

Il trojan di Stato e la difesa strutturalmente limitata: tre vulnera strutturali nella disciplina italiana del captatore informatico

di Giuseppe Daniele Riefolo

<https://www.drforensics.it/>

Nota metodologica. Quanto segue è un contributo di critica scientifica e giuridica, costruito su norme vigenti, provvedimenti giurisdizionali pubblici e atti già versati in procedimenti penali (verbali d'udienza, informative tecniche, corrispondenza tra la società fornitrice del servizio e uffici di Procura). Ogni affermazione di fatto è ancorata a una fonte citata; le valutazioni sono espresse come lettura critica del dato normativo e giurisprudenziale, non come addebito di condotte a soggetti individuati. Dove si richiamano dichiarazioni rese a verbale, si tratta di testimonianze assunte in pubblica udienza su fatti di rilevante interesse pubblico, riportate nei limiti di verità, pertinenza e continenza propri del diritto di cronaca e di critica giudiziaria.

1. Premessa

Il captatore informatico (il cosiddetto trojan di Stato) è oggi lo strumento investigativo più invasivo previsto dall'ordinamento italiano: trasforma il dispositivo dell'indagato in un microfono ambientale itinerante, capace di seguirlo ovunque si trovi. Il legislatore lo ha ammesso a condizioni via via più permissive dal 2017 a oggi, mentre la giurisprudenza ne ha progressivamente definito i confini applicativi. Altro è, tuttavia, disciplinare quando il captatore possa essere legittimamente impiegato; altro è garantire che, una volta impiegato, la difesa possa verificare come la prova si sia concretamente formata, lungo l'intero suo percorso: dal microfono del telefono al server della Procura.

È su questo secondo piano, quello del controllo difensivo sulla genesi della prova, che si annidano tre lacune che le riforme succedutesi non hanno colmato e che, a nostro avviso, la riflessione della classe forense non ha ancora adeguatamente sistematizzato.

2. Il quadro normativo in sintesi

Provvedimento

D.L. 152/1991 conv. L. 203/1991, art. 13

L. 103/2017 (delega) e D.Lgs. 216/2017

L. 3/2019 ("spazzacorrotti")

D.L. 161/2019 conv. L. 7/2020

D.L. 105/2023 conv. L. 137/2023

L. 114/2024 ("riforma Nordio")

L. 47/2025 ("legge Zanettin")

Contenuto essenziale

Regime derogatorio per la criminalità organizzata, matrice del regime speciale del captatore

Introduce nel codice l'uso del captatore su dispositivo portatile (art. 266 comma 2 e 2-bis c.p.p.)

Estende il regime derogatorio ai delitti dei pubblici ufficiali contro la P.A.

Assetto oggi vigente: art. 266 comma 2-bis, art. 268 comma 3 (garanzia tecnica degli impianti in Procura), art. 89 disp. att. c.p.p.

Richiede "autonoma valutazione" del giudice sulle ragioni concrete del ricorso al captatore (art. 267 comma 1 c.p.p.)

Tutele rafforzate su comunicazioni difensive e divieto di pubblicazione

Limite di durata massima delle intercettazioni (45 giorni, salvo deroghe)

Il perno delle garanzie difensive resta l'art. 268 comma 3 c.p.p.: le operazioni di registrazione devono avvenire "esclusivamente" mediante impianti installati presso la Procura, a pena, testualmente, di inutilizzabilità. È una norma pensata per assicurare che il luogo in cui la prova si cristallizza sia sotto il controllo dell'autorità giudiziaria, e non del fornitore privato del servizio.

3. Il perimetro tracciato dalla giurisprudenza

Le Sezioni Unite Scurato (Cass. S.U. n. 26889/2016) hanno per prime riconosciuto la natura "itinerante" del captatore. Le Sezioni Unite Cavallo (n. 51/2019) hanno definito i limiti di utilizzabilità dei risultati in procedimenti diversi. Un filone più recente, riconducibile, tra le altre, a Cass. n. 2707/2020, ha introdotto una distinzione decisiva per il tema che qui interessa: quella tra registrazione (protetta dalla sanzione di inutilizzabilità ex art. 268 comma 3 c.p.p.) e mero transito tecnico dei dati captati (non protetto, perché non equiparabile alla registrazione). Su questa distinzione si regge la legittimità dell'architettura tecnica oggi diffusa (server di captazione CSS, server di smistamento HDM, server di registrazione finale IVS), anche quando i primi due nodi della catena non si trovano fisicamente in Procura.

Un più recente arresto, Cass. Sez. III n. 18464/2025¹, si muove nella direzione opposta, e merita di essere isolato perché incide proprio sul nodo appena descritto. La Corte ha equiparato, ai fini dell'accesso difensivo, i file di log delle operazioni di captazione ai supporti contenenti le registrazioni, imponendo al pubblico ministero di metterli a disposizione della difesa con congruo anticipo rispetto all'udienza di riesame. La ratio è tanto semplice quanto rilevante: se la distinzione tra registrazione e mero transito si regge sulla premessa che il dato, nel passaggio da CSS a HDM a IVS, non subisca alterazioni, l'unico modo per verificare che quella premessa sia effettivamente vera, e non una mera dichiarazione del fornitore del servizio, è la lettura dei log di sistema, gli unici elementi tecnici in grado di attestare cosa sia realmente accaduto durante il transito. Equiparando i log ai supporti, la Sezione III ha dunque riconosciuto, sia pure indirettamente, che il controllo difensivo non può arrestarsi al server finale, ma deve poter raggiungere anche il segmento intermedio che la giurisprudenza precedente aveva qualificato come esente da garanzie formali.

Sono dunque due linee di segno diverso. La prima allarga la zona esente da controllo formale; la seconda offre alla difesa lo strumento, in linea di principio, per verificare se quella zona sia stata utilizzata in modo conforme alla sua qualificazione giuridica. Il condizionale è d'obbligo: come si vedrà nei paragrafi che seguono, lo strumento riconosciuto da Cass. n. 18464/2025 incontra, nella prassi, due ostacoli che ne ridimensionano fortemente la portata: l'assenza di un obbligo di conservazione dei log per un tempo commisurato ai tempi del processo (v. *infra*, par. 5) e l'impossibilità, per la difesa, di verificare in modo indipendente ciò che i log, quando ancora esistono, effettivamente attestano (v. *infra*, par. 6). È da qui che muove la parte propositiva di questo contributo.

4. Primo vulnus: la zona franca tra "registrazione" e "transito"

La distinzione registrazione/transito non è scritta dal legislatore: è un'elaborazione giurisprudenziale. E coincide, con una precisione che merita di essere sottolineata, con la zona tecnicamente più vulnerabile dell'intera catena. Dalle deposizioni acquisite in un procedimento relativo all'uso del captatore nei confronti di un magistrato (Tribunale di Perugia, sezione GIP/GUP, udienza del 3 maggio 2021) risulta, per stessa ammissione del responsabile tecnico della società fornitrice: assenza di cifratura del dato all'epoca dei fatti ("all'epoca no"), assenza di firma digitale o hash sui file captati, credenziali amministrative comuni a tutti gli amministratori di sistema sul CSS e sull'HDM, accesso in linea teorica sempre possibile per l'amministratore di sistema su qualunque server della catena, con possibilità, sempre nelle parole del teste, di "alterare il dato" e di farlo "manualmente" nell'arco dei pochi minuti in cui il file staziona sul server intermedio.²

La sanzione di inutilizzabilità dell'art. 268 comma 3 c.p.p., la più severa prevista dal sistema, protegge dunque il segmento più sorvegliato (il server finale, IVS) e lascia fuori dal proprio perimetro il segmento meno sorvegliato (CSS e HDM), proprio perché la giurisprudenza lo ha qualificato come "mero transito". È una torsione che inverte la ratio della norma: la garanzia formale si concentra dove il rischio sostanziale è minore.

A ciò si aggiunge un dato che, per quanto ci risulta, non è stato ancora adeguatamente valorizzato in sede difensiva: la stessa documentazione tecnica versata in atti in alcuni procedimenti descrive la possibilità di accesso da postazioni remote, collegate al server di registrazione tramite VPN, "installate nei locali della Procura o nelle sedi remote".³ Se l'operatività sul dato può avvenire da remoto, la collocazione fisica del server presso gli uffici di Procura, il presupposto su cui l'art. 268 comma 3 c.p.p. fonda l'intera garanzia, protegge la sede della macchina, non la sede da cui la macchina viene amministrata. È uno scarto che il testo di legge non contempla e che la giurisprudenza finora non ha affrontato.

5. Secondo vulnus: un diritto riconosciuto sulla carta e reso inefficace dal tempo

Il diritto di accesso ai file di log riconosciuto da Cass. n. 18464/2025 (v. *supra*, par. 3) presuppone, tuttavia, che i log esistano ancora nel momento in cui la difesa li richiede: nessuna norma impone alla società fornitrice, o alla Procura, di conservarli per un periodo commisurato alla durata reale di un procedimento penale, che tra indagini, dibattimento ed eventuali gradi di impugnazione può tranquillamente superare il quinquennio.

Non si tratta di un'ipotesi di scuola. In un procedimento per delitti di criminalità organizzata relativo a un'intercettazione mediante captatore avviata nel 2017, la stessa società fornitrice ha comunicato formalmente alla Procura procedente, nel marzo 2022, che "non sono raccolti log sulle interfacce di rete, né log del firewall e non sono più presenti i log del sistema operativo riferiti ai periodi temporali nei quali sono stati eseguiti i decreti di intercettazione".⁴ Non un'ipotesi contestata: una comunicazione ufficiale, agli atti, che attesta la scomparsa del materiale che sarebbe l'unico mezzo per verificare, anche solo in astratto, se l'accesso teoricamente sempre possibile dell'amministratore di sistema si sia mai tradotto in un intervento concreto.

Il diritto di accesso riconosciuto da Cass. 18464/2025 è dunque, nella pratica, condizionato a un fattore del tutto estraneo alla volontà della difesa: la rapidità con cui viene esercitato rispetto ai tempi fisiologici del processo, in assenza di qualunque obbligo legale di conservazione. Per i procedimenti più risalenti, quel diritto è già oggi, strutturalmente, privo di oggetto.

6. Terzo vulnus: nessuna verifica indipendente, solo dichiarazioni

Il terzo profilo è il più insidioso perché non riguarda un'ipotesi teorica di vulnerabilità, ma la concreta possibilità per la difesa di controllare ciò che le viene dichiarato.

In un procedimento per criminalità organizzata relativo a un R.I.T. attivato nell'ottobre 2017, il consulente tecnico della difesa ha formalmente richiesto alla Procura procedente, nel maggio 2021, l'elenco degli indirizzi IP di transito e, per ciascuno, i log della relativa macchina per il periodo di permanenza dei dati captati.⁵ La società fornitrice, in una nota tecnica del gennaio 2021 relativa allo stesso R.I.T., aveva dichiarato che le intercettazioni "vengono fatte in modo tale che la comunicazione dal captatore venga stabilita direttamente con il relativo server installato in Procura, quindi non vengono utilizzati Proxy di appoggio".⁶ Circa quattro mesi e mezzo dopo, in risposta alla richiesta specifica del consulente, la stessa società, tramite la Procura, ha comunicato che, per la gran parte della durata di quella stessa intercettazione (da ottobre 2017 ad aprile 2019), i dati erano transitati non su un server in Procura, ma su un server collocato presso la sede privata della società a Napoli.⁷

Non è in discussione, in questa sede, la ragione di quella discrasia, che potrebbe derivare da

un'imprecisione nella prima risposta, da un fraintendimento della domanda o da altro. Ciò che rileva, ai fini del presente contributo, è che a fronte della medesima domanda tecnica, sullo stesso procedimento, la risposta ottenuta è cambiata in modo sostanziale in pochi mesi, e che la richiesta di log, formulata espressamente dal consulente, non ha ricevuto risposta in termini di dati tecnici verificabili, ma solo in termini di narrazione descrittiva e di indirizzi IP.

A questo si affianca un secondo dato, di segno concorde: gli accertamenti tecnici svolti sui medesimi server hanno rilevato, per lo stesso procedimento, migliaia di file rimasti sul server di smistamento ben oltre il tempo di transito dichiarato (mediamente 2-3 minuti), comprese decine di registrazioni audio rimaste ferme per oltre venti ore. Un dato quantitativo, non un'opinione, che smentisce nei fatti la premessa (il "mero transito") su cui si fonda l'esenzione di quel segmento dalle garanzie dell'art. 268 comma 3 c.p.p.

Quando un reperto di questo tipo emerge, la reazione istituzionale osservabile in un procedimento collegato (relativo, questa volta, a un'intercettazione disposta nei confronti di un magistrato) è stata di minimizzazione: l'ordinanza del giudice, chiamata a valutare il ritrovamento di file residui sul server intermedio, lo ha qualificato come prova che il sistema "avesse correttamente cancellato pressoché integralmente il flusso intercettato", attribuendo la presenza dei residui a "un mero errore di sistema", senza che la circostanza fosse oggetto di approfondimento tecnico autonomo, ad esempio tramite perizia.

Il punto non è se quella specifica valutazione giudiziale fosse corretta nel merito. Il punto è strutturale: la difesa non dispone, in nessuna fase, di un dato tecnico proprio e autoverificabile con cui confrontare la versione fornita dal soggetto privato che gestisce il sistema. Riceve dichiarazioni, non prove; e quando le dichiarazioni cambiano, o quando i fatti tecnici (i file residui) sembrano contraddirle, l'unico foro di verifica è lo stesso circuito (fornitore, Procura, giudice) che ha prodotto la dichiarazione originaria.

7. Perché è una violazione del diritto di difesa, e non solo un disagio pratico

Gli artt. 24 e 111 della Costituzione, e l'art. 6 CEDU, garantiscono non un generico diritto di essere informati, ma un diritto di partecipare effettivamente alla formazione della prova e di contestarla nel contraddittorio. Una prova che si forma attraverso un processo tecnico che la difesa non può in alcun modo verificare, perché il codice sorgente è segreto industriale, perché i log non esistono più quando servono, perché le dichiarazioni sull'architettura cambiano nel tempo senza che nessuno le riscontri in modo indipendente, non è una prova sottratta al controllo difensivo per un limite contingente. È una prova strutturalmente sottratta al contraddittorio sulla sua stessa genesi.

Lo standard che la giurisprudenza richiede alla difesa per far scattare l'inutilizzabilità, l'indicazione di elementi concreti di manomissione, non di una mera possibilità astratta, è, in questo contesto, logicamente inesigibile nell'ipotesi peggiore: una cancellazione selettiva ben eseguita non lascia, per definizione, alcuna incoerenza visibile da segnalare. Pretendere la prova concreta di ciò che, se davvero accaduto, sarebbe stato costruito apposta per non lasciare traccia equivale, nella sostanza, a rendere la garanzia dell'art. 268 comma 3 c.p.p. inesigibile proprio nell'ipotesi che la norma dovrebbe prevenire.

8. Proposte de lege ferenda: percorsi attuativi

Un contributo che si limiti alla denuncia senza indicare una via d'uscita rende un cattivo servizio alla comunità forense. Le direttrici che seguono sono ordinate non per importanza, ma per il diverso strumento che ne consentirebbe l'attuazione: alcune richiedono un intervento del legislatore, una è raggiungibile anche in via amministrativa o tecnico-regolamentare, una richiede una modifica ordinamentale più ampia. Per ciascuna si indica anche la via attraverso cui l'esigenza potrebbe imporsi all'attenzione del legislatore.

a) *Obbligo di conservazione* (via legislativa). Introduzione di un obbligo legale di conservazione dei log di sistema, di accesso e di audit dei server impiegati per la captazione, per un periodo non inferiore alla durata massima ragionevole del procedimento (indagini più gradi di giudizio), assistito da sanzione di inutilizzabilità in caso di distruzione non giustificata prima di tale termine. È l'intervento più urgente: senza di esso, il diritto di accesso riconosciuto da Cass. n. 18464/2025 resta, come illustrato al par. 5, privo di oggetto per i procedimenti più risalenti.

b) *Estensione degli strumenti di congelamento dei dati* (via legislativa, su normativa già esistente). Estensione all'infrastruttura del captatore degli strumenti di "congelamento" dei dati già previsti dall'art. 254-bis c.p.p. per i fornitori di servizi di comunicazione, da disporsi fin dall'avvio delle operazioni, quando la conservazione è ancora tecnicamente possibile. Si tratterebbe di un intervento su una norma già collaudata, non della creazione di un istituto nuovo.

c) *Hash crittografico all'origine* (via legislativa o, in subordine, tecnico-regolamentare). Apposizione di un hash crittografico al momento della captazione sul dispositivo, e non soltanto, come oggi eventualmente avviene, in sede di estrazione forense per il giudizio, in modo da ancorare l'integrità del dato al momento della sua genesi e non a un momento successivo, spesso di molti anni dopo. Trattandosi di un requisito tecnico, potrebbe essere introdotto anche in via di capitolato tecnico o di provvedimento regolamentare, in attesa di un consolidamento legislativo.

d) *Ridefinizione legislativa del concetto di "registrazione"* (via legislativa, suscettibile di essere sollecitata in via incidentale). Ridefinizione del concetto di "registrazione" ai fini dell'art. 268 comma 3 c.p.p., che includa espressamente ogni fase in cui il dato captato sosta, anche temporaneamente, su un server esterno agli uffici giudiziari, indipendentemente dalla sua qualificazione giurisprudenziale come "transito". È il punto sul quale un intervento spontaneo del legislatore appare meno probabile, ma potrebbe essere sollecitato da un'eccezione di legittimità costituzionale sollevata, in un procedimento concreto, sull'art. 268 comma 3 c.p.p., nella parte in cui, per come interpretato dal diritto vivente, non riconduce il segmento di transito sotto le medesime garanzie formali. Una pronuncia della Corte costituzionale, anche non additiva, che segnali l'esigenza di ricondurre l'intero percorso del dato captato, e non solo il suo approdo finale, sotto la sanzione di inutilizzabilità, offrirebbe al legislatore l'occasione, se non lo stimolo, per intervenire in modo organico.

e) *Organismo tecnico terzo di validazione* (via ordinamentale). Istituzione di un organismo tecnico terzo, indipendente dal fornitore e dall'accusa, incaricato della validazione periodica dei sistemi di captazione in uso presso le Procure, con accesso, nel rispetto del segreto industriale, tramite modalità riservate analoghe a quelle già previste per altri ambiti sensibili, quantomeno alla verifica dell'integrità dei meccanismi di cifratura, cancellazione e audit dichiarati dal fornitore. È l'intervento di maggior respiro, e presumibilmente il più lontano nel tempo, ma è anche quello che offrirebbe alla difesa, per la prima volta, un contraddittorio tecnico reale e non meramente cartolare.

9. Conclusioni

Il captatore informatico non è, di per sé, uno strumento incompatibile con le garanzie difensive. Lo diventa quando il sistema che lo circonda, normativo, tecnico, procedurale, rende strutturalmente impossibile, per la difesa, verificare ciò che le viene dichiarato. I tre profili qui esaminati non sono ipotesi accademiche: sono documentati da atti processuali, corrispondenza ufficiale e accertamenti tecnici già versati in procedimenti reali. La comunità forense ha, a nostro avviso, il dovere di portare questi rilievi, con il rigore tecnico e la precisione delle fonti che meritano, davanti ai giudici di merito, e di portarli con la medesima determinazione all'attenzione del legislatore, prima che la prassi consolidi definitivamente un modello di prova che la difesa può soltanto subire, mai verificare.

Riferimenti normativi e giurisprudenziali essenziali

Normativa: Cost., artt. 24, 111; CEDU, art. 6; c.p.p., artt. 266, 266-bis, 267, 268, 270, 271, 360; disp. att. c.p.p., art. 89; D.L. 152/1991 conv. L. 203/1991; L. 103/2017; D.Lgs. 216/2017; L. 3/2019; D.L. 161/2019 conv. L. 7/2020; D.L. 105/2023 conv. L. 137/2023; L. 114/2024; L. 47/2025.

Giurisprudenza: Cass. S.U. n. 26889/2016 (Scurato); Cass. S.U. n. 51/2019 (Cavallo); Cass. S.U. Civ. n. 22302/2021; Cass. n. 2707/2020; Cass. n. 3591/2022; Cass. Sez. III n. 18464/2025; Cass. n. 29382/2025; C. Cost. n. 366/1991, n. 170/2023.

Note

¹ Cass. pen., Sez. III, sent. n. 18464/2025 (data di deposito non riportata nelle fonti secondarie consultate; si raccomanda verifica sul testo integrale prima della pubblicazione).

² Deposizione del teste Ing. Duilio Bianchi, ai sensi dell'art. 210 c.p.p., Tribunale di Perugia, Sezione Penale GIP/GUP, udienza del 3 maggio 2021, Proc. R.G. 1390/19 – 6652/18 R.G.N.R. ("Palamara Luca + altri"): sull'assenza di cifratura del dato all'epoca dei fatti ("all'epoca no"), sull'assenza di firma digitale o hash, sull'accesso in astratto sempre possibile dell'amministratore di sistema e sulla possibilità teorica di alterazione manuale del dato nell'arco del tempo medio di transito (dichiarato in circa 137 secondi).

³ Nota tecnica RCS S.p.A. del 28 gennaio 2021, rif. RCS21-0502, indirizzata alla Procura della Repubblica presso il Tribunale di Reggio Calabria – Direzione Distrettuale Antimafia, Proc. Pen. n. 408/19 R.G.N.R. DDA – R.I.T. 1603/17, a firma dell'Ing. Duilio Bianchi, Direttore Divisione IP: "L'ascolto dei dati può essere fatto tramite la postazione fornita da RCS con il software client denominato IVS Viewer. La postazione può essere installata nei locali della Procura o nelle sedi remote, da dove si può raggiungere il server IVS tramite una connessione VPN."

☞ Nota della Procura della Repubblica presso il Tribunale di Reggio Calabria – Direzione Distrettuale Antimafia, Proc. n. 408/19 R.G.N.R. mod. 21 DDA – N. 53/22 Reg. Mast., datata 21 marzo 2022, a firma del Sostituto Procuratore Dott.ssa Antonella Crisafulli, indirizzata al CTP Giuseppe Daniele Riefolo (per c.c. Avv.ti Guido Contestabile e Giuseppe Milicia), in risposta a richiesta del CTP del 9 marzo 2022 relativa ai R.I.T. 1603/17, 2160/18, 242/19 e 1573/19, e richiamante la nota tecnica RCS n. RCS22-1243 del 17 marzo 2022 (punto 10 della nota).

☞ Richiesta del CTP Giuseppe Daniele Riefolo, PEC del 28 maggio 2021, ore 09:07, Proc. Pen. n. 408/2019 R.G.N.R. DDA – n. 2863/2019 R.G. GIP DDA.

☞ Nota tecnica RCS S.p.A. del 28 gennaio 2021, rif. RCS21-0502, Proc. Pen. n. 408/19 R.G.N.R. DDA – R.I.T. 1603/17, a firma dell'Ing. Duilio Bianchi.

☞ Nota della Procura della Repubblica presso il Tribunale di Reggio Calabria – DDA, Proc. n. 408/2019 R.G.N.R. mod. 21, datata 9 giugno 2021, a firma della Dott.ssa Giulia Pantano, richiamante la nota tecnica RCS n. RCS21-2927 del 4 giugno 2021.

☞ Relazione del CT Giuseppe Daniele Riefolo, Proc. n. 408/19 R.G.N.R. DDA, R.I.T. 1603/17: 2.384 file rilevati sull'HDM oltre il tempo di transito dichiarato, tra cui 65 file audio della durata di 1-21+ ore.

☞ Ordinanza del GUP presso il Tribunale di Perugia, Proc. n. 1390/19 R.G. – 6652/18 R.G.N.R. ("Palamara Luca + altri"), Perugia, 17 giugno 2021, Dott. Piercarlo Frallotta.