Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di polizia fedpol

Ufficio di comunicazione in materia di riciclaggio di denaro (MROS)

Rapporto d'attività 2020

Maggio 2021

Ufficio di comunicazione in materia di riciclaggio di denaro MROS

Rapporto d'attività 2020

Maggio 2021

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di polizia fedpol
Ufficio di comunicazione in materia di riciclaggio di denaro
3003 Berna

Telefono: (+41) 058 463 40 40
E-Mail: mros.info@fedpol.admin.ch

Internet: http://www.fedpol.admin.ch

Indice

1. Prefazione

Anche il 2020 ha rappresentato un anno di sfide per l'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS). Grazie all'introduzione del sistema di informazione elettronico goAML è stato possibile affrontare la situazione eccezionale dovuta alla pandemia da COVID. La pandemia tuttavia ha anche offerto ai criminali varie opportunità per arricchirsi illegalmente, aumentando così il rischio di riciclaggio di denaro. Questo rischio si è manifestato con un nuovo incremento del numero di comunicazioni di sospetto inviate a MROS. Le 5334 segnalazioni pervenute nel 2020 hanno riguardato oltre 9000 relazioni d'affari, una cifra superiore di circa il 25 per cento a quella del 2019. Tale aumento è in linea con quello registrato nel 2018 e nel 2019. Nel corso del 2020 MROS ha inoltre trattato oltre 6000 relazioni d'affari segnalate durante il periodo compreso tra il 2016 e il 2019 che alla fine del 2019 risultavano ancora in corso di analisi.

Più di 1000 comunicazioni effettuate nel 2020 hanno riguardato dei sospetti di truffa in relazione con crediti accordati dagli istituti finanziari svizzeri su fideiussione della Confederazione. Tali comunicazioni hanno portato MROS a trasmettere oltre 800 denunce alle autorità di perseguimento penale. Centinaia di istruzioni penali sono state aperte. Questa particolarità si riflette anche nelle statistiche. La truffa è stata pertanto indicata come reato preliminare in oltre la metà delle comunicazioni di sospetto inviate a MROS nel 2020 (58 %), un incremento considerevole rispetto al 2019 (25 %). Per la prima volta, nell'anno in esame, il monitoraggio delle transazioni è l'elemento all'origine delle comunicazioni più menzionato dagli intermediari finanziari.

Il sistema goAML si è affermato tra gli intermediari finanziari. Nel dicembre 2020 circa il 90 per cento delle comunicazioni inviate a MROS sono pervenute per via elettronica. Questo risultato incoraggiante è il frutto degli sforzi intrapresi dagli intermediari finanziari per adeguarsi al nuovo sistema. MROS, dal canto suo, ha destinato risorse importanti al fine di sostenere e accompagnare gli intermediari finanziari e le autorità in questa fase di transizione. I dati trasmessi, tuttavia, per poter esser analizzati richiedono talvolta ancora un notevole lavoro di correzione e rifinitura da parte di MROS. Le importanti risorse che MROS ha dovuto impiegare nel 2020 a tale scopo in futuro andranno destinate all'analisi. Occorre pertanto adottare miglioramenti e adeguamenti per poter utilizzare a pieno il potenziale offerto dalle comunicazioni elettroniche.

Per la prima volta MROS presenta nel proprio rapporto d'attività alcune tipologie tematiche allo scopo di richiamare l'attenzione degli intermediari finanziari sui rischi costituiti da riciclaggio di denaro, criminalità organizzata o finanziamento del terrorismo di difficile individuazione. Abbiamo deciso di evidenziare tipologie specifiche concernenti i rischi in materia di finanziamento del terrorismo, partecipazione a un'organizzazione criminale, tratta di esseri umani e riciclaggio di denaro tramite criptovalute o identificazione online. Lo sviluppo dell'analisi strategica e la sensibilizzazione degli intermediari finanziari sono obiettivi centrali della nuova strategia di

MROS. Il trattamento elettronico di comunicazioni di sospetto offre al riguardo nuove opportunità che MROS intende sfruttare maggiormente nei prossimi anni.

Quale ulteriore novità, MROS presenta quest'anno statistiche sullo scambio d'informazioni con le autorità nazionali. Tale scambio ha acquistato infatti nuova importanza, dal punto di vista sia del contenuto sia degli oneri che comporta per MROS. Gli scambi con gli omologhi esteri hanno fatto registrare ugualmente un nuovo aumento durante l'anno in esame. Nel settembre 2020, il legislatore ha adottato una modifica della legge del 10 ottobre 1997 sul riciclaggio di denaro (LRD)[1] che concede a MROS maggiori competenze in tale ambito. In futuro, MROS potrà chiedere agli intermediari finanziari, alle condizioni previste da un nuovo art. 11a cpv. 2bis LRD, informazioni su relazioni d'affari oggetto di informazioni provenienti da un omologo estero. Tali miglioramenti contribuiranno a rafforzare l'efficacia del dispositivo antiriciclaggio svizzero.

I risultati raggiunti da MROS non sarebbero stati possibili senza il lavoro e l'impegno delle sue collaboratrici e dei suoi collaboratori. A loro va tutto il nostro riconoscimento e ringraziamento.

Berna, maggio 2021

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di polizia fedpol

Ufficio di comunicazione in materia di riciclaggio di denaro MROS

[1] RS **955.0**

2. Nuova organizzazione e strategia di MROS 2020-2021

Il 2020 è stato un anno di svolta per MROS all'insegna della trasformazione e dell'innovazione. Con l'entrata in vigore al 1° gennaio 2020 della modifica dell'ordinanza del 25 agosto 2004 sull'Ufficio di comunicazione in materia di riciclaggio di denaro (OURD)[2], è entrato pure in funzione il nuovo sistema d'informazione di MROS, denominato goAML. Sempre lo stesso giorno, MROS ha adottato una nuova strategia che è complementare alla strategia del Dipartimento federale di giustizia e polizia (DFGP) di lotta alla criminalità 2020-2023.[3] Queste trasformazioni hanno posto le basi per la riorganizzazione interna di MROS volta ad assicurare l'utilizzo di goAML e l'attuazione della nuova strategia (cfr. n. 2.3). Queste evoluzioni interdipendenti nascono dalla volontà di trasformare MROS in un'autorità moderna, proattiva e in grado di affrontare le sfide poste dal continuo sviluppo delle tecniche di riciclaggio di denaro, dei reati preliminari del riciclaggio, della criminalità organizzata e del finanziamento del terrorismo.

2.1 Un decennio di evoluzioni nel settore della lotta contro il riciclaggio di denaro, la criminalità organizzata e il finanziamento del terrorismo

Tra il 2010 e il 2019 il numero delle relazioni d'affari segnalate dagli intermediari finanziari svizzeri a MROS si è moltiplicato per sette. Anche gli scambi d'informazione con le Financial Intelligence Unit (FIU) estere sono aumentati e MROS deve far fronte a un numero sempre maggiore di richieste da parte delle autorità nazionali nell'ambito dell'assistenza amministrativa. Queste tendenze si sono confermate anche nell'anno in esame (cfr. n. 4) e nulla lascia suppore una loro inversione. Dal 2013 MROS beneficia di competenze supplementari nell'ambito dello scambio d'informazioni con i suoi omologhi esteri e gli intermediari finanziari.[4] Un'ulteriore estensione di queste competenze è prevista a partire dal 1° luglio di quest'anno (cfr. n. 6.2).
Sebbene a ritmi e livelli diversi, numerose FIU si sono viste confrontate con evoluzioni analoghe. Il volume delle informazioni finanziarie ricevute dalle FIU aumenta, le tecniche di riciclaggio di denaro evolvono soprattutto in relazione all'utilizzo di nuove tecnologie (cfr. n. 5.5), il ruolo delle FIU nel dispositivo antiriciclaggio acquisisce sempre maggiore importanza e le loro competenze si estendono, in particolare per quanto concerne lo scambio d'informazioni nazionale e internazionale. Tali evoluzioni sono riconducibili al potenziamento globale dei dispositivi di lotta contro il riciclaggio di denaro, i reati preliminari al riciclaggio di denaro, la criminalità organizzata e il finanziamento del terrorismo che genera una maggiore quantità di informazioni e dati. Non tutti questi elementi sono tuttavia rilevanti per il perseguimento penale, il ruolo di filtro assolto dalle FIU è pertanto essenziale.

---

[2] RS **955.23**

[3] Cfr. *strategia del DFGP di lotta alla criminalità 2020-2023.*

[4] Cfr. in proposito il *rapporto d'attività 2013 di MROS,* pagg. 55 e seg., disponibile sul sito internet di MROS.

Il paradigma nel quale operano le FIU è cambiato sul piano internazionale. Sono passati più di vent'anni da quando sono state fissate le prime norme internazionali antiriciclaggio e lo scopo del dispositivo normativo era di individuare e sequestrare i valori patrimoniali provenienti da un crimine. Da allora, l'obiettivo repressivo è stato integrato con una componente preventiva. Il ruolo assegnato alle FIU e la loro missione sono evoluti di conseguenza: non si tratta soltanto di identificare le informazioni utili alle autorità di perseguimento penale, ma anche di utilizzare tutti gli elementi segnalati dal dispositivo di lotta contro il riciclaggio di denaro, i reati preliminari del riciclaggio, la criminalità organizzata e il finanziamento del terrorismo in modo da individuarne i punti deboli. A tal fine le FIU allestiscono analisi strategiche volte a identificare i metodi e le tendenze in questi ambiti e condividono le loro constatazioni con gli intermediari finanziari, i commercianti, autorità terze, i responsabili politici o il pubblico interessato (*follow the money*).
Nell'ultimo decennio le risorse di MROS sono aumentate, ma non in modo sufficientemente rapido per permettergli di svolgere le proprie mansioni con i metodi attuali. I cambiamenti posti in essere a partire dall'inizio del 2020 scaturiscono dalla volontà di stare al passo con le evoluzioni del decennio trascorso così da poter affrontare meglio le sfide del futuro.
L'introduzione di goAML, un sistema informatico in grado di garantire il trattamento digitale delle informazioni segnalate a MROS, è l'elemento chiave di questa strategia. Il sistema consente di comunicare in modo rapido e sicuro con gli intermediari finanziari le autorità nazionali. Permette inoltre agli analisti di MROS di trattare le informazioni segnalate senza l'incomodo di doverle prima registrare nel sistema manualmente. Aldilà dell'accresciuta efficienza, questo passo verso la digitalizzazione costituisce soltanto una tappa del percorso verso un maggiore utilizzo di tecniche di analisi che si servono dell'intelligenza artificiale per analizzare quantità ingenti di dati (*intelligence led policing*). Al numero 3 tracceremo un primo bilancio dell'utilizzo di goAML a un anno dalla sua introduzione.

2.2 Strategia di MROS 2020-2021

Con l'inizio del 2020 MROS ha adottato una nuova strategia per gli anni 2020-2021 che si articola intorno a sette principi interdipendenti.

1) Le analisi di MROS sono effettive
2) La qualità delle comunicazioni di sospetto viene aumentata
3) MROS rafforza la prevenzione delle forme gravi e transnazionali di criminalità
4) Le autorità di perseguimento penale ricevono un sostegno ottimale da parte di MROS
5) La cooperazione internazionale è rafforzata ed effettiva
6) Le capacità tecniche di MROS sono ampliate
7) Le collaboratrici e i collaboratori di MROS sono formati adeguatamente

Il primo obiettivo di questa strategia è il trattamento più effettivo delle informazioni ricevute da MROS. Questo presuppone un triage rapido che permetta di determinare in modo appropriato il tipo di analisi cui sottoporre le informazioni in modo da impiegare le risorse di MROS laddove possono apportare il maggiore valore aggiunto. A lungo termine, anche tale triage dovrà essere eseguito con strumenti di intelligenza artificiale in grado, ad esempio, di individuare rapidamente gli elementi salienti di una comunicazione di sospetto o di ricollegare questi elementi a casi in corso. Dal 1° gennaio 2020 la profondità dell'analisi di MROS, ad esempio il numero e il tipo di verifiche eseguite dai collaboratori, è determinata in funzione di questo triage. In tale contesto vengono considerati sia gli elementi che caratterizzano la comunicazione (ad es. la complessità delle operazioni segnalate), sia la strategia del DFGP di lotta alla criminalità 2020-2023 e le esigenze delle autorità di perseguimento penale. Infine, la profondità dell'analisi dipende anche dai criteri di priorizzazione interni.
Sempre a partire dal 1° gennaio 2020 sono stati intrapresi notevoli sforzi per far sì che l'analisi risponda al meglio alle esigenze delle autorità di perseguimento penale. MROS ha quindi regolarmente incontrato i propri partner. Il nuovo sistema d'informazione permette di trasmettere informazioni tratte dalle comunicazioni di sospet-

to sotto forma digitale. I casi di poca rilevanza sono inoltre trattati rapidamente e i processi interni di MROS sono stati ridisegnati in modo da ridurre il fabbisogno in materia di risorse.
Come secondo obiettivo, la strategia intende incrementare la dimensione preventiva, già menzionata, del ruolo svolto da MROS. A tal fine occorre rafforzare l'analisi strategica dei rischi, delle tendenze e dei metodi di riciclaggio di denaro e finanziamento del terrorismo e condividere le constatazioni con gli intermediari finanziari, i commercianti e con le autorità interessate, ad esempio nell'ambito del processo di valutazione nazionale dei rischi eseguito sotto l'egida del Gruppo di coordinamento interdipartimentale per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo (GCRF). Questi lavori proseguiranno nel 2021.
L'attuazione di questa strategia richiede scambi più intensi tra MROS e i suoi partner, a prescindere che si tratti di autorità nazionali o internazionali, di organizzazioni internazionali (in primis il Gruppo di azione finanziaria [GAFI] e il gruppo Egmont) o del settore privato. Occorre inoltre accrescere la qualità delle informazioni scambiate con gli omologhi esteri, obiettivo il cui raggiungimento sarà facilitato anche dalle nuove competenze di MROS. Infine, la collaborazione con gli intermediari finanziari dovrà essere istituzionalizzata mediante un partenariato pubblico-privato che permetterà agli intermediari finanziari di individuare meglio i rischi e le operazioni sospette, di inviare comunicazioni di sospetto di qualità e di agire in chiave preventiva (*public private partnership*).

2.3 Nuova organizzazione di MROS

Nel 2019 il Consiglio federale ha accordato a MROS dodici posti a tempo pieno supplementari. Il 31 dicembre 2020 MROS disponeva di 57 posti equivalenti a un totale di 48,8 posti a tempo pieno, di cui 10,3 erano occupati con contratti a tempo determinato. L'attuazione della strategia di MROS 2020-2021 ha reso necessario riorganizzare questa divisione di fedpol. Dal primo gennaio 2020 MROS è quindi composto da sei settori, ciascuno con compiti specifici. Tre settori si occupano dell'analisi operativa, e più precisamente del trattamento delle comunicazioni di sospetto pervenute a MROS. Il settore Analisi preliminare riceve le informazioni e funge da coordinatore per la ricezione, il triage e l'attribuzione delle comunicazioni di sospetto. Tratta inoltre i casi per i quali occorre un'analisi rapida. Dell'analisi approfondita si occupano il settore Analisi operativa Cantoni, per i casi di competenza cantonale, e il settore Analisi operativa Confederazione, per i casi di competenza federale. Il settore Questioni internazionali è responsabile dello scambio internazionale di informazioni e dei lavori correlati alla partecipazione di MROS alle attività di organizzazioni internazionali (GAFI, gruppo Egmont).
Il settore Analisi strategica studia i metodi e le tendenze nell'ambito del riciclaggio di denaro e adempie i compiti relativi all'analisi nazionale dei rischi conferita a MROS. Il settore Pianificazione e questioni politiche assolve i compiti di conduzione dell'intera divisione, dello scambio di informazioni con autorità nazionali e si occupa delle procedure giuridiche che vedono il coinvolgimento di MROS.

2.4 Sfide future

Il 2020 è stato un anno intenso per MROS. Durante i primi mesi, la priorità è stata accordata alla messa in funzione del nuovo sistema d'informazione per le comunicazioni di sospetto. Questa scelta si è rivelata appropriata visto che goAML ha permesso a MROS di eseguire i propri compiti nonostante le circostanze straordinarie intercorse a partire da marzo a causa della pandemia.
L'introduzione del sistema ha tuttavia richiesto diversi adeguamenti e le sfide che ne sono scaturite non sono state ancora tutte risolte, segnatamente per quanto concerne la qualità delle informazioni trasmesse dagli intermediari finanziari e dai commercianti. Questo è un problema che MROS intende affrontare in modo prioritario. Serviranno sforzi considerevoli nella fase iniziale, ma a lungo termine sarà possibile ridurre la durata di trattamento delle comunicazioni di sospetto e incrementare la qualità dell'analisi. Nel corso del 2020 MROS ha inoltre evaso le oltre 6000 relazioni d'affari segnalate durante il periodo compreso tra il 2016 e il 2019 che alla fine del 2019 risultavano ancora in corso di analisi. Le priorità di MROS

nel 2021 saranno incentrate sull'attuazione della strategia. Il lavoro di (cfr. n. 4.13) analisi strategica ne risulterà potenziato e lo scambio di informazioni con gli intermediari finanziari rafforzato.

3. Introduzione del nuovo sistema d'informazione goAML in seno a MROS

Il 1° gennaio 2020 MROS ha introdotto il sistema d'informazione goAML. Il passaggio al nuovo sistema è stato un passo indispensabile nel processo di digitalizzazione. Da un lato, goAML permette agli intermediari finanziari, ai commercianti, alle autorità e agli organismi (organismi di autodisciplina [OAD] e organismi di vigilanza [OVI]) che rientrano nel campo di applicazione della LRD di inviare elettronicamente le proprie comunicazioni di sospetto tramite un portale online. Dall'altro lato, consente a MROS di trasmettere, a sua volta, sulla base dell'art. 23 cpv. 4 LRD, in formato digitale rapporti di analisi e la documentazione ad essi allegati alle competenti autorità svizzere di perseguimento penale, nonché di scambiare per via elettronica informazioni con autorità svizzere alle condizioni dell'art. 29 LRD.
Da allora goAML si è dimostrato uno strumento di comunicazione sicuro ed efficiente tra gli utenti che vi fanno ricorso. Inoltre, grazie alla trasmissione e al trattamento elettronico delle comunicazioni di sospetto, non soltanto è stato ridotto drasticamente il consumo di carta, ma ora è anche possibile lavorare senza vincoli temporali o spaziali. Nel contesto della pandemia di COVID quest'ultimo aspetto si è rivelato estremamente vantaggioso.
Il sistema ha, tuttavia, posto MROS dinanzi ad alcune sfide per quanto riguarda la trasmissione dei dati. Alcuni adeguamenti concernenti il numero di transazioni da registrare elettronicamente sono stati già pubblicati il 21 luglio 2020. Al più tardi a partire dal 1° aprile 2021 dovranno essere segnalate per via elettronica a MROS soltanto le transazioni sospette ai sensi dell'art. 3 cpv. 1 lett. h OURD. [5]
Occorre inoltre sottolineare che i dati trasmessi non sempre presentano la qualità richiesta (cfr. n. 3.5).

3.1 Numero di intermediari finanziari registrati

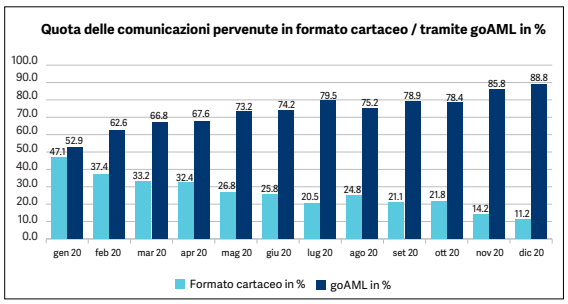
Al 31 dicembre 2020 si erano registrati in goAML 728 intermediari finanziari e 1494 persone ad essi collegate. Alcuni intermediari finanziari hanno iniziato la procedura di registrazione, senza tuttavia completare la fase successiva.
Su 728 intermediari finanziari registrati, soltanto 252 finora hanno inviato a MROS una comunicazione di sospetto tramite goAML.

3.2 Quota delle comunicazioni di sospetto inviate elettronicamente

Dal passaggio a goAML, gli intermediari finanziari si sono avvalsi frequentemente della possibilità di inviare le comunicazioni per via elettronica. Già a gennaio, la quota di comunicazioni di sospetto inviate tramite goAML si è attestata a oltre il 50 per cento, facendo registrare un aumento costante nei mesi successivi. A dicembre 2020 la quota delle comunicazioni di sospetto inviate elettronicamente ha raggiunto il 90 per cento. Il

[5] Cfr. documento pubblicato sul sito Internet di MROS *Adeguamento della prassi in materia di comunicazione tramite goAML.* Questa pubblicazione è stata sostituita in data 30 marzo 2021 dalla versione 2.0 (*Adeguamento della prassi per le comunicazioni tramite goAML valida dal 1 aprile 2021*).

grafico seguente illustra le comunicazioni pervenute, suddivise per modalità di invio (elettronico e cartaceo).



Nel corso del 2020, goAML ha dimostrato la sua utilità anche per quanto riguarda le richieste di informazioni inviate da MROS in virtù dell'art. 11a LRD. Gli intermediari finanziari possono assolvere gli obblighi derivanti dall'articolo di legge in questione tramite goAML compilando la scheda relativa al tipo di rapporto appropriato. In tale ambito, la quota dei documenti e delle informazioni inviate in formato digitale mediante goAML è soddisfacente e da gennaio a dicembre 2020 è aumentata dal 46 per cento al 68 per cento. MROS spera incrementare ulteriormente tale percentuale nel 2021.

3.3 Modalità di invio di comunicazioni di sospetto tramite goAML

Per rispondere adeguatamente alle esigenze degli intermediari finanziari, sono state sviluppate diverse soluzioni tecniche per inviare elettronicamente le comunicazioni di sospetto a MROS. Attualmente è possibile avvalersi di tre modalità di invio tramite goAML (v. di seguito). Ulteriori informazioni e documenti relativi alle diverse soluzioni sono disponibili online.[6]

3.3.1 Elaborazione automatica dei dati (*upload*)

Per allestire una comunicazione in modo automatizzato, l'intermediario finanziario autore della comunicazione di sospetto deve aver programmato un applicativo interno. Quest'ultimo permette di estrarre i dati dal sistema dell'autore della comunicazione e di importarli in un file XML dalla struttura predefinita. Il file è in seguito caricato sul portale online di goAML e trasmesso a MROS. Incombe agli intermediari finanziari autori delle comunicazioni sviluppare la soluzione informatica necessaria a tale scopo.

3.3.2 Registrazione semiautomatica

La registrazione semiautomatica prevede una registrazione manuale della comunicazione nel portale online di goAML seguita, tuttavia dal caricamento delle informazioni relative ai conti e alle transazioni tramite file XML. Le informazioni mancanti possono in seguito essere integrate manualmente. Il vantaggio di questa modalità è che gli intermediari finanziari che non intendono introdurre la soluzione automatizzata possono comunque risparmiare tempo anche qualora abbiano un numero elevato di transazioni da segnalare. Per poter impiegare questa modalità di invio, le transazioni devono essere estratte dal sistema bancario, salvate localmente in un file XML in base a una struttura predefinita e in seguito caricate su goAML Web.

3.3.3 Registrazione manuale

La registrazione manuale di una comunicazione avviene direttamente nel portale online di goAML e non richiede alcun requisito tecnico, a parte l'accesso a Internet e ai dati di login personali. Questa procedura prevede la registrazione dei dati rilevanti e la compilazione di ciascun campo previsto. A seconda della tipologia di comunicazione, la registrazione manuale può richiedere molto tempo, soprattutto se le transazioni da registrare sono numerose.

3.4 Supporto goAML

Con l'introduzione di goAML è stata messa a disposizione una guida per la registrazione

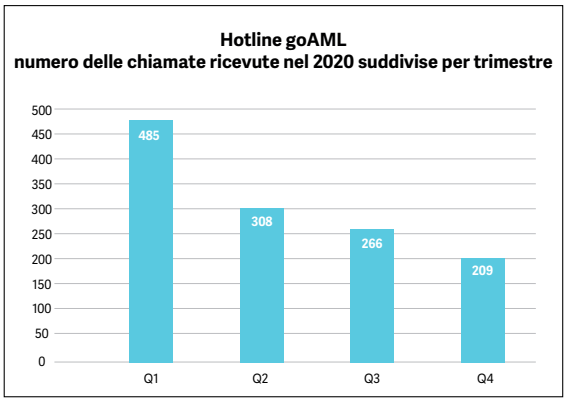
[6] Cfr. documento pubblicato sul sito Internet di MROS Informazione concernente l'introduzione del nuovo sistema di trattamento dei dati goAML presso MROS.

manuale di comunicazioni sul portale online. Nel 2020, MROS ha inoltre allestito un documento contenente le risposte alle domande frequenti[7] poste dagli intermediari finanziari e ha aggiornato il manuale goAML Web.[8] Gli ulteriori documenti accessibili online hanno lo scopo di agevolare agli intermediari finanziari la registrazione delle comunicazioni di sospetto. Una newsletter fornisce regolarmente consigli utili agli autori delle segnalazioni registrati su goAML. Le newsletter sono uno strumento utile per comunicare direttamente con gli utenti di goAML e in futuro saranno pubblicate con cadenza regolare.

3.4.1 *Hotline* di goAML

Per poter fornire il miglior sostegno possibile agli intermediari finanziari, alle autorità e ad altri utenti nel passaggio a goAML, MROS ha inoltre allestito un'apposita *hotline* (raggiungibile telefonicamente o tramite posta elettronica).
Per tale supporto tecnico (p. es. per la registrazione sul portale, per domande specifiche sulla registrazione di una comunicazione o sull'impostazione della registrazione automatica tramite file XML), MROS ha messo a disposizione i propri collaboratori. Già durante la fase di registrazione sul portale e nella prima metà dell'anno, la *hotline* di goAML è stata contattata da decine di utenti ogni giorno. Oggi il sistema d'informazione goAML gode di una diffusa accettazione da parte degli autori delle segnalazioni. I riscontri positivi da parte degli intermediari finanziari dimostrano inoltre che l'onere supplementare cui ha dovuto far fronte MROS in aggiunta alle sue attività quotidiane ha portato i suoi frutti.

Il grafico seguente illustra la panoramica del carico di lavoro della *hotline* di goAML nel 2020. Complessivamente, nel 2020 i collaboratori della *hotline* di MROS hanno risposto a 1268 richieste telefoniche e a numerose altre chiamate effettuate ai numeri diretti (p. es. domande successive alle prime richieste).



3.5 Qualità delle informazioni pervenute

Come accennato, durante il primo anno la qualità dei dati trasmessi dagli intermediari finanziari, e in particolare delle informazioni relative alle transazioni, si è rivelata in parte insufficiente. Ciò ha comportato per MROS un notevole onere nel lavoro di correzione. Tali compiti aggiuntivi sono stati inoltre svolti in prevalenza manualmente affinché si potessero avere a disposizione dati corretti e utilizzabili nell'attività di analisi. Spesso non erano ad esempio chiari quali persone o quali relazioni d'affari fossero oggetto della comunicazione. MROS si è inoltre impegnato a illustrare agli intermediari finanziari gli errori sistematici nello sviluppo delle interfacce informatiche in modo tale da ridurre la percentuale delle comunicazioni rifiutate automaticamente dal sistema per problemi legati alla qualità dei dati.
Tali considerazioni mostrano quanto sia importante per MROS e le autorità di perseguimento penale ricevere dati di buona qualità. Occorre evitare che MROS debba correggere sistematicamente dati sbagliati e che vada dunque perso uno dei vantaggi principali offerti da un sistema elettronico di comunicazione.

Per MROS è fondamentale ricevere dati corretti e utilizzabili affinché MROS e le competenti autorità di perseguimento penale possano analizzarli in modo efficiente e mirato. Nella comunicazione di transazioni è indispensabile che le necessa-

[7] Cfr. documento pubblicato sul sito Internet di MROS *goAML: Domande frequenti (FAQ)*
[8] Cfr. *goAML Web – Manuale* disponibile sul sito Internet di MROS.

rie informazioni di base fornite (dati relativi alle persone, ai conti ecc.) siano complete e corrette, affinché le summenzionate autorità possano svolgere la propria attività di analisi.

3.6 Prospettive

Il software goAML è fornito dalla UNODC (*Ufficio delle Nazioni Unite sulla Droga e il Crimine*), l'agenzia delle Nazioni Unite con sede a Vienna ed è attualmente impiegato in oltre 60 Paesi. L'UNODC intende inoltre continuare a sviluppare il software e ad oggi sta lavorando allo sviluppo di ulteriori funzionalità in particolare per quanto riguarda i settori delle criptovalute, delle *Entity-to-Entity-Relation* e delle persone politicamente esposte (PPE). Tali adeguamenti sono effettuati in stretta collaborazione e sulla base delle esigenze espresse dalle FIU interessate. Una nuova versione di goAML è in corso di elaborazione.

4. Statistica annuale di MROS

Il modo di contare le comunicazioni di sospetto ricevute da MROS è cambiato con l'introduzione di goAML. A partire dal 1° gennaio 2020 non viene più contato il numero delle relazioni d'affari segnalate, bensì il numero delle comunicazioni pervenute a MROS. Visto che all'interno della medesima comunicazione di sospetto possono essere segnalate più relazioni d'affari, è difficile eseguire un confronto esatto tra le cifre relative al 2020 e quelle degli anni precedenti.
Per poter offrire almeno un'idea della progressione cronologica delle statistiche, è stato deciso di pubblicare, laddove possibile, le cifre sotto forma percentuale. Nel 2019 ciascuna comunicazione di sospetto inviata a MROS dagli intermediari finanziari svizzeri comprendevano in media 1,8 relazioni d'affari. Questa media è stata utilizzata per valutare la progressione delle comunicazioni ricevute da MROS nel 2020 e, per quanto possibile, eseguire confronti con le cifre degli anni precedenti.

4.1 Panoramica statistica MROS 2020

Riassunto dell'anno d'esercizio 2020
(1° gennaio-31 dicembre 2020)

Numero di comunicazioni	2020 Assoluto	2020 Relativo
Totale pervenuto	**5 334**	**100,0 %**
Comunicazioni trattate	4 505	84,5 %
In corso di analisi al 31 dicembre 2020	829	15,5 %
Ramo d'attività dell'intermediario finanziario		
Banche	4 773	89,5 %
Fornitori di servizi di pagamento	185	3,5 %
Altri	121	2,3 %
Carte di credito	83	1,6 %
Amministratori patrimoniali / Consulenti in materia d'investimenti	45	0,9 %
Fiduciarie	30	0,6 %
Case da gioco	29	0,5 %
Assicurazioni	20	0,4 %
Operazioni di credito, leasing, factoring e forfetizzazione	19	0,4 %
Commercio di materie prime e metalli preziosi	12	0,2 %
Avvocati e notai	6	0,1 %
Trustees	4	0,1 %
Uffici di cambio	3	0,1 %
Agenti in valori di borsa	2	0,0 %
Organismi di autodisciplina (OAD)/ FINMA/CFMG	2	0,0 %

La tabella fornisce una panoramica delle comunicazioni ricevute da MROS durante l'anno in esame, ma non delle comunicazioni complessivamente trattate nel 2020. Alla fine del 2019, 6095 relazioni d'affari segnalate tra il 2016 e il 2019 erano ancora in fase di analisi. Queste relazioni

d'affari sono state evase sostanzialmente nel corso del 2020 (cfr. n. 4.13) senza tuttavia figurare nella tabella sopra riportata.

Denunce	1939	100,0 %
Al Ministero pubblico della Confederazione	175	9,0 %
Ai Ministeri pubblici cantonali	1764	91,0 %

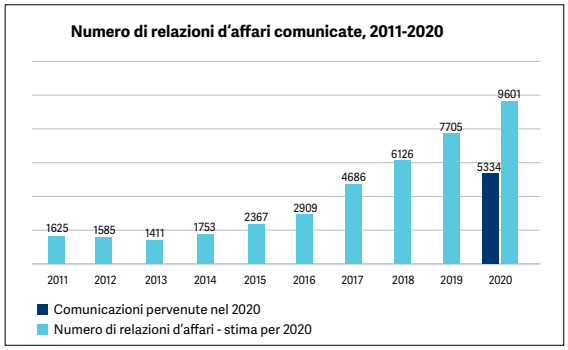
La presente tabella offre una panoramica delle denunce eseguite da MROS nel 2020 alle autorità di perseguimento penale. Contrariamente al 2019, le denunce non consistono più nella trasmissione, ad analisi effettuata, delle comunicazioni ricevute da MROS. Per denunce s'intendono i rapporti elaborati da MROS sulla base delle informazioni a sua disposizione provenienti principalmente dalle comunicazioni, ma non solo. Le informazioni contenute in una denuncia possono essere tratte da fonti provenienti da diverse autorità e da più di una comunicazione (cfr. n. 4.12). In alcuni casi, le denunce effettuate nel 2020 contengono informazioni segnalate negli anni precedenti, cosicché il numero di denunce trasmesse nell'anno in esame non può essere ricollegato al numero di comunicazioni ricevute nello stesso periodo.

4.2 Osservazioni generali

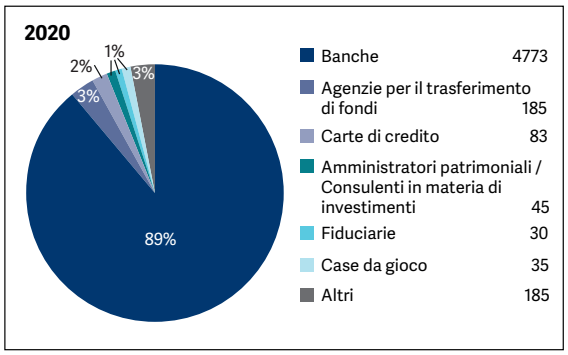
1. Nel 2019 sono state comunicate a MROS 7705 relazioni d'affari. Nel 2020, invece l'Ufficio comunicazione ha ricevuto 5334 comunicazioni di sospetto. Considerato che nel 2019 le comunicazioni di sospetto inviate a MROS dagli intermediari finanziari comprendevano in media 1,8 relazioni d'affari, si stima che le 5334 comunicazioni ricevute da MROS nel 2020 corrispondano a un aumento circa del 25 per cento delle relazioni d'affari segnalate (pari a 9601 relazioni d'affari stimate per il 2020) rispetto al 2019.
2. Tale aumento è in parte riconducibile alle numerose comunicazioni inviate a MROS per sospetti di appropriazione indebita o conseguimento fraudolento di crediti COVID.
3. Come nel 2019, la stragrande maggioranza delle comunicazioni (89,5 %) è stata segnalata dal settore bancario.
4. Nel 58 per cento delle comunicazioni inviate nel 2020 è la truffa il reato preliminare indicato dagli intermediari finanziari. Sebbene a livello statistico non sia possibile eseguire un confronto esatto con gli anni precedenti, si tratta comunque di una percentuale che colloca la truffa in vetta alla classifica dei presunti reati preliminari maggiormente indicati dagli intermediari finanziari.
5. Per la prima volta, gli intermediari finanziari hanno indicato la sorveglianza delle transazioni quale elemento che maggiormente contribuisce a suscitare sospetti (cfr. n. 4.8).

4.3 Comunicazioni di sospetto

Poiché il modo di contare le comunicazioni di sospetto è stato adeguato in concomitanza con la messa in funzione di goAML, per permettere un confronto con gli anni precedenti si fa riferimento alla media di relazioni d'affari per comunicazione inviata a MROS dagli intermediari finanziari svizzeri durante il 2019. Questa media è pari a 1,8 relazioni d'affari per comunicazione. Le 5334 comunicazioni ricevute da MROS nel 2020 corrispondono quindi a 9601 relazioni d'affari. Secondo questa stima, il numero delle comunicazioni pervenute nel 2020 è pertanto incrementato di quasi il 25 per cento rispetto al 2019. Ciò conferma la tendenza rilevata sin dal 2015.



4.4 Ramo d'attività degli intermediari finanziari autori delle comunicazioni



- Quasi il 90 per cento delle comunicazioni di sospetto pervenute sono state inviate dal settore bancario.
- La ripartizione per ramo d'attività dei vari intermediari finanziari autori di comunicazioni di sospetto è molto stabile. Come nel 2019, le fiduciarie, gli amministratori patrimoniali / i consulenti in materia di investimenti e le case da gioco hanno inviato complessivamente l'un per cento delle comunicazioni, mentre i fornitori di servizi di pagamento sono passate dal quattro al tre per cento delle comunicazioni trasmesse.

Per un confronto: 2011-2020[9]

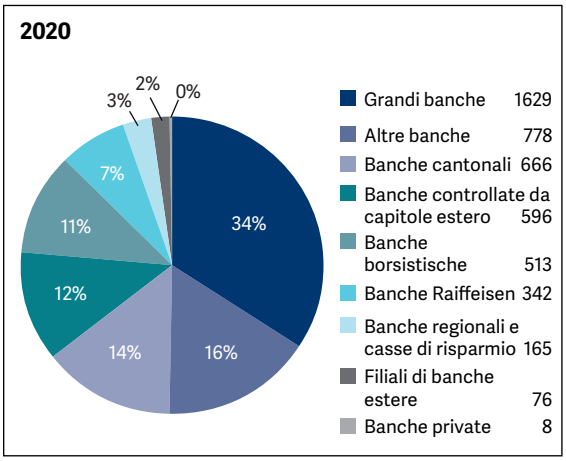
Ramo d'attività	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in valori assoluti	Media 2011-2020
Banche	66,5	66,2	79,6	85,3	91,3	86,0	91,0	88,8	89,9	89,5	4773	**83,4**
Fornitori di servizi di pagamento	23,3	22,9	5,2	6,1	2,4	4,4	3,1	4,4	4,0	3,5	185	**7,9**
Altri	0,1	0,3	0,1	0,2	0,2	0,7	0,4	2,3	0,6	2,3	121	**0,7**
Emittenti di carte di credito	0,6	1,4	1,0	0,5	0,5	0,7	0,3	1,2	1,3	1,6	83	**0,9**
Amministratori patrimoniali / i consulenti in materia di investimenti	1,7	3,1	5,2	2,3	1,9	2,2	1,9	1,0	0,9	0,8	45	**2,1**
Fiduciarie	3,8	4,1	4,9	2,8	2,0	1,5	1,1	0,7	0,8	0,6	30	**2,2**
Case da gioco	0,4	0,4	0,6	0,5	0,1	0,5	0,6	0,5	0,7	0,5	29	**0,5**
Assicurazioni	0,7	0,6	1,3	0,6	0,5	3,1	0,5	0,6	0,3	0,4	20	**0,9**
Operazioni di credito, leasing, factoring e forfetizzazione	0,3	0,1	0,3	0,2	0,3	0,3	0,3	0,3	0,3	0,4	19	**0,3**
Commercio di materie prime e metalli preziosi	0,1	0,2	0,7	0,2	0,3	0,1	0,2		0,3	0,2	12	**0,2**
Avvocati e notai	1,9	0,8	0,6	0,6	0,3	0,2	0,1	0,1	0,1	0,1	6	**0,5**
Trustees										0,1	4	**0,0**
Uffici di cambio	0,2									0,1	3	**0,0**
Agenti di valori in borsa	0,0	0,1	0,1	0,6	0,1	0,1	0,3	0,1	0,3	0,0	2	**0,2**
OAD	0,1			0,1					0,1	0,0	2	**0,0**
Operazioni in valute estere	0,4		0,4			0,1			0,3	0,0	0	**0,1**
Autorità				0,1							0	**0,0**
Distributori di fondi d'investimento							0,1				0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**5334**	**100,0**

[9] Le cifre assolute per gli anni 2011-2019 sono pubblicate nei rapporti d'attività di MROS relativi agli anni corrispondenti. Per motivi di completezza, occorre precisare che i commercianti non figurano in questa statistica perché MROS ha ricevuto solo una comunicazione di sospetto da un commerciante nel 2017 e una nel 2019. Ciò corrisponde a meno dello 0,1 per cento del totale delle comunicazioni di sospetto ricevute in quegli anni.

– La categoria «Altri» racchiude in modo particolare i fornitori di servizi finanziari in relazione alle monete virtuali (*virtual asset service provider (VASP)*)[10]. La crescita del numero di comunicazioni inviate da tale categoria è anche parzialmente dovuta alla nuova modalità con l'introduzione di goAML di recensire le comunicazioni di sospetto trasmesse.

4.5 Banche

Il grafico a lato indica il numero di comunicazioni inviate da ogni tipo di banca.



Per un confronto: 2011-2020[11]

Tipo di banca[12]	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in valori assoluti	Media 2011-2020
Banche cantonali	6,9	7,6	6,4	5,0	5,8	7,6	5,2	5,5	5,3	14,0	666	**6,9**
Banche regionali e casse di risparmio	28,7	29,3	28,9	31,7	35,3	31,1	26,3	26,7	28,2	34,1	1629	**30,0**
Banche regionali e casse di risparmio	1,4	1,8	0,5	0,9	0,5	1,2	0,6	1,1	1,3	3,5	165	**1,3**
Banche Raiffeisen	5,6	6,1	7,0	9,0	5,8	6,2	3,9	3,2	3,1	7,2	342	**5,7**
Banche borsistiche	14,4	12,1	10,2	10,6	14,0	12,4	12,7	20,8	25,1	10,7	513	**14,3**
Altre banche	2,5	4,0	20,5	14,3	9,9	12,9	9,6	9,5	8,6	16,3	778	**10,8**
Banche private	2,4	5,7	4,6	2,6	1,8	2,3	1,7	1,9	1,3	0,2	8	**2,5**
Banche controllate da capitale estero	36,0	33,1	21,4	25,6	26,6	26,3	39,8	31,0	26,9	12,5	596	**27,9**
Filiali di banche estere	1,9	0,2	0,4	0,2	0,3	0,1	0,1	0,3	0,2	1,6	76	**0,5**
Istituti con sfera d'affari speciale	0,1	0,0	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**4773**	**100,0**

– La tabella indica importanti cambiamenti rispetto al 2019: la percentuale delle comunicazioni inviate da banche private, banche borsistiche e banche controllate da capitale estero ha subito una flessione (rispettivamente dall'1 allo 0 %, dal 25 all'11 % e dal 27 al 12 %), mentre la quota delle comunicazioni effettuate da grandi banche, banche cantonali, banche Raiffeisen e altre banche è aumentata (rispettivamente dal 28 al 34 %, dal 5 al 14 %, dal 3 al 7 % e dall'8 al 16 %).
– Questi cambiamenti sono in parte dovuti al modo diverso di contare le comunicazioni di sospetto (cfr. n. 4 e 4.13). Il peso degli intermediari finanziari che tendono a comunicare molteplici relazioni d'affari non è più così

[10] Per VASP s'intendono le borse di criptovalute, i fornitori di wallet, i fornitori di servizi finanziari in relazione con l'emissione, l'offerta e la vendita di valori patrimoniali virtuali e altri possibili servizi d'intermediazione finanziaria offerti in relazione a criptovalute.

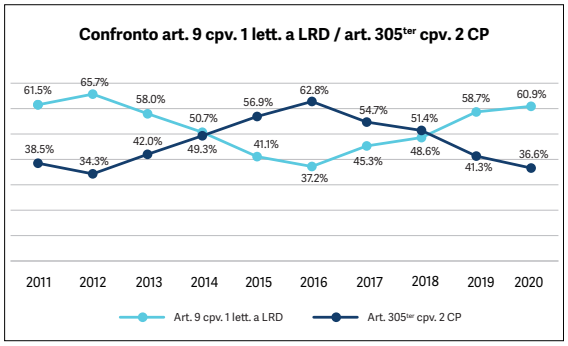
[11] Le cifre assolute per gli anni 2011-2019 sono pubblicate nei rapporti d'attività di MROS relativi agli anni corrispondenti.

[12] I tipi di banche e l'ordine indicato corrispondono a quelli utilizzati dalla Banca nazionale svizzera. Cfr. la pubblicazione *Le banche in Svizzera 2019*, pag. 9.

importante perché è il numero delle comunicazioni e non più quello delle relazioni d'affari che è considerato nella statistica.
– La crescita delle comunicazioni trasmesse dalle banche cantonali (dal 5,3 % nel 2019 al 14 % nel 2020) è in parte riconducibile alle numerose comunicazioni correlate ai crediti COVID.

4.6 Basi legali delle comunicazioni di sospetto

Delle 5334 comunicazioni pervenute nell'anno in esame, 3248 (pari al 60,9 % del totale) sono state inviate in virtù dell'obbligo di comunicazione sancito dall'art. 9 cpv. 1 lett. a LRD e 1952 (pari al 36,6 %) in virtù del diritto di comunicazione retto dall'art. 305ter cpv. 2 del Codice penale svizzero del 21 dicembre 1937 (CP)[13]. 129 comunicazioni sono state inviate in virtù dell'art. 9 cpv. 1 lett. b LRD (2,4 %) e due in virtù dell'art. 27 cpv. 4 LRD.



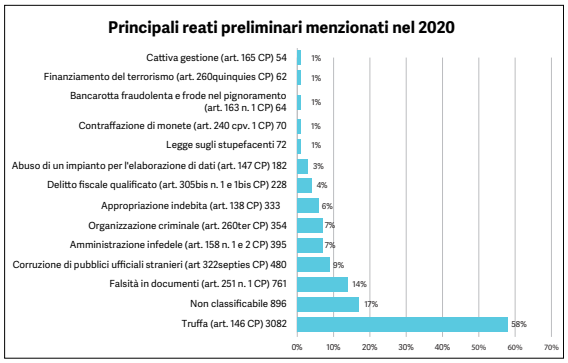
Prosegue pertanto l'aumento della percentuale di comunicazioni inviate conformemente all'art. 9 cpv. 1 lett. a LRD osservato a partire dal 2016. Considerando che la stragrande maggioranza delle comunicazioni ricevute da MROS sono inviate dal settore bancario, questa tendenza illustra soprattutto il comportamento di tale settore. Tra le banche svizzere che inviano comunicazioni, il ricorso al diritto o all'obbligo di comunicazione dipende fortemente dal tipo di banca autrice della segnalazione. La tabella indicata di seguito evidenzia questa situazione.

4.7 Reati preliminari

Il grafico illustra le percentuali relative ai presunti reati preliminari indicati nelle comunicazioni di sospetto pervenute nel 2020. Contrariamente ai criteri applicati fino nel 2019, a partire dal 2020 l'intermediario finanziario può indicare diversi potenziali reati preliminari per ciascuna comunicazione. È quindi possibile determinare la percentuale relativa a un reato preliminare indicato nelle comunicazioni pervenute. La somma di tali percentuali supera tuttavia il 100 per cento, motivo per cui il confronto con i valori degli anni precedenti risulta falsato e ha carattere meramente indicativo.

Tipo di banca	Art. 9 cpv. 1 lett. a LRD	in %	Art. 305ter cpv. 2 CP	in %	Altri	in %	Totale	in %
Banche cantonali	554	83,1	106	15,9	6	0,9	666	100,0
Grandi banche	790	48,5	829	50,8	10	0,6	1629	100,0
Banche regionali e casse di risparmio	97	58,7	60	36,3	8	4,8	165	100,0
Banche Raiffeisen	305	89,1	28	8,1	9	2,6	342	100,0
Banche borsistiche	230	44,8	250	48,7	33	6,4	513	100,0
Altre banche	663	85,2	101	12,9	14	1,8	778	100,0
Banche private	3	37,5	5	62,5	0	0,0	8	100,0
Banche controllate da capitale estero	301	50,5	269	45,1	26	4,3	596	100,0
Filiali di banche estere	12	15,7	64	84,2	0	0,0	76	100,0
Total	**2955**	**61,9**	**1712**	**35,8**	**106**	**2,2**	**4773**	**100,0**

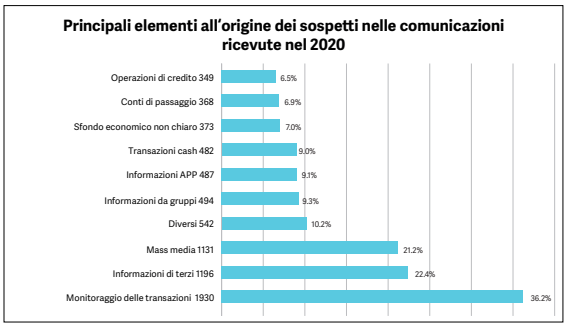
[13] RS **311.0**



– Le notevoli differenze rilevate tra il 2020 e gli anni precedenti sono dovute in parte alla possibilità ora offerta agli intermediari finanziari di indicare più presunti reati preliminari selezionandoli da un elenco generale aggiornato e ampliato.
– Nell'anno in esame il numero dei sospetti per truffa ha fatto registrare un'impennata: se nel 2018 questo reato preliminare era stato indicato nel 20 per cento delle comunicazioni e nel 2019 nel 25 per cento e nel 2020 tale percentuale è aumentata al 58 per cento. Questa crescita è in parte riconducibile al notevole numero di segnalazioni pervenute in relazione alla concessione di crediti COVID (cfr. n. 5.1).
– Nel 2020 il numero delle comunicazioni con il presunto reato preliminare di corruzione ha subito una flessione drastica. La corruzione di pubblici ufficiali stranieri è stata indicata in 480 comunicazioni (9 %), la corruzione attiva di pubblici ufficiali svizzeri in 21 comunicazioni (0,39 %) e la corruzione passiva di pubblici ufficiali svizzeri in 17 casi (0,32 %). Queste tre categorie, che negli anni precedenti non figuravano in modo distinto, nel 2018 rappresentavano ancora il 27 per cento delle comunicazioni e nel 2019 il 24 per cento.
  È difficile trovare un motivo in grado di spiegare simili differenze che intercorrono tra un anno e l'altro. La riduzione dei sospetti di riciclaggio di denaro correlati a fatti di corruzione è in parte dovuta a determinati complessi di casi internazionali che negli ultimi anni hanno influenzato la piazza finanziaria svizzera e, contrariamente a ora, hanno suscitato numerose comunicazioni a MROS.

4.8 Elementi che suscitano sospetto

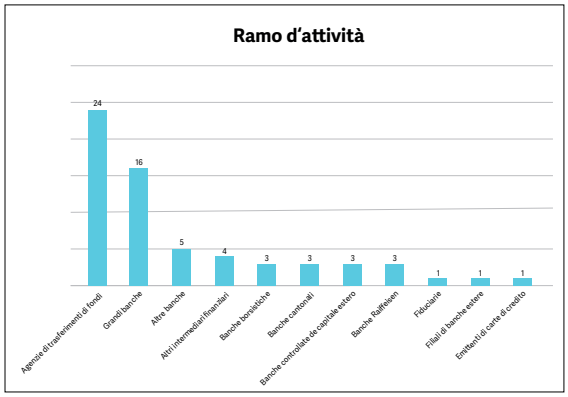
Il grafico indica il tasso percentuale di ricorrenza degli elementi che suscitano sospetto indicati nelle comunicazioni pervenute nel 2020. Come per i reati preliminari e contrariamente al passato, il nuovo sistema d'informazione goAML permette agli intermediari finanziari di indicare più di un elemento che ha suscitato sospetto. È quindi possibile calcolare la misura in cui un elemento particolare è stato determinante nella decisione di inviare una comunicazione, mentre non è più possibile procedere ad un confronto esatto di questi importi con quelli degli anni precedenti.



– Non è pertinente confrontare queste cifre con quelle degli anni precedenti, quando poteva essere indicato un unico elemento che suscitasse sospetto.
– Per la prima volta, nell'anno in esame il monitoraggio delle transazioni è l'elemento che suscita il sospetto più indicato nelle comunicazioni (36,2 % nel 2020 rispetto al 31 % nel 2019 e il 25 % nel 2018). È una conferma della maggiore sensibilizzazione degli intermediari finanziari nel procedere con i chiarimenti e con le analisi transazionali in applicazione dell'art. 6 cpv. 2 LRD.
– Nel 2020, le informazioni dei mass media hanno suscitato in misura assai meno importante il sospetto all'origine della comunicazione rispetto agli anni precedenti quando esso era l'elemento più frequente a suscitare sospetti negli intermediari finanziari (21,2 % dei casi rispetto al 35 % nel 2019 e il 38 % nel 2018).

4.9 Finanziamento del terrorismo

Nell'anno in esame, MROS ha ricevuto 64 comunicazioni per sospetto finanziamento del terrorismo e/o per sospetta violazione della legge federale che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate [14], pari all'1,2 per cento del totale delle comunicazioni pervenute. Poiché si suppone che in ogni comunicazione venga segnalata una media di circa 1,8 relazioni d'affari, queste 64 comunicazioni corrisponderebbero a circa 115 relazioni d'affari, ovvero un numero pressoché identico a quello registrato nel 2019 (114). Queste 64 comunicazioni di sospetto sono associate anche ad altri reati preliminari, in concreto all'appartenenza a un'organizzazione criminale (19 casi), alla truffa (7 casi), alla corruzione di pubblici ufficiali stranieri (3 casi) mentre in dieci casi sono stati indicati altri presunti reati preliminari.
L'elemento che suscita sospetto maggiormente indicato dagli intermediari finanziari, segnatamente dai fornitori di servizi di pagamento, è il monitoraggio delle transazioni (33 casi), seguito dalle informazioni pubblicate dai mass media (20 casi), dalle transazioni in contanti (15 casi), dalle informazioni di terzi (13 casi), dai legami con Paesi a rischio (8 casi), mentre in 12 casi sono stati indicati altri elementi.
La maggior parte delle comunicazioni (34) sono state inviate dalle banche, mentre i fornitori di servizi di pagamento ne hanno allestite 24. Solo sei comunicazioni rientranti in questa categoria sono state inviate da altri tipi di intermediari finanziari.



Delle 64 comunicazioni pervenute nel 2020, 47 sono state oggetto di una decisione di non trasmissione da parte di MROS mentre due erano ancora in corso di analisi da parte di MROS alla fine dell'anno in esame. Le informazioni tratte dalle restanti 15 segnalazioni hanno generato 14 denunce presso le autorità di perseguimento penale competenti. In tre casi, i procedimenti penali sono stati formalmente aperti, ma uno di questi è stato avviato per traffico di esseri umani e non per violazione della legge federale che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate.

4.10 Organizzazioni criminali

Nel 2020 MROS ha ricevuto 354 comunicazioni per sospetto legame con un'organizzazione criminale, pari al 6,6 per cento delle comunicazioni complessive. Considerando le riserve espresse sopra in merito al confronto delle cifre del 2020 con quelle degli anni precedenti, tale percentuale rappresenta una crescita rispetto al 2019, quando le comunicazioni relative a questi sospetti ammontavano soltanto al 2,4 per cento del totale delle relazioni d'affari comunicate.
Nell'anno in esame, nelle comunicazioni per sospetto legame con un'organizzazione criminale erano indicati anche altri potenziali reati preliminari: corruzione di pubblici ufficiali stranieri (111 casi), truffa (72 casi), contraffazione di monete (67 casi), falsità in documenti (26 casi) e finanziamento del terrorismo (23 casi).

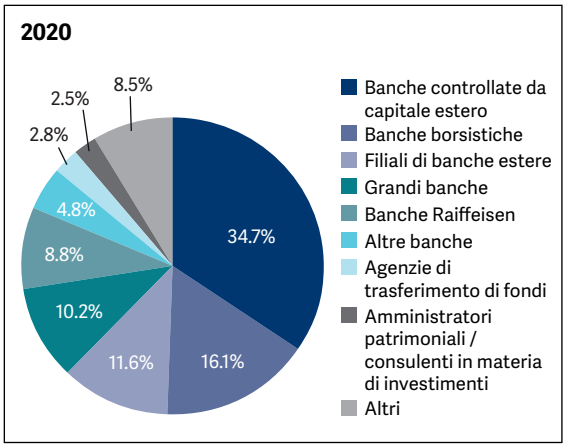
[14] RS **122**

Principali altri reati preliminari menzionati nelle comunicazioni di sospetto per sospetto legame di appartenenza ad organizzazioni criminali	Numero di menzioni	in %
Corruzione di pubblici ufficiali stranieri	111	31,4
Truffa	72	20,3
Contraffazione di monete	67	18,9
Falsità in documenti	26	7,3
Finanziamento del terrorismo	23	6,5
Legge sugli stupefacenti	20	5,6
Appropriazione indebita	12	3,4
Amministrazione infedele	9	2,5
Estorsione	5	1,4
Legge sulle armi	4	1,1
Furto	2	0,6
Infedeltà nella gestione pubblica	2	0,6
Corruzione di pubblici ufficiali svizzeri. Corruzione attiva	1	0,3

I seguenti elementi che suscitano sospetto sono all'origine nel 2020 della trasmissione ad MROS delle comunicazioni che, tra gli altri, indicavano come motivo alla base della comunicazione l'appartenenza a un'organizzazione criminale.

Elementi all'origine del sospetto	Numero di menzioni	in %
Mass media	168	47,5
Monitoraggio delle transazioni	115	32,5
Transazioni cash	82	23,2
Diversi	76	21,5
Informazioni di terzi	42	11,9
Informazioni da gruppi	28	7,9
Informazioni APP	20	5,6
Apertura di relazioni d'affari	18	5,1
Paesi a rischio	16	4,5

La stragrande maggioranza (88,7 %) delle comunicazioni per sospetto legame con un'organizzazione criminale ricevute da MROS proviene dal settore bancario, seguito da quello dei fornitori di servizi di pagamento (2,82 %), dagli amministratori patrimoniali / dai consulenti in materia di investimenti (2,54 %) e dalle assicurazioni (2,26 %). I principali tipi di banche all'origine di tali comunicazioni sono i seguenti.



Delle 354 comunicazioni, 256 (pari al 73,2 %) sono state oggetto di una decisione di non trasmissione mentre 24 sono ancora in corso di analisi. Delle 74 comunicazioni restanti, MROS ha trasmesso 46 denunce alle autorità alle autorità di perseguimento penale competenti: otto sono state oggetto di decreti di non luogo a procedere mentre le altre 38 sono ancora in corso di trattamento da parte delle competenti autorità di perseguimento penale.

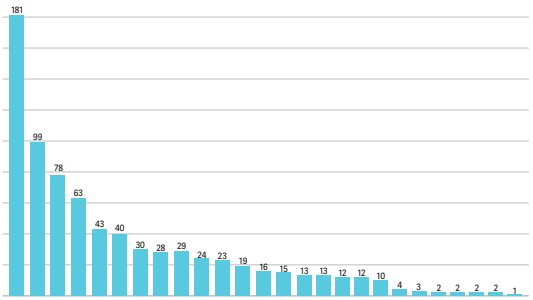
4.11 Pandemia da COVID

Il 2020 è stato caratterizzato dalla pandemia da CODIV che ha offerto ai criminali varie opportunità per arricchirsi illegalmente, aumentando così il rischio di riciclaggio di denaro. Dalle statistiche di MROS emergono, tra le diverse tipologie di presunto riciclaggio di denaro indicate nelle comunicazioni di sospetto trasmesse a MROS nell'anno in esame (cfr. n. 5.1), l'appropriazione indebita e l'utilizzo fraudolento di crediti accordati dagli istituti finanziari svizzeri su fideiussione della Confederazione. Tra l'introduzione di questi crediti tramite l'ordinanza del 25 marzo 2020 sulle fideiussioni solidali COVID-19[15] e la fine del 2020, MROS ha ricevuto 1046 comunicazioni di sospetto relative a questa tipologia che vertevano su 1054 crediti COVID, accordati da 43 banche

[15] RS **951.261.** Il 19 dicembre 2020 quest'ultima è stata sostituita dalla legge federale del 18 dicembre 2020 concernente i crediti garantiti da una fideiussione solidale in seguito al coronavirus (Legge sulle fideiussioni solidali COVID-19, LFiS-COVID-19; RS **951.26**).

diverse per un importo complessivo di 146 853 347 franchi.[16]
Nel 2020 MROS ha trasmesso 764 denunce alle autorità di perseguimento penale in relazione a 914 comunicazioni di sospetto. Alla fine del 2020, 27 comunicazioni concernenti crediti COVID erano ancora in corso di analisi.
Il grafico seguente indica le autorità di perseguimento penale alle quali sono state effettuate delle denunce. In seguito alle trasmissioni di MROS, le autorità di perseguimento penale hanno aperto svariate centinaia di istruzioni penali. Nell'ambito di questa pandemia così pesante e dagli sviluppi inattesi, MROS ha confermato il suo ruolo centrale (cfr. n. 5.1).

Denunce relative ai crediti COVID inviate alle autorità di perseguimento penale competenti nel 2020



Legenda

AG	Aargau	NW	Nidwalden
AI	Appenzel Inner Rhodes	OW	Obwalden
AR	Appenzel Outer Rhodes	SG	St. Gallen
BE	Bern	SH	Schaffhausen
BL	Basel-Landschaft	SO	Solothurn
BS	Basel-Stadt	SZ	Schwyz
CH	Office of the Attorney General of Switzerland	TG	Thurgau
FR	Fribourg	TI	Ticino
GE	Geneva	UR	Uri
GL	Glarus	VD	Vaud
GR	Graubunden	VS	Valais
JU	Jura	ZG	Zug
LU	Lucerne	ZH	Zurich
NE	Neuchatel		

4.12 Denunce alle autorità di perseguimento penale

Nel 2020 MROS ha trasmesso alle autorità di perseguimento penale 1939 denunce. Con la modifica dell'OURD[17] entrata in vigore il 1°gennaio 2020, le comunicazioni non sono più trasmesse alle autorità di perseguimento penale. Al fine di garantire la protezione delle fonti, non è neppure trasmessa alcuna indicazione relativa all'autore della comunicazione o alla persona che ha comunicato informazioni trasmesse alle autorità di perseguimento penale (cfr. art. 8 cpv. 1 OURD). Le informazioni rilevanti e le analisi di MROS relative a tali informazioni sono infatti trasmesse sotto forma di rapporto per via elettronica alle autorità di perseguimento penale. I rapporti di analisi destinati alle autorità di perseguimento penale possono contenere informazioni provenienti da diverse fonti o varie comunicazioni (art. 1 cpv. 2 lettere a-e OURD). Anche se nella prassi succede ancora che un rapporto contenga in primo luogo le informazioni di una comunicazione, ciò non costituisce più la regola. È la natura aggregata delle informazioni registrate da MROS che determina la loro sorte. Come già annunciato nel nostro rapporto d'attività 2019[18], la nozione di «quota di trasmissione» delle comunicazioni di sospetto non ha pertanto più senso.
Visto che le denunce trasmesse possono contenere informazioni provenienti da diverse fonti e varie comunicazioni, talvolta pervenute in anni diversi, non è più possibile ricollegarle al numero di comunicazioni ricevute in un determinato anno.
Le denunce trasmesse nel 2020 contenevano informazioni provenienti da:

- 2156 comunicazioni di sospetto pervenute nel 2020;
- 179 relazioni d'affari segnalate nel 2019;
- 52 relazioni d'affari segnalate nel 2018;
- 12 relazioni d'affari segnalate nel 2017;
- tre relazioni d'affari segnalate nel 2016;
- una relazione d'affari segnalata nel 2014;
- quattro relazioni d'affari segnalate nel 2011.

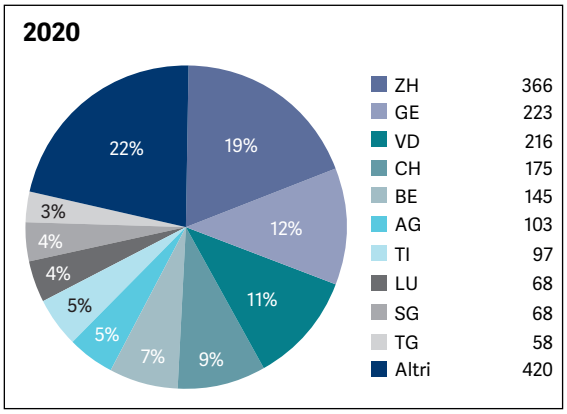
16 Cfr. le statistiche pubblicate in merito sulla pagina Internet di MROS *Crediti transitori COVID-19.*

17 Cfr. *les commentaires à la révision partielle de l'OBCBA* del 24 novembre 2019 (non disponibile in italiano), pag. 9-10 e 16.

18 Cfr. *Rapporto annuale di MROS 2019,* pag. 9.

Il numero delle comunicazioni di sospetto pervenute dopo il 22 novembre 2019[19], ovvero 2235, si riferisce a comunicazioni eventualmente contenenti più di una relazione d'affari. Il numero di comunicazioni pervenute prima di tale data, corrispondeva invece al numero delle relazioni d'affari segnalate.

Autorità di perseguimento penale interessate
Il grafico indica le autorità di perseguimento penale cui MROS ha trasmesso le 1939 denunce nel 2020.



Per un confronto: 2011-2020 (in %)

Autorità	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in valori assoluti	Media 2011-2020
ZH	19,7	14,4	18,4	12,4	13,5	12,0	10,2	12,8	14,3	18,9	366	14,7
GE	12,6	15,1	15,0	12,7	8,4	14,9	12,8	14,1	15,0	11,5	223	13,2
VD	4,7	2,1	2,4	2,5	2,6	3,1	1,8	4,3	5,5	11,1	216	4,0
CH	31,9	35,8	34,2	44,7	53,4	38,1	52,6	48,4	39,9	9,0	175	38,8
BE	3,2	3,8	1,6	4,6	1,8	3,0	1,6	1,8	3,3	7,5	145	3,2
AG	3,3	2,0	1,3	1,8	1,5	2,6	1,2	1,6	1,5	5,3	v	2,2
TI	8,5	13,6	12,5	7,3	6,5	6,0	6,0	3,3	3,3	5,0	97	7,2
SG	4,5	2,2	1,7	3,0	2,0	2,2	2,4	1,3	1,2	3,5	68	2,4
LU	0,6	1,1	1,5	1,8	1,0	1,4	1,4	0,8	1,8	3,5	68	1,5
TG	0,6	1,1	0,7	1,1	0,8	1,5	0,7	0,8	1,3	3,0	58	1,2
FR	0,7	1,2	0,5	0,2	0,6	0,6	1,4	1,6	1,5	2,7	53	1,1
VS	0,5	0,4	1,1	1,0	0,5	1,0	1,2	1,4	0,8	2,7	53	1,1
BS	3,4	2,7	2,2	1,2	1,3	3,3	2,0	0,9	0,9	2,6	50	2,0
ZG	1,3	0,6	1,2	1,3	1,5	1,2	0,6	1,9	1,9	2,5	49	1,4
NE	0,7	0,6	0,7	0,9	1,1	0,9	1,0	1,2	1,4	2,3	44	1,1
BL	0,5	1,3	0,8	0,5	1,5	1,5	1,2	0,8	2,9	2,1	41	1,3
SO	0,9	0,1	1,1	0,7	0,4	4,2	0,4	1,1	1,2	1,9	37	1,2
GR	0,5	0,5	0,9	1,0	0,6	0,3	0,5	0,3	0,4	1,5	29	0,7
SZ	0,6	0,6	0,6	0,2	0,5	0,8	0,5	0,3	0,4	1,0	20	0,6
AR	0,1	0,1	0,2	0,2	0,1	0,3	0,2	0,2	0,3	0,6	12	0,2
SH	0,5	0,4	0,6	0,3	0,1	0,5	0,3	0,1	0,3	0,5	10	0,4
UR	0,0	0,0	0,0	0,1	0,0	0,2	0,0	0,0	0,0	0,3	6	0,1
NW	0,3	0,0	0,4	0,1	0,1	0,0	0,0	0,7	0,2	0,3	5	0,2
JU	0,1	0,1	0,2	0,6	0,0	0,3	0,1	0,1	0,1	0,3	5	0,2
GL	0,0	0,0	0,1	0,0	0,0	0,1	0,1	0,2	0,0	0,2	3	0,1
OW	0,1	0,2	0,0	0,0	0,1	0,0	0,0	0,0	0,3	0,2	3	0,1
AI	0,1	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	0,0
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**0**	**100,0**

[19] A partire da questa data, MROS registra le comunicazioni ricevute nel sistema d'informazione goAML. Rientrano in tale categoria 76 delle 179 comunicazioni pervenute nel 2019 che sono alla base delle denunce trasmesse da MROS alle autorità di perseguimento penale nel 2020. Le 76 comunicazioni vertevano su 153 relazioni d'affari. Il totale delle relazioni d'affari segnalate a MROS nel 2019, sulla cui base sono state allestite le denunce trasmesse alle autorità di perseguimento penale nel 2020, ammonta pertanto a 256.

Per ragioni statistiche e per il differente modo di contare le comunicazioni di sospetto, il confronto con gli anni precedenti non è pertinente. In seguito all'introduzione del sistema d'informazione goAML, una denuncia può riguardare più comunicazioni con più relazioni d'affari e le informazioni trasmesse possono provenire anche da altre fonti, non solo dalle comunicazioni.
Per la prima volta, il Ministero pubblico della Confederazione (MPC) non è l'autorità di perseguimento penale cui MROS ha trasmesso il maggior numero di denunce. Ha infatti ricevuto soltanto il 9 per cento delle denunce effettuate nel 2020 rispetto al 40 per cento nel 2019 e il 49 per cento nel 2018. Questa flessione merita tuttavia di essere spiegata: nella maggior parte dei casi, le denunce trasmesse all'MPC concernono fatti di riciclaggio correlati a reati preliminari compiuti all'estero. Le denunce sono pertanto molto complesse e contengono informazioni che provengono con maggiore frequenza da più relazioni d'affari. Per le denunce trasmesse alle autorità di perseguimento penale cantonali, invece, le informazioni provengono in generale da un'unica comunicazione di sospetto.
Nel 2020 il numero delle denunce trasmesse alle autorità di perseguimento penale del Cantone di Zurigo superano ampiamente quelle destinate al Cantone di Ginevra (19 % rispetto a 12 %). Finora entrambi i Cantoni ricevevano quasi la stessa quantità di denunce da parte di MROS, quelle trasmesse a Ginevra erano leggermente più numerose di quello di Zurigo.
Sempre per la prima volta, sono state trasmesse più denunce alle autorità di perseguimento penale dei Cantoni di Vaud, Berna e Argovia che a quelle del Ticino.
Gli altri 17 Cantoni insieme hanno ricevuto più denunce trasmesse da MROS rispetto al Cantone di Zurigo (420 contro 366). Si tratta di una netta inversione di tendenza rispetto a quanto registrato fino nel 2019, quando i 17 o i 18 Cantoni con meno denunce da parte di MROS raramente raggiungevano un totale superiore al 15 per cento delle denunce.
Oltre ai cambiamenti introdotti dal sistema d'informazione goAML, che rendono difficile il confronto con gli anni precedenti, le differenze constatate sono anche in parte riconducibili al trattamento di numerose comunicazioni inviate a MROS per sospetti correlati ai crediti COVID. Questo spiega la percentuale ridotta di denunce trasmesse all'MPC che in genere non è competente per evadere questo genere di casi e il numero più elevato di denunce trasmesse ai Cantoni di Vaud, Berna e Argovia rispetto al Ticino.

4.13 Evasione delle comunicazioni degli anni 2016-2019 in attesa di analisi

A fine 2019, 6095 relazioni d'affari segnalate a MROS tra il 2016 e il 2019 erano ancora in corso di analisi (10 del 2016, 737 del 2017, 1717 del 2018 e 3631 del 2019). Nell'anno in esame MROS ha dedicato un impegno speciale all'evasione di questi casi. La stragrande maggioranza di esse è stata oggetto di una decisione di non trasmissione (94,5 %), mentre il 4,9 per cento di queste comunicazioni è servito ad allestire le denunce trasmesse alle competenti autorità di perseguimento penale. La tabella seguente illustra i dettagli in base agli anni in cui tali relazioni di affari sono pervenute a MROS.

Anno della ricezione	2016	2017	2018	2019	Total
Decisione di non trasmissione	10	730	1680	3342	5762
Denuncia		6	34	256	296
In corso di analisi		1	3	33	37
Total	**10**	**737**	**1717**	**3631**	**6095**

4.14 Scambi d'informazioni con altre FIU

I servizi omologhi esteri, ovvero le altre FIU, e MROS possono servirsi del canale dell'assistenza amministrativa internazionale per scambiarsi informazioni relative alla lotta contro il finanziamento del terrorismo, il riciclaggio del denaro e i relativi reati preliminari e la criminalità organizzata. Quando MROS riceve una comunicazione di sospetto che concerne persone fisiche o giuridiche domiciliate all'estero, può chiedere informazioni su queste persone o società ai servizi omologhi nei rispettivi Paesi. Le informazioni ottenute sono importanti per l'attività di analisi di MROS, visto che la maggioranza delle comunicazioni di sospetto inviate a MROS presentano legami con l'estero.

Nel 2020 MROS ha ricevuto 795 richieste da FIU di 95 Paesi, meno quindi rispetto alle 844 richieste ricevute da FIU di 103 Paesi nel 2019. MROS ha trattato 684 delle richieste relative al 2020, pari all'86 per cento. La durata media di trattamento di queste richieste è di 41 giorni lavorativi. Nell'anno in esame MROS ha inoltre risposto a 173 richieste d'informazioni che erano pervenute nel 2019.
Nel 2020 sono state trattate 5212 richieste d'informazione di servizi omologhi esteri relative a persone fisiche e giuridiche (2733 persone giuridiche e 2479 persone fisiche). 4169 di esse (2155 persone giuridiche e 1994 persone fisiche) erano oggetto di richieste d'informazione dei servizi omologhi esteri ricevute e trattate nel 2020.
Per informazioni spontanee s'intendono informazione correlate alla Svizzera inviate a MROS da una FIU e che non richiedono alcuna risposta o, viceversa, informazioni inviate da MROS a servizi omologhi esteri. Dal 2015 il numero delle informazioni spontanee trattate nel corso dell'anno è indicato a parte. Nell'anno in esame, MROS ha ricevuto 504 informazioni spontanee da FIU di 47 Paesi e ne ha inviate 365 a 76 FIU.
Nel 2020 MROS ha inviato 126 richieste d'informazione a 46 servizi omologhi esteri. Le richieste riguardavano 364 persone giuridiche e 303 persone fisiche. Per rispondere alle singole richieste, nell'anno in esame le FIU contattate hanno impiegato mediamente 30 giorni lavorativi.

4.15 Scambi d'informazioni con autorità nazionali

MROS non scambia informazioni soltanto con i servizi omologhi esteri, bensì anche con autorità svizzere, come le autorità di vigilanza o altre autorità attive nella lotta contro il riciclaggio di denaro e i relativi reati preliminari, la criminalità organizzata o il finanziamento del terrorismo. MROS è autorizzato a scambiare informazioni con tali autorità nel rispetto delle condizioni sancite dall'art. 29 LRD. Le statistiche su questi scambi finora non venivano pubblicate nei rapporti d'attività. Nel frattempo gli scambi d'informazioni hanno tuttavia acquisito una nuova importanza sia riguardo al loro contenuto sia all'onere che rappresentano per MROS.

Nel 2020, 26 autorità svizzere si sono rivolte a MROS con 392 richieste d'informazioni su persone fisiche e società nell'ambito di indagini su fatti di riciclaggio di denaro, criminalità organizzata o finanziamento del terrorismo. Circa nell'80 per cento dei casi, le richieste provenivano dalle polizie cantonali e dalla Polizia giudiziaria federale. Queste 392 richieste d'informazioni corrispondono a un aumento superiore al 200 per cento rispetto agli anni precedenti: nel 2018 e nel 2019 MROS aveva ricevuto 117 richieste d'informazioni da autorità svizzere.
Il ruolo di MROS nei confronti di altre autorità svizzere impegnate nella lotta contro il riciclaggio di denaro e i relativi reati preliminari, la criminalità organizzata e il finanziamento del terrorismo, non si limita a rispondere alle richieste d'informazioni da loro inviate. Nell'ambito delle sue analisi, MROS è anche autorizzato a trasmettere spontaneamente informazioni in suo possesso ad altre autorità svizzera attive nella vigilanza in materia e nella lotta al riciclaggio di denaro, dei reati preliminari al riciclaggio di denaro, alla criminalità organizzata o al finanziamento del terrorismo. In tale contesto, MROS nel 2020 ha trasmesso 69 informazioni spontanee. MROS può inoltre chiedere alle autorità federali, cantonali e comunali la consegna delle informazioni di cui ha bisogno per eseguire le proprie analisi. Questa tipologia di richiesta non è riportata nelle cifre di cui sopra.

5. Tipologie per la sensibilizzazione degli intermediari finanziari

Le tipologie illustrate qui di seguito non scaturiscono, per scelta precisa, dalle comunicazioni di sospetto rappresentative del 2020, ma, se si eccettuano i casi legati alla pandemia da COVID (cfr. n. 5.1), riguardano fatti segnalati con frequenza relativamente minore nell'anno in esame. Nel 2020, ad esempio, le comunicazioni di sospetto correlate a organizzazioni criminali e al finanziamento del terrorismo hanno costituito appena il 7,8 per cento del numero complessivo di segnalazioni trasmesse a MROS. In entrambi i casi si tratta di categorie di reato su cui è incentrata la strategia del DFGP di lotta alla criminalità 2020-2023.
Gli esempi concreti di seguito riportati descrivono in che modo vengono riciclati i presunti proventi di reato. Inoltre mettono in luce le nuove tendenze e i metodi ricorrenti utilizzati e permettono di trarre conclusioni al riguardo. Queste tipologie servono da un lato come base per lavori scientifici e, dall'altro, sono uno strumento importante per sensibilizzare gli intermediari finanziari. Lo scopo è indicare a questi ultimi quali tipi di conto, di strumenti finanziari e di modelli di comportamento necessitano di una maggiore attenzione alla luce dei rischi individuati da MROS.

5.1 Casi correlati alla pandemia da COVID

L'incremento del numero di comunicazioni ricevute da MROS nel 2020 è ascrivibile alla segnalazione di sospetti di riciclaggio di denaro correlati alla pandemia da COVID, che rappresentano circa un terzo delle comunicazioni trasmesse a MROS nel 2020. La situazione particolare generata dalla pandemia ha infatti offerto ai criminali innumerevoli opportunità per arricchirsi illegalmente, aumentando così il rischio di riciclaggio di denaro. I rischi individuati a livello internazionale nell'ambito della lotta al riciclaggio di denaro, alle organizzazioni criminali e al finanziamento del terrorismo sono di molteplice natura.[20] Tali rischi spaziano dalla sottrazione di somme stanziate da organi statali o sovranazionali per la lotta alla pandemia all'aumento del fenomeno della cibercriminalità, favorito dal ricorso generalizzato al telelavoro, passando per le truffe legate alla commercializzazione di materiale sanitario fino al rischio accresciuto di immissione di beni patrimoniali di origine illecita nei settori economici in difficoltà.
Il 2 e il 29 aprile 2020 MROS ha contattato, a titolo preventivo, gli intermediari finanziari svizzeri, tramite goAML, per metterli in guardia dai rischi legati alla pandemia nonché ai crediti COVID.
Come accennato, tra le comunicazioni di sospetto ricevute da MROS si evidenziano tre rischi specifici di riciclaggio di denaro correlati alla pandemia. Il primo concerne la sottrazione o l'utilizzo indebito di prestiti concessi alle imprese dietro garanzia delle autorità pubbliche svizzere. Il 25 marzo 2020 il Consiglio federale ha adottato un'ordinanza concernente le fideiussioni

[20] Dalla primavera del 2020, diversi organismi nazionali e internazionali hanno pubblicato analisi e avvisi su questo tema. Si veda ad esempio l'analisi pubblicata dal GAFI a maggio 2020 (www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html) e aggiornata a dicembre dello stesso anno.

solidali legate al COVID-19 [21], che ha permesso alle imprese individuali, alle società di persone o alle persone giuridiche con sede in Svizzera di ottenere dagli istituti di credito svizzeri prestiti garantiti dalla Confederazione a condizioni agevolate. L'ordinanza è stata sostituita il 19 dicembre 2020 dalla legge federale del 18 dicembre 2020 sulle fideiussioni solidali COVID-19 (LFiS-COVID-19)[22]. Il rischio che questi crediti possano essere oggetto di appropriazione indebita è reale. Nel 2020 MROS ha ricevuto più di 1000 segnalazioni riguardanti oltre 1100 crediti da parte di intermediari finanziari allarmati dal prelievo in contanti o dal trasferimento verso conti personali di fondi concessi in tale ambito, da fatturati visibilmente gonfiati o dall'utilizzo di crediti in violazione delle condizioni stabilite dall'ordinanza del Consiglio federale.[23]

Più di 800 denunce sono state sporte in questo ambito alle competenti autorità di perseguimento penale, in particolare per sospetta truffa e/o falsità in documenti e amministrazione infedele. In seguito a tali trasmissioni, le autorità di perseguimento penale hanno aperto diverse centinaia di inchieste penali.

Un'altra tipologia di criminalità economica che ha trovato terreno fertile durante la pandemia è quella delle truffe via Internet mediante il ricorso al *phishing* o all'ingegneria sociale. I relativi reati preliminari, pur non essendo direttamente correlati al COVID, sono diventati più frequenti per via delle misure di confinamento adottate in diversi Paesi. Tali misure hanno infatti avvicinato a Internet persone che normalmente non lo utilizzano e che risultano quindi più vulnerabili alle truffe che vi proliferano. L'aumento di questi casi, che è stato peraltro significativo nella maggior parte dei Paesi, ha determinato anche un leggero incremento delle comunicazioni trasmesse a MROS in questo ambito.

Se le somme interessate da quest'ultima tipologia sono generalmente modeste, lo stesso non si può dire per quelle coinvolte nei reati commessi nel quadro del commercio di materiale sanitario, che ammontano infatti spesso a diversi milioni di franchi. Le ordinazioni massicce di maschere, di liquido idroalcolico e di altri prodotti sanitari da parte di autorità statali e, talvolta, anche di aziende private sono state effettuate in una situazione di urgenza, spianando la strada agli abusi e in parte anche alle truffe. Gli acquirenti si sono così ritrovati con del materiale inefficace o di cattiva qualità, ad attendere invano una fornitura o a pagare un prezzo gonfiato. Inoltre il panico generato dalla pandemia ha portato gran parte della popolazione a rifornirsi di materiale di questo tipo, spesso su Internet, e a dar credito a pubblicità ingannevoli di sedicenti medicamenti anti-COVID. I casi di questo tipo riguardano alcune decine di segnalazioni per sospette truffe, commesse perlopiù all'estero. I principali elementi all'origine dei sospetti sono la dubbia autenticità dei contratti presentati per giustificare le transazioni, il repentino cambiamento del settore d'attività di una società senza alcuna esperienza precedente nel commercio di materiale sanitario, la moltiplicazione sospetta di intermediari tra fornitore e acquirente, articoli di stampa concernenti società che praticano prezzi troppo elevati rispetto al materiale fornito o, infine, le domande di restituzione delle somme versate presentate dalle banche degli acquirenti truffati.

Presunto riciclaggio di denaro nel settore della commercializzazione di materiale sanitario

Un intermediario finanziario constata in merito a una relazione d'affari destinata alla gestione patrimoniale, intestata a una società di sede di una giurisdizione del Pacifico, tre versamenti provenienti da un Paese terzo per un totale di diverse decine di milioni di franchi. La società di domicilio in questione appartiene a un cittadino europeo attivo nell'industria estrattiva e domiciliato in un Paese del Golfo. Secondo le indicazioni del cliente, le somme trasferite corrisponderebbero a una vendita di 10 milioni di mascherine mediche effettuata per soddisfare la

[21] Cfr. nota 15

[22] Cfr. nota 15

[23] Cfr. le statistiche sul tema pubblicate sulla pagina Internet di MROS: *Crediti transitori COVID-19*

domanda di un Paese. I fondi provengono da un conto aperto a nome di un ente pubblico. Il cliente fungerebbe da intermediario tra tale ente e i fornitori stranieri. Una parte delle somme versate su questo conto è trasferita poco dopo su diverse relazioni bancarie aperte nel Paese dei fornitori. L'intermediario finanziario rileva diverse incoerenze tra le informazioni ottenute dal cliente e la situazione nello Stato che agisce in qualità di acquirente, nutre dubbi sull'attendibilità delle transazioni commerciali e sospetta che dietro di esse si celino le fattispecie di truffa e infedeltà nella gestione pubblica. Dagli accertamenti effettuati da MROS è emerso che, nonostante il suo carattere inusuale, la transazione in questione era stata debitamente autorizzata e che le mascherine ordinate erano state effettivamente consegnate. La FIU del Paese in cui sono state ordinate le mascherine è stata informata del carattere inusuale di questa transazione.

Mentre i tre tipi di rischi appena descritti, legati alla pandemia da COVID sono stati ampiamente documentati da MROS, altri rischi, seppur tangibili, hanno trovato poco spazio all'interno delle segnalazioni pervenute. È il caso in particolare del riciclaggio di denaro da parte di organizzazioni criminali che approfittano dell'attuale crisi sanitaria e delle relative ripercussioni economiche per rafforzare la loro influenza, rilevando ad esempio società svizzere indebitate o beni immobiliari da persone fisiche o giuridiche che versano in difficoltà finanziarie. Sebbene il rischio accresciuto di infiltrazione delle organizzazioni criminali nell'economia sia stato segnalato da diverse istanze internazionali e sia stato documentato in diverse inchieste giornalistiche, MROS ha ricevuto al riguardo soltanto due comunicazioni di sospetto. Va tuttavia rilevato che in alcuni casi le truffe sul credito segnalate sono state apparentemente commesse da persone collegate tra loro o perlomeno secondo un modus operandi analogo. Tuttavia, MROS non dispone finora di elementi che dimostrino il coinvolgimento di note organizzazioni criminali in schemi di questo tipo.

Un credito COVID a beneficio di una società appartenente a un membro di un'organizzazione criminale?
Un intermediario finanziario constata la restituzione di un prestito privato, vietata dall'art. 2 cpv. 2 lett. b LFiS-COVID-19, su una relazione d'affari intestata a una società attiva nel settore della manutenzione e riparazione di veicoli, destinataria di un credito COVID. Dopo aver effettuato ulteriori accertamenti, si imbatte in un articolo di stampa che riferisce dell'arresto del detentore della società in questione in un Paese terzo per appartenenza a un'organizzazione criminale. La relazione in questione evidenzia versamenti in contanti e transazioni con conti di terzi aperti nel Paese in questione. Le somme implicate ammontano ad alcune decina di migliaia di franchi.

5.2 Organizzazioni criminali

I fatti finora segnalati a MROS in relazione a organizzazioni criminali indicano che gli elementi di sospetto degli intermediari finanziari autori delle comunicazioni si fondano il più delle volte su articoli di stampa o su informazioni contenute in banche dati private.
I conti di membri di organizzazioni criminali non presentano spesso alcuna transazione o schema di transazione significativo e sono pertanto qualificati come «non sospetti» e quindi non segnalati.
La difficoltà degli intermediari finanziari nell'individuare i membri di organizzazioni criminali ai sensi dell'art. 260ter CP è probabilmente riconducibile a una serie di cause. Ad esempio, al trasferimento in contanti di proventi di reato o al fatto che le transazioni in denaro restano sotto una certa soglia. Inoltre le aziende oggetto delle segnalazioni operano spesso in settori dove le transazioni in contanti sono molto diffuse (ristorazione, garage, ecc.). Tuttavia, anche altri settori (come l'intermediazione nel settore immobiliare, il settore dell'edilizia, ecc.) potrebbero essere potenzialmente toccati.

Appartenenza a un'organizzazione criminale e transazioni in contanti
Nel 2020 un intermediario finanziario ha segnalato due richieste di carta di credito in virtù dell'art. 9 cpv. 1 lett. b LRD (tentativo di riciclaggio di denaro). Secondo una registrazione in World-Check, uno dei due richiedenti sarebbe infatti membro dell'organizzazione criminale 'Ndrangheta. Le carte di credito di entrambi i richiedenti sono collegate allo stesso conto intestato a una gelateria. I richiedenti delle carte di credito sono residenti in un determinato Cantone, mentre la società ha sede in un Cantone di confine.
Sulla base delle informazioni riportate nella segnalazione, MROS ha potuto richiedere le informazioni necessarie ai sensi dell'art. 11a cpv. 2 e 3 LRD relative ai conti bancari delle persone fisiche nonché il conto bancario della gelateria. Successivamente l'intermediario finanziario interpellato ha trasmesso una comunicazione di sospetto, fondata in particolare su fonti pubblicamente accessibili nonché sulla richiesta di informazioni da parte di MROS.
Dall'analisi effettuata da MROS sulle relazioni bancarie in questione è emerso il quadro seguente:
l'80 per cento delle relazioni d'affari segnalate erano state oggetto di versamenti in contanti insolitamente frequenti. Tutti i titolari delle aziende segnalate o le controparti sono in possesso della cittadinanza italiana. Nell'80 per cento delle relazioni d'affari sono state riscontrate diverse transazioni da o verso l'Italia.
Da un'analisi dei comportamenti nelle transazioni, MROS ha potuto inoltre rilevare che il 60 per cento delle relazioni d'affari presentava un legame con la Calabria o con Napoli. Inoltre da un'analisi della documentazione del conto della gelateria è emerso che quest'ultima probabilmente non era neanche in attività. Stando alle dichiarazioni del proprietario, quest'ultima sarebbe stata riconvertita nel corso della pandemia in attività di ristorazione.

Come illustrato, esistono tuttavia fattori la cui concomitanza potrebbe essere indicativa del transito di proventi di reato su una relazione d'affari. In particolare l'interazione tra transazioni in contanti, società non operative e la presenza di determinati fattori di rischio (p. es. il legame con la Calabria nel caso di cui sopra) potrebbero aiutare a individuare i conti di possibili membri di un'organizzazione criminale.

5.3 Finanziamento del terrorismo

Attrattività delle criptovalute per il finanziamento del terrorismo
Un intermediario finanziario mette a disposizione dei propri clienti il servizio Crypto ATM. Questo servizio permette di effettuare versamenti in franchi presso un bancomat e in seguito di far convertire tali somme in bitcoin da parte dell'intermediario finanziario. Per il cambio di franchi in bitcoin l'intermediario finanziario in questione collaborava con una borsa di criptovalute di un Paese dell'Europa meridionale.
Questa borsa aveva segnalato all'intermediario finanziario che dalla Svizzera era stata eseguita una transazione del valore di 0,00897707 bitcoin (100 franchi) a beneficio di un indirizzo bitcoin riconducibile al gruppo terroristico Al-Qaïda. Tale indirizzo sarebbe stato oggetto di indagini da parte di un pubblico ministero in un Paese terzo.
Nell'effettuare il versamento tramite Crypto ATM, l'esecutore del bonifico segnalato a MROS aveva dovuto fornire soltanto un'informazione di contatto, riuscendo così a rimanere nell'anonimato. Tuttavia, grazie proprio a quest'informazione, MROS è stato in grado di identificarlo. Gli accertamenti condotti hanno mostrato che questa persona si era già contraddistinta quattro anni prima nei media sociali per aver condiviso propaganda violenta di natura jihadista.
Da un'analisi delle transazioni sono emerse ulteriori 17 transazioni effettuate a beneficio dello stesso indirizzo bitcoin per un valore complessivo di circa 3000 franchi. Secondo quanto indicato da uno strumento di analisi

della blockchain, l'indirizzo è riconducibile all'al Qaeda Bitcoin Transfer Office.

Il caso di specie dimostra come i gruppi terroristici facciano ricorso anche alle nuove tecnologie per autofinanziarsi. Il monitoraggio e il tracciamento successivo delle transazioni in criptovaluta come pure i relativi chiarimenti ai sensi dell'art. 6 cpv. 2 LRD costituiscono un compito centrale degli intermediari finanziari. L'esempio illustrato testimonia inoltre come la semplice indicazione di un'informazione di contatto sia stata sufficiente a MROS per individuare i legami esistenti.

Attenzione rivolta a esecutori e beneficiari dei bonifici anziché alle somme coinvolte
Un intermediario finanziario autorizzato in Svizzera è stato informato dalla società madre avente sede all'estero che determinate persone, secondo informazioni in possesso di un'autorità estera di perseguimento penale, avrebbero effettuato transazioni sospette finalizzate al finanziamento del terrorismo per il suo tramite. Il lavoro di MROS è stato notevolmente facilitato da un'analisi documentata delle transazioni e delle persone coinvolte da parte dell'intermediario finanziario. Nella propria segnalazione, quest'ultimo ha indicato anche i nomi dei destinatari del denaro, consentendo a MROS di ottenere ulteriori indicazioni utili. Nello specifico è emerso che due persone appartenenti a una cerchia islamista incline alla violenza, una delle quali imparentata con un foreign terrorist fighter svizzero, hanno trasferito importi a tre fino a quattro cifre, in particolare verso due Paesi dell'Europa sudorientale nonché verso un Paese asiatico dove il fratello di uno dei due soggetti coinvolti avrebbe ritirato il denaro trasferito. Secondo fonti d'informazione pubblicamente accessibili, un altro destinatario del denaro avrebbe soggiornato in un Paese critico prima di essere condannato da un tribunale al suo ritorno.

Lo schema delle transazioni è tipico di due modalità di finanziamento del terrorismo descritte dal GAFI.[24] Queste modalità sono presenti anche in Svizzera ormai da anni, pur passando spesso inosservate. Una di esse riguarda il trasferimento di denaro da un Paese a estremisti, talvolta noti persino ai media, che utilizzano tali fondi per il proprio sostentamento nel Paese di destinazione o che li ritrasferiscono a terzi eventualmente per la progettazione di attentati. La seconda modalità riscontrata nel caso in esame consiste nel trasferimento di fondi, tramite diversi Paesi, destinati presumibilmente alla commissione di attentati di matrice estremista allo scopo di occultarne la fonte di finanziamento.
In questa catena di trasferimento del denaro la Svizzera rappresenta il punto di partenza o soltanto di transito. A causa dei loro importi marcatamente esigui, i bonifici effettuati tramite agenzie di trasferimento di fondi o conti di *retail-banking* tendono a non destare sospetti, rendendo così difficile una loro individuazione. Il motivo principale risiede nel fatto che il monitoraggio delle transazioni considera prevalentemente l'importo delle somme trasferite. Questa strategia, per quanto possa risultare vincente nell'individuare i flussi di denaro in caso di presunte operazioni di riciclaggio, risulta meno efficace per rilevare i casi di finanziamento del terrorismo, dove è invece fondamentale concentrare l'attenzione sull'esecutore e sul destinatario dei trasferimenti di denaro.

[24] Cfr. la pubblicazione del GAFI *Terrorist Financing Risk Assessment Guidance*.

5.4 Tratta di esseri umani

Smurfing, settore a luci rosse, Paesi a rischio e indicazioni precise sul destinatario del denaro

Un fornitore di servizi di trasferimento di fondi ha segnalato nell'arco di due mesi cinque relazioni d'affari individuali che presentavano sovrapposizioni riguardo allo schema delle transazioni e alle caratteristiche demografiche (per esempio l'età, il sesso, l'origine, la professione, ecc.) delle persone coinvolte e contenevano indizi relativi alla tratta di esseri umani (art. 182 CP) e/o al promovimento della prostituzione (art. 195 CP).

Le cinque clienti segnalate hanno effettuato diversi pagamenti dal medesimo importo in uno stesso periodo a beneficio di diversi privati che hanno ritirato in seguito il denaro in un Paese caraibico e in un Paese europeo. Si presume che il pagamento sia stato suddiviso intenzionalmente in diverse tranche per non superare la soglia di 5000 franchi ed evitare così ulteriori accertamenti. In parte sono state individuate corrispondenze tra i diversi beneficiari, il che ha permesso all'intermediario finanziario di stabilire un chiaro collegamento tra le diverse relazioni d'affari. In un caso tra i clienti segnalati è stato effettuato un bonifico, il cui importo è stato in seguito nuovamente trasferito nello stesso Paese caraibico.

La maggior parte dei clienti lavora nel settore a luci rosse o vi intrattiene legami. Quasi tutti i pagamenti sono stati effettuati dalla stessa filiale nei pressi di un noto quartiere a luci rosse della Svizzera. Analizzando le singole transazioni, l'intermediario finanziario autore della segnalazione ha potuto esaminare e ricostruire lo schema delle transazioni, individuando legami importanti tra le relazioni d'affari apparentemente indipendenti tra loro.

Il fatto che l'intermediario finanziario abbia trasmesso cognomi, nomi, date di nascita e indirizzi di tutte le persone coinvolte ha permesso a MROS di condurre ricerche approfondite e mirate sulle persone e di individuare in questo modo diversi elementi che confermassero il sospetto iniziale dell'intermediario finanziario. In particolare le indicazioni precise sui beneficiari del denaro all'estero hanno consentito a MROS di indirizzare richieste mirate agli uffici di comunicazione esteri, una misura, questa, di estrema efficacia nel caso di reati transfrontalieri quale la tratta di esseri umani.

Nel presente caso due clienti hanno fornito indirizzi riconducibili a un quartiere a luci rosse. Due indirizzi forniti dalle clienti sono invece risultati falsi. Ciò ha contribuito a rafforzare il sospetto che i bonifici effettuati fossero di origine criminale. I Paesi di origine delle potenziali vittime e delle controparti sono considerati, anche sulla base di altri fattori, come ad alto rischio.

L'intermediario finanziario autore della segnalazione ha fondato la propria analisi su una serie di indicatori che, secondo il rapporto dell'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) del 2019 intitolato *Following the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings*[25], rivelano possibili attività o reati in materia di tratta di esseri umani:

- utilizzo di indirizzi di noti quartieri a luci rosse in cui viene esercitata la prostituzione;
- ricorso a prestanome;
- coinvolgimento di istituti non appartenenti al tradizionale sistema finanziario;
- bonifici effettuati da diverse regioni a beneficio di persone residenti in Paesi notoriamente classificati come ad alto rischio per la tratta di esseri umani;
- bonifici frazionati *smurfing*;
- pagamenti elevati e/ o frequenti [...] non compatibili con l'utilizzo personale o con l'attività esercitata dalla singola persona (denaro è utilizzato da terzi).

Per l'elenco completo dei diversi indicatori e degli strumenti di analisi finanziaria in materia di tratta di esseri umani, stilato dal rappresentante speciale OSCE e coordinatore per la lotta alla tratta

[25] Cfr. pubblicazione OSCE disponibile al seguente indirizzo https://www.osce.org/cthb/438323 (documento in inglese)

di esseri umani, si rinvia alla pubblicazione OSCE citata in precedenza.

5.5 Comunicazioni correlate a prestatori di servizi in materia di virtual asset

Truffatori di phishing sfruttano una borsa svizzera di criptovalute per riciclare valori patrimoniali ottenuti in modo fraudolento

Un intermediario finanziario ha segnalato un conto commerciale di una borsa svizzera di criptovalute sul quale, nel giro di pochi giorni, sono confluiti complessivamente 30 000 franchi provenienti da conti di clienti di diverse banche. I clienti di questi istituti finanziari erano stati indotti con e-mail fasulle a comunicare i propri dati di accesso all'account di e-banking (cosiddetto phishing). Gli ordini di pagamento in questione erano stati in seguito effettuati da terzi ignoti. Gli istituti finanziari la cui clientela era stata vittima degli attacchi di phishing hanno informato l'intermediario finanziario autore della segnalazione del denaro addebitato illegalmente. Parallelamente, anche la borsa svizzera di criptovalute ha segnalato a MROS l'acquisto di bitcoin sulla propria piattaforma commerciale tramite proventi di reato. La borsa di criptovalute ha comunicato a MROS gli indirizzi bitcoin e IP dei presunti truffatori che hanno commissionato l'acquisto. Le transazioni sono state effettuate tramite una cosiddetta API (Application Programming Interface, ovvero un'interfaccia di programmazione di un'applicazione) messa a disposizione dalla borsa svizzera di criptovalute sul proprio sito Internet. L'API funge da interfaccia software collegata a una piattaforma commerciale della borsa e consente ai clienti di effettuare in modo semplificato e automatizzato transazioni di acquisto e vendita fino a 5000 franchi al giorno senza dover fornire informazioni dettagliate in merito alla propria identità al momento della registrazione. Per le transazioni di acquisto e vendita tramite l'API, la borsa richiede ai clienti unicamente i dati concernenti i conti di provenienza dei fondi, i quali sono di norma controllati dal legittimo committente, nonché un indirizzo di criptovaluta sul quale trasferire le criptovalute acquistate. Una volta concluso l'ordine di acquisto generato tramite l'API, i clienti ricevono un numero di riferimento che devono comunicare al momento del bonifico bancario sul conto commerciale della borsa. Tutti gli ordini di acquisto ammontavano esattamente a 5000 franchi o poco meno (cosiddetto smurfing), onde evitare che la borsa di criptovalute potesse richiedere ai committenti ulteriore documentazione KYC (Know Your Customer).

Riciclaggio tramite una borsa svizzera di criptovalute di criptoasset ottenuti in modo fraudolento

Nel 2019 è stato lanciato un attacco informatico nei confronti di una borsa estera di criptovalute durante il quale sono stati rubati valori patrimoniali sottoforma di criptovaluta «F» corrispondenti a diversi milioni di franchi svizzeri. Si presume che i presunti autori appartenessero a un gruppo di hacker. Per confondere le proprie tracce, gli hacker hanno in seguito cambiato in bitcoin i valori patrimoniali sottratti (cosiddetto chain-hopping, ovvero il cambio dalla blockchain di criptovaluta «F» alla blockchain di bitcoin che rende difficile risalire all'origine di tali operazioni tramite software di tracciamento). A tale scopo, i cibercriminali hanno scelto, apparentemente in modo mirato, borse di criptovalute sparse in tutto il mondo che, per effettuare questo tipo di operazioni, prevedevano una procedura semplificata di identificazione dei clienti. Al momento della registrazione del cliente, tale procedura richiedeva infatti unicamente il rispettivo indirizzo di posta elettronica o il numero di telefono fintanto che i valori patrimoniali cambiati non superassero una determinata soglia. I criminali hanno suddiviso le somme rubate di criptovaluta «F» in importi minori e li hanno inviati tramite diversi indirizzi «F» (cosiddetti hop) per poi depositarli presso le diverse borse di criptovalute al fine di effettuare l'operazione di cambio. In questo modo,

hanno potuto impedire il tracciamento delle operazioni, aggirando al contempo i sistemi di sicurezza delle borse di criptovalute, poiché non era piu evidente che si trattasse della criptovaluta rubata in seguito all'attacco informatico.
Anche in questo caso è stata utilizzata abusivamente l'interfaccia software API di una borsa svizzera di criptovalute. Gli autori di reato hanno aperto presso la borsa in questione più conti e hanno cambiato il bottino della criptovaluta «F» in bitcoin prestando attenzione a non superare la soglia di 5000 franchi per non dover sottostare ad analisi approfondite sulla loro identità (procedura KYC). La borsa di criptovalute è entrata dunque in possesso di provento di reato. Le tracce lasciate sulla blockchain dalle transazioni in questione e ricostruite grazie al software di tracciamento hanno permesso di risalire, nonostante gli sforzi dei cibercriminali di coprire le proprie tracce, all'attacco informatico perpetrato nei confronti della borsa estera di criptovalute. I bitcoin trasferiti dalla borsa di criptovalute ai cibercriminali non mostravano, tuttavia, sulla blockchain di bitcoin alcuna correlazione con l'attacco alla borsa estera, bensì soltanto con la borsa svizzera. Dopo aver scoperto l'utilizzo abusivo della propria piattaforma, la borsa svizzera interessata ha potuto bloccare alcune transazioni di bitcoin in uscita e ha segnalato il caso a MROS.

Nel 2019 sono state hackerate più borse di criptovalute che in qualsiasi altro anno precedente.[26] Poiché le criptovalute (p. es. i bitcoin) possono essere scambiate direttamente tra controparti in tutto il mondo e in modo relativamente anonimo, il luogo in cui viene hackerata una borsa è del tutto irrilevante. Le criptovalute incriminate possono confluire nel giro di pochi secondi verso altre piazze finanziarie ed essere riciclate tramite quest'ultime.
I due casi illustrati evidenziano il ruolo centrale assunto dallo *smurfing* e dall'elusione degli obblighi di identificazione[27] nell'ambito dei VASP. Per evitare tali rischi è essenziale impiegare software di tracciamento che consentano di ricostruire il percorso effettuato dalle transazioni. I cibercriminali cercano a loro volta di eludere tali sistemi di allarme facendo confluire le criptovalute di provenienza illecita su più indirizzi di criptovalute prima di trasferirle all'indirizzo di destinazione vero e proprio. Un indirizzo di criptovalute in una simile catena di transazioni rappresenta pertanto soltanto una tappa intermedia (cosiddetta *hop*). Ai fini di un tracciamento efficace è pertanto essenziale ricostruire le transfazioni avvenute sui diversi *hop*.
I casi illustrati mostrano inoltre ancora una volta quanto siano fondamentali gli strumenti di analisi del tracciamento delle transazioni di criptovalute. Affinché MROS possa ricorrere ai propri strumenti di analisi, è necessario che gli intermediari finanziari documentino i propri chiarimenti ai sensi dell'art. 6 LRD e le relative analisi concernenti il tracciamento delle transazioni di criptovalute (art. 3 cpv. 1 lett. h OURD).

5.6 Video identificazione e identificazione online

A marzo 2016, l'Autorità federale di vigilanza sui mercati finanziari (FINMA) ha pubblicato la circolare 2016/7 sugli obblighi di diligenza degli intermediari finanziari all'avvio di relazioni d'affari attraverso i canali digitali. Nel 2018[28], alla luce dei

[26] Cfr. pubblicazione di gennaio 2020 di Chainalysis *The 2020 State of Crypto Crime.* Nel 2019 è stato raggiunto il record rispetto agli anni precedenti di attacchi *hacker* nei confronti di borse di criptovalute (Chainalysis ha individuato 11 attacchi hacker nel 2019); tuttavia, il volume dei valori patrimoniali sottratti è inferiore rispetto agli anni precedenti (2019: 282,6 mio. USD; 2018: 875,5 mio. USD; 2014: 483,1 mio. USD).

[27] Occorre, tuttavia, evidenziare che con l'entrata in vigore il 1° gennaio 2021 dell'art. 51a dell'ordinanza FINMA sul riciclaggio di denaro del 3 giugno 2015 (ORD-FINMA; **RS 955.033.0**), il valore soglia delle operazioni con criptovalute è stato abbassato da 5000 franchi a 1000 franchi attuando in tal modo la nota esplicativa della raccomandazione 15 del GAFI pubblicata a metà del 2019 sulla gestione dei cosiddetti VASP. Queste disposizioni sono state riprese anche dagli OAD, i quali annoverano tra i loro membri prestatori di servizi di criptovalute.

[28] Cfr. comunicato stampa: https://www.finma.ch/it/news/2018/07/20180717-mm-video-online-id/.

recenti sviluppi tecnologici, la FINMA ha sottoposto a revisione parziale la circolare sulla video identificazione e identificazione online e nel 2020 ha proposto ulteriori modifiche che hanno fatto l'oggetto di un'indagine conoscitiva conclusasi il 1° febbraio 2021.[29] La maggior parte degli istituti bancari svizzeri offre la possibilità di avviare una relazione d'affari in questo modo. Alcuni intermediari finanziari, in particolare quelli attivi nel commercio delle criptovalute ricorrono sistematicamente a tale possibilità. I casi segnalati a MROS da intermediari finanziari che avevano manifestato dubbi durante il processo di identificazione online dei propri clienti al momento dell'avvio di una relazione d'affari per via elettronica sono pertanto sempre più frequenti. Quasi due terzi degli intermediari finanziari in questione fanno riferimento all'utilizzo di criptovalute. Uno dei casi complessi segnalati in passato riguardava ad esempio l'identificazione online di potenziali investitori nel quadro di una *Initial Coin Offering*.[30] L'apertura di relazioni d'affari tramite canali digitali non è esente da rischi. Sono sostanzialmente due le alternative a disposizione dei cibercriminali che intendono avviare relazioni d'affari tramite questi canali per riciclare i propri proventi illeciti: ricorrere a falsi documenti d'identità oppure a documenti, spesso rubati, di altre persone la cui identità è stata usurpata.[31] I casi appena descritti sono menzionati spesso nelle comunicazioni di sospetto ricevute da MROS, con una predominanza delle segnalazioni effettuate dopo l'individuazione di documenti falsi, probabilmente perché reperibili più facilmente rispetto ai documenti rubati.

Nel 2020 MROS ha ricevuto una comunicazione da parte di un intermediario finanziario che offriva la possibilità di aprire conti online mediante una procedura di identificazione che prevedeva l'invio della copia del documento d'identità tramite Internet. I sospetti dell'intermediario nascevano da informazioni negative, reperite da fonti pubbliche, che accusavano i clienti in questione di truffa ai danni di investitori nel quadro di un progetto di innovazione tecnologica. Grazie alle proprie ricerche, MROS ha constatato che la carta d'identità utilizzata da uno dei detentori del controllo su una delle società intestatarie del conto segnalato era stata oggetto di una denuncia per furto tre giorni prima dell'apertura del conto.

Poiché il ricorso a documenti falsi o usurpati al momento dell'avvio di una relazione d'affari online non permette di identificare gli effettivi detentori del controllo o gli aventi economicamente diritto delle relazioni d'affari in questione, è particolarmente arduo stabilire correlazioni tra i valori patrimoniali oggetto della comunicazione di sospetto e i reati preliminari al riciclaggio di denaro. La collaborazione tra MROS e le autorità di polizia svizzere e i propri omologhi esteri assume pertanto un'importanza fondamentale; tuttavia, è la precisione delle informazioni fornite dall'intermediario finanziario autore delle comunicazioni di sospetto a determinarne l'efficacia.

Interruzione delle trattative

Un intermediario finanziario attivo nel commercio di criptovalute riceve lo stesso giorno tre richieste di apertura di un conto sulla propria piattaforma informatica. Osserva che in tutti e tre i casi, il documento d'identità estero fornito dai potenziali clienti presenta la medesima fotografia ma informazioni diverse relative al nome e alla data di nascita. L'intermediario finanziario interrompe le trattative per l'avvio della relazione d'affari ed effettua verifiche approfondite su clienti recenti, segnalando i propri sospetti a MROS ai sensi dell'art. 9 cpv. 1 lett. b LRD (tentativo di riciclaggio di denaro). Tali accertamenti hanno permesso di identificare altri tre clienti i cui documenti d'identità riportavano la stessa fotografia. Le relazioni d'affari sono dunque state segnalate a MROS. L'analisi di MROS ha permesso di identificare i conti esteri a partire dai quali i tre clienti già accettati hanno effettuato gli

[29] Cfr. comunicato stampa: https://www.finma.ch/it/news/2020/11/20201116-mm-online-identifizierung/.

[30] Metodo utilizzato per reperire fondi che prevede l'emissione di virtual asset convertibili in criptovalute o valuta fiat durante la fase iniziale di un progetto.

[31] Cfr. la pubblicazione del GAFI *Guidance on digital identity,* pubblicata in marzo 2020.

accrediti sul conto dell'intermediario finanziario per acquistare le criptovalute. Grazie alle informazioni ricevute dalla FIU del Paese dal quale sono stati eseguiti i bonifici, MROS ha potuto confermare che i fondi trasferiti al fine di acquistare le criptovalute provenivano da truffe commesse all'estero. Inoltre, grazie alle informazioni fornite dall'intermediario finanziario autore della segnalazione, MROS ha potuto trasmettere al proprio omologo estero l'indirizzo IP dei PC dai quali sono partiti i bonifici, consentendogli in tal modo di denunciare gli autori della truffa e del successivo riciclaggio di denaro alle competenti autorità di perseguimento penale.

Diversi intermediari finanziari esposti ai rischi derivanti dalla procedura di identificazione online sembrano aver ridotto tali rischi migliorandole e seguendo così le raccomandazioni del GAFI, hanno così sostituito le verifiche manuali eseguite dai responsabili del controllo di conformità con quelle svolte da specifici software preposti alla verifica dell'autenticità dei documenti rivelatesi maggiormente affidabili.
Abbiamo peraltro costatato che il numero delle comunicazioni effettuate in seguito a un'interruzione delle trattative per l'avvio di una relazione d'affari rimane esiguo. L'utilizzo di documenti di legittimazione falsi potrebbe a nostro avviso condurre a segnalazioni effettuate in virtù dell'art. 9 cpv. 1 lett. b LRD.

6. La prassi di MROS

6.1 Trasmissione di informazioni – non di comunicazioni

Con la modifica dell'OURD entrata in vigore il 1°gennaio 2020, le comunicazioni non sono più trasmesse alle autorità di perseguimento penale. Al fine di garantire la protezione delle fonti, non è neppure trasmessa alcuna indicazione relativa all'autore della comunicazione o alla persona che ha comunicato informazioni alle autorità di perseguimento penale (cfr. art. 8 cpv. 1 OURD). Le informazioni rilevanti e le analisi di MROS relative a tali informazioni sono infatti trasmesse sotto forma di rapporto per via elettronica alle autorità di perseguimento penale. I rapporti di analisi destinati alle autorità di perseguimento penale possono contenere informazioni provenienti da diverse fonti o varie comunicazioni (art. 1 cpv. 2 lettere a-e OURD). È la natura aggregata delle informazioni registrate da MROS che determina la loro sorte. Come già menzionato precedentemente (cfr. n. 4.12), la nozione di «quota di trasmissione» delle comunicazioni di sospetto non ha pertanto più senso.
Il secondo punto su cui occorre insistere è in relazione con il primo. Una volta terminato il trattamento delle informazioni provenienti da una comunicazione di sospetto, secondo l'art. 23 cpv. 5 e 6 LRD MROS segnala agli intermediari finanziari se le informazioni comunicate sono state trasmesse o meno. Tale segnalazione ha solo due funzioni pratiche: in caso di trasmissione, secondo l'art. 10 LRD gli intermediari finanziari sono tenuti a bloccare i valori patrimoniali delle relazioni segnalate. In casi di decisone di non trasmissione a un'autorità di perseguimento penale, secondo l'art. 30 ORD-FINMA gli intermediari finanziari possono decidere in modo autonomo se proseguire la relazione d'affari segnalata. Come in passato, queste decisioni di non trasmettere le informazioni non permettono all'intermediario finanziario di trarre in alcun caso conclusioni sulla liceità degli averi correlati alle relazioni d'affari segnalate. Il fatto che MROS abbia deciso di non trasmettere un caso alla competente autorità di perseguimento penale non significa che le informazioni non siano state ritenute pertinenti per una loro trasmissione ad una FIU estera o ad una autorità amministrativa nazionale, o è possibile che le informazioni importanti della comunicazione sono state segnalate in un rapporto senza che fosse giustificata la trasmissione di tutte le informazioni della comunicazione.

6.2 Nuove competenze connesse all'art. 11a cpv. 2bis LRD

6.2.1 Il nuovo art. 11a cpv. 2bis LRD

Il 25 settembre 2020 il Parlamento ha approvato il «Decreto federale che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata».[32] Tale decreto modifica la LRD introducendovi in particolare il nuovo art. 11a cpv. 2bis dal seguente tenore:

[32] FF **2020** 6945, 6957.

«Se dall'analisi di informazioni provenienti da un Ufficio di comunicazione estero risulta che, in una transazione o in una relazione d'affari relativa a queste informazioni, sono o sono stati coinvolti intermediari finanziari sottoposti alla presente legge, questi consegnano su richiesta all'Ufficio di comunicazione tutte le informazioni pertinenti, sempreché ne siano in possesso.»

Il 31 marzo 2021 il Consiglio federale ha deciso che le nuove disposizioni entreranno in vigore il 1° luglio 2021.[33]
Con la sua entrata in vigore questa modifica della LRD conferirà a MROS nuove competenze nell'ambito della lotta contro il riciclaggio di denaro, i reati preliminari al riciclaggio, la criminalità organizzata o il finanziamento del terrorismo.
Dal 1° novembre 2013, sulla base dell'analisi transazionale eseguita MROS ha la possibilità di chiedere ad altri intermediari finanziari svizzeri informazioni supplementari necessarie per le sue analisi, quando identifica altri conti presso intermediari finanziari terzi con i quali sono state effettuate transazioni dalla relazione d'affari segnalata. Lo scopo del legislatore era di affidare a MROS a certe condizioni strumenti supplementari per approfondire le sue analisi e di tenere traccia, a determinate condizioni, delle transazioni (*paper trail*). In pochi anni questa disposizione si è rivelata fondamentale per MROS.
L'uso delle richieste di informazioni supplementari in virtù dell'art. 11a LRD collegato alla possibilità di MROS di scambiare informazioni con i suoi omologhi all'estero e con altre autorità nazionali ha infatti permesso di migliorare le analisi di MROS ed evitare di oberare le autorità di perseguimento penale.
Finora, le richieste effettuate in virtù dell'art. 11a LRD erano tuttavia limitate all'analisi dei casi in cui MROS era già in possesso di una comunicazione di sospetto da parte di un intermediario finanziario svizzero. Di conseguenza, quando si trattava di analizzare le informazioni provenienti da altre FIU, MROS poteva procedere a tali richieste soltanto se erano in relazione con informazioni finanziarie comunicate a MROS da un intermediario svizzero. Se rivelavano un nesso con una comunicazione, MROS era in grado di rispondere. Nel caso contrario, l'Ufficio di comunicazione non poteva fornire informazioni finanziarie alla FIU richiedente.
Questa lacuna è stata critica in occasione della valutazione della Svizzera da parte del GAFI nel 2016. Per questo motivo la Svizzera è stata giudicata soltanto «parzialmente conforme» (una valutazione insufficiente) alla raccomandazione 40 del GAFI e il livello di efficacia raggiunto dalla Svizzera nella cooperazione internazionale (RI 2) è stato giudicato «modesto», anche questa una valutazione insufficiente.[34] La correzione di questa lacuna importante faceva pertanto parte degli otto ambiti di intervento prioritari segnalati alla Svizzera dagli autori della valutazione ed era giustificata anche in considerazione della forte internazionalizzazione della piazza finanziaria svizzera.
La valutazione insufficiente della Svizzera ha anche provocato una procedura di conformità nei confronti di MROS in seno al gruppo Egmont, il forum per lo scambio operativo delle FIU. Conformemente alle regole sull'applicazione dei principi di questo gruppo, MROS è oggetto di una procedura di monitoraggio e deve rendere conto delle misure prese per ovviare alle insufficienze riscontrate dalla valutazione del GAFI. Nel caso in cui le norme svizzere non venissero adeguate entro un determinato termine, MROS rischierebbe di essere sospeso dal gruppo Egmont.
Occorre rammentare che la maggioranza delle comunicazioni di sospetto che pervengono a MROS presentano un legame con l'estero e che in simili casi è fondamentale che MROS possa ricorrere alle informazioni di cui dispongono le FIU del gruppo Egmont. Il nuovo art. 11a cpv. 2bis LRD dovrebbe permettere di soddisfare gli standard internazionali e di porre fine alla procedura di monitoraggio nei confronti di MROS in seno al gruppo Egmont.
In futuro, grazie al nuovo art. 11a cpv. 2bis LRD, MROS sarà infatti in grado di chiedere agli intermediari finanziari informazioni su una o più transazioni oppure su una relazione d'affari

[33] Cfr. il comunicato di stampa *Lotta al terrorismo: il Consiglio federale pone in vigore disposizioni penali più severe.*

[34] Cfr. *mer-suisse-2016.pdf (fatf-gafi.org).*

segnalata da un'altra FIU, ad esempio per mezzo di un'informazione spontanea, o su una relazione oggetto di una domanda di una FIU estera, anche in assenza di una comunicazione di sospetto di un intermediario finanziario svizzero. Questa competenza più estesa sarà utile anche agli intermediari finanziari svizzeri in quanto permetterà di attirare la loro attenzione sui rischi potenziali finora ignorati delle loro relazioni d'affari e di aumentare in tal modo la sicurezza in Svizzera. Questo miglioramento dello scambio d'informazioni (*financial intelligence*) tra FIU permetterà di fornire sostegno all'assistenza internazionale e, sussidiariamente, al perseguimento penale.

6.2.2 Lo scambio d'informazioni con le FIU estere

L'assistenza amministrativa internazionale tra MROS e le FIU estere è disciplinata dagli articoli 30 e 31 LRD. MROS scambierà pertanto con le altre FIU le informazioni finanziarie ottenute grazie al nuovo art. 11a cpv. 2bis LRD alle condizioni finora vigenti. Il Consiglio federale ha avuto l'occasione di pronunciarsi più volte in merito.[35] Prima di scambiare informazioni con un'altra FIU MROS deve verificare il rispetto delle condizioni di cui all'art. 30 LRD. Si tratta in particolare dell'applicazione del principio di specialità, della reciprocità e del rispetto del segreto d'ufficio. Le richieste degli omologhi esteri devono rispettare i requisiti di cui all'art. 31 LRD. MROS non entra pertanto in materia nel caso di richieste che non presentano alcun legame con la Svizzera (*fishing expedition*). Non risponde neppure alle richieste tese a eludere la via dell'assistenza internazionale in materia penale. Infine, l'Ufficio di comunicazione non fornisce informazioni se la richiesta potrebbe compromettere gli interessi nazionali o la sicurezza e l'ordine pubblici in Svizzera. Le informazioni ricevute possono essere usate dalla FIU destinataria soltanto nell'ambito delle sue analisi riguardanti il riciclaggio di denaro, i reati preliminari, la criminalità organizzata e il finanziamento del terrorismo. Previa autorizzazione di MROS, le informazioni trasmesse a una FIU estera possono anche essere comunicate ad altre autorità del Paese in questione. Per la concessione dell'autorizzazione, MROS verifica l'adempimento delle condizioni presenti all'art. 30 capoversi 4 e 5 LRD. Occorre rammentare che le informazioni trasmesse possono essere usate solo a titolo di informazione (*intelligence*) e non come mezzo di prova e che sono trasmesse sotto forma di rapporto (art. 30 cpv. 3 LRD).

6.2.3 Prime domande relative all'applicazione del nuovo art. 11a cpv. 2bis LRD

L'entrata in vigore della nuova disposizione pone agli intermediari finanziari qualche problema di applicazione pratica che merita di essere illustrato in questa sede. Le regole che gli intermediari finanziari saranno tenuti a rispettare quando ricevono una richiesta di consegna di informazioni basata sul nuovo art. 11a cpv. 2bis e 3 LRD equivalgono alle regole consolidate adottate nel 2013 per le domande fondate sull'art. 11a LRD.[36] Per ottenere informazioni supplementari, MROS usa moduli adattati conformemente all'art. 11a cpv. 1 e 2 LRD. Nei moduli è previsto un elenco di documenti/informazioni da inoltrare. MROS seleziona quelli pertinenti secondo la base legale corrispondente (art. 11 cpv. 1 e art. 11a cpv. 2 o 2bis LRD). Il contenuto del modulo usato per le richieste fondate sull'art. 11a cpv. 2bis sarà identico a quello per le richieste basate sull'art. 11a cpv. 2 LRD. Gli intermediari registrati in goAML riceveranno le richieste d'informazione e saranno pregati di rispondervi per mezzo di questo canale, basandosi sulla prassi documentata nel manuale loro destinato.[37]
Ricordiamo che tal richiesta tuttavia non deve implicare automaticamente una comunicazione

---

35 Cfr. p. es. il messaggio del 14 settembre 2018 concernente l'approvazione e la trasposizione della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo con relativo Protocollo addizionale nonché il potenziamento del dispositivo penale contro il terrorismo e la criminalità organizzata, FF **2018** 5439, 5511 seg. e il messaggio del 27 giugno 2012 concernente la modifica della legge sul riciclaggio di denaro, FF **2012** 6199, 6237 seg.

36 Cfr. il rapporto d'attività 2013 di MROS, pagg. 55 e seg.

37 Cfr. *goAML Web – Manuale*, pagg. 22 e 47.

di sospetto a MROS. L'intermediario finanziario che riceve una richiesta di consegna di informazioni deve rispondere. Non può tuttavia ignorare che si tratta di una domanda di un'autorità fondata su un sospetto di riciclaggio di denaro, di un reato preliminare, di criminalità organizzata o di finanziamento del terrorismo. L'intermediario finanziario deve pertanto procedere a chiarimenti complementari in virtù dell'art. 6 LRD e, in caso di sospetto semplice o fondato, comunicare il caso a MROS. Se non identifica alcun sospetto, l'intermediario finanziario si limita a trasmettere a MROS le informazioni richieste in virtù dell'art. 11a cpv. 2bis LRD e a documentare i chiarimenti (cfr. art. 7 LRD e 31 ORD FINMA).
Come in passato, in caso di sospetto l'intermediario finanziario che deciderà di segnalare la relazione oggetto di una richiesta d'informazioni di MROS potrà adempire il suo obbligo allegando le informazioni e i documenti richiesti alla sua comunicazione di sospetto sempreché quest'ultima sia effettuata entro il termine di risposta stabilito da MROS. Tale termine è fissato da MROS in conformità con l'art. 11a cpv. 3 LRD. L'intermediario finanziario richiesto fornirà a MROS le informazioni di cui dispone. Come precisato dal Consiglio federale in merito all'art. 11a LRD, «per disponibili s'intendono tutte le informazioni in possesso delle entità di un'impresa o che possono essere acquisite, ammesso che tali entità siano soggette alla giurisdizione svizzera».[38]

6.3 Ordini di consegna delle autorità di perseguimento penale e obbligo di comunicazione

Occorre procedere a una comunicazione di sospetto nel momento in cui è stato ordinato un sequestro penale da parte di un'autorità di perseguimento penale? Si tratta di una domanda ripetutamente posta a MROS dagli intermediari finanziari o da altri interessati.

Tale questione è già stata risolta da MROS più di dieci anni fa[39] ed è stata confermata dalla giurisprudenza del 2018 del Tribunale federale (TF).
Il messaggio del Consiglio federale concernente l'adozione della LRD precisa il senso e lo scopo della legge:

«Al centro di questi sforzi vi è la lotta contro la criminalità organizzata. Pertanto non si tratta unicamente di rintracciare e di confiscare i valori patrimoniali illeciti, bensì di istituire le basi documentarie (paper trail) e il canale d'informazione (obbligo di comunicare) per individuare e punire penalmente le persone colpevoli di riciclaggio di denaro».[40]

Le disposizioni della LRD mirano pertanto innanzitutto a reprimere in generale il reato di riciclaggio di denaro e a perseguire penalmente gli imputati di tale reato. Il blocco e il sequestro dei beni patrimoniali potenzialmente incriminati è certamente un elemento non indifferente, ma esso non riveste un carattere né esclusivo né preponderante. Occorre quindi sottolineare che gli obiettivi della LRD non sono alternativi. La realizzazione del primo obiettivo non implica necessariamente la realizzazione del secondo o, in altre parole, le due finalità indicate sono indipendenti e devono essere raggiunte, per quanto possibile, in maniera coordinata.
Dal 2007 MROS ha integrato le finalità della LRD nella sua prassi amministrativa relativa all'obbligo di comunicazione degli intermediari finanziari in caso di ricezione di un ordine di perquisizione e/o di sequestro. All'epoca MROS aveva sottolineato che tale questione non deve essere risolta in modo definitivo.

Deve invece essere valutata caso per caso, tenendo conto dei risultati dei chiarimenti complementari che l'intermediario finanziario è tenuto a svolgere in tali casi in applicazione dell'art. 6 cpv. 2 LRD in combinato disposto con gli articoli 15

---

38 FF **2018** 5439, 5512.

39 Cfr. il n. 5.5 «Ordinanze di pubblicazione delle autorità di perseguimento penale e obbligo di comunicazione» del *rapporto annuale 2007* di MROS, pagg. 86 seg. e il n. 4.1 del *rapporto annuale 2017 di MROS* (pag. 57) in cui la prassi pubblicata nel 2007 è stata confermata. Cfr. anche la prassi di MROS: *Pubblicazioni dell'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS).*

40 FF **1996** III 993, 1008.

e seguenti dell'ORD-FINMA: «In linea di principio va detto che un'ordinanza di pubblicazione e/o di sequestro fa sempre scattare l'obbligo di chiarimento speciale».[41]

Se i risultati dei chiarimenti complementari in seguito alla ricezione di un ordine di perquisizione e/o di sequestro permettono all'intermediario finanziario di identificare elementi di sospetto supplementari a livello sia delle transazioni sia delle relazioni d'affari e se tali elementi di sospetto gli permettono di giungere a un sospetto fondato ai sensi dell'art. 9 cpv. 1 lett. a LRD, l'intermediario deve trasmettere una comunicazione di sospetto a MROS.
È ad esempio il caso quando i chiarimenti complementari conducono all'identificazione di altre relazioni d'affari rispetto a quelle oggetto dell'ordine di perquisizione e/o sequestro ricevuto. L'intermediario finanziario può individuare persone menzionate nell'ordine che sono implicate in quanto titolari, aventi diritto economico o di firma, detentori del controllo o responsabili di ordini oppure beneficiari dei versamenti interni o internazionali. L'intermediario finanziario deve giungere allo stesso risultato ed effettuare una comunicazione se l'analisi delle transazioni della relazione d'affari oggetto dell'ordine di consegna dei documenti e/o di sequestro rivela transazioni sospette al di fuori del lasso di tempo indicato dal pubblico ministero. Va inoltre considerato che l'intermediario finanziario non è legato alle circostanze di fatto, in genere succinte, indicate dall'autorità di perseguimento penale responsabile dell'ordine di perquisizione e/o di sequestro. Questo implica che se, in occasione dei chiarimenti complementari secondo l'art. 6 cpv. 2 LRD in combinato disposto con gli articoli 15 e seguenti ORD-FINMA, l'intermediario finanziario individua elementi di sospetto supplementari o nuovi in relazione con le stesse o con altre persone menzionate nell'ordine di consegna dei documenti e/o di sequestro oppure implicate nella relazione d'affari i cui beni patrimoniali sono oggetto di sequestro o in altre relazioni d'affari, l'intermediario finanziario è obbligato, in caso di nuovi elementi di sospetto fondati, a comunicarlo in applicazione dell'art. 9 cpv. 1 lett. a LRD. In questi casi, l'intermediario deve sempre allegare alla propria comunicazione il relativo ordine di perquisizione e/o sequestro (art. 3 cpv. 1 lett. h OURD).[42] MROS esercita un'attività di verifica e di coordinamento con le autorità di perseguimento penale competenti che permette di valutare le informazioni ricevute e di decidere se occorre trasmettere le informazioni comunicate alle autorità competenti. Nel 2020, ad esempio, nel 9,1 per cento dei casi gli intermediari finanziari autori di una comunicazione hanno dichiarato che all'origine del sospetto vi erano informazioni delle autorità di perseguimento penale. Nella maggioranza dei casi le informazioni risultanti dalle comunicazioni sono trasmesse da MROS alle autorità di perseguimento penale competenti perché si tratta di informazioni nuove ritenute utili per lo svolgimento del procedimento penale in corso.
Per contro, se l'obbligo di chiarimento dell'intermediario finanziario non conduce a maggiori informazioni rispetto a quanto l'autorità di perseguimento penale esige mediante l'ordine di consegna dei documenti o la decisione di sequestro, l'intermediario finanziario può rinunciare a una comunicazione di sospetto supplementare a MROS. Infatti, una tale comunicazione costituirebbe un doppione inutile.
Questo vale anche per l'intermediario finanziario terzo (gestore di patrimoni, fiduciario, ecc.) che è stato informato da una banca in merito all'obbligo di consegna ai sensi dell'art. 265 Codice di procedura penale del 5 ottobre 2007[43] (dopo la scadenza di un eventuale divieto di informare qualsiasi persona) o, conformemente all'art. 10a cpv. 3 LRD, in merito al fatto che è stata effettuata una comunicazione di sospetto in virtù dell'art. 9 LRD.
Secondo la giurisprudenza del TF[44] l'obbligo di comunicazione non si conclude con il ricorso alle

---

41 Cfr. *rapporto annuale 2007* di MROS, pag. 86.

42 Cfr. *rapporto annuale 2017* di MROS (pag. 57) e *les commentaires à la révision partielle de l'OBCBA* del 24 novembre 2019 (non disponibile in italiano), pag. 14 nota 37.

43 RS **312.0**

44 Cfr. DTF 144 IV 391, consid. 3.1 e 3.3-3.4; DTF 142 IV 276, consid. 5.4.2

autorità di perseguimento penale: esso perdura fintanto che i beni possono essere scoperti e confiscati.[45] L'apertura di un'inchiesta non significa ancora che le condizioni per la pronuncia di un sequestro penale siano soddisfatte. Per contro, la comunicazione dell'intermediario finanziario a MROS conformemente agli articoli 9 LRD e 3 OURD può portare molto rapidamente al blocco degli averi sulla base dell'art. 10 LRD. La segnalazione di operazioni sospette è un obbligo specifico dell'intermediario finanziario, a prescindere da un'eventuale procedimento penale.
L'intermediario finanziario che riceve un ordine di perquisizione e/o di sequestro s'impegna, conformemente agli obblighi di diligenza specifici dell'art. 6 cpv. 2 LRD in combinato disposto con gli articoli 15 e seguenti ORD FINMA, a individuare la totalità dei valori patrimoniali potenzialmente incriminati ancora depositati sui suoi conti o sulle relazioni d'affari ormai chiuse e a identificare eventuali altri elementi di sospetto. Fintanto che quest'attività non è conclusa, l'intermediario finanziario non è in grado di escludere un eventuale sospetto fondato.
Una comunicazione di sospetto ai sensi dell'art. 9 cpv. 1 LRD, seguita da una denuncia di MROS ai sensi dell'art. 23 cpv. 4 LRD e dal blocco dei beni che ne risulta (art. 10 LRD), rappresenta pertanto il solo strumento possibile per garantire l'individuazione di tali beni affinché l'autorità di perseguimento penale competente possa pronunciare un nuovo ordine di perquisizione e di sequestro che apra la strada a un'eventuale confisca. La comunicazione di sospetto permette anche di identificare e di perseguire penalmente eventuali altri colpevoli di riciclaggio di denaro.

6.4 Ricezione delle comunicazioni di sospetto da parte di MROS

A MROS sono inviate regolarmente comunicazioni che a causa della mancanza di competenza materiale e territoriale non possono essere accettate e quindi neppure trattate come comunicazioni ai sensi della LRD o della legge federale del 18 dicembre 2015 sui valori patrimoniali di provenienza illecita (LVP)[46].
Gli autori di tali comunicazioni sono persone fisiche o giuridiche che non sottostanno alla LRD oppure a cui si applica l'LRD ma che nell'ambito dei fatti comunicati non operano in qualità di intermediari finanziari ai sensi dell'art. 2 LRD o di persone e istituzioni ai sensi dell'art. 7 LVP.
MROS è l'unico servizio in Svizzera autorizzato a ricevere e trattare comunicazioni di intermediari finanziari, commercianti, autorità e organismi ai sensi della LRD inviate per sospetto di riciclaggio di denaro, di reato preliminare al riciclaggio, di appartenenza a un'organizzazione criminale o di finanziamento del terrorismo. MROS decide se trasmettere le informazioni ricevute a un'autorità di perseguimento penale (art. 23 cpv. 4 LRD). Inoltre riceve informazioni di persone e istituzioni ai sensi dell'art. 7 cpv. 1 e 2 LVP e le trasmette al Dipartimento federale degli affari esteri (DFAE) e all'Ufficio federale di giustizia (UFG, art. 7 cpv. 6 LVP).
Se non può accettare comunicazioni di sospetto perché non dispone della competenza materiale e territoriale, MROS non può trattare le informazioni ivi contenute né trasmetterle a un'autorità di perseguimento penale conformemente all'art. 23 cpv. 4 LRD.
In virtù del principio di specialità MROS può viceversa accettare e trattare le comunicazioni di sospetto soltanto se è competente sotto il profilo materiale e territoriale.
Tutte le altre persone (fisiche o giuridiche) non sottoposte alla LRD e alla LVP che hanno un suddetto sospetto sono pertanto tenute a rivolgersi direttamente alle autorità di perseguimento penale. Di norma le denunce alla polizia sono sporte nel luogo di domicilio dell'autore della denuncia.
Nel 2020 MROS ha ricevuto 140 lettere di cittadini e 8 messaggi designati come comunicazioni di sospetto ai sensi dell'art. 9 LRD o 305ter CP, per i quali non era competente sotto il profilo materiale e/o territoriale.
Quando riceve una comunicazione, MROS verifica d'ufficio la sua competenza. Può tuttavia

[45] Cfr. DTF 144 IV 391, consid. 3.1

[46] RS **196.1**

esaminare soltanto in modo sommario se l'entità dichiarante sottostà alla LRD o meno, soprattutto perché per legge non ha la competenza di decidere materialmente in merito all'assoggettamento alla LRD. Tale compito incombe in gran parte alla FINMA, che in base alla sua competenza di riconoscere gli OAD e gli OV è competente per queste ultime e indirettamente per le entità da esse sorvegliate. La FINMA pubblica infatti sul suo sito Internet i nomi delle istituzioni che dispongono di una determinata forma di autorizzazione.[47] Secondo l'art. 12 LRD, la vigilanza sull'osservanza degli obblighi secondo la LRD compete, oltre che alla FINMA, alla Commissione federale delle case da gioco (CFCG), all'Autorità intercantonale di vigilanza, d'esecuzione secondo l'art. 105 della legge federale sui giochi in denaro (LGD)[48], ovvero l'autorità intercantonale di vigilanza sui giochi in denaro (Gespa), o agli OAD o OV riconosciuti. Le pertinenti informazioni sono pubblicate sui siti Internet di questi organi. Inoltre, in tale contesto MROS può scambiare informazioni con la FINMA, la CFCG, la Gespa (cfr. art. 29 cpv. 1 LRD in applicazione congiunta con l'art.. 7 cpv. 1 lett. d OURD).
Quando si invia una comunicazione di sospetto così come per la registrazione in goAML occorre anche indicare l'autorità o l'organismo che vigila sull'intermediario finanziario ai sensi dell'art. 12 LRD o dell'art. 43a della legge sulla vigilanza dei mercati finanziari del 22 giugno 2007[49] (cfr. art. 3 cpv. 1 lett. b OURD).
MROS svolge una verifica sommaria anche nel caso in cui un'entità che, non disponendo dell'autorizzazione in senso stretto di un'autorità e le cui, attività non sono così soggette nella loro totalità alla LRD per la mancata constatazione di un'autorità in occasione della procedura di autorizzazione, abbia operato in qualità di intermediario finanziario. Anche in questo caso possono essere scambiate informazioni con le autorità di vigilanza alle condizioni dell'art. 29 cpv. 1 LRD.

---

47 Vgl. https://www.finma.ch/it/finma-public/istituti-persone-e-prodotti-autorizzati/, https://www.finma.ch/it/autorizzazione/organismi-di-autodisciplina-oad/ricerca-di-affiliati-oad/

48 RS **935.51**

49 RS **956.1**

7. Links

7.1 Svizzera

7.1.1 Ufficio di comunicazione in materia di riciclaggio di denaro

www.fedpol.admin.ch
Ufficio federale di polizia (fedpol)

https://www.fedpol.admin.ch/fedpol/it/home/kriminalitaet/geldwaescherei.html
Ufficio di comunicazione in materia di riciclaggio di denaro (MROS)

https://www.fedpol.admin.ch/fedpol/it/home/kriminalitaet/geldwaescherei/meldung.html
Informazioni su goAML

7.1.2 Autorità di vigilanza

www.finma.ch
Autorità federale di vigilanza sui mercati finanziari (FINMA)

www.esbk.admin.ch
Commissione federale delle case da gioco (CFCG)

www.gespa.ch
Autorità intercantonale di vigilanza sui giochi in denaro (Gespa)

7.1.3 Associazioni e organizzazioni nazionali

www.swissbanking.org
Associazione Svizzera dei Banchieri (ASB)

www.abps.ch
Associazione delle banche private svizzere

www.foreignbanks.ch
Associazione delle banche estere in Svizzera

www.svv.ch
Associazione Svizzera d'Assicurazioni (ASA)

www.vsv-asg.ch
Associazione Svizzera di Gestori di Patrimonio (ASG)

www.am-switzerland.ch
Asset Management Association Switzerland

www.svig.org
Schweizer Verband der Investmentgesellschaften (SVIG)

7.1.4 Organismi di autodisciplina

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

www.arif.ch
Association Romande des Intermédiaires Financiers (ARIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

www.oadfct.ch
Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT)

www.polyreg.ch
PolyReg Associazione Generale di Autodisciplina

www.sro-sav-snv.ch
Organismo di autodisciplina della Federazione Svizzera degli Avvocati e della Federazione Svizzera dei Notai (FSA/FSN)

www.leasingverband.ch
Organismo di autodisciplina dell'Associazione Svizzera delle società di leasing (ASSL)

http://www.sro-treuhandsuisse.ch/it/home
Organismo di autodisciplina dell'Unione Svizzera dei Fiduciari (OAD-FIDUCIARI ¦SUISSE)

www.vqf.ch
Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF)

www.sro-svv.ch
Organismo di autodisciplina dell'Association Suisse d'Assurances (OAR-ASA)

7.1.5 Organismi di vigilanza

https://www.aoos.ch/
Organismo di vigilanza per Gestori patrimoniali e Trustees (AOOS)

http://www.fincontrol.ch/
FINcontrol Suisse AG

https://osif.ch/
Organismo di vigilanza degli istituti finanziari (OSIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

https://osfin.ch/
Organismo di vigilanza finanziaria (OSFIN)

7.1.6 Altri

www.ezv.admin.ch
Amministrazione federale delle dogane (AFD)

www.snb.ch
Banca nazionale svizzera (BNS)

www.bundesanwaltschaft.ch
Ministero pubblico della Confederazione (MPC)

https://www.seco.admin.ch/seco/it/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html
Segreteria di Stato dell'economia (SECO; sanzioni economiche in virtù della legge sugli embarghi)

www.estv.admin.ch
Amministrazione federale delle contribuzioni (AFC)

https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.html
Servizio delle attività informative della Confederazione (SIC)

www.bstger.ch
Tribunale penale federale (TPF)

7.2 Internazionale

7.2.1 Uffici di comunicazione esteri

https://www.egmontgroup.org/en/membership/list
Elenco dei membri del Gruppo Egmont, in alcuni casi con aggiunta dei link verso i loro siti Internet

7.2.2 Organizzazioni internazionali

www.fatf-gafi.org
Financial Action Task Force on Money Laundering (FATF)

www.unodc.org
United Nations Office on Drugs and Crime (UNO-DC)

www.egmontgroup.org
Gruppo Egmont

www.cfatf-gafic.org
Caribbean Financial Action Task Force (CFATF)

7.2.3 Altri link

www.interpol.int
Interpol

www.europol.europa.eu
Europol