e 9-10, in particolare, si soffermano sugli obblighi gravanti in capo all'Impresa-struttura, affermando, rispettivamente,

- che «2. *Le imprese presidiano il rischio che venga compromessa l'attendibilità dei dati raccolti in assenza di contatto diretto con il cliente, il beneficiario o con gli esecutori, anche tramite frodi connesse al furto di identità elettronica; a tal fine: a) riscontrano i dati identificativi del cliente attraverso una copia del documento di identità, ottenuta tramite fax , posta, anche elettronica, o con modalità analoghe; b) svolgono ulteriori verifiche dei dati acquisiti secondo le modalità ritenute più*

38 A titolo esemplificativo, se da un lato, a mezzo del Provvedimento in discorso, la Banca d'Italia «*pone in capo agli intermediari un generico onere di definire e formalizzare (nel documento di policy antiriciclaggio) procedure di adeguata verifica della clientela sufficientemente dettagliate e di individuare quelle maggiormente adeguate al rischio ed alle esigenze dell'intermediario stesso, senza tuttavia indicare quali dovrebbero essere gli elementi che dovrebbero orientare la scelta*», dall'altro «*l'EBA dice qualcosa in più. L'EBA specifica che gli intermediari dovrebbero tenere traccia delle fasi, dei requisiti e delle valutazioni preliminari alla scelta, che dovrebbero includere almeno: a) una valutazione sull'adeguatezza della soluzione in ordine alla completezza ed all'accuratezza dei dati e dei documenti da raccogliere, nonché dell'attendibilità e indipendenza delle fonti di informazione che utilizzate; b) una valutazione sull'impatto dell'utilizzo della soluzione scelta sui rischi a livello aziendale, compresi i rischi ML/TF, operativi, reputazionali; c) l'individuazione delle possibili misure di mitigazione e delle azioni correttive per ciascuno dei rischi di cui sopra; d) l'individuazione, e conseguente effettuazione, di test per valutare se la soluzione scelta possa esporsi a frodi (così come delineato dalla previsione 43 delle Linee guida EBA in materia di ICT e security risk management); e) la previsione di un test end-to-end sulla compatibilità della soluzione scelta con la tipologia di clientela, prodotti e servizi offerti dall'intermediario*» (cfr., sul punto, T. ATRIGNA, Slide presentate nel corso del Webinar "*Adeguata verifica a distanza: nuove Linee guida EBA*", organizzato, in modalità telematica, dalla rivista *"DB Non solo Diritto Bancario"* in data 7 febbraio 2023).

idonee in relazione al profilo di rischio associato al cliente. 3. Se l'impresa non è in grado di ottenere i dati e le informazioni indicate non dà corso all'operazione, non avvia il rapporto continuativo ovvero pone in essere le limitazioni al rapporto già in essere previste dall'articolo 42, comma 2, e valuta se inviare una segnalazione di operazione sospetta. 4. L'impresa tiene la stessa condotta anche quando non riesce a verificare l'attendibilità degli stessi dati o ad avere certezza circa la coincidenza fra il cliente da identificare e il soggetto cui si riferiscono i dati e le informazioni trasmesse ovvero se dalle verifiche effettuate e dalle misure adottate emerge la falsità o l'incoerenza delle informazioni fornite a distanza. 5. L'impresa può identificare il cliente o il beneficiario, in caso di persone fisiche, anche da remoto tramite strumenti digitali di registrazione audio/video, purché sia utilizzato un sistema che garantisca la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente»

- e che «*9.L'impresa definisce una procedura scritta per condurre la sessione audio/video, prevedendo: a) l'acquisizione del consenso alla videoregistrazione e alla sua conservazione e dell'esplicita volontà del cliente di instaurare il rapporto continuativo; b) la conferma della data e dell'ora della registrazione, del numero di telefonia mobile e dell'indirizzo di posta elettronica, dei dati identificativi e degli altri dati inseriti in moduli antecedentemente compilati in forma elettronica da parte del cliente; c) la dichiarazione da parte del personale delle proprie generalità; d) l'inquadratura del messaggio inoltrato dall'impresa al numero di telefonia mobile dichiarato, del fronte e del retro del documento di riconoscimento e del codice fiscale esibiti; e) la conferma dell'indirizzo di posta elettronica dichiarato tramite accesso all'indirizzo 50 Pag. 38/53 14980/19 appositamente predisposto per la verifica. 10. Le imprese conservano i dati di registrazione memorizzati in file audio-video, immagini e metadati strutturati in formato elettronico con modalità conformi alle previsioni in materia di conservazione di dati, documenti e informazioni, previsti dal decreto antiriciclaggio*».

Per quanto concerne, invece, le linee di condotta che il personale deve seguire, esse sono trattate nei commi 6-8, i quali precisano *che «6.Il personale addetto effettua la video-identificazione da remoto, a condizione che: a) le immagini video siano a colori e consentano una chiara visualizzazione dell'interlocutore, in termini di luminosità, nitidezza, contrasto, fluidità delle immagini; b) l'audio sia chiaramente udibile, privo di distorsioni o disturbi; c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del cliente e dell'operatore, sia effettuata in ambienti privi di elementi di disturbo. 7. Nel corso della video-identificazione il personale richiede l'esibizione di un valido documento d'identità, di cui viene*

acquisita copia non modificabile in formato elettronico. 8. Il personale incaricato si astiene dall'avviare il processo di identificazione o lo sospende nel caso in cui la qualità dell'audio o del video, inclusa quella riferita al documento esibito, siano scarse o non adeguate a consentire l'identificazione del cliente o del beneficiario».

3. Cybersecurity e Protezione dei Dati

Le "*Linee Guida Eba*" in materia di *remote onboarding* si inseriscono, come già ricordato, nella Strategia di finanza digitale per l'UE rappresentata dalla Commissione al Parlamento UE nel settembre 2020, posto che le procedure di *Customer Due Diligence* (CDD) relative al *remote onboarding* si svolgono attraverso piattaforme telematiche ed ICT. Di qui il centrale ruolo, anche con riguardo alla *Customer Due Diligence* (CDD), della tematica, da tempo all'attenzione dell'Autorità, dei mercati, degli operatori, della Cybersicurezza[39], nonché della correlata tematica, solo apparentemente antagonista[40], della Protezione dei Dati.

Nel suesposto contesto viene, quindi, in considerazione anche il diritto alla Protezione dei Dati sancito, in primo luogo, dall'art. 16, paragrafo 1, del TFUE, secondo cui «*Ogni persona ha diritto alla protezione*

39 Termine, questo, che l'art. 1, comma 1, lett. a), del d.l. 14 giugno 2021, n. 82, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*, definisce come «*l›insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l›integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell›interesse nazionale nello spazio cibernetico*».

40 Il diritto che funge da contraltare rispetto alla cybersicurezza è, come intuibile, la protezione dei dati personali, configurandosi, in tal modo, una sorta di rivalità insanabile tra l'Autorità per la Cybersicurezza Nazionale (ACN) ed il Garante per la Protezione dei Dati personali (GPDP), la quale, tuttavia, risulta essere solo apparente, non foss'altro perché entrambe le Autorità, in quanto pubbliche, risultano perseguire finalità di interesse collettivo. Infatti, come da un lato non potrebbe dirsi esistente qualsivoglia diritto di libertà ove non fossero garantiti contestualmente la sicurezza e l'ordine pubblico, dall'altro non potrebbe dirsi effettivo il diritto alla Protezione dei Dati personali in un contesto di totale assenza di cybersicurezza. Quanto appena affermato trova d'altra conferma nella circostanza che, ove l'ACN non operasse al fine di potenziare le misure di sicurezza cibernetica e, altresì, al fine di rafforzare la resilienza delle infrastrutture digitali, si rischierebbe di dover assistere, sul piano della Protezione dei Dati personali, a scenari non proprio rassicuranti. È sufficiente pensare, infatti, alle innumerevoli banche dati, pubbliche o private che siano, oggetto, per le finalità più disparate, di potenziali aggressioni cybernetiche, potendosi, in taluni casi, anche mettere a repentaglio la sicurezza nazionale. Si evince, dunque, chiaramente come il diritto alla Protezione dei Dati personali, oggi più che mai, non si limiti ad una mera dimensione individuale, ma si estenda fino a ricomprendere il più alto livello collettivo-nazionale: la sempre più rapida digitalizzazione, infatti, ha posto fuori dal controllo delle Autorità Nazionali ed Internazionali la odierna principale infrastruttura attraverso cui transitano i dati personali, rappresentata dal web, ed in particolar modo, dai *social network*.

dei dati di carattere personale che la riguardano», e dell'art. 8 della Carta dei diritti fondamentali dell'Unione, secondo il quale *«Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano»*, e, in secondo luogo, dal Regolamento UE n. 2016/679 (GDPR), nel cui art. 4 viene fornita la defizione dei "dati di carattere personale" consistenti in «(q)*ualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*»; elementi, tutti (o, comunque, per buona parte), utilizzati e/o utilizzabili ai fini dello svolgimento dell'attività di adeguata verifica della clientela.

La necessità di garantire una vera e propria Protezione dei Dati di cui si viene in possesso non passa, tuttavia, esclusivamente attraverso le canoniche previsioni del GDPR, quali, a titolo esemplificativo, i divieti di vendita a soggetti terzi o di diffusione presso il pubblico dei dati medesimi, quanto anche (e soprattutto) attraverso la *data protection* offerta dai sistemi di sicurezza informatica degli enti creditizi e finanziari nei confronti di possibili incursioni *hacker* e *data breach*, sempre più frequenti ed aggressive[41] in danno, senz'alcuna distinzione, di infrastrutture digitali pubbliche e di istituzioni private d'impresa[42].

Il collegamento tra la sicurezza dei sistemi informatici e la tutela dei dati personali si può spiegare attraverso il grande valore economico che questi ultimi rivestono nel contesto economico globale attuale, specie in ragione del loro peso commerciale e politico[43].

41 Secondo l'ultimo rapporto CLUSIT, «(n)*el 2020 gli attacchi con impatto "Critico" rappresentavano il 14% del totale, quelli di livello "Alto" il 36%, quelli di livello "Medio" il 32% ed infine quelli di livello "Basso" il 19%. Complessivamente, gli attacchi gravi con effetti molto importanti (High) o devastanti (Critical) nel 2020 erano il 50% del campione. Nel 2021 la situazione è molto diversa e francamente impressionante: gli attacchi gravi con effetti molto importanti (High) sono il 47%, quelli devastanti (Critical) rappresentano il 32%, quelli di impatto significativo (Medium) il 19%, e quelli con impatto basso solo il 2%. In questo caso gli attacchi con impatto Critical e High sono il 79%*».

42 Le aggressioni, mirate a colpire la *supply chain* (id est: la catena di distribuzione) di imprese di interesse nazionale ovvero di PPAA, pur risultando, per ovvie ragioni, più complesse ciberneticamente rispetto a quelle da muovere nei confronti di un privato cittadino, appaiono essere tuttavia più attrattive e, anche, potenzialmente più profittevoli.

43 A tale riguardo è possibile, a titolo esemplificativo, fare riferimento alla vicenda "Cambridge Analytica". Quest'ultima, fondata nel 2013 con lo scopo ultimo di occuparsi delle strategie di comunicazione politica per finalità elettorali, quale filiale della società britannica SCL Group, si occupava prevalentemente di *big data* e *data mining*, Essa, attraverso l'esercizio di dette attività, aveva sintetizzato vari modelli comportamentali-psicologici relativi alle diverse tipologie di utenti che navigavano in rete. La divisione di Cambridge Analytica – che è stata artefice di plurime campagne elettorali in molteplici Paesi (tra cui quella presidenziale di Donald Trump nel 2016 e, nello stesso

La conseguenza più immediata è che banche dati di dimensioni rilevanti, quali possono essere quelle di enti creditizi o finanziari, sono bersagli estremamente appetibili per i professionisti del *cybercrime*, i quali, non solo potrebbero rivendere le informazioni ottenute a terzi, ma, come sempre più frequentemente accade, potrebbero estorcere denaro tanto per la "restituzione" dei dati sottratti, quanto per liberare da vincoli, da essi apposti, i sistemi informatici dell'ente[44].

In aggiunta è necessario sottolineare come, in una società sempre più digitalmente interconnessa, sia piuttosto semplice, da parte dei professionisti del *cybercrime*, arrecare danni, partendo dalla sottrazione dei dati di singoli soggetti privati, a soggetti strategicamente rilevanti per l'interesse nazionale, definiti, dall'art. 3 del d.lgs. 65/2018, "*Operatori di servizi essenziali*", vale a dire «*soggett(i) pubblic(i) o privat(i), della tipologia di cui all'allegato II*[45]*, che soddisfa i criteri di cui all'articolo 4, comma 2*[46]», nel cui ambito rientrano gli intermediari bancari e finanziari, in quanto fornitori di servizi essenziali per il mantenimento di attività economiche fondamentali.

Di qui le ragioni della prevista vigilanza sull'adeguatezza della sicurezza informatica dei sistemi degli enti creditizi e finanziari, in quanto Operatori di servizi essenziali, da parte della nuova Agenzia per la Cybersicurezza Nazionale (ACN), istituita ai sensi artt. 5-9 del d.l. 82/2021 (convertito, con modificazioni, nella L. 4 agosto 2021, n. 109), che si concretizza in attività di matrice consulenziale, ispettiva e

anno, quella *pro-Brexit*) - è stata resa celebre per via di un enorme scandalo relativo alla commercializzazione dei dati personali.

44 La maggior parte delle incursioni risulta condotta attraverso *ransoware,* vale a dire attraverso una specifica tipologia di virus che rende inaccessibili i file dei *device* infettati, al fine di richiedere, in cambio del loro ripristino, utilità di vario genere (denaro, criptovalute, etc.): così facendo, il *cybercrime* riesce a finanziarsi adeguatamente potenziando il proprio potenziale aggressivo cibernetico ed instaurando un vero e proprio circolo vizioso di incursioni sempre più devastanti seguiti da riscatti sempre più elevati. Secondo quanto affermato dal "*Rapporto Clusit 2022 sulla sicurezza ICT in Italia*", nell'anno 2018 l'utilizzo di *ransomware* rappresentava il 23% dei complessivi *malware*, nel 2019 raggiungevano il 46%, nel 2020 arrivavano al 67% con un numero di 220 attacchi, mentre nel 2021 la misura arrivava quasi al 75%. Lo stesso Rapporto afferma che *«il C.N.A.I.P.I.C. (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche), ha gestito 256 eventi ransomware (contro i 220 del 2020), di cui 61 contro Infrastrutture Critiche (IC), Operatori di Servizi Essenziali (OSE) e Piccole Amministrazioni Locali (PAL) e 195 attacchi ad aziende»*..

45 L'allegato prende in considerazione i seguenti settori: a) Energia (1. Energia Elettrica, 2. Petrolio, 3. Gas); b) Trasporti (1. Trasporto aereo, 2. Trasporto ferroviario, 3. Trasporto via acqua, 4. Trasporto su strada); c) Settore bancario; d) Infrastrutture dei mercati finanziari; e) Settore Sanitario; f) Forniture e distribuzione di acqua potabile; g) Infrastrutture digitali.

46 I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti: a) un soggetto fornisce un servizio che e' essenziale per il mantenimento di attivita' sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

sanzionatoria.

E' necessario, altresì, evidenziare come, nell'ambito dell'adeguata verifica a distanza, la cybersicurezza rilevi anche sotto un ulteriore profilo, rappresentato dalla tutela dell'integrità dei *server*, delle reti di connessione e, più genericamente, del sistema informatico-cibernetico di cui risultano dotati gli istituti di credito o finanziari[47].

È, infatti, ragionevole immaginare la possibilità che un professionista del *cybercrime* possa, con sufficiente facilità, aggirare i sistemi di sicurezza approntati dai citati istituti, ove essi non siano in linea con *standard* e *Best practice* internazionali, al fine di ledere, tra gli altri, i presidi antiriciclaggio, così da aprire una breccia nell'intero sistema AML/CFT: appare ipotizzabile, a titolo d'esempio, l'inserimento illegale di falsa documentazione nella banca dati degli intermediari o, anche, la modificazione di contenuti della documentazione già presente all'interno delle suddette banche dati (*id est*: importi di operazioni; localizzazioni geografiche, etc.).

47 A riprova della rilevanza rivestita dal tema della Cybersicurezza in relazione al mondo della finanza, è possibile citare quanto dichiarato dalla Consob nel Comunicato stampa *"Cybersecurity e società quotate: Sec, Esma e Consob a confronto sulla disciplina di trasparenza Ciocca: valutare se la resilienza agli attacchi hacker debba entrare nella reportistica periodica L'Autorità Usa per una comunicazione obbligatoria e non discrezionale Il punto oggi e domani all'Università Cattolica"*, all'interno del quale si precisa che «*Le società quotate in Borsa dovrebbero prepararsi ad includere le informazioni sulla cybersecurity nella rendicontazione periodica obbligatoria resa al mercato, perché gli investitori hanno interesse a sapere quanto l'impresa in cui investono i propri soldi sia robusta o vulnerabile rispetto al rischio di attacchi hacker. È questa la posizione espressa da Luna Bloom della Sec (Securities and Exchange Commission), l'autorità di regolamentazione e di vigilanza sui mercati finanziari degli Stati Uniti, intervenendo al convegno "Cybersecurity, market disclosure & industry" in corso oggi e domani all'Università Cattolica del Sacro Cuore. I rischi cyber sono in crescita e hanno subito un'accelerazione a seguito della digitalizzazione dell'economia e della finanza, con forti impatti operativi, legali e reputazionali sulle società quotate, ha osservato Bloom. È cruciale dotarsi di regole stringenti e di competenze nei CdA delle quotate, ha aggiunto Bloom, secondo cui la trasparenza in materia di cybersecurity deve essere obbligatoria e non discrezionale. "Il rischio cyber ha un potenziale impatto sistemico", ha osservato Paolo Ciocca, Commissario Consob. "La questione non è se dare l'informazione, ma quando darla, come darla e cosa dire al mercato. Questo pone un onere a carico dei CdA". "Una divulgazione di informazioni sulla cybersecurity, coerente, comparabile e orientata alle decisioni, metterebbe gli investitori – ha commentato Elena Beccalli, preside della Facoltà di Scienze bancarie, finanziarie e assicurative della Cattolica - in una posizione migliore per comprendere rischi e incidenti". "La pandemia, la guerra in Ucraina e il frequente ricorso a fornitori esternalizzati hanno aumentato la minaccia di rischi sistemici", ha osservato, invece, Alexander Harris dell'Esma, secondo cui è necessaria la collaborazione tra regolatori e gli altri attori del mercato. Per i mercati finanziari dell'Unione Europea sarebbe un radicale cambiamento di prospettiva. Ad oggi, infatti, gli attacchi hacker sono soggetti alla disciplina di trasparenza degli eventi price sensitive. Questo significa che devono essere resi noti solo se e quando si verifica l'emergenza. È la stessa società, inoltre, a valutare se l'episodio sia oppure no di interesse per il mercato e in quali tempi eventualmente comunicare. Se le proposte della Sec fossero recepite anche in ambito Ue, l'informativa sulla cybersecurity diventerebbe non più volontaria ma obbligatoria e sarebbe sottoposta ad una disciplina di trasparenza secondo criteri predefiniti e validi per tutti*».

Tali circostanze assumono carattere di ancor maggiore problematicità ove si consideri il fenomeno, sempre più frequente, della collaborazione criminale che da tempo - attesa l'elevata redditività delle incursioni cibernetiche e la scarsa probabilità di identificazione degli autori - si è instaurata tra esponenti della criminalità organizzata "tradizionale" ed i professionisti del *cybercrime,* disponibili, nel contesto del c.d. *dark web*[48], ad offrire, a fronte di ingenti corrispettivi, le proprie, specifiche competenze professionali.

È dunque di tutta evidenza, alla luce di quanto fin qui rappresentato, il ruolo di primaria importanza rivestito dalla cybersicurezza nel quadro delle soluzioni telematiche utilizzate nelle procedure di *remote onboarding*, nel contesto sia del trattamento e della conservazione dei dati dei clienti sia della protezione degli impianti telematici.

4. Conclusioni

Le Linee Guida EBA in materia di *remote onboarding* hanno il pregio di dettare, in luogo dei singoli interventi statuali, linee di indirizzo uniformi nell'area dell'Unione; esse, tuttavia, per quanto dettagliate e con taluni contenuti di carattere innovativo, necessiteranno, molto probabilmente, di un ulteriore livello di intervento applicativo da parte dell'autorità nazionale.

La tematica è, all'evidenza, figlia della costante evoluzione tecnologica che caratterizza, interessando sia l'utente sia l'impresa (commerciale, bancaria e finanziaria), l'attuale contesto globale, sempre più interconnesso, in cui nascono e si evolvono tumultuosamente nuove pratiche legate all'utilizzo delle *Information and Communication Technologies* (ICT), il cui impiego, nelle sue diverse soluzioni – quale pratica (sempre più pervasiva) in ambito bancario e finanziario – merita particolare attenzione, oltre che dal punto di vista meramente tecnico, per gli impatti che essa determina negli assetti degli intermediari. Da ultimo, alla luce di talune nuove soluzioni innovative, è stato autorevolmente rappresentato come «(i)*ndagini di mercato evidenzi*(no) *che i fornitori di servizi finanziari che ricorrono a soluzioni DLT (Distributed Ledger Technologies) le utilizz*(i)*no principalmente come infrastruttura per l'offerta di servizi relativi a cripto-attività e, più in generale, alla tokenizzazione di attività, quali ad esempio le digitalizza-*

48 Il "*dark web*" (in italiano: *web oscuro* o *rete oscura*) è il termine usato per definire i contenuti del *World Wide Web* ("rete di ampiezza mondiale") nelle *darknet* (reti oscure) che creano imitazioni di *software*, configurazioni e accessi autorizzativi. Il *dark web*, non essendo raggiungibile dai classici motori di ricerca poiché si sovrappone alle normali reti e alle architetture delle reti private, rende molto difficile l'accesso, permettendo così lo svolgimento (in anonimato) di attività illegali.

zioni di oggetti del mondo reale (immobili, opere d'arte, ecc.) attraverso l'uso dei cosiddetti non-fungible-tokens. Le potenzialità connesse con l'adozione di "contratti intelligenti" (smart contracts) stanno oggi guidando ulteriori sviluppi nel campo della "finanza decentralizzata" (DeFI)». Tali soluzioni, per quanto meritevoli di attenzione, necessitano tuttavia di approfondimenti in ordine alle conseguenze, di ordine giuridico, tecnico ed economico, che, dal loro impiego, potrebbero discendere, dovendosi «(...) *garantire* (ai fruitori dei servizi) *le stesse condizioni che oggi si richiedono per i sistemi tradizionali: sicurezza, continuità operativa, scalabilità, sostenibilità ambientale, certezza nei meccanismi di governance e nella gestione delle relazioni tra tutte le parti coinvolte (nel caso di specie il coinvolgimento riguarda gli effetti della "legge algoritmica" che regola questi sistemi)* (...)». E ciò a dimostrazione che l'innovazione, per quanto ricca di risvolti positivi, non è esente da pericoli: «(...) *il Fintech può costituire un volano per la crescita e lo sviluppo competitivo del sistema finanziario e produttivo. Il dialogo e il confronto con tutti gli operatori del mondo Fintech rappresentano un elemento fondante della strategia con la quale la Banca d'Italia opera affinché la transizione digitale generi benefici in favore della collettività*»[49].

Anche con riguardo alla pratica del *remote onboarding* appare dunque necessario coniugare i numerosi profili di vantaggio, economico e di speditezza, offerti dalle nuove tecnologie, con la fondamentale esigenza, rappresentata nelle Linee Guida oltre che nelle presenti riflessioni, di assicurare, nel continuo, livelli di funzionalità tecnologica ed assetti organizzativi (*id est*: di *governance*) adeguati; obiettivo, questo, da perseguire attraverso l'adozione di solide e formali procedure di adeguata verifica, che implicano l'inevitabile coinvolgimento di diversi livelli di competenza e responsabilità, improntate a criteri di affidabilità e sicurezza, specie dal punto di vista delle soluzioni tecniche prescelte[50].

Un primo aspetto da tenere in considerazione, in tale pratica, è legato alla valutazione dei rischi gra-

49 Cfr. I. VISCO, *La Banca d'Italia per l'innovazione finanziaria: Milano Hub alla seconda Call for Proposals*, Milano, 25 novembre 2022.

50 Si segnala, a titolo esemplificativo, quanto indicato, in proposito, da E. MORLINI, cit.: «*Le immagini in bianco nero sono scartate perché non attendibili. L'immagine del documento a colori e la filigrana sono utilizzate per individuare manomissioni. Nel processo di acquisizione automatica l'algoritmo differenzia l'oggetto da acquisire digitalmente dagli altri elementi presenti nello sfondo (Background Detection) e tiene conto della luminosità dell'ambiente in cui viene acquisita l'immagine e il tipo di riflesso di luce sul documento che rappresenta un elemento di disturbo (Glare detection)I dati acquisiti vengono analizzati in tempo reale, verificando il rispetto degli standard previsti e confrontandoli con le informazioni disponibili negli archivi pubblici (es. SCIPAFI): i. correttezza formale dei dati relativi ai documenti identificativi acquisiti; ii. assenza di anomalie rilevanti nell'indirizzo; iii. esito positivo della verifica del documento su archivi pubblici. (...) Utilizzo dello SPID rafforzato previsto per i servizi che richiedono un grado di sicurezza maggiore. Tale opzione evita di richiedere sistematicamente al cliente l'upload del documento identificativo (i cui dati vengono trasmessi dal gestore di identità digitale) eccetto il caso di documento scaduto*».

vanti sull'intermediario in ordine alla potenziale violazione, da parte di agenti esterni, delle barriere di sicurezza dei propri apparati, a cui deve aggiungersi, come già segnalato, in ragione della (ormai esistente) globalità delle interconnessioni, l'altrettanto, potenziale pericolo che, attraverso il singolo intermediario, si finisca per accedere ad altri soggetti al medesimo, direttamente e/o indirettamente, collegati: si è avuto modo, infatti, di rammentare, come, nell'utilizzo delle nuove tecnologie a fini di *remote onboarding*, faccia premio la fondamentale tematica, riguardante ogni soggetto solo appena informatizzato, rappresentata dalla Cybersicurezza, anche oggetto da ultimo di particolare attenzione da parte del legislatore tanto nazionale (si veda, *ex multis*, il d.l. 21 settembre 2019, n. 105, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"* e, anche, il d.l. 14 giugno 2021, n. 82, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*) quanto Europeo [si veda, *ex multis*, la Direttiva Ue 2016/1148 recante "*misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" (c.d. Direttiva NIS)]. Le ICT, come noto, rappresentano varchi attraverso cui sono possibili incursioni *hacker* da parte di professionisti del *cyber-crime*, volti non solo a danneggiare i sistemi di cui gli enti dispongono, ma anche, ove vi siano obiettivi di ordine economico, a sottrarre ed impadronirsi di ogni dato personale disponibile. Di qui il profilo di convergenza tra l'attività degli istituti finanziari e creditizi e quella condotta dall'ACN, la quale, oltre ad esercitare nei loro confronti attività consulenziale ed ispettiva, ha anche il potere, in costanza di violazioni normative, di irrogare sanzioni.

Sotto altro profilo, la pratica del *remote onboarding*, in ragione delle articolate e trasversali implicazioni di ordine tecnico ed organizzativo che presenta, necessita di attenzione anche sotto il profilo gestionale. Invero, l'elaborazione e la trattazione di tale procedura, pur essendo collocata, formalmente, nell'ambito delle attività riconducibili nel perimetro della Funzione Antiriciclaggio, ha bisogno, al pari di qualunque altra attività di pari complessità, dell'ausilio di variegate competenze, sia pure in larga parte tecniche; ciò, tuttavia, non dev'essere di ostacolo né (i) a che il risultato ultimo della complessiva elaborazione della procedura [articolantesi in valutazioni (di ordine sia organizzativo sia tecnico), *policy*, etc.] - necessariamente condotta con il contributo delle competenti risorse professionali interne e, laddove necessario, con l'ausilio di adeguati sostegni consulenziali – resti, come richiesto dalla Direttiva UE 2018/843, nell'alveo delle attribuzioni assegnate alla Funzione AML/CFT, né (ii) a che la sua approvazione sia sottoposta alle valutazioni e deliberazioni dell'Organo amministrativo, quale principale responsabile di ogni scelta gestionale, a *fortiori* ove le decisioni assunte in ordine alla tipologia di procedura prescelta risultassero, ex art. 2392, comma 1, c.c., imprudenti. Va ricordato, in proposito,

«*come in materia di responsabilita` degli amministratori di societa` di capitali, l'insindacabilita` del merito delle scelte di gestione* (cd. "*business judgement rule*") *trovi un limite nella ragionevolezza delle stesse da compiersi "ex ante" secondo i parametri della diligenza del mandatario, tenendo conto della mancata adozione delle cautele, delle verifiche e delle informazioni preventive, normalmente richieste per una scelta di quel tipo e della diligenza mostrata nell'apprezzare preventivamente i margini di rischio connessi all'operazione da intraprendere*»[51].

E' evidente, dunque, come la complessità delle sfide imprenditoriali, sempre più spesso trasversali a più tematiche e ad elevato tasso di tecnicismo, implichi ed esiga un adeguato assetto di governo dell'ente, tale da permettergli di affrontare adeguatamente, ove munito delle necessarie (e variegate) competenze, ogni tematica, ricadente nell'oggetto sociale, da sottoporsi al proprio vaglio. L'adeguatezza dell'organo di governo, da sempre cruciale, è, come noto, oggetto del "*supervisory review and evaluation process*" (SREP), i cui risultati, con riguardo all'anno 2022, nell'evidenziare (tra le altre) criticità legate all'efficacia e alla composizione degli organi di amministrazione, alla loro idoneità complessiva e al loro ruolo di presidio sui rischi, sottolineano, quale principale elemento di preoccupazione, la «*suboptimal compositions of the management body, including in terms of IT experience among board members and lack of formally independent board members, and allocation of responsibilities, compromising*

51 Cfr. sul punto, Cass., Ord., Sez. I, del 24.1.2023, che a sua volta richiama, Cass. n.15470/2017. Sul delicato tema della c.d. «*business judgement rule*», cfr., *ex plurimis*, Cass. Civ., Sez. I, 28.4.1997, n. 3652, a tenore della quale «(a) *l'amministratore di una società non può essere imputato a titolo di responsabilità ex art. 2392 c.c. di aver compiuto scelte inopportune dal punto di vista economico, atteso che una tale valutazione attiene alla discrezionalità imprenditoriale e può pertanto eventualmente rilevare come giusta causa di revoca dell'amministratore, non come fonte di responsabilità contrattuale nei confronti della società. Ne consegue che il giudizio sulla diligenza dell'amministratore nell'adempimento del proprio mandato non può mai investire le scelte di gestione (o le modalità e circostanze di tali scelte), ma solo l'omissione di quelle cautele, verifiche e informazioni preventive normalmente richieste per una scelta di quel tipo, operata in quelle circostanze e con quelle modalità*», nonché Cass. Civ., Sez. I, 2.2. 2015, n.1783, la quale ha stabilito che «(i)*n tema di responsabilità degli amministratori verso la società, il giudizio sulla violazione del generale obbligo di diligenza, cui l'amministratore deve attenersi nell'adempimento dei doveri imposti dalla legge o dall'atto costitutivo, non può tradursi nella valutazione dell'opportunità economica delle scelte di gestione operate dall'amministratore, ma deve riguardare il modo in cui esse sono compiute. Ne consegue che la responsabilità dell'amministratore può essere generata, ai sensi dell'art. 2392, comma 1, c.c., dall'eventuale omissione di quelle cautele, verifiche e informazioni preventive normalmente richieste prima di procedere a quel tipo di scelta. (Nella fattispecie, la Suprema corte ha ritenuto che correttamente la Corte d'appello avesse affermato la responsabilità di un amministratore di una società per azioni, il quale, nell'imminenza della pubblicazione di una decisione arbitrale, aveva definito una controversia con una transazione oggettivamente sfavorevole per la società omettendo però di consultare preventivamente il legale della società, onde acquisire informazioni sul probabile esito della controversia, anche alla luce dell'attività istruttoria svolta, nonché elementi di valutazione circa il peso delle concessioni da offrire alla controparte e l'entità di quelle da richiedere)*»

the management body's oversight and challenging capacity, especially in its supervisory function»[52]. Nello SREP, inoltre, viene specificato come «*The main deficiencies in the operational resilience framework include (i) the management of risks related to IT outsourcing and reliance on third-party service providers for critical functions and services, and (ii) IT security and cyber risk management, including cyber hygiene measures and cyber resilience. More specifically, operational risk (including IT and cyber risk) has increased recently as a consequence of accelerated digitalisation triggered by the pandemic, changes in consumer preferences, competition from fintechs, an increased reliance on IT outsourcing and stronger headwinds stemming from the current geopolitical situation»*[53]; circostanza, questa, che trova conferma anche nell'Intervento del Presidente del Consiglio di vigilanza della BCE svolto in sede di conferenza stampa sui risultati del ciclo SREP 2022, nel quale si sottolinea come «(l)*a composizione degli organi di amministrazione* (sia) *spesso inadeguata, soprattutto in termini di esperienza informatica.* (...) *Il rischio di attacchi cibernetici, che era già aumentato durante la pandemia, si è intensificato ulteriormente nell'attuale contesto. Ora più che mai le banche devono affrontare le carenze strutturali negli accordi di esternalizzazione e nei sistemi di sicurezza informatica e di resilienza cibernetica. La digitalizzazione dei servizi bancari e finanziari esacerba anche altri rischi tra cui frodi, riciclaggio di denaro, carenze di competenze informatiche interne e perdita potenziale di clienti dovuta al mutare delle preferenze dei con-*

52 Tale preoccupazione è data riscontrarla anche negli *"Orientamenti della Banca d'Italia sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI"* del 29 novembre 2022, in cui è precisato che «(l)*a compresenza nel board di esponenti con profili e sensibilità differenti (cd. diversity) contribuisce ad assicurare il buon funzionamento dei meccanismi di governo societario delle banche. La diversity permette infatti che nelle discussioni consiliari siano riportati differenti punti di vista, così da evitare il rischio di fenomeni di group thinking, promuovere l'adozione di decisioni più partecipate, consapevoli e ponderate, rafforzare il monitoraggio sul management e l'apprezzamento dei rischi connessi al perseguimento delle strategie aziendali. Come previsto dalla normativa, gli organi sociali devono essere adeguatamente diversificati in termini di età, genere, durata di permanenza nell'incarico e – limitatamente alle banche operanti in modo significativo in mercati internazionali – provenienza geografica degli esponenti. Inoltre, devono essere presenti soggetti dotati di professionalità adeguate al ruolo da ricoprire, anche in eventuali comitati endo-consiliari, e calibrate in relazione alle caratteristiche operative e dimensionali della banca. La disponibilità di un'ampia gamma di conoscenze all'interno del board può costituire un elemento utile anche per affrontare efficacemente le sfide della digitalizzazione e della sostenibilità. Si rammenta, inoltre, che in base alle Disposizioni della Banca d'Italia, spetta al CdA identificare preventivamente la propria "composizione quali-quantitativa ottimale" e verificare la rispondenza tra questa e quella effettiva risultante dal processo di nomina, per garantire nel continuo l'adeguatezza dei profili e delle competenze dei propri esponenti, collettivamente considerati. Diversificazione delle competenze. Dall'analisi tematica è emerso che le competenze dei consiglieri non sono molto diversificate e che, in particolare, risultano meno frequenti quelle in materia di IT (compresi i profili relativi a fintech/cybersecurity), risk management e organizzazione/HR. A questo proposito si richiama quanto previsto dal Decreto Ministeriale 23 novembre 2020 n. 169, e dalle Disposizioni sul governo societario della Banca d'Italia, in merito alla composizione collettiva degli organi»*

53 Per un esame più ampio dei risultati dello SREP, si veda, da ultimo, E.DELLAROSA, *Le attese di BCE sulla governance delle Banche: chiavi di lettura dei risultati SREP*, in *Diritto Bancario*, 15.2.2023.

sumatori e alla crescente concorrenza da parte degli operatori fintech.

La maggior parte dei progetti digitali delle banche mira ad attrarre e fidelizzare la clientela e a migliorare l'efficienza in termini di costi. Tuttavia, l'entità degli investimenti delle banche resta limitata. Nel 2021 gli investimenti degli enti vigilati nella trasformazione digitale sono stati pari in media ad appena il 2,8% dei ricavi operativi netti.

Per monitorare l'ordinato processo di trasformazione digitale a sostegno di modelli di business solidi, la Vigilanza bancaria della BCE ha avviato diverse iniziative connesse alla digitalizzazione nel settore bancario. Il loro esito confluirà nella valutazione di vigilanza nel prossimo ciclo SREP».

Il cruciale tema della *diversity* riceve attenzione anche in ambito AML/CFT, ricordando al riguardo gli «*Orientamenti sulle politiche e le procedure relative alla gestione della conformita` e al ruolo e alle responsabilita` del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849*» (EBA/GL/2022/05 14 giugno 2022) che l'Organo di Gestione, in quanto «11 (...) *responsabile dell'approvazione della strategia complessiva dell'ente creditizio o dell'istituto finanziario in materia di AML/CFT e della supervisione della sua attuazione*», dovrebbe, tra l'altro, «*possedere collettivamente conoscenze, abilità ed esperienze adeguate per poter capire i rischi di riciclaggio e del finanziamento del terrorismo (ML/TF) correlati alle attivita` e al modello di business dell'ente creditizio o dell'istituto finanziario, comprese le conoscenze del quadro giuridico e normativo nazionale in materia di prevenzione dell'ML/TF.* (...)» e dovrebbe, altresì, «(...) *14.* (...) *garantire che il membro dell'organo di gestione di cui alla sezione 4.1.3* (cioè "(...) *del membro dell'organo di getione dell'AML/CFT*") *o, laddove applicabile, l'alto dirigente di cui alla sezione 4.1.4* (cioè dell'"(...) *alto dirigente responsabile dell'AML/CFT in assenza di un organo di gestione*") *che è responsabile dell'attuazione delle disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttiva (UE) 2015/849:* a) *possieda le conoscenze, le competenze e le esperienze necessarie per individuare, valutare e gestire i rischi di ML/TF cui è esposto l'ente creditizio o l'istituto finanziario nonché l'attuazione di politiche, controlli e procedure in materia di AML/CFT; b) possieda una buona comprensione del modello di business dell'ente creditizio o dell'istituto finanziario e del settore in cui esso opera, nonché della misura in cui tale modello di business espone l'ente creditizio o l'istituto finanziario a rischi di ML/TF; c) sia tempestivamente informato delle decisioni che possono incidere sui rischi cui è esposto l'ente creditizio o l'istituto finanziario. (...) 17. In particolare, il membro dell'organo di gestione da identificare ai sensi dell'articolo 46, paragrafo 4, della direttiva (UE) 2015/849 dovrebbe possedere sufficienti conoscenze, competenze ed esperienze concernenti i rischi di ML/TF e l'attuazione delle politiche, dei controlli e delle procedure in materia di AML/CFT, unitamente a*

una buona comprensione del modello di business dell'ente creditizio o dell'istituto finanziario e del settore in cui l'ente o l'istituto opera. 18. Il membro dell'organo di gestione di cui all'articolo 46, paragrafo 4, della direttiva (UE) 2015/849 dovrebbe dedicare tempo sufficiente e disporre di risorse adeguate per assolvere efficacemente i propri compiti relativi all'AML/CFT. Dovrebbe riferire esaurientemente sui propri compiti, come indicato nella sezione 4.1.5, e informare regolarmente l'organo di gestione nella sua funzione di supervisione strategica, laddove necessario e senza indebito ritardo»[54].

54 Cfr., sul tema, E.DELLAROSA, *Le nuove Linee Guida Eba sulla governance antiriciclaggio: quali cambiamenti per il Board delle banche*, in *Bancaria*, 1, 2023.