



ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

NEWSLETTER MENSILE DI AIRA

Edizione n. 168 della Newsletter di AIRA

ANTIRICICLAGGIO NEWS

OTTOBRE 2026

168



IN QUESTO NUMERO

3. Editoriale del **Presidente**
5. Rassegna UIF I semestre 2026: qualità del processo e valore della collaborazione attiva – **Piercarlo Felice**
7. UNODC: la Dichiarazione di Abu Dhabi per contrastare le nuove minacce criminali nell'era digitale – **Giorgia Azzellini**
9. Anticorruzione: a Roma il confronto europeo su nuove regole, efficacia delle Autorità e strategie comuni – **Elisa Gorra**
10. EUROPOL: i responsabili delle forze dell'ordine dell'UE si riuniscono per affrontare le nuove sfide della sicurezza europea – **Antonio Arrotino**
11. Europol sollecita un'azione tempestiva per proteggere le criptovalute e i dati sensibili dalle minacce quantistiche – **Gloria Lazzaro**
12. UIF: aggiornate le FAQ sulle comunicazioni oggettive e sulla verifica dei dati trasmessi – **Silvia Marini**
14. Prossime iniziative
15. Redazione e contatti



Editoriale del Presidente

Cari Amici,

la sicurezza europea si trova oggi ad affrontare una fase di profonda trasformazione, nella quale l'evoluzione tecnologica, la crescente dimensione transnazionale della criminalità e l'emergere di nuove forme di minaccia rendono sempre più indispensabile una risposta coordinata tra Stati, istituzioni e operatori dei diversi settori. È proprio in questo scenario che si inserisce la Convention europea dei capi di polizia 2026, organizzata da Europol dal 28 al 30 settembre presso la propria sede, che ha riunito oltre 500 rappresentanti delle forze dell'ordine provenienti da 59 Paesi e 15 organizzazioni internazionali.

L'incontro ha rappresentato un'importante occasione di confronto sulle principali criticità che interessano la sicurezza globale, ponendo al centro del dibattito il ruolo dell'Intelligenza artificiale, l'accesso legittimo ai dati, la diffusione della disinformazione, i processi di radicalizzazione e il rafforzamento della cooperazione internazionale, anche in ambito doganale. Argomenti sui quali, come saprete, sono più volte tornato.

Uno degli aspetti maggiormente significativi emersi dalla Convenzione riguarda la progressiva digitalizzazione delle attività criminali. Le tecnologie non costituiscono più soltanto strumenti accessori alla commissione dei reati, ma rappresentano ormai una componente strutturale delle strategie adottate dalle organizzazioni criminali. In tale contesto, è stata ribadita la necessità di affiancare alle competenze investigative nazionali strumenti operativi condivisi a livello europeo, investendo in capacità tecnologiche comuni e riducendo, al contempo, le dipendenze strategiche da infrastrutture e soluzioni digitali esterne. Noi possiamo fare molto su questo.

Particolare attenzione è stata dedicata all'Intelligenza artificiale, il cui sviluppo presenta opportunità e rischi strettamente interconnessi. Da un lato, l'impiego illecito di sistemi generativi, contenuti deepfake e strumenti automatizzati favorisce la diffusione di frodi, attacchi informatici e ulteriori attività criminali, comprese quelle legate al traffico di migranti e allo sfruttamento dei minori. Dall'altro, le medesime tecnologie possono contribuire a migliorare sensibilmente l'efficacia delle indagini, accelerando l'elaborazione delle informazioni e potenziando le capacità di analisi delle autorità competenti. Diventa pertanto essenziale promuoverne un utilizzo responsabile, sostenuto da investimenti adeguati, regole chiare e una collaborazione internazionale sempre più solida. L'utilizzo dell'IA nella detection AML è già realtà anche presso le vostre strutture.

Un ulteriore tema di rilievo ha riguardato il contrasto alla radicalizzazione, fenomeno che assume manifestazioni ideologiche differenti e trova nell'ambiente digitale un importante fattore di amplificazione. La diffusione della propaganda online, l'azione di soggetti isolati e la crescente difficoltà nell'individuare tempestivamente comportamenti potenzialmente pericolosi richiedono strategie di prevenzione capaci di integrare attività investigative, scambio informativo, coinvolgimento delle comunità e maggiore responsabilizzazione delle piattaforme digitali.



Editoriale del Presidente

(continua)

Non meno importante è il contributo richiesto al settore privato, soprattutto nella prevenzione delle frodi finanziarie online. È emersa, infatti, l'esigenza di intensificare la collaborazione tra istituti bancari, autorità investigative, operatori delle telecomunicazioni e piattaforme social, affinché le attività fraudolente possano essere individuate e interrotte prima che le somme sottratte vengano trasferite, assicurando una tutela più efficace anche ai soggetti maggiormente vulnerabili. Ricordo che questi reati sono spesso propedeutici al riciclaggio.

Sul versante della cooperazione operativa, merita particolare attenzione la sottoscrizione del Piano d'azione congiunto 2026-2027 tra Europol e l'Organizzazione mondiale delle dogane, finalizzato a rafforzare lo scambio di informazioni, l'analisi strategica e le capacità di contrasto alla criminalità transfrontaliera.

La Convenzione ha inoltre valorizzato l'innovazione nelle attività di polizia attraverso il conferimento degli Europol Excellence Awards 2026, riconoscendo iniziative capaci di coniugare progresso tecnologico, efficacia operativa e attenzione ai principi etici e di inclusione.

Quanto emerso da questo importante appuntamento internazionale conferma, dunque, che la sicurezza non può più essere considerata una responsabilità circoscritta ai singoli ordinamenti o alle sole autorità di contrasto. La complessità delle minacce contemporanee impone una visione integrata, nella quale cooperazione istituzionale, innovazione tecnologica e collaborazione pubblico-privato diventino elementi complementari di una strategia comune. Una sfida che riguarda l'intera comunità europea e che richiede un impegno costante per garantire, anche nell'attuale contesto digitale, la protezione dei cittadini, la tenuta delle istituzioni e la salvaguardia dei valori democratici.

L'Italia su questo è avanti e noi non mancheremo mai di fornire il nostro (modesto) supporto.

Il Presidente

Ranieri Razzante

.

Rassegna UIF I semestre 2026: qualità del processo e valore della collaborazione attiva

Piercarlo Felice

La Rassegna normativa UIF relativa al primo semestre 2026 dedica uno specifico approfondimento alle Istruzioni per la rilevazione e la segnalazione delle operazioni sospette, adottate il 18 dicembre 2025 e applicabili dal 1° luglio 2026. L'interesse dell'approfondimento risiede soprattutto nella lettura sistematica del modello di collaborazione attiva delineato dalle Istruzioni. La SOS emerge come l'esito di un processo nel quale individuazione dell'anomalia, approfondimento, decisione e rappresentazione del sospetto costituiscono fasi distinte ma strettamente connesse. È una prospettiva particolarmente rilevante per le Funzioni antiriciclaggio, perché sposta l'attenzione dal singolo adempimento alla qualità complessiva del processo che conduce alla decisione di segnalare o di non segnalare. Uno dei passaggi centrali riguarda la distinzione tra anomalia e sospetto. Indicatori, schemi, regole di selezione, classificazioni di rischio e strumenti informatici consentono di individuare situazioni meritevoli di approfondimento, ma non determinano automaticamente l'esito della valutazione.

L'individuazione dell'anomalia apre, piuttosto, una fase di esame nella quale devono essere utilizzate tutte le informazioni pertinenti e tempestivamente disponibili. Non è richiesto l'accertamento di una fattispecie criminosa né la dimostrazione della provenienza illecita delle risorse: il sospetto deriva dall'apprezzamento professionale delle circostanze oggettive e soggettive considerate nel loro insieme.

Diventa quindi centrale la contestualizzazione. Profilo del cliente, controparti, rapporti, operazioni effettuate o tentate, finalità dichiarate, collegamenti con altri soggetti e ulteriori informazioni disponibili devono concorrere alla ricostruzione del quadro complessivo.

La qualità della collaborazione attiva si misura proprio nella capacità di governare questo spazio tra rilevazione e decisione. Una fattispecie riconducibile a un indicatore può non condurre alla SOS se l'approfondimento fornisce una spiegazione coerente; allo stesso modo, circostanze non riconducibili meccanicamente a indicatori predeterminati possono assumere rilievo quando considerate nel contesto concreto.

La Rassegna attribuisce particolare rilievo alla qualità delle segnalazioni, da valutare attraverso pertinenza, completezza, chiarezza, tempestività e attendibilità delle informazioni.

Completezza e selettività non sono criteri contrapposti. Una SOS completa non è quella nella quale confluisce indiscriminatamente tutto il patrimonio informativo disponibile, ma quella che contiene gli elementi necessari a comprendere il contesto e le ragioni del sospetto.

Ne consegue l'esigenza di evitare elenchi sovrabbondanti di movimentazioni, allegazioni scarsamente selezionate o la mera riproduzione nella parte descrittiva di informazioni già contenute nei campi strutturati. L'aumento dei dati disponibili non determina, di per sé, un corrispondente incremento della qualità dell'informazione finanziaria. In questa prospettiva assume rilievo la narrativa, che deve completare i dati strutturati rendendo comprensibile il percorso logico seguito dal segnalante. Non dovrebbe limitarsi alla cronologia delle operazioni o al richiamo dell'indicatore rilevato, ma evidenziare le incoerenze riscontrate, i collegamenti significativi e le ragioni per le quali l'operatività assume rilievo nel caso concreto.

La selezione delle informazioni risponde anche all'esigenza di tutelare i soggetti segnalati. Diligenza e buona fede richiedono di evitare elementi eccedenti o non pertinenti e valutazioni non adeguatamente supportate.

Le Istruzioni riconoscono espressamente il possibile impiego di strumenti informatici e di intelligenza artificiale per l'individuazione e la selezione delle anomalie. Il loro utilizzo deve però inserirsi in un processo governato, fondato su dati oggettivi e verificabili, coerente con l'approccio basato sul rischio e sottoposto a supervisione umana.

Non vi è, dunque, una contrapposizione tra automazione e giudizio professionale. Gli strumenti tecnologici possono ampliare la capacità di intercettazione, selezionare fenomeni ricorrenti e contribuire alla prioritizzazione degli approfondimenti. La decisione richiede però che gli esiti prodotti dai sistemi siano interpretati alla luce delle informazioni disponibili e delle caratteristiche della fattispecie.

Per la Funzione antiriciclaggio ciò implica anche un tema di governo degli strumenti utilizzati: criteri di selezione e prioritizzazione, qualità dei dati, adeguatezza delle regole e possibilità di ricostruire il percorso che ha condotto all'emersione dell'anomalia diventano componenti della qualità del processo.

Analoga importanza assume la tracciabilità delle valutazioni. Quando l'approfondimento non conduce a una SOS, non sussiste un obbligo generalizzato di formalizzare analiticamente ogni decisione negativa; costituisce però buona prassi conservare evidenze sufficienti a consentire la ricostruzione, anche sintetica, del percorso valutativo.

La tracciabilità non dovrebbe trasformarsi in una produzione documentale fine a sé stessa. La sua funzione è rendere verificabile la valutazione effettuata, non generare motivazioni standardizzate che rischierebbero di aggiungere forma senza migliorare la sostanza del controllo.

Misure restrittive: il richiamo di Banca d'Italia sui sistemi di controllo

(continua)

Anche la tempestività assume una dimensione organizzativa. Il riferimento normativo alla segnalazione “senza ritardo” non individua un termine rigido: devono essere considerate la conoscibilità dell'anomalia, la complessità della fattispecie e la profondità degli approfondimenti necessari.

Ciò non significa che l'organizzazione interna possa dilatare i tempi della valutazione. Flussi informativi inefficienti, passaggi decisionali non necessari o accumuli di anomalie non adeguatamente priorizzate possono incidere sulla tempestività della collaborazione attiva.

Per gli intermediari, il punto assume particolare rilievo nella definizione delle procedure interne e dei flussi tra strutture operative e Funzione antiriciclaggio. L'efficacia della procedura non dipende dalla mera riproduzione delle disposizioni applicabili, ma dalla capacità di definire responsabilità, criteri di escalation, strumenti e tempi coerenti con natura, dimensione e complessità dell'attività.

Completa questo circuito il flusso di ritorno della UIF, finalizzato ad accrescere nei destinatari la consapevolezza sulla qualità delle informazioni trasmesse e sull'utilità delle segnalazioni ai fini dell'analisi finanziaria. Gli esiti e le indicazioni ricevute possono essere utilizzati per perfezionare le modalità di rilevazione, analisi e rappresentazione delle operazioni sospette, fermo restando che non costituiscono un giudizio sul livello di rischio del singolo cliente.

Il feedback assume così una funzione che va oltre il riscontro sulla singola SOS: può concorrere alla revisione dei criteri di selezione, alla calibrazione dei controlli, alla qualità della narrativa e alla programmazione della formazione.

Un ulteriore profilo riguarda il rapporto tra SOS e altri obblighi previsti dalla disciplina antiriciclaggio e da normative contigue. Astensione, comunicazioni oggettive, comunicazioni al MEF, dichiarazioni relative alle operazioni in oro, adempimenti connessi alle misure restrittive e denunce all'Autorità giudiziaria rispondono a presupposti e finalità differenti.

L'esistenza di uno di tali adempimenti non determina automaticamente la necessità della segnalazione, così come la SOS non può essere utilizzata in loro sostituzione. Anche in questi casi deve essere preservata l'autonomia della valutazione richiesta dall'art. 35 del d.lgs. 231/2007.

Il principio assume particolare importanza nell'attuale contesto, caratterizzato dalla moltiplicazione dei flussi informativi e degli obblighi di controllo. La SOS conserva una funzione specifica e non dovrebbe trasformarsi in uno strumento generale di cautela attraverso il quale rappresentare alla UIF qualsiasi circostanza problematica emersa nell'attività dell'intermediario.

La lettura offerta dalla Rassegna restituisce, in definitiva, un modello nel quale qualità della decisione e qualità della segnalazione sono parti dello stesso processo. Per le Funzioni antiriciclaggio la sfida non consiste soltanto nell'intercettare le anomalie, ma nel governare criteri, strumenti, informazioni e valutazioni che consentano di stabilire quali di esse assumano effettiva rilevanza ai fini della collaborazione attiva.

È su questo terreno che selettività e qualità possono rafforzarsi reciprocamente: non riducendo l'attenzione verso le anomalie, ma aumentando la capacità di trasformare quelle effettivamente significative in informazione finanziaria utile per la UIF e, più in generale, per il sistema di prevenzione del riciclaggio e del finanziamento del terrorismo.

UNODC: la Dichiarazione di Abu Dhabi per contrastare le nuove minacce criminali nell'era digitale

Giorgia Azzellini

Il 26 settembre 2026, in occasione dell'apertura del quindicesimo Congresso delle Nazioni Unite sulla prevenzione del crimine e la giustizia penale, svoltosi ad Abu Dhabi, gli Stati membri hanno adottato per acclamazione la Dichiarazione di Abu Dhabi, un quadro d'azione globale volto a rafforzare la cooperazione internazionale in materia di giustizia penale e a contrastare le minacce criminali in rapida evoluzione, con particolare riferimento allo sfruttamento delle tecnologie digitali. Il documento individua le principali sfide emergenti nel panorama della criminalità contemporanea e definisce le direttrici per un'azione coordinata di prevenzione e contrasto, promuovendo al contempo l'innovazione dei sistemi giudiziari nel rispetto delle garanzie fondamentali.

Il Congresso, ospitato dal Governo degli Emirati Arabi Uniti e organizzato con il supporto dell'United Nations Office on Drugs and Crime (UNODC), rappresenta uno dei principali appuntamenti internazionali dedicati alla prevenzione del crimine e alla giustizia penale. All'incontro partecipano rappresentanti di 119 Paesi, oltre 40 ministri della Giustizia e altri funzionari di alto livello, per un totale di più di 5.100 partecipanti provenienti da Stati membri, settore privato, società civile e mondo accademico. I lavori, dedicati al tema «Protecting People and Planet in the Digital Age», si sono svolti dal 26 settembre al 1° ottobre 2026.

La Dichiarazione si inserisce in un contesto caratterizzato dalla crescente complessità delle attività criminali e dall'impiego sempre più sofisticato delle infrastrutture e delle tecnologie digitali. Gli Stati membri evidenziano, in particolare, l'emergere di modelli quali il «crime as a service» e il «violence as a service», nei quali servizi, strumenti e capacità operative possono essere messi a disposizione di soggetti criminali. Il documento richiama inoltre lo sfruttamento delle infrastrutture informatiche e delle tecnologie digitali per realizzare o agevolare attività illecite.

Tra le minacce che richiedono un intervento coordinato figurano il cybercrime e le frodi, fenomeni che possono beneficiare della diffusione delle tecnologie e della capacità delle reti criminali di operare oltre i confini nazionali. La Dichiarazione riconosce pertanto la necessità di rafforzare la cooperazione internazionale in materia di giustizia penale, affinché gli strumenti di prevenzione e contrasto possano rispondere all'evoluzione delle condotte illecite e alle nuove modalità di sfruttamento delle tecnologie.

Un elemento centrale riguarda il rapporto tra innovazione tecnologica e attività criminale. Le tecnologie digitali, pur offrendo opportunità per migliorare l'efficienza dei sistemi giudiziari, possono essere utilizzate per agevolare frodi, inganni e altre forme di sfruttamento. L'evoluzione tecnologica impone quindi alle Autorità di sviluppare capacità adeguate a individuare e contrastare le nuove minacce, senza trascurare le garanzie necessarie a tutelare i diritti delle persone coinvolte nei procedimenti.

In questa prospettiva, gli Stati membri si impegnano a promuovere la digitalizzazione dei sistemi giudiziari e a valorizzare le potenzialità delle nuove tecnologie, compresa l'intelligenza artificiale, nelle attività di prevenzione e risposta alla criminalità. L'impiego di tali strumenti è considerato una componente dell'evoluzione della giustizia penale, con l'obiettivo di rafforzare le capacità istituzionali e migliorare la risposta alle sfide emergenti.

UNODC: la Dichiarazione di Abu Dhabi per contrastare le nuove minacce criminali nell'era digitale (continua)

La Dichiarazione sottolinea, tuttavia, che l'innovazione deve essere accompagnata da adeguate garanzie. Tra i principi richiamati figurano la supervisione umana, la trasparenza, il rispetto del giusto processo e la protezione dei dati. Tali presidi assumono particolare rilievo nell'utilizzo dell'IA e degli altri strumenti digitali nell'ambito della giustizia penale, affinché il ricorso alla tecnologia rimanga compatibile con la tutela dei diritti fondamentali e con i principi dello Stato di diritto.

Il documento richiama inoltre l'importanza della cooperazione internazionale quale presupposto per affrontare fenomeni criminali caratterizzati da una crescente dimensione transnazionale. La capacità delle reti criminali di sfruttare tecnologie e infrastrutture digitali rende necessario un coordinamento tra gli Stati e un rafforzamento degli strumenti condivisi di prevenzione e contrasto. In tale contesto, l'UNODC svolge il ruolo di segretariato del Congresso e sosterrà l'attuazione della Dichiarazione di Abu Dhabi.

L'adozione del documento costituisce il punto di partenza per una fase successiva, incentrata sulla traduzione degli impegni internazionali in iniziative concrete. In questo quadro, si colloca l'iniziativa volontaria Pledge4Justice, attraverso la quale gli Stati partecipanti annunciano azioni specifiche, concrete e soggette a scadenze definite per promuovere la prevenzione del crimine e il miglioramento della giustizia penale fino al 2031.

L'iniziativa mira quindi a favorire il passaggio dagli impegni assunti a livello internazionale alla loro attuazione, attraverso misure individuate dai singoli Paesi. La previsione di azioni concrete e temporalmente definite consente di orientare il seguito dei lavori verso interventi destinati a rafforzare le politiche di prevenzione e contrasto, in coerenza con le priorità individuate nella Dichiarazione.

Nel complesso, la Dichiarazione di Abu Dhabi individua nella cooperazione internazionale, nell'innovazione tecnologica e nel rafforzamento dei sistemi di giustizia penale gli elementi centrali per affrontare le nuove minacce criminali. Il crescente sfruttamento delle tecnologie digitali impone agli Stati di adeguare le proprie capacità di prevenzione e contrasto, favorendo al contempo la digitalizzazione dei sistemi giudiziari e l'impiego responsabile dell'intelligenza artificiale.

L'attuazione degli impegni richiederà pertanto il coordinamento tra gli Stati e la definizione di interventi concreti, accompagnati da garanzie in materia di supervisione umana, trasparenza, giusto processo e protezione dei dati. La Dichiarazione e l'iniziativa Pledge4Justice delineano, in questa prospettiva, un percorso volto a tradurre il consenso internazionale in azioni verificabili, rafforzando la capacità dei sistemi di giustizia penale di rispondere all'evoluzione della criminalità nell'era digitale.

Anticorruzione: a Roma il confronto europeo su nuove regole, efficacia delle Autorità e strategie comuni

Elisa Gorra

La costruzione di un sistema europeo di prevenzione e contrasto della corruzione sempre più integrato è stata al centro della European Conference on Anti-Corruption Agency Effectiveness, svoltasi a Roma dal 16 al 18 settembre 2026. L'iniziativa, promossa dall'Autorità Nazionale Anticorruzione (ANAC) insieme alla International Anti-Corruption Academy (IACA), ha riunito rappresentanti ed esperti provenienti da oltre 40 Paesi, coinvolgendo istituzioni europee, organismi internazionali, autorità di controllo, mondo accademico e società civile.

L'appuntamento ha offerto un'importante occasione di confronto sulle prospettive di evoluzione delle politiche anticorruzione dell'Unione europea, concentrando l'attenzione su tre direttrici fondamentali: il nuovo quadro normativo europeo, la valutazione dell'effettiva capacità operativa delle autorità nazionali e la definizione di una strategia comune di lungo periodo.

Particolare rilievo è stato attribuito alla prima Direttiva europea specificamente dedicata al contrasto della corruzione, destinata a favorire una maggiore armonizzazione delle disposizioni nazionali in materia di prevenzione, repressione e perseguimento dei fenomeni corruttivi. L'obiettivo è superare le disomogeneità tra gli ordinamenti degli Stati membri, promuovendo standard condivisi e una più efficace collaborazione transfrontaliera. La portata dell'intervento europeo comprende anche il rafforzamento delle strutture istituzionali incaricate di prevenire e contrastare la corruzione. In questa prospettiva, indipendenza, disponibilità di risorse adeguate e competenze specialistiche rappresentano condizioni imprescindibili per assicurare un'effettiva capacità di intervento. E la nostra Autorità è già perfettamente allineata.

Un secondo ambito di approfondimento ha riguardato la necessità di sviluppare strumenti attendibili per misurare l'efficacia delle autorità anticorruzione. Su questo fronte assume particolare importanza la metodologia elaborata nel 2025 dalla IACA nell'ambito del Global Programme on Measuring Corruption, orientata a una valutazione fondata su dati ed evidenze verificabili. L'approccio proposto mira a superare una lettura esclusivamente quantitativa delle attività istituzionali, privilegiando l'analisi dell'impatto concreto delle misure adottate e delle condizioni organizzative che ne determinano il successo. La disponibilità di indicatori comuni e il confronto tra esperienze nazionali possono infatti contribuire a individuare criticità, valorizzare le migliori pratiche e orientare con maggiore precisione le future politiche pubbliche.

Il dibattito ha inoltre affrontato il percorso di elaborazione della prima Strategia organica anticorruzione dell'Unione europea, concepita come strumento per ricondurre le diverse iniziative nazionali ed europee all'interno di una visione coordinata. La futura Strategia punta a integrare prevenzione, attività di contrasto, cooperazione internazionale e partecipazione della società civile, traducendo gli indirizzi comuni in interventi concreti e obiettivi misurabili.

Il Convegno ha dunque evidenziato come la lotta alla corruzione richieda oggi un approccio che sappia coniugare solidità normativa, autonomia istituzionale e capacità di valutare concretamente i risultati raggiunti. La futura architettura europea, fondata sull'integrazione tra Direttiva, Strategia comune e strumenti di misurazione dell'efficacia, rappresenta un passaggio significativo verso sistemi di prevenzione e contrasto più omogenei, trasparenti e responsabili. Una prospettiva nella quale la cooperazione tra istituzioni e la condivisione delle conoscenze assumono un ruolo determinante per rafforzare lo Stato di diritto e consolidare la fiducia dei cittadini nell'azione pubblica.

EUROPOL: i responsabili delle forze dell'ordine dell'UE si riuniscono per affrontare le nuove sfide della sicurezza europea

Antonio Arrotino

La trasformazione digitale della criminalità, l'impiego crescente dell'intelligenza artificiale da parte delle organizzazioni criminali e il contrasto alla radicalizzazione sono stati i temi centrali dell'European Police Chiefs Convention 2026, l'importante appuntamento organizzato da Europol che ha riunito all'Aia oltre 500 capi delle forze di polizia e rappresentanti delle autorità di contrasto provenienti da 59 Paesi e 15 organizzazioni internazionali.

L'evento ha rappresentato un'occasione strategica per fare il punto sulle principali minacce alla sicurezza che interessano l'Europa e per rafforzare la cooperazione internazionale nella lotta al crimine organizzato e alle minacce emergenti. Tra i temi affrontati figurano l'utilizzo dell'intelligenza artificiale nelle attività criminali, l'accesso legale ai dati per le indagini, le campagne di disinformazione finalizzate a destabilizzare le società europee, la prevenzione della radicalizzazione e il potenziamento della cooperazione tra forze di polizia e autorità doganali.

Nel corso dei lavori, il Direttore esecutivo ad interim di Europol, Jürgen Ebner, ha evidenziato come il crimine organizzato sia ormai "digitale per impostazione predefinita", sottolineando che la tecnologia non rappresenta più soltanto uno strumento a supporto delle attività illecite, ma sempre più spesso ne costituisce il motore principale. Per questo motivo, secondo Europol, è necessario sviluppare capacità operative nazionali solide, integrate da strumenti e piattaforme di cooperazione condivisi a livello europeo.

Uno dei temi più dibattuti è stato l'impatto dell'intelligenza artificiale sul panorama della sicurezza. Europol ha evidenziato come tecnologie quali l'IA generativa, i deepfake e gli agenti autonomi stiano ampliando le capacità operative dei gruppi criminali, facilitando attività di frode, cybercriminalità, traffico di migranti e altre forme di criminalità organizzata. Allo stesso tempo, le stesse tecnologie offrono opportunità significative per le forze dell'ordine, consentendo analisi più rapide dei dati, migliori capacità investigative e strumenti avanzati di intelligence.

Nel corso della convention è stato inoltre ribadito il valore della cooperazione tra autorità pubbliche e settore privato. In particolare, è stata evidenziata la necessità di rafforzare la collaborazione tra forze dell'ordine, istituti finanziari, piattaforme digitali e operatori delle telecomunicazioni per contrastare con maggiore efficacia le frodi online e proteggere cittadini e imprese dalle minacce emergenti.

L'incontro conferma il ruolo di Europol quale piattaforma centrale per il coordinamento delle attività di sicurezza nell'Unione europea e testimonia la crescente consapevolezza che le sfide del futuro, sempre più tecnologiche e transnazionali, richiedono risposte comuni, innovative e basate su una cooperazione internazionale sempre più stretta. Per l'Italia, il confronto europeo assume particolare rilevanza anche in relazione al contrasto della criminalità organizzata, del riciclaggio e delle frodi digitali. La crescente integrazione tra strumenti tecnologici, circuiti finanziari e reti criminali transnazionali richiede un rafforzamento della collaborazione tra forze dell'ordine, autorità competenti e operatori privati. In tale contesto, lo scambio informativo e la capacità di individuare tempestivamente comportamenti anomali diventano componenti fondamentali della strategia nazionale ed europea di prevenzione e contrasto.

Europol sollecita un'azione tempestiva per proteggere le criptovalute e i dati sensibili dalle minacce quantistiche

Gloria Lazzaro

Europol ha pubblicato, lo scorso 7 ottobre, due rapporti ufficiali volti a sollecitare i governi, il settore delle criptovalute e le organizzazioni ad una transizione proattiva al fine di anticipare le potenziali future capacità quantistiche di minare la crittografia a protezione dei portafogli di criptovaluta, al fine di evitare la possibilità di decifrare le informazioni sensibili raccolte negli anni precedenti.

Ad oggi risulta difficile prevedere i tempi entro i quali le suddette capacità quantistiche possano svilupparsi, tuttavia risulta essere chiaro l'imminenza di adattare i sistemi e coordinare l'approccio strategico e le azioni di mitigazioni richieste al fine di realizzare soluzioni di crittografia post-quantistica.

Entrambi i rapporti evidenziano la necessità di identificare e prioritizzare le risorse al fine di concretizzare una transizione graduale attraverso aggiornamenti dei wallet, crittografia post-quantistica e coordinamento tra sviluppatori, miner, exchange e utenti da parte dell'industria di settore.

In particolare, il primo rapporto (*"Quantum Computing and Cryptocurrencies"*) sviluppato dal Centro europeo per la criminalità informatica di Europol, esamina le implicazioni per le risorse digitali e prevede le possibilità di minaccia del mondo delle criptovalute da parte dell'informatica quantistica.

Il punto principale di esposizione a tale minaccia viene identificato nella concreta possibilità della tecnologia quantistica di risalire alla chiave privata a partire da quella pubblica esposta, permettendo in tal modo di svuotare i wallet.

Il secondo rapporto (*"Harvest Now, Decrypt Later"*), sviluppato congiuntamente da Europol e dall'Università Carlos III di Madrid (UC3M) come parte del gruppo consultivo Europol EC3 sulla ricerca e lo sviluppo, ha esaminato invece un rischio differente consistente nell'attuale intercettazione, raccolta e archiviazione di comunicazioni riservate, dati aziendali e segreti commerciali cifrati con l'obiettivo di decifrarli successivamente non appena la tecnologia quantistica sarà disponibile.

Entrambi i rapporti, pertanto, raccomandano ai governi e alle organizzazioni di settore di identificare dove viene utilizzata la crittografia, al fine di valutare concretamente: (i) quali risorse destinare a tale minaccia; (ii) quali informazioni necessitano di protezione a lungo termine; (iii) il criterio con cui prioritizzare i sistemi più esposti a futuri attacchi quantistici.

Le azioni di mitigazioni raccomandate da Europol, per neutralizzare l'impatto di tale transizione tecnologica, sono le seguenti:

- identificare l'uso della crittografia, mappando tutti gli algoritmi attualmente implementati nei propri sistemi informatici;
- Rimuovere protocolli obsoleti, sostituendo tempestivamente le difese crittografiche deboli e non aggiornabili;
- Limitare la conservazione dei dati, riducendo al minimo i dati storici archiviati per depotenziare l'efficacia dei futuri attacchi retroattivi;
- Testare soluzioni post-quantistiche, integrando e sperimentando fin da subito soluzioni software agili sul piano crittografico.

UIF: aggiornate le FAQ sulle comunicazioni oggettive e sulla verifica dei dati trasmessi

Silvia Marini

Con il comunicato del 29 settembre 2026, l'Unità di Informazione Finanziaria per l'Italia (UIF) ha richiamato l'attenzione dei soggetti tenuti alle comunicazioni oggettive (OGG) sulla qualità dei dati trasmessi. Le verifiche condotte dall'Unità hanno evidenziato informazioni non conformi alle istruzioni, riconducibili a tre criticità: errata localizzazione geografica delle operazioni, inclusione di movimentazioni di «contante virtuale» e importi anomali, talvolta particolarmente elevati, dovuti a difetti di classificazione o di estrazione. L'aggiornamento delle FAQ, pubblicato nella stessa data, chiarisce i criteri applicativi dell'adempimento previsto dall'art. 47 del d.lgs. 231/2007 e sollecita una revisione mirata dei presidi segnalati.

Il luogo effettivo dell'operazione, non quello di contabilizzazione

La FAQ n. 16 precisa che la localizzazione deve identificare il comune nel quale il contante è materialmente versato o prelevato, e non la sede di contabilizzazione né la filiale presso cui è incardinato il rapporto. Il criterio vale anche per ATM, gestori del contante, casseforti intelligenti (cash-in machine) installate presso la clientela e canali operativi esternalizzati. Il codice ABICAB relativo al luogo di esecuzione è richiesto soltanto per operazioni effettuate presso sportelli o punti operativi bancari o postali; l'ABICAB della filiale del rapporto, quando dovuto, è invece indicato in un campo distinto. Ne deriva l'esigenza di verificare la corretta associazione tra canale utilizzato, punto di effettiva movimentazione e dati acquisiti dai sistemi informativi, soprattutto in presenza di processi accentrati o affidati a terzi.

Contante reale e contante virtuale: la corretta determinazione delle soglie

La FAQ n. 4 ribadisce che rilevano esclusivamente le movimentazioni fisiche di banconote: i passaggi contabili qualificabili come «contante virtuale» non concorrono al calcolo delle soglie. Nell'esempio proposto dalla UIF, un prelevamento contabile di 1.500 euro, associato al contestuale versamento di 1.000 euro su un libretto e all'effettiva consegna di 500 euro, assume rilievo soltanto per questi ultimi 500 euro, inferiori alla soglia minima di 1.000 euro per singola operazione. La distinzione non legittima, tuttavia, compensazioni tra movimenti effettivi di segno opposto: come chiarito dalla FAQ n. 5, prelievi e versamenti in contanti su rapporti del medesimo intestatario si sommano ai fini del raggiungimento della soglia mensile di 10.000 euro.

La selezione delle operazioni richiede inoltre di applicare correttamente i criteri di aggregazione soggettiva. Le FAQ nn. 6 e 7 precisano che un'operazione va comunicata una sola volta, anche se concorre alla soglia per più soggetti, mentre le movimentazioni riconducibili alla stessa persona fisica si cumulano indipendentemente dal ruolo assunto, senza duplicare quelle nelle quali il soggetto rivesta più ruoli. Si tratta di verifiche essenziali per evitare sia omissioni sia sovrarappresentazioni dei flussi.

Qualità del dato, controlli e gestione delle anomalie

Il terzo profilo segnalato riguarda operazioni di importo eccezionalmente elevato, riconducibili non a effettiva operatività in contanti, bensì a errori nella classificazione o nell'estrazione delle informazioni. Il richiamo UIF attribuisce centralità all'affidabilità dell'intera filiera del dato: corretta qualificazione delle causali, selezione delle operazioni, aggregazione degli importi e coerenza del tracciato XML. Sul piano organizzativo, risulta pertanto opportuno introdurre controlli automatici di plausibilità sugli importi, riconciliazioni con le evidenze contabili, verifiche sui criteri di mappatura delle causali e procedure di gestione documentata delle eccezioni.

Anche la regola di troncamento degli importi all'unità di euro prima dell'aggregazione, richiamata dalla FAQ n. 10, richiede coerenza nei motori di calcolo. In questa prospettiva, la funzione antiriciclaggio e le strutture responsabili dei sistemi informativi dovrebbero condividere un processo di data quality che documenti la provenienza del dato, le trasformazioni applicate e gli esiti dei controlli. La disponibilità di evidenze di riconciliazione, test sulle modifiche applicative e tracciatura delle anomalie facilita la verifica dell'effettiva tenuta del processo segnalato.

La verifica non si esaurisce con la trasmissione del file. Le FAQ nn. 31-35 ricordano che la comunicazione si considera acquisita soltanto in presenza dell'«Esito positivo controlli»; scarti e rilievi, anche confermabili, devono essere gestiti entro il termine previsto. Per correggere dati già inviati sono disponibili la sostituzione integrale del flusso mensile (SUBSTITUTION) e la rettifica delle sole osservazioni interessate (INTEGRATION). La scelta deve tenere conto della natura dell'errore e della necessità di preservare completezza e tracciabilità delle informazioni comunicate.



UIF: aggiornate le FAQ sulle comunicazioni oggettive e sulla verifica dei dati trasmessi (*continua*)

La scadenza del 15 marzo 2027 e le priorità di adeguamento

Le modifiche alle procedure segnaletiche devono trovare applicazione a partire dalle comunicazioni relative alle operazioni contabilizzate dal 1° gennaio 2027, da trasmettere entro il 15 marzo 2027. In presenza di gravi impedimenti al rispetto del termine, la UIF invita a darne tempestiva notizia all'indirizzo VIT.Oggettive@bancaditalia.it, indicando le tempistiche previste per superarli. Per le funzioni antiriciclaggio, compliance e controllo interno, il passaggio prioritario è tradurre i chiarimenti in regole operative verificabili: censire le anomalie nei dati trasmessi, valutarne le eventuali esigenze di correzione, aggiornare le logiche applicative e documentare l'efficacia dei controlli. Il messaggio della UIF è netto: l'adempimento non si misura soltanto nella puntualità dell'invio, ma anche nell'accuratezza, completezza e attendibilità del patrimonio informativo acquisito.



Prossime iniziative AIRA e Preferred Partner



ASSOCIAZIONE ITALIANA RESPONSABILI ANTIRICICLAGGIO

Webinar gratuito "A COLLOQUIO CON"

- Riservato ai soli soci di AIRA -

De-risking: opportunità senza abusi. Il KYC "strategico"

Un confronto sui rischi di de-risking, sull'importanza di un approccio proporzionato e sulle modalità con cui il KYC può diventare uno strumento strategico di gestione del rischio.



Data

Venerdì 6 Novembre 2026



Orario

10.00 - 11.00
(durata 1 ora)



Piattaforma

Microsoft Teams

Per iscriversi scrivere a segreteria@iusconsulting.it





Redazione e contatti

REDAZIONE

Ranieri Razzante

Direttore Editoriale

Piercarlo Felice

Responsabile Comunicazione

Riccardo Scardino

Segreteria di Redazione

PRESIDENZA

Via Guidubaldo del Monte 13 – Roma

Tel. 06 8417399

Email: segreteria@iusconsulting.it

© 2026 AIRA – Associazione Italiana Responsabili Antiriciclaggio
Tutti i diritti riservati