

CULTURA PENALE E SPIRITO EUROPEO

SAMUEL BOLIS

Red Flags

Segnalazioni antiriciclaggio in mala fede, vuoti sanzionatori e tutela del soggetto segnalato

Il contributo esamina la disciplina della segnalazione di operazione sospetta (SOS) prevista dal d.lgs. 231/2007, evidenziando l'assenza nell'ordinamento interno di un apparato sanzionatorio dedicato alla segnalazione consapevolmente falsa o gravemente colposa, nonostante la sua espressa previsione nelle direttive unionali. L'analisi ricostruisce il fondamento europeo del canone di buona fede/mala fede, sancito dall'art. 23 della Direttiva (UE) 2019/1937 ed espressamente esteso alla materia antiriciclaggio, per poi verificarne la mancata trasposizione nell'ordinamento interno, nonostante il recepimento della Direttiva (UE) 2024/1640 (sesta direttiva antiriciclaggio) che tale fondamento direttamente richiama. Vengono esaminati i profili di non corretta trasposizione e di sproporzione per difetto rispetto al diritto dell'Unione, il problema di ragionevolezza ex art. 3 Cost., il rischio di uno stimolo strutturale da parte dell'ordinamento alla segnalazione difensiva indiscriminata e le conseguenze, sul piano fiscale, per il soggetto ingiustamente segnalato, anche alla luce della recente giurisprudenza della Corte europea dei diritti dell'uomo in tema di accesso ai dati bancari. Vengono altresì esaminati il deficit di sorveglianza istituzionale sulla banca dati SIVA e l'assenza, per il segnalato, di un diritto di accesso realmente conoscitivo. Lo scritto si chiude con una proposta *de iure condendo* di adeguamento del d.lgs. 231/2007 al modello sanzionatorio del *whistleblowing* generale contemplato dal d.lgs. 24/2023.

Red Flags. AML Reports Filed in Bad Faith, Gaps in Sanctions, and Protection of the Reported Party.

*The paper examines the discipline of suspicious transaction reporting (STR) under Legislative Decree 231/2007, highlighting the absence, within the domestic legal system, of a sanctioning apparatus dedicated to knowingly false or grossly negligent reporting, despite its express provision in EU directives. The analysis reconstructs the European basis of the good faith/bad faith standard, enshrined in Article 23 of Directive (EU) 2019/1937 and expressly extended to anti-money laundering matters, in order to then verify its failure to be transposed into domestic law, notwithstanding the transposition of Directive (EU) 2024/1640 (the Sixth Anti-Money Laundering Directive), which directly refers back to that same basis. The paper examines the profiles of incorrect transposition and of disproportionality by defect with respect to EU law; the issue of reasonableness under Article 3 of the Italian Constitution, the risk of a structural incentive toward indiscriminate defensive reporting, and the consequences – on the tax front – for the person wrongly reported, also in light of recent case law of the European Court of Human Rights on access to banking data. The paper also examines the deficit of institutional oversight over the SIVA database and the absence, for the reported subject, of a genuinely informative right of access. The paper closes with a *de iure condendo* proposal to align Legislative Decree 231/2007 with the sanctioning model of general whistleblowing set out in Legislative Decree 24/2023.*

SOMMARIO: 1. Introduzione: il segnalante tra tutela e responsabilità. – 2. Il canone della buona fede e il *reasonable belief test* nelle fonti convenzionali ed unionali relative alle segnalazioni preventive. – 2.1. Le sanzioni per la segnalazione consapevolmente falsa: l'art. 23 della Direttiva (UE) 2019/1937. – 3. La

normativa europea antiriciclaggio e il richiamo alla Direttiva (UE) 2019/1937. – 3.1. La norma di recepimento interna e l’omessa attuazione della specificità. – 4. Confronto sistematico con la disciplina *whistleblowing* generale. – 4.1. Il regime sanzionatorio del d.lgs. 24/2023. – 4.2. Dolo e colpa grave quale linea comune al diritto interno. – 4.3. Un nodo irrisolto: il momento di cessazione della tutela. – 5. L’irragionevolezza del diverso trattamento: il profilo unionale della proporzionalità. – 5.1. Segue: il profilo costituzionale della ragionevolezza. – 6. I dati UIF: un volume di segnalazioni sproporzionato rispetto agli esiti penali. – 7. Il rischio di uno stimolo statale alla delazione. – 7.1. Segue: la risposta regolamentare all’*over-reporting* nelle nuove Istruzioni UIF. – 7.2. Il nesso tra qualità della collaborazione attiva e iniziative sanzionatorie: le Istruzioni UIF e il perimetro residuo del vuoto normativo. – 8. Le conseguenze per il segnalato: la banca dati SIVA e l’uso dei dati ai fini fiscali. – 8.1. La programmazione delle verifiche fiscali. – 8.2. L’acquisizione autonoma dei conti correnti da parte del Nucleo speciale e la trasmissione ai reparti ordinari. – 8.3. L’aggiornamento del sistema autorizzatorio ordinario: l’utilizzabilità diretta ai fini fiscali dei dati bancari acquisiti in ambito valutario. – 9. I profili di garanzia del canale valutario: la sentenza Ferrieri e Bonassisa c. Italia della Corte EDU e il deficit convenzionale e istituzionale. – 9.1. Il deficit di sorveglianza istituzionale: l’estraneità di SIVA ai sistemi di controllo previsti per l’anagrafe tributaria e per le banche dati di polizia. – 9.2. I diritti del segnalato: il confronto con le banche dati di polizia e l’assenza di un accesso realmente conoscitivo nel canale valutario. – 10. Considerazioni conclusive.

1. *Introduzione: il segnalante tra tutela e responsabilità.* Il tema della responsabilità del segnalante rappresenta, nel diritto delle segnalazioni preventive¹ – categoria che qui si impiega in senso funzionale, per accomunare istituti che, pur distinti sul piano della fonte e del regime applicativo, condividono l’attivazione di una indagine conoscitiva a

¹ Si definisce qui «segnalazione preventiva» l’obbligo, imposto a soggetti professionalmente radicati nel sistema da sorvegliare, di comunicare a un’autorità pubblica fatti sintomatici di un illecito sulla base di uno standard soggettivo di sospetto qualificato (fondati motivi, ragionevoli motivi, *reasonable belief*), a prescindere dall’accertamento giudiziale del fatto. Si tratta di un *genus*, di matrice sostanzialmente unionale, sino ad oggi non elaborato come categoria dogmatica autonoma dalla dottrina italiana, che ne ricomprende almeno quattro sottosistemi: la segnalazione di operazione sospetta antiriciclaggio (art. 35 d.lgs. 231/2007); il *whistleblowing* generale (d.lgs. 24/2023, di recepimento della Direttiva (UE) 2019/1937); la segnalazione di operazioni e ordini sospetti in materia di abusi di mercato, c.d. STOR (art. 16 Regolamento (UE) 596/2014); e la segnalazione di eventi nella sicurezza aerea (Regolamento (UE) 376/2014), quest’ultima ispirata al principio della *just culture*, che esclude la sanzionabilità dell’errore onesto e involontario, ferma restando la responsabilità per dolo o colpa grave. Il denominatore comune non è solo lo *standard* soggettivo del sospetto, ma una più ampia strategia di controllo diffuso: il legislatore unionale distribuisce la vigilanza tra soggetti privati in posizione di percepire per primi l’anomalia, anziché affidarla in via esclusiva ad apparati pubblici centralizzati. La dottrina italiana, tuttavia, tratta i sottosistemi in modo isolato, limitandosi tutt’al più a confronti a coppie; sul punto si veda BORRELLI, *Segnalazione di operazioni sospette in materia di antiriciclaggio e segnalazione di condotte illecite (whistleblowing): modelli a confronto*, in Id., *Presidi, strumenti e modelli di prevenzione per la tutela della legalità nell’economia: una prospettiva integrata*, Quaderni dell’antiriciclaggio – Analisi e studi, UIF – Banca d’Italia, 2025, 30, 57 ss.

prescindere dall'accertamento giudiziale del fatto e l'ancoraggio ad uno *standard* soggettivo di sospetto qualificato, quali la segnalazione di operazione sospetta ex art. 35 d.lgs. 231/2007 e il *whistleblowing* ex d.lgs. 24/2023 – il controbilanciamento di un istituto che dottrina e legislatore hanno per lungo tempo osservato, quasi per pudore, dal solo versante della tutela: un rovescio della medaglia rimasto, sinora, praticamente quasi del tutto inesplorato². Il legislatore italiano si è premurato di costruire, su impulso unionale, un canale riservato attraverso cui un soggetto porta a conoscenza dell'autorità competente un sospetto di illecito, sollevandolo da responsabilità nella misura in cui abbia agito in buona fede. Ciò che in questa sede si intende per l'appunto verificare è se, e in quale misura, l'ordinamento interno abbia recepito anche la componente speculare di tale bilanciamento – la responsabilizzazione del segnalante che abbia agito con dolo o mala fede, espressamente contemplata nella normativa europea – nel peculiare ambito della segnalazione di operazione sospetta (SOS) ai fini antiriciclaggio disciplinata dal d.lgs. 231/2007 e se l'eventuale lacuna sia compatibile con i principi del diritto dell'Unione europea e con il canone di ragionevolezza di cui all'art. 3 Cost.

2. *Il canone della buona fede e il reasonable belief test nelle fonti convenzionali ed unionali relative alle segnalazioni preventive. I c.d. red flags* – gli indicatori di anomalia elaborati dalla prassi e dalla regolamentazione antiriciclaggio per orientare l'obbligato nell'individuazione di elementi sintomatici di un possibile fenomeno di riciclaggio o di finanziamento del terrorismo – costituiscono il presupposto fattuale di ogni segnalazione preventiva. Il sistema delle segnalazioni preventive è imperniato, a valle di tale processo di individuazione, su di un canone di buona fede³ secondo il quale

² Il tema della tutela del segnalato è quasi del tutto assente nella dottrina italiana anche se taluno ha modo di osservare, con riferimento alla tutela delle persone giuridiche in materia di *whistleblowing* di cui si dirà esaustivamente *infra*, che «occorre che il legislatore tenga in conto i diritti del segnalato oltre che la posizione dell'ente chiamato in causa, anche ma non solo a fronte di segnalazioni che potrebbero dimostrarsi non fondate, dovendosi dunque evitare che esse mettano a repentaglio la reputazione dell'ente»; così in PARISI, *La funzione del whistleblowing nel diritto internazionale ed europeo*, in *Lavoro Diritti Europa*, 2 luglio 2020.

³ Sul progressivo affrancamento della clausola di buona fede dai confini tradizionali civilistici e sul suo

devono sussistere fondati motivi in forza dei quali il segnalante possa ritenere veri i fatti riportati alla luce delle circostanze e delle informazioni disponibili al momento della segnalazione: tale standard – c.d. *reasonable grounds to believe*, di natura oggettiva in quanto ancorato alla ragionevolezza del convincimento e non alla mera convinzione soggettiva del segnalante – opera quale salvaguardia contro le segnalazioni malevole, frivole o abusive, senza tuttavia penalizzare l'errore incolpevole⁴ dovuto alla naturale condizione di asimmetria informativa in cui versa il segnalante che segnala fatti dei quali ha percezione.

Tale *standard* non nasce con la Direttiva (UE) 2019/1937, ma affonda le proprie radici in una risalente tradizione convenzionale europea, che già subordinava la tutela del segnalante alla duplice condizione della buona fede e del ragionevole sospetto⁵.

2.1. *Le sanzioni per la segnalazione consapevolmente falsa: l'art. 23 della Direttiva (UE) 2019/1937.* A questo canone di matrice generale, comune all'intero diritto europeo delle segnalazioni, si affianca un presidio più specifico, dedicato al versante opposto della tutela: quello della segnalazione consapevolmente falsa.

inquadramento nel dovere solidaristico di cui all'art. 2 Cost., anche con riguardo al diritto penale, si rinvia a GRASSO-RIPEPI, *Buona fede e diritto penale: un'indagine di sistema*, in *Ratio Iuris*, 10 luglio 2024, spec. §§ 1 e 5; nonché, in prospettiva storico-sistemica, PIVETTI, *La Buona Fede tra valutazione della condotta e attuazione della norma giuridica*, in *La Magistratura*, 3 febbraio 2023.

⁴ Sul *reasonable belief test* quale *standard* cardine del sistema di tutela delineato dalla Direttiva (UE) 2019/1937, si veda MARENGHI, *Il c.d. Qatargate e le nuove norme del Parlamento europeo in materia di whistleblowing: troppo tardi e troppo poco?*, in *Eurojus*, 2024, 3, 116 ss. e spec. 120, ove si sottolinea come il legislatore europeo si sia «volutamente» discostato dal concetto di buona fede, trasfondendo nell'art. 6, § 1, lett. a), della direttiva il solo criterio oggettivo dei «fondati motivi di ritenere» veri i fatti segnalati.

⁵ Si veda la Convenzione civile sulla corruzione, adottata dal Consiglio d'Europa a Strasburgo il 4 novembre 1999, ratificata in Italia con L. 112/2012, ed in particolare il suo art. 9: «Ciascuna Parte prevede nel suo diritto interno un'adeguata tutela contro qualsiasi sanzione ingiustificata nei confronti di dipendenti i quali, in buona fede e sulla base di ragionevoli sospetti, denunciano fatti di corruzione alle persone o autorità responsabili». Il medesimo *standard* della buona fede e del ragionevole sospetto è ripreso dall'art. 33 della Convenzione delle Nazioni unite contro la corruzione, adottata a Merida nel 2003, che tuttavia configura la tutela come mera facoltà, non come obbligo («each State Party shall consider», nel testo in inglese), per gli Stati aderenti; per un commento dell'art. 33 si veda ROSE-KUBICIEL-LANDWEHR, *The United Nations Convention against corruption. A Commentary*, Oxford, 2019, 339 ss.

A questi principi se ne affianca un secondo, ad esso complementare: l'art. 23 della Direttiva (UE) 2019/1937, infatti, introduce un obbligo per gli Stati membri di prevedere sanzioni effettive, proporzionate e dissuasive, unite a misure di risarcimento del danno, nei confronti del segnalante che abbia consapevolmente riportato o pubblicamente divulgato informazioni false⁶. Si tratta di una norma di armonizzazione minima, non derogabile *in peius*, che gli Stati membri sono tenuti a recepire in ogni settore materiale ricompreso nell'ambito applicativo della Direttiva – tra cui, per quanto qui rileva, la prevenzione del riciclaggio e del finanziamento del terrorismo, espressamente enumerata quale segmento dei servizi finanziari⁷.

Come noto, il sistema costruito dalla Direttiva (UE) 2019/1937 riposa su un equilibrio a doppio binario: da un lato, la protezione del segnalante che agisca in buona fede; dall'altro, l'espressa esclusione di tale protezione – e la previsione di conseguenze sanzionatorie – per chi segnali consapevolmente il falso⁸.

3. *La normativa europea antiriciclaggio e il richiamo alla Direttiva (UE) 2019/1937.* Il legame tra la disciplina antiriciclaggio e la Direttiva (UE) 2019/1937, invero, non è di semplice prossimità sistematica, ma di espresso richiamo normativo. La riforma del pacchetto antiriciclaggio del 2024 ha reso tale legame ancora più diretto: la Direttiva (UE) 2024/1640 – sesta direttiva antiriciclaggio, che ha abrogato e sostituito la Direttiva (UE) 2015/849 – reca nel proprio titolo addirittura la dicitura che ne segnala la funzione

⁶ Direttiva (UE) 2019/1937, art. 23: gli Stati membri prevedono sanzioni effettive, proporzionate e dissuasive nei confronti di chi ostacoli la segnalazione, si vendichi o violi la riservatezza del segnalante (§ 1); analoghe sanzioni, unite a misure di risarcimento del danno, sono previste nei confronti del segnalante che abbia consapevolmente riportato o pubblicamente divulgato informazioni false (§ 2).

⁷ Direttiva (UE) 2019/1937, art. 2, § 1, lett. a), punto (ii), che ricomprende nell'ambito applicativo della Direttiva i servizi, prodotti e mercati finanziari e la prevenzione del riciclaggio e del finanziamento del terrorismo.

⁸ Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione; si veda, in particolare, il Considerando n. 32: il segnalante deve avere fondati motivi per ritenere veri, alla luce delle circostanze e delle informazioni disponibili al momento della segnalazione, i fatti riportati; il requisito è qualificato come salvaguardia essenziale contro le segnalazioni dolose e futili o infondate, mentre resta protetto l'errore incolpevole.

modificativa della Direttiva (UE) 2019/1937⁹, a conferma della scelta del legislatore unionale di innestare il *whistleblowing* antiriciclaggio nel sistema generale del 2019 anziché duplicarlo in un regime autonomo. Inoltre, l'art. 60 della Direttiva (UE) 2024/1640 prevede espressamente l'applicazione della Direttiva (UE) 2019/1937 all'intera disciplina complessiva delle segnalazioni di violazioni antiriciclaggio. Sul fronte interno, tuttavia, il d.lgs. 122/2026 ha recepito soltanto gli artt. 11, 12, 13 e 15 della Direttiva (UE) 2024/1640, relativi al registro dei titolari effettivi, senza toccare l'art. 60 né, più in generale, l'intero atto: la trasposizione della disciplina *whistleblowing* in materia antiriciclaggio resta, allo stato, priva di un veicolo normativo interno dedicato; va peraltro precisato che il termine generale di recepimento della Direttiva (UE) 2024/1640 – cui è soggetto, tra l'altro, l'art. 60 – scade il 10 luglio 2027, e non risulta dunque, a oggi, ancora spirato¹⁰.

⁹ La Direttiva (UE) 2024/1640 reca già nel suo stesso titolo la dicitura «amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849». Il fondamento di tale scelta è esplicitato dal Considerando 110 della medesima direttiva, ove si chiarisce che la Direttiva (UE) 2019/1937 si applicava già, in forza della Parte II del proprio allegato, alla segnalazione delle violazioni della previgente Direttiva (UE) 2015/849 e alla tutela dei relativi segnalanti, e che tale rinvio, a seguito dell'abrogazione di quest'ultima, deve ora intendersi riferito alla Direttiva (UE) 2024/1640; il medesimo Considerando precisa tuttavia che restano necessarie regole di dettaglio complementari alla disciplina generale del 2019, in particolare quanto all'obbligo di istituire canali di segnalazione interni e all'individuazione delle autorità competenti a riceverle. Per una compiuta ricostruzione dell'evoluzione della normativa antiriciclaggio in ambito europeo si rinvia a RICCARDI, *Il Single Rulebook dell'Unione europea in materia antiriciclaggio e contrasto al finanziamento del terrorismo: dall'armonizzazione normativa alla governance sovranazionale ai sensi dell'art. 114 TFUE*, in *Eurojus*, 2026, 3. A ulteriore conferma della scelta sistematica del legislatore unionale, la medesima estensione della Direttiva (UE) 2019/1937 alla materia antiriciclaggio è ribadita, con effetto diretto e non subordinato a recepimento, anche dall'art. 14 del Regolamento (UE) 2024/1624 e dall'art. 90 del Regolamento (UE) 2024/1620, istitutivo dell'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (AMLA), che assegna a quest'ultima il compito di predisporre appositi canali di segnalazione con estensione della relativa tutela alle persone segnalanti. Sul tema si veda BORRELLO, *Segnalazione di operazioni sospette*, cit., 74, n. 31.

¹⁰ Cfr. d.lgs. 10 giugno 2026, n. 122, recante «Recepimento degli articoli 11, 12, 13 e 15 della direttiva (UE) 2024/1640 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica la direttiva (UE) 2019/1937, e modifica e abroga la direttiva (UE) 2015/849», in G.U., Serie generale, n. 156 dell'8 luglio 2026. Il recepimento della Direttiva (UE) 2024/1640 è scaglionato: l'art. 74 andava recepito entro il 10 luglio 2025 (termine spirato, con conseguente avvio di procedura d'infrazione, poi sanato dal d.lgs. 210/2025); gli artt. 11, 12, 13 e 15 entro il 10 luglio 2026 (termine anch'esso spirato, e recepito, sia pur a ridosso della scadenza, dal citato d.lgs. 122/2026); l'art. 18 entro il 10 luglio 2029; tutte le restanti disposizioni – ivi compreso l'art. 60 – entro il termine generale del 10 luglio 2027, non ancora spirato. In realtà, l'impianto della Direttiva (UE) 2019/1937 si applicava già, come ricostruito nella nota precedente, alla segnalazione delle violazioni della previgente Direttiva (UE) 2015/849 in materia antiriciclaggio.

Ne discende che il segnalante antiriciclaggio europeo non gode di uno statuto di maggior favore rispetto al *whistleblower* generale: la sua posizione è, o dovrebbe essere, integralmente governata dal medesimo bilanciamento tra protezione della buona fede e sanzione della mala fede.

3.1. *La norma di recepimento interna e l'omessa attuazione della specificità.*
Il d.lgs. 231/2007, per vero, disciplina la posizione del segnalante SOS secondo un modello strutturalmente diverso da quello unionale sopra ricostruito. L'art. 35 (già art. 41, nella numerazione antecedente alla riforma del 2017) del decreto antiriciclaggio impone l'obbligo di segnalazione quando il soggetto obbligato «sa, sospetta o ha motivi ragionevoli per sospettare» che siano in corso o siano state compiute operazioni di riciclaggio o di finanziamento del terrorismo; il correlato regime di tutela è imperniato su una clausola di esenzione da responsabilità (*safe harbour*), per cui le segnalazioni effettuate in buona fede e per le finalità di legge non comportano responsabilità di alcun tipo, anche quando il sospetto si riveli infondato¹¹. Sul piano comparatistico, merita evidenziare come un ordinamento come quello tedesco, per contro, condiziona espressamente l'esenzione da responsabilità all'assenza di dolo o colpa grave nella segnalazione, offrendo un modello comparatistico di quella clausola di responsabilizzazione che il legislatore italiano non ha ancora introdotto¹². Significativo, in tal senso, è che lo stesso

¹¹ L'art. 35 del d.lgs. 21 novembre 2007, n. 231, già art. 41 nella numerazione antecedente alla riforma di cui al d.lgs. 25 maggio 2017, n. 90, rubricato obbligo di segnalazione delle operazioni sospette prevede una clausola di esenzione da responsabilità per le segnalazioni effettuate in buona fede e per le finalità di legge, che esclude qualsiasi conseguenza anche quando il sospetto si riveli infondato. Sul piano amministrativo, tale lettura è confermata da Comando generale della Guardia di finanza, Circolare n. 83607/2012, rubricata *Attività della Guardia di Finanza a tutela del mercato dei capitali*, vol. I, 75, ove si precisa che la segnalazione, se effettuata «per le finalità previste dalla legislazione antiriciclaggio ed in buona fede, non comporta responsabilità di alcun tipo, non costituisce violazione agli obblighi di segretezza, del segreto professionale o di eventuali restrizioni alla comunicazione di informazioni imposte in sede contrattuale o da disposizioni legislative».

¹² Si veda § 48, co. 1, Geldwäschegesetz (la legge antiriciclaggio tedesca) in tema di esenzione di responsabilità: «Wer Sachverhalte nach § 43 meldet [...] darf deshalb nicht nach zivilrechtlichen oder strafrechtlichen Vorschriften verantwortlich gemacht oder disziplinarrechtlich verfolgt werden, es sei denn, die Meldung [...] ist vorsätzlich oder grob fahrlässig unwahr erstattet worden» (chi effettua la segnalazione non risponde civilmente né penalmente, salvo che essa sia stata resa con dolo o colpa grave); per un commento allo specifico articolo si rinvia a ZENTES-GLAAB, *Geldwäschegesetz (GwG)*, Francoforte, 2025, 1352 ss. A differenza dell'art. 35 d.lgs. 231/2007, la clausola tedesca di esenzione da responsabi-

legislatore delegato abbia accolto il criterio oggettivo del «ragionevole convincimento» nella disciplina generale del *whistleblowing*, discostandosene invece nella specifica materia antiriciclaggio: l'art. 16, co. 1 del d.lgs. 24/2023 subordina infatti la protezione del segnalante al fondato motivo di ritenere vere le informazioni segnalate, in piena continuità con l'art. 6 della direttiva, mentre l'art. 35 d.lgs. 231/2007 resta ancorato al canone soggettivo della buona fede¹³. A questa clausola si affianca un regime di riservatezza a protezione del segnalante e del processo di analisi finanziaria – *i.e.*: tutela dell'identità, divieto di comunicazione, disciplina dell'analisi e del flusso di ritorno delle informazioni – che non trova simmetria in alcuna analoga garanzia procedurale a favore del segnalato¹⁴.

Senonché, questa impostazione – di per sé coerente con il principio di incentivazione della segnalazione difensiva, di cui si dirà più avanti – si arresta al solo versante della tutela del segnalante in buona fede. Il legislatore delegato non ha introdotto, in modo simmetrico, alcuna disposizione speciale che preveda la perdita espressa delle garanzie di riservatezza per il segnalante che abbia agito con dolo o mala fede, una sanzione amministrativa o disciplinare dedicata alla segnalazione consapevolmente falsa, né un meccanismo di risarcimento del danno distinto dalle ordinarie azioni di

tà è dunque geneticamente condizionata all'assenza di dolo o colpa grave nella segnalazione, anticipando così, nel diritto interno tedesco, la medesima soglia soggettiva che l'art. 21 d.lgs. 24/2023 ha successivamente introdotto, per il solo *whistleblowing* generale, anche nel nostro ordinamento (v. *infra*, § 4.2).

¹³ Sul passaggio, operato dalla Direttiva (UE) 2019/1937, dal canone soggettivo della buona fede allo *standard* oggettivo della ragionevolezza, e sulla relativa attuazione nell'art. 16, co. 1 del d.lgs. 24/2023, si rinvia a COSSU-VALLI, *Il whistleblowing: dalla Direttiva 1937/2019 al Decreto Legislativo 24/2023*, in *federalismi.it*, 2023, 19, 164, spec. § 1.3, e 174-175, spec. § 2.8. Le Autrici osservano come la direttiva sposti l'attenzione «sulla sussistenza dell'elemento obbiettivo della ragionevolezza, anziché su quello soggettivo della buona fede» e come tale *standard* sia stato pienamente recepito, per il *whistleblowing* generale, dall'art. 16, co. 1 del d.lgs. 24/2023: un'ulteriore riprova, complementare a quella già emersa sul piano sanzionatorio, di come lo stesso legislatore nazionale abbia allineato la disciplina generale del *whistleblowing* allo *standard* unionale, lasciando indietro, sotto questo ulteriore profilo, la disciplina della SOS antiriciclaggio.

¹⁴ Si vedano gli articoli del Titolo II, Capo III, del d.lgs. 231/2007: l'art. 38 impone la tutela della riservatezza dell'identità del segnalante e del contenuto della segnalazione; l'art. 39 vieta al segnalante e a terzi di comunicare l'avvenuta segnalazione o il suo esito; l'art. 40 disciplina l'analisi della segnalazione da parte della UIF; l'art. 41 il flusso di ritorno delle informazioni verso i segnalanti. Il regime di riservatezza, così strutturato a tutela del segnalante e del sistema di analisi finanziaria, non ha un contrappeso equivalente a tutela del segnalato, che non è messo a conoscenza né della segnalazione né, se non indirettamente, dei suoi sviluppi.

diritto comune. L'unico argine rimane, per implicito, il venir meno dell'esimente di buona fede, con conseguente riespansione della responsabilità comune per calunnia o diffamazione: una tutela indiretta e residuale, che replica il diritto penale comune senza dare attuazione all'obbligo specifico imposto dall'art. 23, § 2 della Direttiva (UE) 2019/1937 nella sua declinazione antiriciclaggio. Come spesso accade alle stratificazioni normative cresciute per successivi innesti anziché per organica ideazione, anche il d.lgs. 231/2007 – pur successivamente novellato in più occasioni, da ultimo per adeguarsi al pacchetto AML 2024 – non risulta avere colmato questa lacuna di coordinamento con la disciplina *whistleblowing* generale. Il rilievo si inserisce, del resto, in un più generale giudizio critico sulla qualità del recepimento italiano della Direttiva (UE) 2019/1937, di cui anche il Servizio ricerche del Parlamento europeo ha dato atto¹⁵.

Il rilievo trova, del resto, una conferma indipendente e convergente in dottrina istituzionale: proprio con riferimento all'art. 48 d.lgs. 231/2007, si è osservato come tale norma contempli il solo *whistleblowing* «interno», disattendendo così le indicazioni dell'art. 61 della Direttiva (UE) 2015/849, che raccomandava l'adozione di «meccanismi efficaci e affidabili per incoraggiare la segnalazione» – a differenza di quanto il legislatore ha invece previsto, con un doppio canale interno ed esterno, per il settore bancario e finanziario (artt. 52-bis e 52-ter. TUB; artt. 4-*undecies* e 4-*duodecies* TUF)¹⁶. Il dato conferma, su un piano distinto ma sistematicamente convergente con quello qui esaminato, la tendenza del legislatore italiano a un recepimento incompleto della disciplina *whistleblowing* in materia antiriciclaggio rispetto agli *standard* unionali.

4. *Confronto sistematico con la disciplina whistleblowing generale.* Si è già detto che nel sistema antiriciclaggio esiste una sorta di incentivazione alla

¹⁵ Si veda il documento dell'*European Parliamentary Research Service (EPRS)*, DEL MONTE-FAUCHEUX, *Protecting whistle-blowers in the EU*, Briefing PE 747.103, settembre 2024, 11, ove si dà atto del rilievo di *Transparency International* secondo cui la legge italiana di recepimento della Direttiva (UE) 2019/1937 limiterebbe, in alcuni profili, la tutela riconosciuta ai segnalanti che si rivolgano al canale esterno rispetto alla disciplina previgente.

¹⁶ Sul tema si veda BORRELLO, *Segnalazione di operazioni sospette*, cit., § 4, 69.

segnalazione difensiva dovuta ad una asimmetria sanzionatoria: ciò è rilevabile nella unidirezionalità del sistema sanzionatorio antiriciclaggio secondo cui mentre l'omessa segnalazione è presidiata da sanzioni amministrative pecuniarie, nulla è previsto sul versante opposto della segnalazione consapevolmente falsa o gravemente colposa¹⁷.

Il raffronto con il d.lgs. 24/2023 – che ha recepito proprio la Direttiva (UE) 2019/1937 per le materie diverse dall'antiriciclaggio – rende ancora più evidente l'asimmetria ormai presente tra differenti discipline inerenti alle segnalazioni preventive presenti nell'ordinamento interno.

4.1. *Il regime sanzionatorio del d.lgs. 24/2023.* L'art. 21, co. 1, lett. c) del decreto prevede che l'ANAC possa irrogare una sanzione amministrativa pecuniaria nei confronti del segnalante quando ne sia accertata, anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o calunnia commessi con la segnalazione o la denuncia, ovvero, in alternativa, la responsabilità civile per lo stesso titolo nei casi di dolo o colpa grave, salvo che il segnalante sia già stato condannato, anche in primo grado, per i medesimi reati; la medesima condotta comporta, cumulativamente, l'irrogazione di una sanzione disciplinare e la perdita delle tutele di riservatezza altrimenti garantite¹⁸. Il sistema *whistleblowing* generale presenta dunque tre livelli di reazione – la sanzione amministrativa dedicata, la sanzione disciplinare interna che gli enti dotati di modello organizzativo ex d.lgs. 231/2001 sono tenuti a codificare, e la caducazione espressa delle garanzie di riservatezza – tutti assenti, o solo indirettamente rinvenibili, nella disciplina SOS. Il descritto mutamento di paradigma – dalla segnalazione

¹⁷ Si veda sempre BORRELLO, *Segnalazione di operazioni sospette, cit.*, § 5, 70, ove si osserva come «un elemento di forte differenziazione tra i due istituti attiene all'obbligatorietà che caratterizza le segnalazioni di operazioni sospette, assistita da sanzioni amministrative pecuniarie che colpiscono l'omessa segnalazione, rispetto alla spontaneità e volontarietà che caratterizza le segnalazioni di whistleblowing».

¹⁸ L'art. 21, co. 1, lett. c) del d.lgs. 24/2023 prevede una sanzione amministrativa pecuniaria da 500 a 2.500 euro irrogabile dall'ANAC nel caso di cui all'art. 16, co. 3 – accertamento, anche con sentenza di primo grado, della responsabilità penale del segnalante per diffamazione o calunnia commesse con la segnalazione o la denuncia, ovvero della sua responsabilità civile per lo stesso titolo nei casi di dolo o colpa grave – salvo che il segnalante sia già stato condannato, anche in primo grado, per i medesimi reati; la medesima condotta comporta, ai sensi dell'art. 16, co. 3, la perdita delle tutele previste dal Capo III del decreto (tra cui la riservatezza ex art. 12) e l'irrogazione di una sanzione disciplinare.

quale atto di sacrificio personale all'esercizio di un diritto presidiato da un apparato di garanzie – trova oggi conferma nella più recente dottrina che ha commentato sistematicamente l'impianto del d.lgs. 24/2023¹⁹. La stessa ANAC, peraltro, ne ha di recente rimarcato i limiti applicativi, segnalando l'inadeguatezza del tetto sanzionatorio previsto dal decreto e suggerendone una revisione in ragione del contenuto poco dissuasivo, sia in assoluto sia rispetto alle previsioni sanzionatorie di altri settori dell'ordinamento: una notazione che, *mutatis mutandis*, rafforza il rilievo per cui il regime SOS, privo persino di una sanzione dedicata, si colloca su un piano di tutela ancora più arretrato²⁰.

4.2. *Dolo e colpa grave quale linea comune al diritto interno.* La soglia del dolo o della colpa grave²¹ adottata dall'art. 21 d.lgs. 24/2023, a ben vedere, non è un *unicum* sperimentale, ma riprende un criterio già collaudato dalla giurisprudenza di legittimità in tema di responsabilità del lavoratore che segnali (anche fuori dallo schema *whistleblowing* in senso stretto) un illecito del datore di lavoro: la responsabilità disciplinare del dipendente sussiste, secondo un orientamento costante, solo quando sia dimostrata la consapevolezza dell'insussistenza del fatto denunciato, non già il semplice errore di valutazione²². Si tratta, in altri termini, di un principio generale

¹⁹ Per un commento sistematico all'impianto del d.lgs. 24/2023 qui posto a termine di paragone – ivi compreso il mutamento di paradigma per cui la segnalazione non è più concepita come atto di sacrificio personale ma come esercizio di un diritto assistito da un apparato di garanzie – si veda il volume CANTONE-PARISI-TAMBASCO, *Whistleblowing: Commento sistematico alla disciplina del d.lgs. n. 24/2023*, Milano, 2025; per un approfondimento sulla derivazione europea dell'istituto si rimanda a MASIERO, *La disciplina del whistleblowing alla luce della direttiva 2019/1937/UE. Tra prevenzione dei fenomeni corruttivi e tutela del denunciante*, in *Arch. pen. web*, 8 giugno 2020.

²⁰ Si veda la Relazione illustrativa alle Linee guida in materia di *whistleblowing* sui canali interni di segnalazione, ANAC, Delibera n. 478 del 26 novembre 2025, 23, ove si suggerisce una riflessione sulla revisione del tetto massimo della sanzione amministrativa, attese il contenuto peso dissuasivo sia in assoluto, sia rispetto alle previsioni sanzionatorie di altri settori dell'ordinamento.

²¹ In questa sede non è possibile soffermarsi sul complesso tema del dolo e della colpa grave quali autonome categorie dogmatiche, per cui ci si limita a rinviare, per una trattazione monografica, a DEMURO, *Il dolo. Svolgimento storico del concetto*, Milano, 2007, vol. I, e *Il dolo. L'accertamento*, Milano, 2010, vol. II; nonché, sulla nozione di colpa grave quale autonoma soglia di responsabilità, a CASTRONUOVO, *La colpa «penale»: misura soggettiva e colpa grave*, in *Riv. it. dir. proc. pen.*, 2013, 1723 ss.

²² Sul principio per cui, al di fuori dello schema *whistleblowing* propriamente detto, la responsabilità del lavoratore che segnali un illecito datoriale sussiste solo in presenza di dolo o consapevolezza dell'insussistenza del fatto denunciato, si è espressa la Suprema corte, in ultimo in Cass. Sez. lav., 21 di-

dell'ordinamento interno in tema di responsabilità del segnalante – che rende ancor più singolare la sua mancata trasposizione, sia pure in forma di sanzione amministrativa dedicata, nella disciplina antiriciclaggio, che pure condivide la medesima *ratio* di fondo.

Il principio ha trovato di recente una conferma diretta e particolarmente autorevole all'interno dello stesso schema *whistleblowing*, con una pronuncia della Cassazione che ha sintetizzato in termini pressoché identici lo standard operante tanto nell'art. 54-*bis* quanto nell'art. 16, co. 3 d.lgs. 24/2023, riscontrandone altresì la piena corrispondenza con l'analoga clausola di esclusione prevista dall'art. 26, co. 3-*bis* del Codice delle pari opportunità (d.lgs. 198/2006) per le ritorsioni conseguenti a reclami o denunce di discriminazioni di genere²³: la tutela del segnalante viene meno solo in presenza di una condanna penale, anche di primo grado, per calunnia o diffamazione, ovvero di un'infondatezza della denuncia riconducibile a dolo o colpa grave, da apprezzare secondo la situazione esistente *ex ante* e assicurando una ragionevole tolleranza, a favore del denunciante, rispetto a profili minori rimasti in ipotesi non suffragati; diversamente, l'amministrazione datrice di lavoro non può legittimamente procedere a contestazione disciplinare nei confronti del segnalante, pena la vanificazione dell'intero assetto della tutela. Anche questa conferma giurisprudenziale, sia pure maturata al di fuori del perimetro specifico dell'antiriciclaggio, rafforza l'idea di uno standard ormai consolidato nel diritto interno, di cui la disciplina della SOS resta l'unica, ingiustificata eccezione.

cembre 2024, n. 33746. Si tratta di uno *standard* coerente con la clausola del *reasonable belief* vista in precedenza, che a livello di diritto dell'Unione esclude parimenti la responsabilità per l'errore incolpevole; la costante applicazione di tale criterio nella giurisprudenza di legittimità conferma la sua natura di principio generale dell'ordinamento interno in tema di responsabilità del segnalante, che la disciplina antiriciclaggio non ha tuttavia mai declinato in un apparato sanzionatorio dedicato.

²³ Si veda Cass. Sez. lav., 21 dicembre 2024, n. 33746, *cit.*, §§ 4.2-4.3, ove si ricostruisce il quadro normativo comune all'art. 54-*bis*, co. 9 d.lgs. 165/2001, all'art. 16, co. 3 d.lgs. 24/2023 e all'art. 26, co. 3-*bis* d.lgs. 198/2006, e si precisa che «l'insieme delle norme porta a concludere che, quanto meno rispetto a segnalazioni o reclami in ambito e nel corso di rapporti di lavoro, solo l'esistenza della condanna penale, anche in primo grado, o l'accertamento di un'infondatezza destinata a risalire a dolo o colpa grave siano circostanze che fanno recedere le regole di tutela»; § 5.2, ove si precisa che, al di fuori di tali ipotesi, «fatto costitutivo della legittima reazione contro il denunciante non è la denuncia in sé» e che una contestazione disciplinare anticipata rispetto all'accertamento di dolo o colpa grave comporterebbe che «ne verrebbe sostanzialmente vanificato l'intero assetto della tutela del c.d. whistleblowing»; § 9, primo principio di diritto enunciato ai sensi dell'art. 384 c.p.c.

4.3. *Un nodo irrisolto: il momento di cessazione della tutela.* Ad ogni modo, anche a voler prescindere dall'assenza di una sanzione dedicata, resta aperto – nella stessa disciplina *whistleblowing* generale, e *a fortiori* in quella antiriciclaggio priva di qualunque riferimento sul punto – il problema del momento in cui debba considerarsi cessata la tutela del segnalante in mala fede: se già con una pronuncia sfavorevole di primo grado, come inizialmente ritenuto in sede di prassi amministrativa, o solo con il passaggio in giudicato della sentenza di condanna, soluzione preferibile in nome del principio del giusto processo²⁴. Il legislatore del 2023 ha optato per una soluzione intermedia, ancorando la sanzione amministrativa al solo accertamento, anche non definitivo, della responsabilità: una scelta che il d.lgs. 231/2007 non riproduce, semplicemente perché non prevede alcuna sanzione dedicata cui applicarla. Nello stesso senso si sono espresse le Linee guida dell'ANAC, che precisano come il segnalante riacquisti il diritto alla protezione, ove la sentenza di condanna sia riformata in senso in suo favore nei successivi gradi di giudizio, solo a seguito del passaggio in giudicato della relativa pronuncia²⁵.

5. *L'irragionevolezza del diverso trattamento: il profilo unionale della proporzionalità.* Ebbene, sotto il profilo del diritto dell'Unione, l'assenza di un regime sanzionatorio dedicato per la SOS in mala fede espone il sistema di recepimento italiano a un duplice ordine di censure. In primo luogo, un

²⁴ Sul dibattito circa il momento in cui debba ritenersi cessata la tutela del segnalante che abbia riportato il falso, l'ANAC ha inizialmente ritenuto sufficiente una pronuncia sfavorevole di primo grado (ANAC, Determinazione n. 6 del 28 aprile 2015, *Linee guida in materia di tutela del dipendente pubblico che segnala illeciti*, punto 6); vi è da osservare, tuttavia, come tale soluzione mal si concili con la presunzione di non colpevolezza e con il principio del giusto processo regolato dall'art. 111 Cost., preferendosi la tesi per cui la tutela dovrebbe venir meno solo al passaggio in giudicato della pronuncia di condanna. Il legislatore del 2023 ha risolto la questione in senso intermedio, ancorando all'art. 21, co. 1, lett. c) d.lgs. 24/2023 la sanzione amministrativa al solo accertamento, anche di primo grado, della responsabilità civile o penale del segnalante.

²⁵ Si veda il documento ANAC, Delibera n. 311 del 12 luglio 2023, *Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*, § 4.3 (Limitazioni di responsabilità per chi segnala, denuncia o effettua divulgazioni pubbliche), 68, ove si precisa che la tutela, venuta meno a seguito di sentenza di condanna per i reati di calunnia o diffamazione (o di accertamento della corrispondente responsabilità civile per dolo o colpa grave), è recuperata solo con il passaggio in giudicato della pronuncia che, nei successivi gradi di giudizio, riformi in senso favorevole la condanna.

profilo di non corretta trasposizione della norma unionale: l'art. 23, § 2 della Direttiva (UE) 2019/1937 impone un obbligo di risultato – *i.e.* l'introduzione di sanzioni effettive, proporzionate e dissuasive, unite a misure di risarcimento – che il legislatore interno ha attuato in modo compiuto solo per il segmento *whistleblowing* generale, non per quello antiriciclaggio, pur essendo quest'ultimo espressamente ricompreso nell'ambito applicativo della Direttiva stessa. Il rilievo trova conferma, su scala europea, nella valutazione della Commissione, che ha censurato, tra i profili di recepimento più critici in generale, proprio le sanzioni previste dagli Stati membri per le segnalazioni consapevolmente false, in molti casi ritenute prive di reale efficacia dissuasiva²⁶.

In secondo luogo, un profilo di sproporzione per difetto, speculare a quello – più noto – di sproporzione per eccesso: se il principio di proporzionalità limita l'intervento sanzionatorio a quanto necessario, esso impone parimenti che la tutela di un interesse riconosciuto meritevole – qui, la posizione del terzo ingiustamente segnalato – non sia lasciata priva di qualunque presidio specifico, quando lo stesso legislatore unionale ne ha imposto uno²⁷.

Con la pronuncia del caso Drex²⁸, la Corte ha in passato già evidenziato come una pena sproporzionata al reato²⁹ possa risultare di ostacolo al

²⁶ Si veda il Report Commissione europea al Parlamento europeo ed al Consiglio in ordine all'implementazione ed all'applicazione della Direttiva (UE) 2019/1937, COM(2024) 269 final, 3 luglio 2024, § 3.4.4, 9, ove si rileva che diversi Stati membri hanno introdotto, per le segnalazioni consapevolmente false ex art. 23, § 2 sanzioni «that appear too low to be considered dissuasive».

²⁷ Sulla centralità del principio di proporzionalità, nella sua accezione anche qui rilevante, quale parametro di sindacato della Corte di giustizia sulla compressione dei diritti fondamentali ad opera del sistema antiriciclaggio dell'Unione, si veda Corte di giustizia, sent. 21 maggio 2026, cause riunite C-684/24 e C-685/24 (*Across Fiduciaria e altri*).

²⁸ Cfr. Corte di giustizia, sent. 25 febbraio 1988, causa C-299/86 (*Rainer Drex*), punti 13 ss. La questione riguardava la diversa disciplina del mancato pagamento dell'IVA all'importazione intracomunitaria (anteriore al regime regolato dalla Direttiva 91/680/CEE del Consiglio, del 16 dicembre 1991 che, a partire dal primo gennaio 1993, ha introdotto un regime transitorio, ma tuttora vigente, che regola le operazioni soggette all'IVA intracomunitaria) che prevedeva la pena detentiva e la confisca rispetto a quella del mancato pagamento dell'IVA sulle cessioni di beni all'interno del Paese, sanzionata con misure non penali. Per un approfondimento si veda BERNARDI, *Principi di diritto e diritto penale europeo*, in *Annali Univ. Ferrara*, 1988, II, 75 ss., ed in particolare 199 e, volendo, BOLIS, *Depenalizzazione del contrabbando e attenuata tutela degli interessi finanziari dell'Unione europea*, in *Dir. pen. cont.*, 8 novembre 2016, 20.

²⁹ Per un approfondimento del tema si veda, tra tutti, RECCHIA, *Il principio di proporzionalità nel diritto penale*, Torino, 2020.

conseguimento delle libertà previste dal Trattato – in quella pronuncia con riferimento alla libera circolazione di merci – nella misura in cui vi sia una manifesta sproporzione nel livello di severità delle pene previste, sul piano interno, per due categorie di infrazioni sostanzialmente analoghe sotto il profilo comunitario. Analogamente, con la pronuncia von Colson³⁰ la Corte di giustizia ha richiesto che le sanzioni prescelte dagli Stati membri fossero effettive e dissuasive, e non meramente simboliche, escludendo così, in sostanza, sanzioni sproporzionate «per difetto»: di qui l'obbligo per i giudici nazionali di interpretare il diritto interno in modo da assicurare, per le violazioni attinenti all'ambito comunitario, una tutela che vada «oltre il risarcimento puramente simbolico».

5.1. *Segue: il profilo costituzionale della ragionevolezza.* Non diversamente, sul piano interno, la disparità di trattamento tra il segnalante *whistleblower* generale – assoggettato, come visto, a triplici conseguenze per la segnalazione dolosa o gravemente colposa – ed il segnalante antiriciclaggio – che risponde, nella sostanza, solo secondo le regole ordinarie della calunnia e della diffamazione, con l'ulteriore aggravante di dover attendere l'accertamento, anche di primo grado, della relativa responsabilità prima che l'esimente di buona fede venga meno – pone un problema di ragionevolezza ai sensi dell'art. 3 Cost.

Il *tertium comparationis* appare solido: si tratta, in entrambi i casi, di un soggetto che riceve un canale di segnalazione riservato istituito dalla legge, che gode di un'esenzione da responsabilità condizionata alla buona fede – analogamente a quanto la giurisprudenza amministrativa richiede, nel *whistleblowing* generale, in termini di effettivo perseguimento dell'interesse pubblico e non di scopi meramente egoistici³¹ – e la cui condotta incide allo

³⁰ Cfr. Corte di giustizia, sent. 10 aprile 1984, causa C-14/83 (*von Colson e Kamann contro Land Nordrhein-Westfalen*), punti 18, 22-23, 26 e 28. È stato osservato come in questa sentenza la Corte di giustizia, pur ribadendo che i Trattati all'epoca vigenti lasciassero agli Stati membri la libertà di scegliere il modo ed i mezzi destinati ad assicurare l'attuazione delle direttive, ha osservato come l'effettiva tutela di queste ultime non potesse prescindere dall'adozione di un sistema di sanzioni appropriato, di cui cioè fosse chiara l'efficacia ed il reale effetto dissuasivo; così BERNARDI, *L'armonizzazione delle sanzioni in Europa: linee ricostruttive*, in *Riv. it. dir. proc. pen.*, 2008, 1, 76 ss., ed in particolare 113.

³¹ Sull'esclusione della tutela *whistleblowing* per le segnalazioni sorrette da un interesse esclusivamente

stesso modo, potenzialmente in modo più grave, vista la centralità delle SOS nell'attività di *intelligence* finanziaria e nei conseguenti riflessi su accertamenti fiscali e misure di prevenzione, di cui si dirà a breve, sulla sfera giuridica, patrimoniale e reputazionale del segnalato. Non emerge, a un primo esame, una ragione oggettiva che giustifichi la più favorevole posizione del segnalante antiriciclaggio in mala fede rispetto all'omologo *whistleblower*, se non un difetto di coordinamento normativo tra il d.lgs. 24/2023 e il d.lgs. 231/2007 rimasto, su questo specifico punto, ancorato all'impostazione previgente.

6. *I dati UIF: un volume di segnalazioni sproporzionato rispetto agli esiti penali.* Non solo teoria, dunque: l'analisi statistica dei flussi SOS conferma, sul piano empirico, la rilevanza pratica della lacuna sin qui descritta sul piano astratto. I dati resi noti dall'Unità di informazione finanziaria attestano una crescita marcata e ininterrotta del volume delle segnalazioni ricevute negli ultimi esercizi, culminata in un valore record nell'ultimo anno disponibile³². A fronte di tale crescita, la quota di segnalazioni che riceve un riscontro investigativo qualificabile come positivo da parte degli organi inquirenti resta,

personale, estranee alla tutela dell'integrità della pubblica amministrazione, si veda Cons. Stato Sez. VI, 2 gennaio 2020, n. 28; Cons. Stato Sez. II, 6 dicembre 2021, n. 8150. La giurisprudenza amministrativa precisa, peraltro, che la compresenza di un interesse personale non esclude di per sé la sussistenza dell'interesse pubblico, purché quest'ultimo sia effettivamente perseguito. Nello stesso senso si è espressa, sotto il vigore della disciplina attuale, l'ANAC, secondo cui i motivi che hanno indotto il segnalante ad agire sono irrilevanti ai fini della trattazione della segnalazione e della protezione da misure ritorsive, salvo che la segnalazione abbia ad oggetto una contestazione, rivendicazione o richiesta legata a un interesse di carattere personale del segnalante (ANAC, Delibera n. 311 del 12 luglio 2023, *cit.*, § 2.1.3, 31).

³² Si veda UIF - Banca d'Italia, *Rapporto annuale per il 2025*, n. 18, pubblicato il 16 giugno 2026: nel 2025 la UIF ha ricevuto 162.059 segnalazioni di operazioni sospette (SOS), in aumento dell'11,5% rispetto alle 145.401 del 2024 (a sua volta in calo del 3,3% sul 2023); si tratta del valore più elevato mai registrato in un singolo anno, anche se si può stimare che, dal 2007 ad oggi, le SOS siano state complessivamente oltre 2,2 milioni; si noti che ogni segnalazione riguarda una singola operazione giudicata sospetta e può essere collegata, sul piano soggettivo, ad una pluralità di persone fisiche e giuridiche. Ad ogni modo, nel 2025 la UIF ha analizzato e trasmesso agli organi investigativi 163.888 segnalazioni (+13,9%), anch'esso dato record, mentre il valore complessivo delle operazioni segnalate si è attestato a 100,5 miliardi di euro. La quota di SOS classificate a rischio di riciclaggio basso o nullo si è ridotta al 18,9% (dal 20,4% del 2024), mentre le SOS collegate al finanziamento del terrorismo sono state 310 (340 nel 2024). Il dato è confermato dalle rilevazioni del primo semestre 2026, nel quale la UIF ha ricevuto 90.200 segnalazioni, in aumento dell'11,6% rispetto al corrispondente periodo del 2025 e pari al valore semestrale più elevato finora registrato: si veda *Quaderni dell'antiriciclaggio - Statistiche. Segnalazioni di operazioni sospette*, UIF - Banca d'Italia, 2026, I, Sintesi.

su base storica, sensibilmente inferiore al volume complessivo delle segnalazioni pervenute³³. Dati risalenti ma istruttivi sull'ordine di grandezza del fenomeno confermano che solo una frazione minoritaria delle segnalazioni sviluppate confluisce in procedimenti penali già aperti dalle Procure della Repubblica competenti³⁴, laddove stime giornalistiche anteriori, pur non comparabili per metodologia, indicavano una percentuale ancora più contenuta di esiti rilevanti³⁵.

È necessario, per onestà intellettuale e correttezza metodologica, precisare che tale divario non è di per sé sintomo di abuso del sistema. La soglia di attivazione dell'obbligo di segnalazione – il sospetto, ovvero il motivo ragionevole per sospettare – è strutturalmente più bassa della soglia richiesta per l'esercizio dell'azione penale, e un sistema di prevenzione efficiente deve fisiologicamente produrre un numero di segnalazioni superiore al numero di riscontri penali, pena lo svuotamento della funzione preventiva e di *intelligence* propria dell'istituto. Il dato quantitativo assume rilievo non in sé, ma in combinazione con l'assenza di un correttivo sanzionatorio per le segnalazioni palesemente infondate o effettuate con dolo: un sistema che genera un volume crescente di segnalazioni senza che, sul lato opposto, sia previsto alcun meccanismo dedicato di responsabilizzazione del segnalante

³³ Si veda sempre UIF – Banca d'Italia, *Rapporto annuale per il 2025*, cit., 19: nel biennio 2024-2025 la UIF ha ricevuto circa 44.400 riscontri (*feedback*) positivi dalla Guardia di finanza e, nel solo 2025, circa 8.700 riscontri dalla Direzione nazionale antimafia e antiterrorismo, per lo più relativi a segnalazioni classificate a rischio medio-alto o alto. Rapportando i 44.400 riscontri positivi al totale di circa 307.460 SOS ricevute nel biennio (145.401 + 162.059), la quota di segnalazioni che riceve un riscontro investigativo qualificato come positivo si attesta indicativamente attorno al 14%; si tratta, tuttavia, di un indicatore di utilità informativa per l'attività di *intelligence* finanziaria, non di un indicatore di apertura di procedimento penale né di accertamento di responsabilità.

³⁴ Il dato è tratto dall'Audizione del Comandante generale della Guardia di finanza alle Commissioni riunite di Camera e Senato in data 17 settembre 2019: nel 2018 il Nucleo speciale polizia valutaria ha sviluppato la totalità delle 98.000 segnalazioni pervenute, delle quali 6.187 (pari a circa il 6,3%) sono confluite in procedimenti penali già aperti dalle Procure della Repubblica competenti e affidati anche ad altre Forze di polizia; si tratta di segnalazioni innestatesi in indagini preesistenti, non di procedimenti aperti *ex novo* sulla sola base della SOS.

³⁵ Il dato, riferito al Rapporto annuale 2014 del Nucleo speciale polizia valutaria sulle SOS, secondo cui solo una frazione minima delle segnalazioni pervenute avrebbe registrato un esito investigativo o processuale significativo (nell'ordine dell'1% del totale), è stato ripreso in sede giornalistica; esso non è direttamente comparabile, per metodologia e periodo di riferimento, con i più recenti dati UIF innanzi citati, ma offre un termine di paragone utile per apprezzare la persistenza strutturale del fenomeno nel tempo.

negligente o in mala fede, rischia strutturalmente di perdere la capacità di selezione qualitativa dei flussi informativi, riversando sull'apparato investigativo – e sul segnalato – il costo di tale assenza di filtro.

Vale peraltro segnalare, ai fini della presente analisi statistica, che le nuove Istruzioni della UIF in attuazione dell'art. 41 del d.lgs. 231/2007, applicabili dal 1° luglio 2026, hanno codificato e reso sistematico un flusso di ritorno periodico verso i destinatari sugli esiti delle segnalazioni trasmesse, distinguendo le segnalazioni prive di sufficienti elementi di rischio da quelle classificate a basso rischio³⁶. Si tratta di un patrimonio informativo che, ove in prospettiva reso oggetto di rilevazione statistica aggregata e resa pubblica dalla stessa Unità, potrebbe arricchire, per gli anni a venire, l'analisi del divario tra volume delle segnalazioni ed esiti investigativi qualificati qui condotta sulla base dei soli dati attualmente disponibili.

7. *Il rischio di uno stimolo statale alla delazione.* È in questo preciso punto di frizione che si annida l'interrogativo più delicato: l'assenza di sanzioni dedicate per la SOS falsa o pretestuosa, unita a un regime di responsabilità sostanzialmente azzerato per il segnalante che agisca secondo lo *standard*, comunque permissivo, della buona fede presunta, configura un incentivo – indiretto ma strutturale – alla segnalazione difensiva indiscriminata da parte dei soggetti obbligati. Questi ultimi, esposti essi stessi a sanzioni severe per l'omessa segnalazione³⁷ e a nessuna sanzione dedicata per la segnalazione eccessiva, sono razionalmente incentivati a segnalare, difensivamente, per eccesso di cautela piuttosto che per un concreto fondato sospetto³⁸.

³⁶ Si veda UIF – Banca d'Italia, *Istruzioni per la rilevazione e la segnalazione delle operazioni sospette*, Provvedimento del 18 dicembre 2025, applicabili dal 1° luglio 2026 (di seguito: Istruzioni UIF 2026), e specialmente 13, ove si prevede che l'Unità comunichi ai destinatari, con cadenza almeno semestrale, gli esiti delle segnalazioni trasmesse, distinguendo le segnalazioni per le quali non sono stati ravvisati sufficienti elementi di rischio a supporto del sospetto (c.d. elenco A) da quelle classificate a basso rischio pur in presenza di alcuni elementi a supporto del sospetto (c.d. elenco B), nonché una scheda di *feedback* annuale sulla qualità della collaborazione attiva prestata dal singolo destinatario o dal relativo gruppo di appartenenza.

³⁷ L'art. 58 del d.lgs. 231/2007 prevede una sanzione amministrativa pecuniaria per l'omessa segnalazione di operazione sospetta, pari a 3.000 euro nella fattispecie base (co. 1); la sanzione base viene elevata da 30.000 a 300.000 euro nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime (co. 2).

³⁸ Sulla *ratio* delle sanzioni previste dall'art. 23, § 2, della Direttiva (UE) 2019/1937 per le segnalazioni in mala fede, si rinvia a COSSU-VALLI, *Il whistleblowing*, cit. 163, nonché a DONINI, *La tutela del whist-*

Non si tratta, a rigore, di un incentivo alla delazione in senso proprio – che presuppone un dolo specifico di nuocere, non riscontrabile nella generalità dei casi – quanto piuttosto di un fenomeno di *over-reporting* difensivo, strutturalmente indotto dall'asimmetria tra il rischio sanzionatorio per l'omessa segnalazione e l'assenza di rischio sanzionatorio dedicato per la segnalazione eccessiva o infondata.

Un termine di paragone istruttivo, per quanto risalente, proviene proprio dall'esperienza in cui il sistema della segnalazione premiale è nato: nel diritto inglese medievale e della prima età moderna, il ricorso indiscriminato alle *qui tam actions* da parte dei *common informers* – mossi in parte da un interesse pubblico e in parte da un tornaconto personale – condusse a un uso distorto dello strumento, cui il Parlamento inglese reagì introducendo, a partire dalla seconda metà del XVI secolo, un meccanismo di correzione a tutela del soggetto ingiustamente accusato³⁹. Il precedente storico è utile proprio perché mostra come, ovunque un sistema di segnalazione abbia incentivato la denuncia, l'assenza di un correttivo per l'abuso ne abbia compromesso, prima o poi, la stessa credibilità: una lezione che la disciplina italiana della SOS antiriciclaggio, priva di qualunque meccanismo equivalente, non pare avere ancora recepito.

7.1. Segue: la risposta regolamentare all'over-reporting nelle nuove Istruzioni UIF. Non è privo di significato, in questa prospettiva, che le nuove Istruzioni della UIF muovano proprio nella direzione di arginare il rischio di

leblower tra etica e pragmatismo. La logica premiale del diritto statunitense. Un modello da seguire?, in *Amministr@tivamente*, 2022, I, 216 ss.: le sanzioni per le segnalazioni in mala fede mirano a scoraggiarle proprio perché, da un lato, danneggiano ingiustamente il segnalato e, dall'altro, compromettono la credibilità dell'intero sistema di allerta – una *ratio* che milita, *mutatis mutandis*, anche a favore dell'introduzione di un presidio sanzionatorio dedicato nella disciplina della SOS antiriciclaggio.

³⁹ Nel diritto inglese medievale e della prima età moderna, le c.d. *qui tam actions* – termine che deriva dall'espressione *qui tam pro domino rege quam pro se ipso in hac parte sequitur*, ovvero colui che agisce tanto per il sovrano quanto per se stesso – consentivano al *common informer* di agire, in parte per la Corona e in parte per proprio tornaconto, contro chi avesse violato una legge; esse furono progressivamente circoscritte proprio a fronte del loro uso distorto a fini di denunce fittizie: a partire dalla seconda metà del XVI secolo il Parlamento inglese introdusse la possibilità, per il soggetto ingiustamente convenuto, di proporre domanda riconvenzionale, ottenendo il rimborso delle spese in caso di vittoria e la condanna del proprio accusatore. Il precedente storico è significativo perché mostra come, sin dalle origini del sistema di segnalazione premiale nei paesi di *common law*, all'incentivo alla denuncia si sia accompagnato un correttivo a tutela del soggetto ingiustamente accusato.

segnalazione difensiva indiscriminata sopra descritto, sia pure operando non sul piano, qui esaminato, della responsabilizzazione *ex post* del segnalante, bensì su quello, distinto, dell'individuazione dell'anomalia a monte della segnalazione. Le Istruzioni prescrivono infatti ai destinatari di evitare, nel processo valutativo, automatismi e approcci cautelativi fondati sul mero superamento di soglie quantitative minime, sulla ricezione di richieste di informazioni o sui controlli delle autorità, ed elencano espressamente sei circostanze – tra cui la mera difformità delle informazioni acquisite in sede di adeguata verifica, il rischio elevato attribuito al soggetto, l'individuazione di notizie negative, la ricezione di richieste informative da parte delle Autorità competenti in materia di prevenzione del riciclaggio e la mera ricorrenza di misure reali o personali a carico del soggetto interessato – che, di per sé, non sono sufficienti per effettuare una segnalazione di operazioni sospette⁴⁰. Analoga cautela è richiesta, per la prima volta in un provvedimento della UIF, con riguardo agli strumenti di selezione basati su sistemi di intelligenza artificiale, che devono fondarsi su dati oggettivi e verificabili ed essere accompagnati da adeguate valutazioni svolte con l'intervento umano⁴¹. Si tratta di un intervento regolamentare che conferma, implicitamente, la fondatezza dell'allarme sull'*over-reporting* difensivo qui illustrato; esso tuttavia non incide, come si dirà tra poco, sul diverso e più specifico profilo relativo all'assenza di conseguenze *ex post* per la segnalazione che, pur superando questo vaglio preventivo rafforzato, si riveli comunque dolosamente o colposamente falsa:

⁴⁰ Cfr. Istruzioni UIF 2026, *cit.*, 7, ove si prescrive di evitare, nel processo valutativo, automatismi e approcci cautelativi fondati sul mero superamento di soglie quantitative minime, sulla ricezione di richieste di informazioni o sui controlli delle autorità, e Sezione IV (Segnalazione delle operazioni sospette), 9-10, ove sono elencate, ai punti da *h*) a *vi*), le circostanze che, di per sé, non sono sufficienti per l'invio di una segnalazione di operazioni sospette. Non è privo di significato che un'esigenza analoga fosse già avvertita, sul piano operativo, dalla stessa Guardia di finanza fin dal 2012: cfr. Circolare n. 83607/2012, *cit.*, vol. I, 254, ove si segnala l'esigenza di «orientare i segnalanti in modo più mirato e selettivo [...] quale presupposto indispensabile per l'innalzamento del livello qualitativo del sistema di prevenzione», in un contesto esplicitamente motivato dal «costante incremento del flusso in entrata delle segnalazioni».

⁴¹ Cfr. Istruzioni UIF 2026, *cit.*, 8, e ivi n. 6, con richiamo al Regolamento (UE) 2024/1689 (c.d. AI Act). Sul tema dell'utilizzo degli algoritmi di intelligenza artificiale nell'ambito dell'antiriciclaggio si veda: più in generale, DI VIZIO, *Prevenzione e investigazioni: l'uso di IA, big data e soluzioni tecnologiche in ambito finanziario e nel contrasto al riciclaggio (AML) e al finanziamento del terrorismo (CFT)*, in *disCrimen*, 2024; per un'applicazione tecnica, CARIELLO-DE SIMONI-IEZZI, *Un modello di machine learning per l'identificazione di aziende collegate alla criminalità organizzata in Italia*, Quaderni dell'antiriciclaggio, UIF – Banca d'Italia, 2024, 22.

il contenimento *ex ante* del fenomeno, per quanto opportuno, non equivale alla responsabilizzazione *ex post* del segnalante in mala fede, in quanto non è sufficiente per disincentivare le segnalazioni effettuate in mala fede.

7.2. *Il nesso tra qualità della collaborazione attiva e iniziative sanzionatorie: le Istruzioni UIF e il perimetro residuo del vuoto normativo.* Le medesime Istruzioni UIF sopra citate introducono altresì, per la prima volta, un nesso esplicito tra la qualità della collaborazione attiva prestata dal destinatario e l'assunzione, nei suoi confronti, di eventuali iniziative, anche sanzionatorie. La UIF può infatti chiedere la sostituzione o l'integrazione di una segnalazione incompleta, erronea o comunque non conforme alle Istruzioni; se il destinatario non riscontra la richiesta entro trenta giorni, l'Unità trasmette la segnalazione agli organi investigativi dando atto che l'incompletezza o la scarsa qualità informativa è dovuta a mancata collaborazione da parte del destinatario e, nei casi di particolare gravità, può disporre l'annullamento della segnalazione; i dati relativi a sostituzioni, integrazioni e annullamenti sono utilizzati dalla UIF ai fini della valutazione di eventuali iniziative, anche sanzionatorie, in relazione alla violazione degli obblighi informativi verso l'Unità e alla qualità della collaborazione attiva⁴². Si tratta, tuttavia, di un meccanismo che opera su un piano diverso da quello qui esaminato: esso presidia l'inerzia del destinatario nel collaborare alla correzione di una segnalazione già trasmessa, non la falsità o la gravemente colposa infondatezza del relativo contenuto; né esso è accompagnato, come si è visto sopra, da alcuna forma di tutela, notizia o ristoro in favore del soggetto ingiustamente segnalato, nemmeno per il rimborso o la rifusione delle spese sostenute per la propria difesa⁴³. La novità, per quanto significativa quale indice di una

⁴² Cfr. Istruzioni UIF 2026, *cit.*, 27-28. Le Istruzioni non specificano la base giuridica delle «iniziative, anche sanzionatorie» ivi richiamate; non è chiaro, in particolare, se esse rinvino alla sanzione amministrativa pecuniaria già prevista dall'art. 58 d.lgs. 231/2007 per l'omessa o inadeguata segnalazione (v. supra, nota 37) – la cui fattispecie tipica non sembra tuttavia coincidere appieno con la mancata collaborazione nella fase, distinta, di correzione di una segnalazione già trasmessa – ovvero a un autonomo potere di segnalazione alle Autorità di vigilanza di settore ai fini dell'esercizio dei relativi poteri sanzionatori.

⁴³ Nel sistema statunitense, invece, è espressamente previsto che, qualora si accerti che il segnalato è innocente, che la segnalazione è manifestamente frivola e vessatoria e che la Pubblica amministrazione non è intervenuta nella causa, le spese legali siano poste a carico del segnalante e non dell'accusato; sul punto si veda DONINI, *La tutela del whistleblower*, *cit.*

crescente attenzione della UIF alla qualità – e dunque, indirettamente, alla responsabilizzazione – della collaborazione attiva, non è dunque idonea a colmare il vuoto sanzionatorio dedicato alla segnalazione in mala fede che il presente contributo intende segnalare: essa conferma, semmai, *a contrario*, la persistenza di tale vuoto, giacché il più naturale dei veicoli per introdurre un simile presidio – le stesse Istruzioni UIF di più recente adozione – non vi ha provveduto, limitandosi a colpire il diverso versante, procedurale, della mancata collaborazione nella fase di correzione della segnalazione.

8. *Le conseguenze per il segnalato: la banca dati SIVA e l'uso dei dati ai fini fiscali.* Un ulteriore profilo da esaminare – e il più concretamente rilevante per la posizione del segnalato – riguarda il destino delle informazioni contenute nella SOS una volta trasmessa. Le segnalazioni ricevute dalla UIF, unitamente ai risultati delle relative analisi, sono trasmesse al Nucleo speciale di polizia valutaria della Guardia di finanza e confluiscono nel Sistema informativo valutario (SIVA), archivio informatico che raccoglie e classifica le segnalazioni pervenute, orientando i successivi sviluppi investigativi dei reparti del Corpo della Guardia di finanza⁴⁴.

8.1. *La programmazione delle verifiche fiscali.* Il punto di massima criticità per il segnalato ingiustamente attinto da una SOS infondata risiede nell'uso

⁴⁴ Si veda Comando generale della Guardia di finanza, Circolare n. 83607/2012, *cit.*, vol. I, Parte II, Capitolo 4, che già delineava il percorso operativo di approfondimento delle SOS attraverso il Sistema informativo valutario, con un'analisi pre-investigativa del Nucleo speciale polizia valutaria che attribuisce un codice di priorità alla segnalazione (classificazioni da D1 a D4 e AFI) per orientare lo sviluppo investigativo dei Reparti. Per quanto riguarda la genesi e l'evoluzione della banca dati SIVA, sin dal 2005 la Guardia di finanza si è dotata di una piattaforma virtuale quale sistema dematerializzato per la gestione riservata delle segnalazioni di operazioni sospette e dei dati emergenti dalla relativa analisi e dall'approfondimento investigativo. La banca dati risulta censita, come «S.I.V.A. - Sistema Informativo Valutario», alla scheda n. 54 dell'allegato al decreto del Ministro dell'interno del 24 maggio 2017, adottato ai sensi dell'art. 53, co. 3 del d.lgs. 30 giugno 2003, n. 196, ove le fonti normative del trattamento sono indicate negli artt. 8 e 47 del d.lgs. 231/2007 e nel d.lgs. 19 marzo 2001, n. 68; il decreto non impiega, in questa sede, la sigla «SIVA2», adottata invece nella più recente terminologia interna del Corpo per indicare la versione evoluta della piattaforma, attualmente in fase di ulteriore evoluzione verso SIVA3. Sul tema si veda anche Camera dei deputati, XIX Legislatura, Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere, Resoconto stenografico, Seduta n. 39 di venerdì 22 marzo 2024, Audizione di Andrea De Gemmaro, Comandante generale della Guardia di finanza, 13-14; decreto del Ministro dell'interno 24 maggio 2017, *cit.*, Allegato, Scheda n. 54.

che la stessa Guardia di finanza è legittimata a fare dei dati SIVA anche al di fuori del procedimento antiriciclaggio in senso stretto. La circolare tuttora vigente quale principale direttiva operativa per l'esecuzione di verifiche e controlli fiscali individua espressamente, tra gli strumenti da utilizzare in sede di selezione e programmazione dei soggetti da sottoporre a verifica, le banche dati disponibili – tra cui rientra il patrimonio informativo derivante dalle segnalazioni antiriciclaggio – precisando che il trasferimento agli atti delle verifiche fiscali delle notizie originate dalle ispezioni antiriciclaggio può avvenire solo a conclusione dei relativi accertamenti, con il vincolo di garantire in ogni caso il segreto sull'identità del segnalante⁴⁵.

Infatti, viene espressamente detto che le «segnalazioni di operazioni sospette vanno considerate come fonte di selezione e di innesco a carattere privilegiato non solo per la lotta al riciclaggio o al finanziamento del terrorismo, ma anche per il contrasto di qualsiasi illecito economico e finanziario, ivi compresi quelli di natura tributaria, in particolare allorquando le informazioni fanno emergere un profilo economico del soggetto incompatibile ed incongruo rispetto alla posizione reddituale dichiarata al fisco»⁴⁶.

Ciò conferma che l'iscrizione di un nominativo nella banca dati SIVA quale soggetto segnalato con SOS costituisce, indipendentemente dal successivo ed eventuale esito dell'approfondimento investigativo in sede penale, un elemento di conoscenza che l'Amministrazione finanziaria è legittimata a utilizzare – una volta conclusa la fase di approfondimento antiriciclaggio – ai fini della programmazione nominativa dei controlli fiscali.

8.2. *L'acquisizione autonoma dei conti correnti da parte del Nucleo speciale e la trasmissione ai reparti ordinari.* A monte del meccanismo di

⁴⁵ Il riferimento è a Comando generale della Guardia di finanza, Circolare n. 1/2018 (Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali), Protocollo 357600 del 27 novembre 2017, in vigore dal 1° gennaio 2018: tra gli strumenti da utilizzare in sede di selezione e programmazione dei soggetti da sottoporre a verifica fiscale rientrano le banche dati disponibili, l'attività di *intelligence* e il controllo economico del territorio; il trasferimento agli atti delle verifiche fiscali delle notizie originate dalle ispezioni antiriciclaggio può avvenire solo a conclusione degli accertamenti finalizzati alla verifica del corretto assolvimento degli adempimenti antiriciclaggio, garantendo comunque il segreto sull'identità del segnalante.

⁴⁶ Si veda Circolare n. 1/2018, *cit.*, vol. I, 91.

programmazione dei controlli fiscali innanzi succintamente descritto si colloca un autonomo canale di acquisizione dei dati bancari del segnalato, la cui ricostruzione è necessaria prima di poterne verificare, rispettivamente, l'utilizzabilità in sede tributaria e la compatibilità con le garanzie convenzionali di cui si dirà tra poco. Ricevuta la segnalazione dalla UIF, il Nucleo speciale di polizia valutaria della Guardia di finanza non si limita infatti a recepirne il contenuto dichiarativo trasmesso dal segnalante, ma procede a un'autonoma analisi pre-investigativa che attribuisce alla segnalazione un codice di priorità, funzionale a orientare il successivo sviluppo investigativo dei Reparti del corpo.

Tale analisi si fonda su una base giuridica distinta rispetto a quella tributaria. Oltre ai poteri generali di polizia economica e finanziaria attribuiti in generale alla Guardia di finanza dall'art. 2 del d.lgs. 68/2001, al solo Nucleo speciale di polizia valutaria – incardinato nei Reparti speciali del corpo – sono riconosciute le specifiche potestà di polizia valutaria di cui al d.P.R. 148/1988 – segnatamente gli artt. 25 e 28, in tema di ispezioni e di obbligo di esibizione della documentazione presso gli intermediari finanziari – rese applicabili al procedimento di approfondimento delle segnalazioni di operazioni sospette dall'art. 9, co. 4, lett. a) e a-bis) del d.lgs. 231/2007, nonché l'accesso diretto all'archivio dei rapporti finanziari costituito presso l'anagrafe tributaria ai sensi dell'art. 7, sesto co. del d.P.R. n. 605/1973. In forza di tali potestà, il Nucleo speciale può acquisire, in sede di approfondimento della segnalazione, i dati relativi ai conti correnti e agli altri rapporti finanziari intestati al soggetto segnalato senza dover ricorrere, né in via preventiva né in via successiva, all'autorizzazione prevista dalla legislazione tributaria in senso stretto⁴⁷.

⁴⁷ Sulle potestà esercitabili nel corso delle ispezioni antiriciclaggio, tra cui i poteri di polizia valutaria e l'accesso all'archivio dei rapporti finanziari si veda la Circolare n. 83607/2012, *cit.*, vol. I, 84 ss. Più precisamente, l'art. 9, co. 4, lett. a) d.lgs. 231/2007 attribuisce al Nucleo speciale di polizia valutaria l'esercizio, ai fini degli approfondimenti delle segnalazioni di operazioni sospette, dei poteri di ispezione e di richiesta di esibizione documentale già riconosciuti dalla normativa valutaria (artt. 25 e 28, d.P.R. n. 148/1988); la successiva lett. a-bis), introdotta dall'art. 1, co. 1 d.lgs. 25 maggio 2017, n. 90, ha aggiunto un autonomo potere di acquisizione di dati e informazioni presso i soggetti obbligati, anche al di fuori delle ispezioni in senso stretto. L'Archivio dei rapporti finanziari di cui all'art. 7, co. 6 d.P.R. n. 605/1973 (come modificato dall'art. 37, co. 4 d.l. 223/2006, conv. L. 248/2006) contiene invece i soli dati identificativi dei rapporti intrattenuti da ciascun soggetto con banche e intermediari finanziari, non le relative movimentazioni, che restano acquisibili unicamente mediante l'esercizio dei poteri ispettivi

Da questa autonomia di base giuridica discende un duplice ordine di conseguenze, l'una fattuale e l'altra sistematica. Sul piano fattuale, l'acquisizione degli estratti conto del segnalato costituisce, nella prassi operativa, un *posterius* pressoché automatico rispetto alla sola ricezione della segnalazione, non richiedendo alcuna motivazione, alcuna valutazione preventiva da parte di un organo terzo, né alcuna forma di conoscibilità da parte dell'interessato. Sul piano sistematico, i dati così acquisiti restano depositati nel Sistema informativo valutario, corredati della relativa scheda di analisi economico-finanziaria, e vengono messi a disposizione dei Reparti a competenza ordinaria della Guardia di finanza – Nuclei di polizia tributaria e reparti territoriali – delegati all'approfondimento operativo: il medesimo apparato che, mutata veste, sarà in seguito chiamato a programmare ed eseguire le verifiche fiscali, come si dirà successivamente. La circostanza che tale patrimonio informativo permanga nella disponibilità del Corpo indipendentemente dall'esito, anche negativo, dell'approfondimento antiriciclaggio spiega perché il descritto canale di acquisizione pone, come si vedrà, un problema di utilizzabilità prima ancora che di legittimità convenzionale.

8.3. *L'aggiramento del sistema autorizzatorio ordinario: l'utilizzabilità diretta ai fini fiscali dei dati bancari acquisiti in ambito valutario.* Occorre muovere, per apprezzare la portata dell'innovazione legislativa di cui si dirà, dalla disciplina previgente. Prima della riforma del 2017, la giurisprudenza di legittimità era ferma nel ritenere che il canale valutario appena descritto non esonerasse in alcun modo l'Amministrazione finanziaria dall'osservanza del sistema autorizzatorio ordinario: la polizia tributaria, per esperire accertamenti fondati su dati bancari, doveva in ogni caso munirsi della previa autorizzazione del comandante regionale ai sensi dell'art. 32 del d.P.R. n. 600/1973, «non essendo altrimenti legittima l'acquisizione e utilizzazione della documentazione bancaria, pure se attivata a seguito di segnalazione pervenuta alla Guardia di finanza dal Nucleo Speciale di Polizia valutaria»⁴⁸.

appena richiamati.

⁴⁸ Si veda Cass. Sez. trib., 13 aprile 2009, n. 8766, secondo cui, ai fini dell'accertamento tributario, «la

In questo assetto, dunque, l'autonomia del canale valutario sul piano dell'acquisizione non si traduceva in alcuna corrispondente autonomia sul piano dell'utilizzo fiscale: il dato bancario, per quanto già nella materiale disponibilità del Corpo, doveva essere nuovamente e formalmente acquisito attraverso l'ordinario procedimento autorizzato, che ne doveva valutare la fondatezza dei presupposti.

Tale equilibrio è stato però superato dalla riforma del 2017. Il legislatore ha infatti previsto, con una disposizione la cui portata si è progressivamente ampliata, la diretta utilizzabilità ai fini fiscali dei dati e delle informazioni acquisiti nell'ambito delle attività antiriciclaggio. L'art. 9, co. 9 del d.lgs. 231/2007 sancisce oggi che «i dati e le informazioni acquisite nell'ambito delle attività svolte ai sensi del presente articolo sono utilizzabili ai fini fiscali, secondo le disposizioni e le attribuzioni vigenti»⁴⁹: disposizione che, per collocazione sistematica tra le norme generali del Titolo I del decreto, si applica indistintamente ai dati raccolti nel corso delle ispezioni antiriciclaggio, degli approfondimenti delle segnalazioni di operazioni sospette e, per quanto qui interessa, dell'accesso all'archivio dei rapporti finanziari esercitato con gli speciali poteri di polizia valutaria.

Polizia tributaria [...] deve acquisire la preventiva autorizzazione del Comandante di zona [...] non essendo altrimenti legittima l'acquisizione e utilizzazione della documentazione bancaria, pure se attivata a seguito di segnalazione pervenuta alla Guardia di finanza dal Nucleo Speciale di Polizia valutaria». La perdurante attualità di tale principio, a fronte della sopravvenuta previsione dell'utilizzabilità fiscale diretta ex art. 9, co. 9 d.lgs. 231/2007, è discussa in dottrina, non constando, alla data di pubblicazione del presente contributo, arresti di legittimità successivi alla riforma del 2017 specificamente riferiti al canale valutario di acquisizione. Per un approfondimento sulla previgente normativa si veda, volendo, BOLIS, *L'utilizzabilità in ambito tributario della documentazione bancaria acquisita con i poteri della polizia valutaria*, in *Fisco*, 2010, 24, 1-3780.

⁴⁹Art. 9, co. 9 d.lgs. 231/2007, nella formulazione risultante dalle modifiche apportate dall'art. 1, co. 2 d.lgs. 25 maggio 2017, n. 90 (di recepimento della IV direttiva antiriciclaggio, Direttiva (UE) 2015/849), e successivamente dall'art. 1 d.lgs. 4 ottobre 2019, n. 125, che ha aggiunto alla previsione originaria il riferimento alle «attribuzioni» vigenti, oltre che alle «disposizioni». Sulla portata applicativa della norma, che ricomprende indistintamente i dati acquisiti nel corso di ispezioni e controlli antiriciclaggio nonché di approfondimenti di segnalazioni di operazioni sospette, cfr. Guardia di finanza, Circolare n. 210557 del 7 luglio 2017. La circolare precisa altresì che il trasferimento agli atti della verifica fiscale delle notizie apprese in sede di approfondimento di una segnalazione di operazione sospetta deve avvenire solo a conclusione delle relative procedure e non può in alcun caso determinare l'inserimento, in alcun atto del controllo o della verifica, di riferimenti che, anche in via indiretta, possano disvelare l'identità del segnalante.

L'effetto pratico della novella è precisamente quello di rovesciare l'assetto delineato dalla giurisprudenza del 2009: il dato bancario acquisito in ambito valutario può oggi essere utilizzato direttamente in sede di verifica fiscale, senza che occorra attivare ex novo il procedimento di cui agli artt. 32 e 51 citati con la conseguenza che tale meccanismo consente, di fatto, all'Amministrazione finanziaria di superare la necessità di acquisire nuovamente i dati attraverso l'attivazione dei poteri tipici dell'accertamento fiscale. Pertanto, l'autorizzazione del comandante regionale diviene una soglia procedurale che l'Amministrazione può scegliere arbitrariamente di non attraversare affatto, ove il medesimo patrimonio informativo sia già transitato per il canale valutario.

Va tenuta distinta, rispetto alla mera utilizzabilità appena ricostruita, la questione se ai dati bancari acquisiti in ambito valutario possa applicarsi anche il regime delle presunzioni legali relative di cui agli artt. 32 n. 7 del d.P.R. n. 600/1973 e 51 n. 7 del d.P.R. n. 633/1972, per cui i versamenti non giustificati si presumono ricavi non dichiarati. Si tratta di un profilo che l'art. 9, co. 9 cit. non affronta espressamente e sul quale, in assenza di specifici arresti giurisprudenziali successivi alla riforma del 2017, parte della dottrina ritiene tuttora prudente circoscrivere l'efficacia del dato acquisito in ambito valutario al rango di elemento indiziario – utilizzabile, cioè, per motivare una successiva e autonoma richiesta di autorizzazione bancaria in sede propriamente fiscale – piuttosto che di prova presuntiva diretta⁵⁰. Quale che sia la soluzione preferibile su questo specifico punto, essa non incide sul dato di fondo qui rilevante: anche nella lettura più prudente, il patrimonio

⁵⁰ Sul dibattito relativo all'applicabilità delle presunzioni legali relative di cui agli artt. 32, co. 1, n. 7 d.P.R. n. 600/1973 e 51, co. 2, n. 7 d.P.R. n. 633/1972 ai dati bancari acquisiti con i poteri di polizia valutaria ai sensi dell'art. 9, co. 6, lett. a) e co. 8, lett. a) d.lgs. 231/2007, in assenza di specifici orientamenti giurisprudenziali successivi alla riforma del 2017, si veda la ricostruzione prudenziale proposta in dottrina, che distingue l'utilizzabilità diretta del dato ex art. 9, co. 9 cit. dalla diversa questione dell'efficacia presuntiva del medesimo, quest'ultima subordinata, secondo tale impostazione, alla rinnovata acquisizione della documentazione con le forme prescritte dalla legislazione fiscale; si veda, in particolare, PROCACCINI, *Indagini bancarie tra contraddittorio e vizi motivazionali*, in *Taxnews - suppl. a Riv. trim. dir. trib.*, 28 giugno 2023, nonché GALLUCCIO, *Utilizzo ai fini fiscali dei dati acquisiti nell'ambito dell'attività antiriciclaggio: principi e modalità applicative*, in *Filodiritto*, 19 luglio 2021. Le più recenti Cass. Sez. trib., ord. 15 giugno 2026, nn. 19956 e 19960, pur non affrontando la specifica questione delle presunzioni qui discussa, offrono comunque, sul fronte dell'utilizzabilità, indicazioni che rafforzano l'esigenza di un vaglio autorizzativo effettivo anche per i dati bancari acquisiti in ambito valutario.

informativo bancario del segnalato, acquisito a margine di una SOS che può rivelarsi in seguito infondata, entra comunque nella disponibilità dell'Amministrazione finanziaria attraverso un canale sottratto, in tutto o in parte, alle garanzie procedurali previste per l'accertamento bancario ordinario – garanzie che, come si vedrà, la stessa Corte europea dei diritti dell'uomo ha ritenuto già di per sé insufficienti.

A tale rilievo di ordine convenzionale deve peraltro affiancarsi, quale premessa logicamente antecedente, il fondamento che la dottrina tributaristica interna ha da tempo elaborato in tema di inutilizzabilità della prova illecitamente acquisita nel processo tributario, indipendentemente da qualunque intervento della Corte di Strasburgo. Tale ricostruzione ha peraltro trovato, *medio tempore*, un preciso aggancio di diritto positivo nel nuovo art. 7-*quinquies* dello Statuto dei diritti del contribuente – introdotto dall'art. 1, co. 1, lett. g) del d.lgs. 219/2023, in vigore dal 18 gennaio 2024 – che sancisce l'inutilizzabilità degli elementi di prova acquisiti in violazione di legge, a presidio dei diritti fondamentali del contribuente⁵¹. Muovendo dagli artt. 13, 14 e 15 Cost. e dal potere di cognizione incidentale che l'art. 7, co. 1 e l'art. 2, co. 3 del d.lgs. 546/1992 attribuiscono al giudice tributario sulla regolarità del procedimento di formazione della prova, tale dottrina distingue la prova che l'amministrazione finanziaria abbia essa stessa acquisito in modo illecito dalla prova che, pur pervenuta legittimamente all'amministrazione, sia stata a monte illecitamente formata da un terzo; ipotesi, questa, ricostruita con specifico riferimento al caso di dati bancari sottratti con condotta di rilevanza penale da un dipendente infedele e poi trasmessi all'amministrazione finanziaria, rispetto ai quali si è ritenuto che l'utilizzabilità aggirerebbe il disposto costituzionale e che tali informazioni, ove acquisite, potrebbero avere mero rilievo di stimolo investigativo, senza poter autonomamente

⁵¹ Per un approfondimento del nuovo art. 7-*quinquies* L. 212/2000 si veda MULEO, *Note sull'inutilizzabilità degli elementi di prova acquisiti in violazione di legge nella riforma dello Statuto del contribuente*, in *Riv. dir. tribut.*, 2024, 6, 716 ss.; nonché CHIARIZIA, *Prime riflessioni in merito alla inutilizzabilità delle prove per vizi dell'attività istruttoria introdotta dalla riforma dello Statuto del contribuente di cui al D.Lgs. n. 219/2023*, in *Taxnews - suppl. a Riv. trim. dir. trib.*, 2024, 1, 23 ss. Sulla questione, ancora dibattuta, se analoga inutilizzabilità sussistesse già prima della riforma quale principio di rango costituzionale e convenzionale, si veda Cass. Sez. trib., ord. interlocutoria 11 maggio 2026, n. 13696, che ha rimesso la questione alle Sezioni unite.

fondare la prova dell'accertamento⁵². Lo schema è agevolmente trasponibile al caso qui esaminato. Quando la segnalazione di operazione sospetta che ha innescato l'accesso in ambito valutario sia stata resa con dolo o mala fede – e dunque, come si è innanzi visto, con la piena consapevolezza dell'insussistenza dei fatti riportati, o con colpa grave ad essa equiparabile – il dato bancario che ne deriva non sconta soltanto il *deficit* strutturale di garanzie procedurali di cui si dirà nel seguente paragrafo, ma trae origine da un atto specificamente viziato sul piano soggettivo, riconducibile, sul piano strutturale, proprio alla fattispecie del terzo che fornisce all'amministrazione finanziaria un elemento di conoscenza illecitamente formato. Ne deriva che il segnalato potrebbe, anche a prescindere da qualunque riforma del regime sanzionatorio – e sin da ora, in sede di giudizio tributario – eccepire l'inutilizzabilità del dato bancario acquisito in ambito valutario allegando la matrice dolosa o gravemente colposa della segnalazione a monte, con il conseguente onere per l'amministrazione finanziaria di provarne la legittima acquisizione⁵³. Un'indicazione in tal senso proviene, del resto, dalla stessa giurisprudenza più recente in tema di poteri istruttori fiscali: le Sezioni unite, pur ammettendo che il libero consenso del contribuente possa sanare l'assenza di autorizzazione del pubblico ministero all'apertura di borse e simili in sede di primo accesso, hanno cura di ricordare, in un *obiter dictum*, che i beni intimamente connessi alla persona restano assistiti dalla più pregnante garanzia dell'art. 13 Cost., insensibile persino al consenso dell'avente diritto⁵⁴. Se un simile approdo – pur riferito a un contesto di

⁵² Cfr. MISCALI, *Documentazione illecitamente acquisita e tutela giurisdizionale nel processo tributario*, in *Riv. dir. tribut.*, 2012, I, 759 ss., spec. § 2.1.3, ove il richiamo a Corte cost., 4 aprile 1973, n. 34, secondo cui «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito», e § 5, sul potere-dovere del giudice tributario, ai sensi dell'art. 7 d.lgs. 546/1992, di dichiarare inammissibile il documento risultato illecitamente acquisito o formato, che non potrà pertanto fondare autonomamente la pretesa impositiva. Per un commento più ampio sul tema si veda NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, 1, 3 ss.

⁵³ Sull'onere dell'amministrazione finanziaria di provare la legittima acquisizione della documentazione posta a fondamento dell'accertamento, si veda Cass. Sez. trib., 11 febbraio 2011, n. 3326, richiamata da MISCALI, *Documentazione illecitamente acquisita*, cit., § 5, n. 51: in assenza di prova della legittima acquisizione, la conseguenza sfavorevole ricade sull'amministrazione.

⁵⁴ BOLIS, *Le Sezioni Unite legittimano l'apertura di borse previo consenso libero ed informato del con-*

acquisizione ben diverso e in presenza di consenso – induce a dubitare della sufficienza del solo elemento soggettivo a colmare il *deficit* di giurisdizionalizzazione dell’atto istruttorio, *a fortiori* tale dubbio si impone per l’accesso ai dati bancari in ambito valutario, che non richiede né un’autorizzazione del pubblico ministero né, tantomeno, un qualunque consenso del segnalato, e che può derivare, per giunta, da un atto di segnalazione esso stesso illecito.

Il rilievo pratico di tale possibile eccezione resta, nondimeno, condizionato da un limite strutturale del sistema, di cui si è già dato conto poc’anzi: il Sistema informativo valutario registra indistintamente il dato derivante dalla segnalazione, senza alcuna marcatura che ne segnali la provenienza da un accertamento successivamente rivelatosi infondato, tantomeno da una segnalazione della cui mala fede sia stata giudizialmente accertata la sussistenza. Il dato bancario viziato permane dunque, salvo un intervento correttivo, indistinguibile da quello legittimamente acquisito nel medesimo archivio – ed è per ciò solo destinato a confluire, con le medesime modalità già illustrate, nell’attività di programmazione e selezione dei contribuenti da sottoporre a verifica, ben prima che l’eventuale accertamento della mala fede intervenga, quando interviene, a distanza di tempo e all’esito di un procedimento del tutto autonomo.

9. *I profili di garanzia del canale valutario: la sentenza Ferrieri e Bonassisa c. Italia della Corte EDU e il deficit convenzionale e istituzionale.* Il descritto meccanismo di acquisizione e di utilizzo dei dati bancari in ambito valutario si presta a un ulteriore rilievo, di carattere convenzionale, alla luce della sentenza Ferrieri e Bonassisa c. Italia, con cui la Corte europea dei diritti dell’uomo ha condannato l’Italia, l’8 gennaio 2026, per violazione dell’art. 8 C.E.D.U. in relazione all’accesso ai dati bancari dei contribuenti per finalità di accertamento fiscale⁵⁵. Chiamata a valutare la conformità a Convenzione

tribuyente. Ma un *obiter dictum* lascia aperta la via ad un’eccezione di costituzionalità, nota a Cass. Sez. un., 2 febbraio 2022, n. 3182, in *Taxnews – suppl. a Riv. trim. dir. trib.*, 2022, 2, 427 ss.

⁵⁵ Si veda Corte EDU Sez. I, sent. 8 gennaio 2026, *Ferrieri e Bonassisa c. Italia*, ricorsi nn. 40607/19 e 34583/20, divenuta definitiva a seguito del rigetto, da parte del collegio della Grande camera, della richiesta di rinvio presentata dal Governo italiano ai sensi dell’art. 43 C.E.D.U., ed in particolare i §§ 1,

del sistema di autorizzazione previsto dagli artt. 32 e 51 citati, la Corte ha ritenuto che tale sistema non soddisfacesse il requisito della «qualità della legge» imposto dall'art. 8, § 2, C.E.D.U., sulla base di due ordini di ragioni tra loro distinti. In primo luogo, la base giuridica non delimitava sufficientemente l'ambito della discrezionalità conferita alle autorità nazionali, posto che l'autorizzazione, secondo il diritto interno, non deve essere motivata. In secondo luogo, il quadro giuridico interno non prevedeva alcun controllo giurisdizionale o indipendente realmente effettivo, né *ex ante* né *ex post*, sulle misure adottate, avendo la Corte escluso che il ricorso alle commissioni tributarie, ai tribunali civili o al Garante del contribuente costituisse un rimedio effettivo ai sensi dell'art. 8 C.E.D.U.⁵⁶. Da tale duplice riscontro la Corte ha tratto la conclusione che le ingerenze in questione non fossero «previste dalla legge», ravvisando altresì, ai sensi dell'art. 46 C.E.D.U., un problema di carattere sistemico dell'ordinamento italiano⁵⁷.

Se un simile giudizio di inadeguatezza ha colpito il procedimento ex artt. 32 e 51 – che pure prevede, quantomeno sulla carta, l'intervento di un organo gerarchicamente sovraordinato tenuto a valutare gli elementi indicati nella richiesta – le medesime censure si attagliano, *a fortiori*, al canale di acquisizione in ambito valutario sopra ricostruito. Sotto il primo profilo censurato dalla Corte, quello della delimitazione della discrezionalità, il canale valutario si colloca in una posizione ancora più arretrata: l'accesso ai

6-9, 47-58 (sull'applicabilità dell'art. 8 C.E.D.U. ai dati bancari acquisiti dall'Agenzia delle entrate ai sensi degli artt. 32 d.P.R. n. 600/1973 e 51 d.P.R. n. 633/1972). Per un commento si veda CALZOLARI-CHIARIZIA, *Illegittimità delle indagini bancarie: la Corte EDU colpisce ancora*, in *Corr. trib.*, 2026, 3, 217 ss.

⁵⁶ Si veda, in particolare, *Ferrieri e Bonassisa c. Italia*, cit., §§ 77-82 (sulla mancata delimitazione dell'ambito della discrezionalità conferita alle autorità nazionali e sull'assenza dell'obbligo di motivazione dell'autorizzazione secondo la giurisprudenza di legittimità richiamata al § 27 della sentenza) e §§ 83-102 (sull'assenza di un controllo giurisdizionale o indipendente *ex ante* o *ex post* effettivo, con specifico rigetto dell'idoneità del ricorso alle commissioni tributarie, §§ 88-94, ai tribunali civili, §§ 95-99, e al Garante del contribuente, §§ 100-102); si veda anche la conclusione generale al § 105.

⁵⁷ Si veda, ancora, *Ferrieri e Bonassisa c. Italia*, cit., §§ 111-117, ove la Corte, muovendo dal carattere sistemico della violazione riscontrata (§ 112), indica allo Stato convenuto la necessità di un quadro giuridico interno che precisi le circostanze e le condizioni di accesso ai dati bancari (§ 114) e preveda un controllo giurisdizionale o indipendente effettivo non subordinato all'emissione di un avviso di accertamento (§ 115). Sulla tendenza della Corte a sindacare non la singola misura, ma l'idoneità dell'assetto istituzionale e procedurale che la produce, si veda FIRAT, *Not the Decision but the Machinery: Is the ECtHR Developing a New Mode of Review?*, in *I•CONnect*, 25 agosto 2026.

dati bancari del segnalato non presuppone infatti neppure quel simulacro di autorizzazione gerarchica che la Corte ha giudicato insufficiente, fondandosi piuttosto sulle autonome potestà di polizia valutaria del Nucleo speciale; potestà che, essendo istituzionalmente preordinate alla sola finalità antiriciclaggio, non contemplan alcun vaglio, sia pure endoprocedimentale, dell'utilità dell'accesso ai fini fiscali. Sotto il secondo profilo, quello dell'assenza di un controllo indipendente *ex post*, le medesime carenze già riscontrate dalla Corte per il procedimento ordinario si riproducono identiche anche per il dato bancario acquisito in ambito valutario, senza che a esso corrisponda alcuna successiva verifica indipendente sulla proporzionalità della misura rispetto a un contribuente che, in ipotesi, potrebbe risultare del tutto estraneo a qualsiasi condotta di riciclaggio.

A questi due profili, entrambi già censurati dalla Corte per il procedimento ordinario, se ne aggiunge un terzo, che la sentenza Ferrieri e Bonassisa non ha dovuto affrontare ma che risulta specifico, e particolarmente aggravante, del canale qui esaminato. Mentre nel procedimento ex artt. 32 e 51 il contribuente può quantomeno, sia pure tardivamente e con le insufficienze rilevate dalla Corte, venire a conoscenza dell'autorizzazione una volta ricevuto l'avviso di accertamento, il regime di assoluta riservatezza che presidia l'identità del segnalante e il contenuto della SOS – funzionale, come si è visto, alla tutela del sistema di segnalazione preventiva – impedisce al segnalato di ricostruire, anche *ex post*, l'origine valutaria del dato bancario che ha condotto alla sua selezione per la verifica fiscale. Il contribuente attinto da una verifica innescata da una SOS rivelatasi infondata si trova, in altri termini, privato non solo delle garanzie che la Corte europea ha già giudicato insufficienti nel procedimento ordinario, ma financo della possibilità di individuare l'atto – la segnalazione – da cui l'ingerenza nella propria vita privata finanziaria, ai sensi dell'art. 8 C.E.D.U., ha tratto origine.

Vale infine sottolineare come la conclusione della Corte non risenta, semmai la rafforzi, di una circostanza che avrebbe potuto giocare in senso opposto. La Corte ha infatti riconosciuto che i dati bancari, in quanto informazioni «puramente finanziarie» prive della trasmissione di «dettagli intimi», godono di regola di un margine di apprezzamento particolarmente ampio

riconosciuto agli Stati contraenti; ed è proprio tenendo conto di tale ampio margine – non nonostante la sua assenza – che la Corte ha comunque ravvisato la violazione dell'art. 8 C.E.D.U.⁵⁸: segno che la soglia di inadeguatezza riscontrata nel sistema italiano era, in concreto, particolarmente elevata. Se il procedimento ex artt. 32 e 51, pur beneficiando di un margine di apprezzamento più permissivo proprio in ragione della natura finanziaria – e non intima – del dato, non ha comunque superato il vaglio della Corte, appare difficile ipotizzare un esito diverso per il canale valutario qui esaminato, privo persino di quel minimo di formalizzazione autorizzativa che la Corte ha comunque giudicato insufficiente.

Sul concorso di queste ragioni – l'assenza *tout court* di un'autorizzazione gerarchica motivata e l'aggiuntiva opacità imposta dalla riservatezza del segnalante – il canale valutario di acquisizione dei dati bancari risulta dunque difficilmente compatibile con quello stesso requisito della «qualità della legge» che la Corte ha ritenuto insoddisfatto persino nel procedimento che tale garanzia, per quanto carente, quantomeno formalmente prevedeva. Le indicazioni fornite dalla Corte ai sensi dell'art. 46 C.E.D.U. – la necessità di un quadro giuridico interno che precisi le circostanze e le condizioni di accesso ai dati bancari e preveda un controllo giurisdizionale o indipendente effettivo non subordinato all'emissione di un avviso di accertamento – sembrano dunque destinate, se recepite in sede di adeguamento legislativo, a investire anche il descritto canale di acquisizione in ambito valutario, quale ulteriore e distinto punto di ingresso dei dati bancari del contribuente nel procedimento tributario, sinora rimasto ai margini del dibattito innescato dalla pronuncia.

Un primo, significativo passo in questa direzione è stato compiuto, per il procedimento ordinario ex artt. 32 e 51, dalla stessa Corte di cassazione, che con le ordinanze gemelle nn. 19956 e 19960 del 2026 ha dato concreta

⁵⁸ Si veda *Ferrieri e Bonassisa c. Italia*, cit., § 58, ove la Corte ricorda che i dati bancari, quali informazioni «puramente finanziarie», non riguardano la trasmissione di dettagli intimi e che gli Stati godono, di conseguenza, di un ampio margine di discrezionalità in tale campo; § 105, ove la Corte, nel formulare la propria conclusione, dà atto espressamente di tale ampio margine di apprezzamento riconosciuto agli Stati contraenti in relazione ai dati bancari, in quanto informazioni di natura puramente finanziaria, e dell'importanza del fine perseguito dalle misure in campo fiscale, pur concludendo, nonostante tali fattori giocassero a favore dello Stato convenuto, per la sussistenza della violazione.

attuazione ai principi di *Ferrieri e Bonassisa*, affermando che l'autorizzazione ivi prevista costituisce «il titolo dell'ingerenza nei dati bancari del contribuente» e deve essere preesistente alle indagini nonché resa conoscibile nel suo contenuto essenziale, pena l'inutilizzabilità dei dati acquisiti e l'invalidità, anche solo parziale, dell'avviso di accertamento che su di essi si fonda³⁹. Se un simile principio è stato ritenuto necessario per un procedimento che prevede, quantomeno sulla carta, l'intervento di un organo sovraordinato, esso non può che valere, con maggiore intensità, per il canale valutario qui esaminato, privo persino di quel simulacro di controllo gerarchico oggi ritenuto insufficiente dalla stessa giurisprudenza di legittimità: la conferma interna dei principi convenzionali, per quanto non ancora estesa al canale valutario, rende dunque solo più evidente il vuoto di tutela che lo contraddistingue.

9.1. *Il deficit di sorveglianza istituzionale: l'estraneità di SIVA ai sistemi di controllo previsti per l'anagrafe tributaria e per le banche dati di polizia.* La rilevanza pratica, e dunque non solo meramente teorica, di tale patrimonio informativo trova oggi puntuale riscontro nelle risultanze della Commissione parlamentare d'inchiesta antimafia la quale, nella relazione approvata il 24 febbraio 2026 sul c.d. «dossieraggio» di esponenti politici e del mondo economico, ha ricostruito come un unico militare della Guardia di finanza, tra il 2019 e il 2022, abbia potuto consultare, all'interno della citata banca dati SIVA, 4.124 segnalazioni di operazioni sospette, 171 schede di analisi e 6

³⁹ Le ordinanze gemelle nn. 19956 e 19960 del 2026, *cit.*, offrono la prima applicazione di legittimità dei principi elaborati in *Ferrieri e Bonassisa c. Italia* al procedimento ordinario ex artt. 32, co. 1, n. 7 d.P.R. n. 600/1973 e 51, co. 2, n. 7 d.P.R. n. 633/1972, enunciando il principio secondo cui l'autorizzazione ivi prevista, pur conservando natura di atto preparatorio e organizzativo, «costituisce il titolo dell'ingerenza nei dati bancari del contribuente» e deve essere preesistente alle indagini nonché resa conoscibile nel suo contenuto essenziale, a pena di inutilizzabilità della documentazione bancaria acquisita e di invalidità, anche solo parziale, dell'avviso di accertamento fondato su di essa. Le due ordinanze richiamano altresì, quale ulteriore fronte in evoluzione, la questione rimessa alle Sezioni unite con Cass. Sez. trib., ord. interlocutoria 11 maggio 2026, n. 13696, *cit.*, in tema di inutilizzabilità dei dati e documenti acquisiti in esito ad accessi presso i locali dell'impresa non autorizzati o sorretti da autorizzazione non adeguatamente motivata. Nessuna delle due pronunce riguarda tuttavia, neppure incidentalmente, il canale di acquisizione in ambito valutario oggetto del presente contributo, che resta pertanto tuttora privo di specifici arresti di legittimità. Per un primo commento delle due ordinanze si veda ANDREANI, *Indagini bancarie: la Cassazione ridisegna i limiti*, in *Diritto della crisi*, 17 giugno 2026.

schede di approfondimento, relative a 1.531 persone fisiche e 74 persone giuridiche, per un totale complessivo stimato in oltre 10.000 accessi alle banche dati coinvolte⁶⁰. La Commissione ha ricondotto quanto accaduto non a una falla occasionale, bensì a un vero e proprio vuoto di vigilanza strutturale: i controlli sulla banca dati SIVA risultavano «limitati alla mera verifica degli orari di accesso» da parte dei militari, privi di qualunque sistema di *alert* automatico e di ogni analisi sul contenuto delle interrogazioni effettuate, in un contesto istituzionale nel quale né la Guardia di finanza né la Direzione nazionale antimafia e antiterrorismo, fruitrice ma non titolare della banca dati, risultavano concretamente in grado di vigilare sull'operato del militare infedele.

Il descritto vuoto di garanzie proprio del canale valutario non si esaurisce nel singolo procedimento di acquisizione dei dati bancari, ma investe, a monte, l'assetto stesso della sorveglianza istituzionale sulla banca dati SIVA. Diversamente da quanto accade per le altre grandi banche dati pubbliche italiane, SIVA non risulta infatti soggetta ad alcuna forma di controllo parlamentare o indipendente dedicato.

Da un lato, la Commissione parlamentare di vigilanza sull'anagrafe tributaria, istituita dall'art. 2 della L. 60/1976 ha competenza limitata, per espressa previsione normativa, alla vigilanza sull'anagrafe tributaria di cui al d.P.R. n. 605/1973 e sui sistemi informativi ad essa riferibili in materia di accertamento e riscossione dei tributi – competenza che attiene infatti a SERPICO, non a SIVA, come conferma la stessa ricostruzione comparativa offerta dalla Commissione parlamentare d'inchiesta sulle mafie⁶¹. Dall'altro lato, SIVA non rientra neppure nel sistema di controllo delineato dalla L. 121/1981, che istituisce il Centro elaborazione dati (CED) interforze presso il Dipartimento

⁶⁰ Si veda il documento Camera dei deputati – Senato della Repubblica, XIX Legislatura, *Doc. XXIII n. 15*, Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere (istituita con L. 2 marzo 2023, n. 22), *Relazione sull'attività della Commissione nell'ambito del filone di inchiesta sulle vicende relative al cosiddetto «dossieraggio» di esponenti politici e del mondo economico*, approvata dalla Commissione nella seduta del 24 febbraio 2026, spec. 14 (dati sugli accessi effettuati dal finanziere Pasquale Striano alla banca dati SIVA nel periodo 1° gennaio 2019 – 24 novembre 2022) e 178-183 (§§ 7.9-7.10, conclusioni sistemiche sul «vuoto di vigilanza» riscontrato).

⁶¹ Per un approfondimento del tema si rinvia a *Doc. XXIII n. 15, cit.*, 6.

della pubblica sicurezza, il cui controllo esterno è demandato al Garante per la protezione dei dati personali ai sensi dell'art. 10 – come sostituito – nell'ambito della direzione unitaria delle forze di polizia di competenza del Capo della polizia-direttore generale della pubblica sicurezza ex art. 5. Anche in questo caso, come emerge dalla medesima tabella comparativa, la L. n. 121/1981 costituisce la normativa di riferimento per lo SDI, non per SIVA, il quale trova il proprio fondamento esclusivamente nel d.lgs. 231/2007, nel d.lgs. 109/2007 e nei provvedimenti UIF.

Considerato che SIVA è una banca dati gestita al di fuori dei *server* del Ministero dell'interno e che non risultano, ad oggi, adottati provvedimenti del Ministro dell'interno ovvero del Capo della polizia che ne disciplinino specificamente il regime, ne risulta un vero e proprio vuoto di sorveglianza istituzionale, di cui la vicenda ricostruita dalla Commissione parlamentare d'inchiesta costituisce la più eloquente conferma empirica: nessun organo esterno alla Guardia di finanza dispone di poteri di controllo dedicati su SIVA, e la stessa Direzione nazionale antimafia e antiterrorismo, pur fruitrice delle segnalazioni, non ne è titolare e non dispone degli strumenti tecnici per un *audit* autonomo. Sul punto, la Commissione ha altresì parlato di un «cedimento strutturale del sistema dei controlli interni», generato da un'architettura che ha reso gli illeciti «non soltanto possibili, ma addirittura quasi fisiologici», e di «una condizione endemica, peraltro nota alle relative istituzioni titolari dei dati»⁶²: un'osservazione non priva di significato se raffrontata con le stesse parole rese in sede istituzionale dal Comandante generale della Guardia di finanza⁶³. Tale assetto, che affianca e per certi versi aggrava il *deficit* di garanzie convenzionali sopra illustrato, rafforza ulteriormente l'auspicio di un intervento legislativo che ridefinisca l'intero perimetro di controllo del canale valutario di acquisizione dei dati bancari;

⁶² Doc. XXIII n. 15, *cit.*, 178-179, ovvero il § 7.9 rubricato «Gli accessi alle banche dati e conclusioni sistemiche».

⁶³ Il Comandante generale della Guardia di finanza *pro tempore*, in sede di audizione parlamentare, pur illustrando il sistema di controlli allora vigente su SIVA, ha testualmente riconosciuto: «Siamo tuttavia pienamente consapevoli dell'esigenza di verificare periodicamente il livello di adeguatezza delle misure organizzative interne e degli strumenti di controllo adottati»; così in Audizione del Gen. C.A. Andrea De Gennaro, 22 marzo 2024, *cit.*, 15.

non solo nei confronti del singolo contribuente inciso, ma anche sul piano della sorveglianza sistemica sulla banca dati in quanto tale.

9.2. I diritti del segnalato: il confronto con le banche dati di polizia e l'assenza di un accesso realmente conoscitivo nel canale valutario. Il descritto *deficit* di sorveglianza istituzionale si riflette, a un livello ulteriore, sullo statuto individuale dei diritti riconosciuti al soggetto la cui posizione sia registrata in una banca dati pubblica, e merita pertanto una trattazione autonoma. Per le banche dati di polizia in senso proprio – quali lo SDI, gestito nell'ambito del CED interforze – disciplinate dal d.lgs. 51/2018, di recepimento della Direttiva (UE) 2016/680, l'interessato dispone di un diritto di accesso esercitabile su istanza, volto a ottenere la conferma dell'esistenza di un trattamento che lo riguardi e la comunicazione dei dati in forma intelligibile; ciò anche al fine di consentire all'interessato una verifica dei dati che lo riguardano ed un loro eventuale aggiornamento. Tale diritto può essere ritardato, limitato o escluso solo quando sussista un segreto d'ufficio o d'indagine, ai sensi degli artt. 11 e 14 del medesimo decreto, con rinvio agli istituti di cui agli artt. 116 e 335 c.p.p.⁶⁴: una limitazione, dunque, per sua natura eccezionale, motivata caso per caso e destinata a venir meno con la chiusura del procedimento o con l'accesso agli atti da parte dell'imputato. In caso di diniego, l'interessato può inoltre proporre reclamo al Garante per la protezione dei dati personali, che dispone di un potere di accesso indiretto ai sensi dell'art. 160 del Codice *Privacy*⁶⁵.

Il quadro muta però radicalmente per il segnalato SOS. Infatti, l'art. 39 del d.lgs. 231/2007 pone un divieto assoluto – presidiato addirittura da

⁶⁴ Artt. 11 e 14 d.lgs. 18 maggio 2018, n. 51, che consentono di ritardare, limitare o escludere i diritti dell'interessato quando sussista un segreto d'ufficio o un segreto d'indagine, rispetto al quale operano gli appositi istituti previsti dal codice di procedura penale (artt. 116 e 335 c.p.p.). Per il CED interforze rileva inoltre la disciplina speciale dell'art. 10, co. 3-5 L. 1° aprile 1981, n. 121, che consente di non comunicare al richiedente i dati la cui comunicazione potrebbe pregiudicare operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone notizia al Garante per la protezione dei dati personali (co. 4).

⁶⁵ Art. 160 d.lgs. 196/2003; cfr. Polizia di Stato, *C.E.D. Interforze - Informativa privacy* (art. 10 d.lgs. 18 maggio 2018, n. 51), in www.poliziadistato.it/articolo/37262, 21 gennaio 2015, agg. 29 settembre 2026, § 3: «Nel caso in cui alla richiesta non sia fornita una risposta ritenuta soddisfacente, l'interessato può proporre reclamo al Garante per la protezione dei dati personali».

un'apposita fattispecie di rilevanza penale – di dare comunicazione al cliente interessato dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza di indagini o approfondimenti in materia di riciclaggio⁶⁶. Sul piano del diritto di accesso ai sensi degli artt. 15-22 del Regolamento, l'art. 2-*undecies*, co. 1, lett. a), del Codice *Privacy* stabilisce, inoltre, che tali diritti «non possono essere esercitati» – non semplicemente limitati – qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto agli interessi tutelati in materia di riciclaggio: un pregiudizio che la prassi applicativa tende a presumere pressoché automaticamente, coincidendo esso con la stessa *ratio* del sistema di prevenzione⁶⁷. Il co. 3 del medesimo art. 2-*undecies* prevede, a mitigazione, un accesso mediato tramite il Garante, modellato sulle medesime modalità di cui all'art. 160 del Codice previste per i dati di polizia; l'esito di tale accesso si risolve tuttavia nella sola comunicazione all'interessato che le verifiche necessarie sono state eseguite, senza che gli venga mai rivelata l'esistenza stessa della segnalazione, il suo contenuto, il segnalante o i motivi del sospetto⁶⁸.

L'asimmetria tra i due regimi non è dunque meramente formale, ma sostanziale. Nel caso delle banche dati di polizia, la compressione dei diritti dell'interessato è ancorata a una ragione contingente – il segreto investigativo – per sua natura reversibile: essa cade con l'esaurimento della fase che la giustifica, quando cioè l'interessato, ove sottoposto a procedimento penale, acquisisce piena conoscenza degli atti a fini di difesa. Nel caso della segnalazione antiriciclaggio, per contro, l'esclusione del diritto di accesso non

⁶⁶ Ai sensi dell'art. 39, co. 1 d.lgs. 231/2007, «fuori dai casi previsti dal presente decreto, è fatto divieto ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo».

⁶⁷ Ciò ai sensi dell'art. 2-*undecies*, co. 1, lett. a) d.lgs. 196/2003; per un'applicazione, si rinvia al provvedimento del Garante per la protezione dei dati personali n. 129 del 13 aprile 2023, doc. web n. 9888457, ove l'Autorità dà atto che l'esclusione del diritto di accesso mira a scongiurare che «il soggetto cui è riferita l'operazione» venga informato della presenza a suo carico di indici di anomalia, così «vanificando la possibilità che i fatti di riciclaggio siano scoperti».

⁶⁸ Art. 2-*undecies*, co. 3 Codice *Privacy*, che estende ai casi di cui alla lett. a) del co. 1 – tra cui l'antiriciclaggio – la possibilità di esercitare i diritti dell'interessato «anche tramite il Garante con le modalità di cui all'articolo 160»: in tale ipotesi, ai sensi del medesimo comma, «il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie [...] nonché del diritto dell'interessato di proporre ricorso giurisdizionale», senza alcuna comunicazione nel merito.

è collegata ad alcuna specifica fase procedimentale, ma discende dalla stessa struttura del sistema di prevenzione, ed è pertanto destinata a permanere in eterno anche quando la segnalazione si sia rivelata infondata e sia stata archiviata senza alcun seguito investigativo, proprio l'ipotesi che, come si è innanzi visto, qui maggiormente rileva. Ne discende che il segnalato SOS - a differenza tanto dell'indagato quanto della persona i cui dati siano registrati in una banca dati di polizia - resta privo, come già rilevato, di qualunque strumento di conoscenza e di reazione, se non nella denegata ipotesi in cui la segnalazione sfoci in un procedimento penale a suo carico.

10. *Considerazioni conclusive.* Il quadro che emerge dall'incrocio dei diversi profili qui esaminati restituisce, a ben vedere, l'immagine di una tutela strutturalmente asimmetrica: il segnalato subisce le conseguenze - talora rilevanti, quali la gestione dei propri dati finanziari all'interno di una banca dati priva di controllo e finanche l'apertura di una verifica fiscale - di una segnalazione che può rivelarsi infondata o pretestuosa, senza disporre né della conoscenza dell'atto che le origina, né di uno strumento di reazione nei confronti del segnalante, né infine di un presidio sanzionatorio che responsabilizzi *ex ante* quest'ultimo, come invece avviene, in modo organico, nel sistema *whistleblowing* generale di cui al d.lgs. 24/2023. Nemmeno le più recenti Istruzioni UIF, pur intendendo incidere sul contenimento *ex ante* dell'*over-reporting* difensivo, possono colmare tale vuoto, di rango primario. È dunque auspicabile, *de iure condendo*, un intervento legislativo di adeguamento del d.lgs. 231/2007 al modello sanzionatorio previsto dall'art. 23 della Direttiva (UE) 2019/1937, magari strutturato come quello recepito dall'art. 21 d.lgs. 24/2023, sia pure in occasione del recepimento dell'art. 60 della Direttiva (UE) 2024/1640, entro il termine generale previsto il 10 luglio 2027: è in particolare necessario da un lato introdurre una sanzione amministrativa o penale dedicata e da un altro lato codificare la perdita delle tutele di riservatezza per la mala fede accertata e un meccanismo di risarcimento del danno correlato all'iscrizione in banca dati rivelatasi infondata. Questa è la via che appare più coerente per colmare il descritto difetto di coordinamento, restituendo organicità al sistema e riducendo il

rischio, sopra evidenziato, di uno stimolo strutturale alla segnalazione difensiva indiscriminata. A tale intervento dovrebbe accompagnarsi, per le ragioni sopra esposte, l'estensione al canale di acquisizione valutaria dei dati bancari destinati ad avere un utilizzo fiscale delle medesime garanzie procedurali che la Corte europea dei diritti dell'uomo, con i principi esposti nella sentenza *Ferrieri e Bonassisa c. Italia*, ha imposto per il procedimento ordinario di indagine finanziaria; se ciò non avvenisse, infatti, permarrebbe un varco sistemico attraverso cui gli effetti pregiudizievoli della SOS infondata continuerebbero a prodursi in sede fiscale al riparo da ogni controllo indipendente.

Il medesimo intervento dovrebbe investire anche la sorveglianza istituzionale su SIVA e i diritti del segnalato: da un lato, attribuendo a un organo esterno alla Guardia di finanza - ad esempio, il Garante per la protezione dei dati personali, in coerenza con il ruolo già svolto per il CED interforze, o la Commissione parlamentare di vigilanza sull'anagrafe tributaria, mediante estensione di competenza - un potere di controllo dedicato sulla banca dati valutaria; dall'altro, riconoscendo al segnalato un accesso realmente conoscitivo, analogo a quello previsto per le banche dati di polizia, che non si esaurisca - come avviene oggi ai sensi dell'art. 2-undecies, co. 3 del Codice *Privacy* - nella mera certificazione dell'avvenuto controllo formale.

In definitiva, il sistema antiriciclaggio vigente conosce *red flags* soltanto per il segnalato: nessun segnale d'allarme, e nessuna conseguenza, è previsto per chi segnala il falso o non si cura di verificare quanto riferisce. Colmare questo vuoto non è un mero affinamento tecnico del d.lgs. 231/2007, ma una condizione di legittimità dell'intero apparato delle segnalazioni preventive, la cui credibilità - e la cui stessa attitudine di orientare correttamente le risorse investigative verso i fenomeni di riciclaggio realmente meritevoli di attenzione - dipende dalla capacità di proteggere anche chi da quell'apparato viene, ingiustamente, attinto.