smo. I rapporti vengono pubblicati in versione integrale sul sito dell'organismo (www.fatf-gafi.org).

Il FATF-GAFI ha proseguito l'attività di monitoraggio delle giurisdizioni, al fine di identificare quelle ritenute particolarmente rischiose per la stabilità del sistema finanziario internazionale e di guidarle nell'attività di attuazione delle Raccomandazioni per colmare le lacune normative. Co-presieduto dall'Italia e dagli Stati Uniti, l'ICRG riferisce nelle sedute plenarie del FATFGAFI circa lo stato di adeguamento del sistema AML/CFT rispetto ad alcune specifiche lacune strategiche, identificate anche a seguito di Mutual Evaluation Reports, indicate in un Action Plan concordato con i governi dei paesi sottoposti a monitoraggio. In base alle nuove procedure, i paesi che sono entrati in ICRG nel 2018 sono stati Pakistan, Bahamas, Botswana, Ghana, Panama e Cambogia e la Serbia (uscita nel 2019). I relativi Piani d'Azione prevedono che i governi si impegnino a migliorare l'efficacia dei propri sistemi in alcuni settori particolarmente carenti ed entro delle scadenze previste.

Per lo svolgimento dei suoi compiti l'ICRG continua ad avvalersi di quattro sotto-gruppi re-gionali che seguono l'attuazione dei diversi Action Plan e che, a loro volta, riferiscono periodicamente all'ICRG (l'Italia presiede il gruppo Africa-Middle East). L'attività di monitoraggio ha come esito la pubblicazione di due documenti puntualmente aggiornati, a seguito delle riunioni plenarie del FATF-GAFI, ed entrambi pubblicati anche sul sito del Dipartimento del Tesoro, affinché siano utilizzati dal settore privato italiano nell'ambito delle rispettive valutazioni dei rischi e sono:

- il *FATF Public Statement*, con le valutazioni sulle giurisdizioni che presentano deficienze strategiche in materia di riciclaggio e di finanziamento del terrorismo;
- l'*Improving Global AML/CFT Compliance document*, con un aggiornamento sui progressi, ove esistenti, dei paesi che hanno lacune serie nel sistema di contrasto al riciclaggio e al finanziamento del terrorismo.

X.1.1 L'Iran e GAFI: la valutazione del sistema iraniano contro il riciclaggio di denaro e il finanziamento del terrorismo

L'Iran è sotto esame del FATF-GAFI (Financial Action Task Force - Gruppo d'Azione Finanziaria) dal 2007. Dal 2009 è stato inserito nel FATF Public Statement (c.d. lista nera), con l'invito ai paesi ad adottare le necessarie contromisure. Negli ultimi anni l'Iran ha cercato il dialogo con il FATF, forte anche della recente adozione di una legge contro il finanziamento del terrorismo. Il competente gruppo FATF, l'International Cooperation Review Group (ICRG), i cui co-presidenti sono l'Italia e gli Stati Uniti, ha incontrato le autorità iraniane diverse volte con altre delegazioni, inizialmente concordando un Action Plan e poi verificandone l'attuazione.

Nel 2018 le Plenarie del FATF-GAFI hanno confermato la continuazione della sospensione delle contromisure, perché, pur riconoscendo l'avvenuta scadenza delle date poste come obiettivo dell'Action Plan (gennaio 2018), hanno valorizzato l'approvazione da parte del governo iraniano degli emendamenti alla normativa in materia di lotta al riciclaggio e al finanziamento del terrorismo, anche se restano

ancora da ratificare la Convenzione delle Nazioni Unite per la soppressione del finanziamento al terrorismo (Convenzione TF) e la Convenzione delle Nazioni Unite contro la criminalità organizzata trans-nazionale (Convenzione di Palermo), misure cardine per una piena compliance con gli standard internazionali.

X.1.2 Gruppi regionali associati al FATF-GAFI

Il contrasto internazionale al riciclaggio e al finanziamento del terrorismo si avvale di un network globale nel quale, oltre al FATF-GAFI che emana le Raccomandazioni, operano altri organismi organizzati sul modello del FATF-GAFI, detti FSRBs (*FATF-Style Regional Bodies*) che valutano i loro paesi membri. I gruppi regionali sono nove, con un global network che è giunto a coprire oltre 200 paesi nel mondo.

Tra le attività condotte dal MONEYVAL nel corso del 2018, si citano i rapporti di mutua valutazione dei paesi membri, che vengono adottati, previa discussione in Plenaria. Nel 2018, sono stati pubblicati i rapporti di Albania, Lettonia, Repubblica Ceca e Lituania. Inoltre, il MONEYVAL ha valutato, congiuntamente con il GAFI, l'implementazione degli Standard AML/CFT da parte di Israele, Paese da lungo tempo membro del MONEYVAL, che ha raggiunto i requisiti per l'acquisizione della *membership* ufficiale del GAFI/FATF, ottenuta grazie ai positivi risultati dimostrati.

In aggiunta alla propria consolidata azione di monitoraggio (*peer reviews e follow-up*), il MONEYVAL ha ribadito il proprio status di FSRB a supporto del network globale con importanti iniziative complementari e parallele alle priorità espresse dalla presidenza GAFI di turno. Si fa riferimento al workshop internazionale organizzato a Strasburgo nel marzo 2018 con un focus tematico di approfondimento e di scambio attinente alle più importanti problematiche affrontate dalle autorità investigative e giudiziarie impegnate nella lotta del riciclaggio e del finanziamento del terrorismo, a cui l'Italia ha partecipato. Meritano altresì un cenno le ulteriori attività di *outreach* organizzate a supporto del global network tra cui: due corsi di training per futuri valutatori, il primo tenutosi a Larnaca (Cipro) e il secondo tenutosi a Mosca.

X.2 L'ATTIVITÀ NELL'AMBITO DELL'UNIONE EUROPEA

X.2.1 L'Expert Group on Money Laundering and Terrorist Financing (EGMLTF) e il Supranational Risk Assessment

Nel corso del 2018 sono proseguiti i lavori *dell'Expert Group on Money Laundering and Terrorist Financing (EGMLTF)* che si sono concentrati sui seguenti aspetti:

1) la consueta attività di coordinamento che precede le riunioni plenarie del GAFI, che include una discussione dei rapporti di valutazione tra gli Stati membri;

2) i tempi di recepimento della IV AMLD da parte degli Stati Membri, nonché l'aggiornamento sui negoziati relativi agli emendamenti alla stessa (c.d. V AMLD), e il processo di raccolta dei dati statistici nella materia di prevenzione del rici-

claggio, finanziamento del terrorismo e reati presupposti, in attuazione della IV AMLD;

3) l'aggiornamento del *Supra-national Risk Assessment* (SNRA). Ciò discende da un obbligo giuridico: la IV AMLD prevede, difatti, che la Commissione Europea predisponga un'analisi sovranazionale dei rischi, per individuare i rischi di riciclaggio e di finanziamento del terrorismo che minacciano l'integrità del mercato finanziario comunitario. L'attività, seguita dall'Italia con rappresentanti del Ministero economia e finanze e dalle autorità di volta in volta individuate in base all'agenda, è stata volta all'identificazione dei rischi di riciclaggio e di finanziamento del terrorismo e all'analisi delle vulnerabilità del sistema europeo di prevenzione del riciclaggio e del finanziamento del terrorismo. Il primo *Supranational Risk Assessment* è stato approvato nel mese di luglio 2017 e nel corso del 2018-2019 il gruppo di lavoro ha predisposto un aggiornamento delle minacce ed elaborato una serie di raccomandazioni agli Stati membri circa le misure idonee ad affrontare i rischi individuati e dei fattori di contesto da analizzare.

Nel dossier sulla riforma delle autorità di vigilanza di settore (ESA) è stata predisposta da parte della Commissione a settembre 2018 la proposta legislativa (approvata nel 2019), che consente di accentrare nell'EBA competenze specifiche in materia di antiriciclaggio già preesistenti in ESMA e EIOPA, per avere una maggiore uniformità per le linee guida e per i processi valutativi della supervisione del settore finanziario in materia antiriciclaggio.

Questa proposta deriva dai recenti scandali di riciclaggio che hanno coinvolto alcune banche europee in Estonia, Lettonia, Danimarca e Malta. Si è reso necessario agire prontamente per dare un forte segnale al sistema finanziario europeo e internazionale. A dicembre 2018 sono state adottate le *Council Conclusions* per un Action Plan coordinato dalla Commissione, destinato a migliorare la qualità della supervisione in materia AML, sia a livello europeo che nazionale.

L'Italia è favorevole a un ambiente più armonizzato nel settore della vigilanza, al fine di ottenere un livello qualitativo omogeneo in ambito europeo, visto che alcuni paesi membri dell'Unione europea hanno dimostrato lacune considerevoli nei loro sistemi antiriciclaggio, permeabili da flussi illeciti di derivazione extra-europea.

X.2.2 La metodologia per i paesi terzi a rischio

La IV AMLD (Direttiva (UE) 2015/849), nel garantire meccanismi di protezione efficaci per il mercato interno, al fine di aumentare la certezza del diritto per gli operatori economici e i portatori di interessi diffusi, nei loro rapporti con le giurisdizioni dei paesi terzi, prevede che, con atto delegato del Parlamento europeo, la Commissione europea possa pubblicare una lista di paesi con carenze strategiche nei rispettivi regimi di lotta contro il riciclaggio di denaro e il finanziamento del terrorismo, che pongano minacce significative al sistema finanziario dell'Unione.

Tutti i soggetti obbligati, ai sensi della citata direttiva, dovranno applicare misure rafforzate di adeguata verifica nei loro rapporti con persone fisiche o entità giuridiche che hanno sede in paesi terzi ad alto rischio, garantendo così obblighi equivalenti per i partecipanti al mercato in tutta l'Unione.

L'articolo 9 della IV AMLD conferisce alla Commissione Europea il potere di individuare tali paesi terzi ad alto rischio, e stabilisce i criteri su cui deve basarsi tale valutazione. A tale proposito, è stata definita la metodologia che sarà utilizzata per questo esercizio, che, integrata su specifica richieste degli Stati Membri, attualmente prevede una procedura di confronto con i paesi terzi prima di un eventuale *listing*.

X.3 CYBER SECURITY

Nell'ambito della prevenzione dell'uso del sistema finanziario per fini illegali, una linea di attività nel corso del 2018 ha riguardato la protezione dagli attacchi informatici (cyber attacks). L'integrità del sistema finanziario, considerata la migrazione verso servizi a tecnologia evoluta, è oggi minacciata dal rischio di attacchi cyber: la sempre più diffusa fornitura di servizi e prodotti finanziari attraverso i moderni strumenti messi a disposizione della tecnologia dell'informazione e della comunicazione (cd. Fintech) ha determinato un aumento dei rischi operativi e cyber, sia sotto forma di attacchi che di incidenti, e in maniera rilevante negli ultimi anni. I rischi gravanti sul fintech sono dovuti, in particolare, all'elevata interconnessione degli operatori, sia in ambito intersettoriale sia per il suo marcato carattere transnazionale.

Pertanto, a partire dal 2015 sono iniziati i lavori in materia di cyber security, precisamente quando i partecipanti al G7, concordarono sulla necessità di rafforzare in maniera condivisa la sicurezza cibernetica nel settore finanziario, decidendo di costituire un gruppo di lavoro di esperti in materia: il G7 Cyber Expert Group, G7-GEC. Il mandato del gruppo è stato di rafforzare la cooperazione tra i G7 in materia, riguardo all'identificazione dei rischi cibernetici nel settore finanziario, anche a seguito delle risultanze di una *survey* relativa ai ruoli, alle competenze e alle responsabilità delle varie autorità nazionali, agli approcci adottati, alle procedure per prevenire gli attacchi e per mitigare i rischi.

Dopo l'approvazione da parte dei Ministri e Governatori, agli *Annual Meetings* di Washington, ottobre 2016, dei G7 *Fundamental Elements of* Cybersecurity for the Financial Sector, cioè un set di elementi fondamentali, non legalmente vincolanti per rafforzare le capacità di cybersecurity, e ad ottobre 2017, dei G7 *Fundamental Elements for effective assessment* of Cybersecurity in the Financial Sector, set di elementi fondamentali per la valutazione efficace della cybersecurity del settore finanziario, nell'ottobre 2018 sono stati pubblicati G7 Fundamental Elements for threat-Led Penetration Testing e i G7 Fundamental Elements on third party risk management.

Il G7-CEG ha approvato anche il G-7 Cyber Incident Response Communications Protocol (CIRCP), documento alla base del G7 cybersecurity cross-border exercise, che è stato programmato per giugno 2019.

Sempre nel G7 di ottobre 2018, a Bali, Indonesia, è stato approvato anche il G-7 CEG 2019-21 Mandate (Terms of Reference) del G7-CEG, con l'inserimento, nel nuovo Mandato, del punto voluto dal MEF e da Banca d'Italia (Produce a G-7 CEG 5 Year Impact Assessment Document), al fine di valutare, a distanza di tempo, le attività svolte dal G-7 CEG. Il nuovo mandato contiene l'elenco delle linee di attività proposte per 2019-21: implementazione della cross-sector coordination,

organizzazione e svolgimento di una esercitazione cross-border (regolata dal protocollo CIRCP e con la partecipazione del settore privato) e sviluppo di nuove linee di attività (potenziamento del G-7 Cyber Incident Response Communications Protocol, ricognizione comune delle vulnerabilità in ambito G7 nel settore finanziario, rafforzamento della partnership pubblico-privato in particolare in ambito cross-border).

In ambito europeo è stata recepita la Direttiva 2016/1148 (NIS-Network and Information Security) sulla sicurezza delle reti e dei sistemi informativi che prevede l'aumento dei livelli di sicurezza nell'Unione tramite il decreto legislativo del 18 maggio 2018, n. 65.

Il provvedimento di recepimento individua, come autorità NIS, il MEF relativamente al settore bancario e al settore delle infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob.

Importante ricordare che - con la Decisione del Consiglio n. 797 e il Regolamento del Consiglio n. 796 del 17 maggio 2019 - l'Unione Europea ha istituito un regime di misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati Membri. Le misure restrittive possono essere attivate dal Consiglio in seguito ad attacchi informatici significativi e tentati attacchi informatici potenzialmente significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati Membri. Le misure previste riguardano l'interdizione all'accesso o al transito nel territorio degli Stati Membri delle persone fisiche responsabili e dei loro associati; e il congelamento dei fondi e delle risorse economiche riconducibili a persone fisiche e giuridiche, entità o organismi responsabili di attacchi o tentati attacchi e loro associati. Al momento di stendere queste righe, nessuna misura restrittiva è stata ancora adottata ai sensi del regime cyber.

X.4. L'ATTIVITÀ DEL GRUPPO EGMONT

Le attività del Gruppo Egmont sono proseguite con l'individuazione e l'approfondimento di tipologie di riciclaggio e di finanziamento del terrorismo. In particolare *l'ISIL Project* ha proseguito l'attività, concentrando l'attenzione sul progetto dedicato a *"Lone Actors and Small Cells"*.

Ulteriori progetti in corso sono dedicati al riciclaggio dei proventi da corruzione e allo sviluppo di forme efficaci di collaborazione tra FIU e autorità doganali.

Nel corso del 2018 il Gruppo Egmont ha concluso l'analisi preliminare dei rapporti relativi alle FIU di 10 paesi, finalizzata all'individuazione di iniziative idonee a rimuovere i limiti alla capacità delle FIU di collaborare. Difatti, le verifiche, nel Gruppo Egmont, sono incentrate sulle criticità nella cooperazione internazionale e promuovono l'adozione di adeguati interventi correttivi, anche attraverso iniziative mirate di assistenza tecnica.

X.5 IL COMITATO DI BASILEA

La Banca d'Italia partecipa ai lavori dell'*Anti-Money Laundering Expert Group* (AMLEG), istituito in seno al Comitato di Basilea, con il compito di fornire ausilio al Comitato nel campo della lotta al riciclaggio e al finanziamento del terrorismo.

Nel corso del 2018 - in risposta ai recenti scandali di riciclaggio che hanno interessato diversi istituti bancari europei - il Comitato di Basilea ha approvato un piano di lavoro proposto dall'AMLEG, volto a sviluppare linee guide per promuovere la cooperazione tra Autorità di Vigilanza prudenziale e quelle compenti per la Vigilanza ai fini AML/CFT.

Il piano di lavoro riconosce la necessità di rafforzare la cooperazione e lo scambio di informazioni tra le autorità prudenziali e AML, non solo per prevenire i rischi di riciclaggio e finanziamento del terrorismo e mantenere l'integrità del sistema bancario, ma anche per garantire la solidità e la stabilità prudenziali del sistema bancario e finanziario nel suo complesso, preservandolo da ricadute reputazionali, che possono derivare da un coinvolgimento - anche inconsapevole - in fenomeni di riciclaggio e finanziamento del terrorismo.

L'ultimazione dei lavori previsti nel piano comporterà una modifica alle guidelines del Comitato di Basilea in materia di "*Sound management of risks related to money laundering and financing of terrorism*".

Inoltre, nel corso dell'anno il Comitato di Basilea ha contribuito attivamente alle attività promosse dal FSB per contrastare il fenomeno del declino dei rapporti di corrispondenza (cd. *de- risking*). In tale quadro, è stato completato, d'intesa con il GAFI, il monitoraggio delle modalità con cui vengono attuate a livello nazionale le raccomandazioni prodotte negli ultimi anni dai principali organismi internazionali per contrastare il *de-risking*, e sul tema è stato organizzato - d'intesa con il FSB - un incontro ad ottobre 2018 tra rappresentanti del settore pubblico e l'industria.

Infine, l'AMLEG non ha mancato di fornire supporto alle attività del GAFI per gli aspetti d'interesse del settore bancario.

ALLEGATO 1

IL RUOLO DELLE PUBBLICHE AMMINISTRAZIONI IN FUNZIONE DI PREVENZIONE DEL RICICLAGGIO E DEL FINANZIAMENTO DEL TERRORISMO.

Le disposizioni riguardanti le Pubbliche Amministrazioni sono collocate nel Titolo I Capo II del citato decreto antiriciclaggio, intitolato "Autorità, Vigilanza e Pubbliche amministrazioni".

Tale allocazione sistematica è espressione del ruolo peculiare assegnato alle Pubbliche Amministrazioni nell'ambito del sistema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, in relazione a procedure e procedimenti amministrativi di cui all'articolo 10, comma 1 del decreto antiriciclaggio (e degli ulteriori, eventuali, procedimenti individuati ai sensi del comma 2 del medesimo articolo). Tali procedure e procedimenti possono riguardare anche attività economiche suscettibili di essere utilizzate dai soggetti che partecipano ai procedimenti amministrativi anzidetti per compiere operazioni di riciclaggio o di finanziamento del terrorismo.

I destinatari degli obblighi antiriciclaggio di cui all'articolo 3 del decreto antiriciclaggio (quali, ad esempio, banche, intermediari finanziari, professionisti, intermediari immobiliari) svolgono attività imprenditoriali o professionali consistenti nel compimento, per i propri clienti, di operazioni di gestione o di intermediazione finanziaria, di trasferimento di attività economiche o di beni o nella consulenza per l'esecuzione di tali atti di natura privatistica.

A differenza di tali soggetti, destinatari di stringenti obblighi di adeguata verifica della clientela, di conservazione documentale e di segnalazione alla UIF delle operazioni sospette di riciclaggio e di finanziamento del terrorismo poste in essere dalla clientela, le Pubbliche amministrazioni non svolgono il ruolo di intermediari o di consulenti nelle movimentazioni finanziarie effettuate da individui e imprese; le Pubbliche Amministrazioni svolgono la propria attività istituzionale, nelle diverse materie di competenza, sempre per il perseguimento dell'interesse pubblico, secondo le norme che regolano specificamente l'attività amministrativa in questione.

Le Pubbliche amministrazioni rivolgono la propria attività di tipo provvedimentale nei confronti di soggetti che partecipano ai procedimenti anzidetti e che sono portatori di propri interessi, usualmente di carattere imprenditoriale o professionale. I dati e le informazioni acquisiti nell'ambito dell'istruttoria dei procedimenti di cui all'articolo 10, comma 1 costituiscono oggetto di comunicazione alla UIF qualora, le Pubbliche Amministrazioni ritengano di trovarsi in presenza di operazioni sospette, anche alla luce degli indicatori di anomalia adottati dalla UIF ai sensi del comma 4 del medesimo articolo.

È opportuno precisare, in prima battuta, che le operazioni da prendere in considerazione ai fini della predetta comunicazione non coincidono con l'oggetto in quanto tale del procedimento amministrativo; esse attengono, piuttosto, all'attività posta in essere dal soggetto che partecipa al procedimento amministrativo e il cui operato presenta profili di anomalia tali da far sorgere il sospetto che possa essere coinvolto in attività di riciclaggio o di finanziamento del terrorismo, o comunque che stia utilizzando fondi che, anche indipendentemente dalla loro entità, provengano da attività criminosa.

Il sospetto è valutato alla luce delle caratteristiche del soggetto che si relaziona con le Pubbliche Amministrazioni nell'ambito dei procedimenti di cui all'articolo 10, comma 1, e delle attività e dei comportamenti tenuti dal medesimo nel corso o all'esito degli stessi procedimenti, anche considerati gli indicatori di anomalia emanati dalla UIF ai sensi dell'articolo 10, comma 4. Le Pubbliche Amministrazioni compiono dette valutazioni sulla base dei dati e delle informazioni acquisiti nello svolgimento dei procedimenti amministrativi di competenza.

Si pensi, a titolo d'esempio, al soggetto che richiede una concessione, la cui attività imprenditoriale o professionale può essere valutata come sospetta dalla Pubblica Amministrazione in ragione del profilo soggettivo dell'interessato, della sua attività o del suo comportamento, desumibili dai dati e dalle informazioni di cui l'amministrazione è entrata in possesso nello svolgimento della procedura selettiva per l'assegnazione della concessione.

Pertanto, i dati e le informazioni acquisiti dalle Pubbliche Amministrazioni nello svolgimento dei compiti di amministrazione attiva e di controllo, nell'ambito dei procedimenti di cui all'articolo 10, comma 1, costituiscono oggetto di comunicazione alla UIF qualora, anche alla luce degli indicatori adottati ai sensi del comma 4 del medesimo articolo, si rilevino inerenti ad operazioni sospette aventi le caratteristiche sopra descritte.

Resta fermo l'obbligo per i pubblici funzionari di provvedere alla denuncia all'autorità giudiziaria laddove, nell'esercizio della funzione, ravvisino gli estremi di una fattispecie di reato.

Nella valutazione dei dati e delle informazioni acquisiti sui soggetti privati interessati al procedimento, le Pubbliche amministrazioni dovrebbero prestare tra l'altro particolare attenzione alle notizie inerenti alle persone politicamente esposte, ai soggetti inquisiti ovvero a quelli censiti nelle liste pubbliche di terrorismo.

Si pensi, a titolo d'esempio, ai dati e alle informazioni contenute nel certificato dei carichi pendenti, nel casellario giudiziale, nella dichiarazione unica di regolarità contributiva (DURC) e in ogni altro documento richiesto dalla legge o dal bando di gara a riprova del possesso dei requisiti di carattere generale, tecnico-professionale ed economico/finanziario richiesti per la partecipazione alle procedure di evidenza pubblica.

1. Mappatura, mitigazione e valutazione dei rischi di riciclaggio e di finanziamento del terrorismo cui possono essere esposte le Pubbliche Amministrazioni

Le Pubbliche Amministrazioni procedono alla mappatura dei rischi di riciclaggio e finanziamento del terrorismo in relazione alle caratteristiche soggettive, ai

comportamenti e all'attività espletata dai soggetti interessati ai procedimenti di cui all'articolo 10.

Va in ogni caso considerato che per i procedimenti di cui all'articolo 10, comma 1, l'ordinamento prevede specifiche regole a tutela dell'integrità dell'azione amministrativa. La trasparenza dell'operato della Pubblica amministrazione e la prevenzione e repressione della corruzione sono presidiate dalle disposizioni introdotte dalla legge 6 novembre 2012, n. 190, da ultimo modificata dal decreto legislativo 25 maggio2016, n. 97. In tale sede, il legislatore ha inteso rafforzare i processi organizzativi interni a tutela dell'integrità e imparzialità dell'azione amministrativa, prevedendo che le Pubbliche amministrazioni debbano: definire piani di prevenzione della corruzione idonei a fornire una valutazione del diverso livello di esposizione al rischio di corruzione; individuare gli interventi necessari a prevenire tale rischio; predisporre procedure interne tese a favorire la segnalazione di condotte illecite o di casi di abuso ai soggetti designati ex lege o preposti a riceverle.

Inoltre, nelle procedure di evidenza pubblica strumentali alla scelta del contraente o partner privato, le disposizioni del codice dei contratti pubblici e della legislazione antimafia prevedono meccanismi di monitoraggio e interdizione di soggetti privi dei richiesti requisiti, finalizzati a ridurre il rischio di infiltrazioni criminali e a garantire la trasparente e imparziale gestione delle risorse pubbliche.

La presenza di meccanismi e garanzie procedimentali posti a presidio della legalità, liceità e imparzialità delle procedure regolate dal diritto pubblico rappresenta elemento di mitigazione del rischio che i soggetti che partecipano ai procedimenti amministrativi possano avvalersi in modo illegale dei provvedimenti adottati dalla P.A. nei loro confronti, per esercitare attività di riciclaggio e di finanziamento del terrorismo eventualmente correlato alle attività economiche costituenti oggetto delle predette procedure. D'altro canto, la mole consistente di dati che la Pubblica amministrazione è tenuta ad acquisire nell'espletamento di tali procedimenti costituisce una base informativa preziosa per individuare, anche alla luce degli indicatori di anomalia della UIF, condotte sospette di riciclaggio o di finanziamento del terrorismo, meritevoli di comunicazione alla UIF.

2. Procedure interne

Sulla base di scelte rientranti nella propria autonomia e, tenuto conto delle rispettive dimensioni, della numerosità e complessità delle rispettive attribuzioni e della conseguente complessità organizzativa le Pubbliche Amministrazioni adottano procedure interne idonee a consentire la valutazione, la gestione e la mitigazione dei rischi di riciclaggio e di finanziamento del terrorismo nonché a garantire il reperimento dei dati e delle informazioni concernenti le operazioni sospette, la loro tempestiva comunicazione alla UIF, la massima riservatezza dei soggetti coinvolti nella comunicazione stessa e l'omogeneità dei comportamenti.

In particolare, l'efficace implementazione delle procedure di comunicazione alla UIF richiede l'individuazione di un'unità organizzativa preposta alla comunicazione alla UIF dei dati e delle informazioni concernenti le operazioni sospette nonché alla gestione dei rapporti con la UIF medesima. Tale unità, individuata tenuto conto della complessità organizzativa e dimensionale dell'ente pubblico, non dovrebbe coincidere con l'ufficio o l'unità organizzativa direttamente competenti

allo svolgimento di compiti di amministrazione attiva o di controllo, nell'ambito dei procedimenti o procedure di cui all'articolo 10, comma 1, lettere a), b) e c), del decreto antiriciclaggio.

Nel caso di enti locali, o comunque di Pubbliche Amministrazioni con ridotte dimensioni, è possibile individuare un "gestore" comune ai fini dell'adempimento dell'obbligo di comunicazione dei dati e delle informazioni concernenti le operazioni sospette.

In caso di strutture organizzative particolarmente complesse si può designare più di un soggetto delegato dal gestore alla tenuta dei rapporti con la UIF. In tale ipotesi gli uffici prevedono adeguati meccanismi di coordinamento tra i delegati.

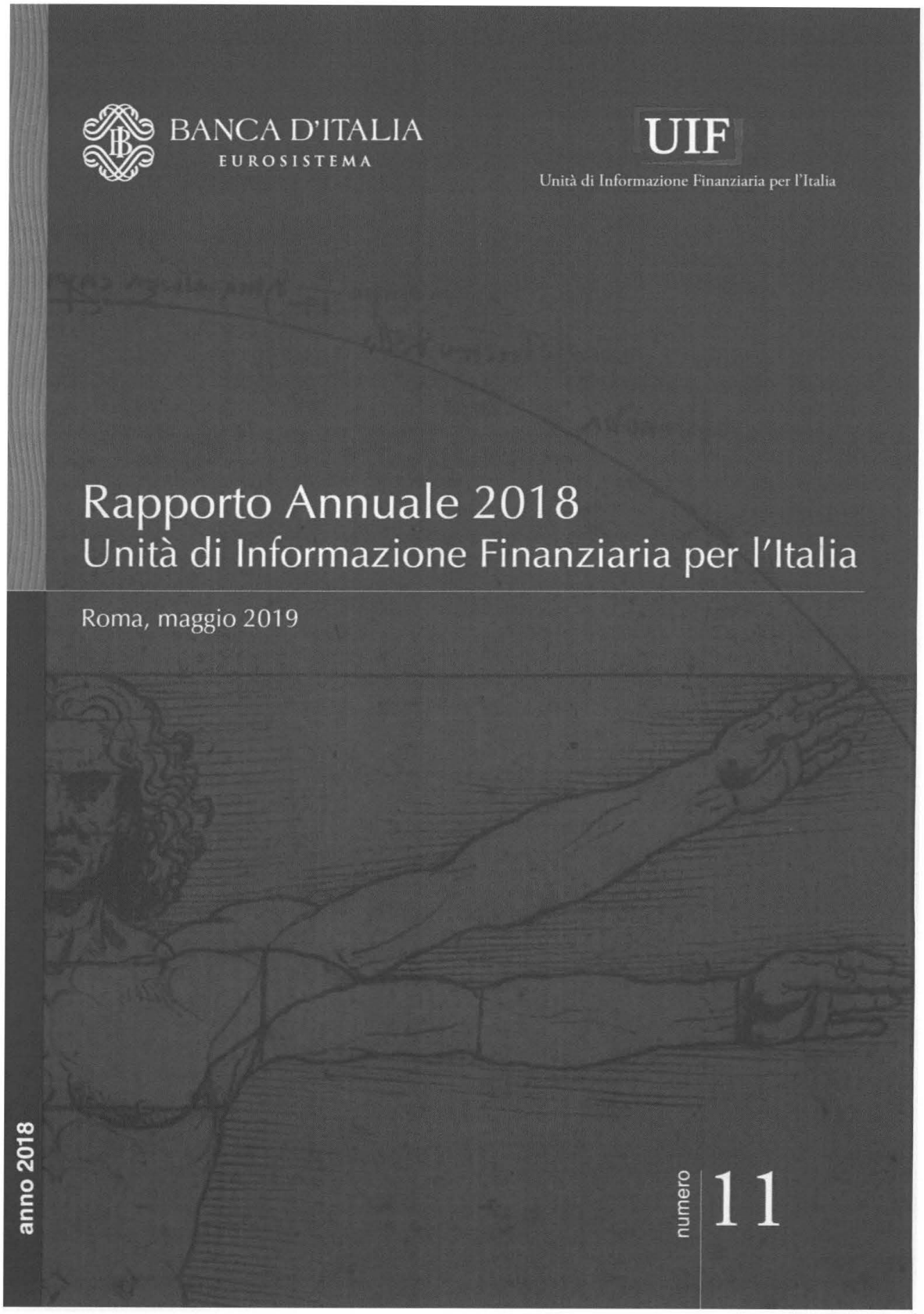
Il gestore effettua la valutazione del carattere sospetto dell'operazione avendo riguardo anche al ricorrere di indici di anomalia, individuati dalla UIF ai sensi dell'articolo 10, comma 4.

Le procedure interne devono assicurare la pronta ricostruibilità delle motivazioni delle decisioni del gestore.

Le amministrazioni assicurano, attraverso specifici piani di formazione, la diffusione ed applicazione degli indicatori di anomalia da parte dei propri dipendenti nonché la conoscenza delle istruzioni relative alle modalità di comunicazione dei dati e delle informazioni concernenti le operazioni sospette, adottate ai sensi dell'articolo 10, comma 4 del decreto antiriciclaggio.

Al fine di agevolare l'individuazione dei dati e delle informazioni rilevanti, le Pubbliche Amministrazioni, possono, nei limiti delle risorse umane, finanziarie e strumentali stanziate in bilancio e nel rispetto dei vincoli di contabilità pubblica posti dall'ordinamento vigente, adottare procedure di selezione automatica delle operazioni anomale basate su parametri quantitativi e qualitativi, in relazione alla complessità dell'attività svolta e alle proprie dimensioni organizzative e operative.

Il trattamento delle informazioni da parte degli uffici avviene nel rispetto delle disposizioni in materia di protezione dei dati personali.


BANCA D'ITALIA
EUROSISTEMA
UIF
Unità di Informazione Finanziaria per l'Italia
Rapporto Annuale 2018
Unità di Informazione Finanziaria per l'Italia
Roma, maggio 2019
anno 2018
numero 11

PAGINA BIANCA

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Rapporto Annuale 2018
Unità di Informazione Finanziaria per l'Italia

Roma, maggio 2019

L'Unità di Informazione Finanziaria per l'Italia (UIF) è l'unità centrale nazionale con funzioni di contrasto del riciclaggio e del finanziamento del terrorismo, istituita presso la Banca d'Italia dal D.lgs. 231/2007, in conformità di regole e criteri internazionali che prevedono la presenza in ciascuno Stato di una Financial Intelligence Unit *(FIU), dotata di piena autonomia operativa e gestionale.*

La UIF riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio o di finanziamento del terrorismo principalmente attraverso le segnalazioni di operazioni sospette trasmesse da intermediari finanziari, professionisti e altri operatori; ne effettua l'analisi finanziaria, utilizzando l'insieme delle fonti e dei poteri di cui dispone, e ne valuta la rilevanza ai fini dell'invio ai competenti Organi investigativi e giudiziari, per l'eventuale sviluppo dell'azione di repressione.

La normativa prevede scambi di informazione tra la UIF e le Autorità di vigilanza, le amministrazioni e gli ordini professionali. L'Unità e gli Organi investigativi e giudiziari collaborano ai fini dell'individuazione e dell'analisi di flussi finanziari anomali. L'Unità partecipa alla rete mondiale delle FIU per gli scambi informativi essenziali a fronteggiare la dimensione transnazionale del riciclaggio e del finanziamento del terrorismo.

Banca d'Italia, 2019

Unità di Informazione Finanziaria per l'Italia

Direttore responsabile
Claudio Clemente

Indirizzo
Largo Bastia, 35
00181 Roma – Italia

Telefono
+39 0647921

Sito internet
http://uif.bancaditalia.it

ISSN 2284-3205 (stampa)
ISSN 2284-3213 (online)

Stampato nel mese di giugno 2019 presso la Divisione Editoria e stampa della Banca d'Italia

Indice

Indice dei riquadri