

M-DG	
PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI SASSARI Ufficio Protocollo 09005402107	
Prot. n° 939	del 8.04.2026
Timbro apposto dopo la firma digitale	



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI SASSARI

OGGETTO: Direttiva in materia di acquisizione di dati digitali contenuti in telefoni cellulari, computer e altre memorie informatiche, ai sensi dell'art. 2, comma 2, della circolare CSM sull'organizzazione degli uffici di Procura.

La materia dell'acquisizione dei dati digitali contenuti negli archivi informatici - siano essi telefoni cellulari, personal computer o altri supporti - è stata oggetto di numerose pronunce della Corte di cassazione, alle quali si aggiungono, con riferimento ad alcune tematiche particolari, la giurisprudenza della Corte costituzionale (sentenza n. 170 del 7 giugno 2023) e della Corte di Giustizia europea (Grande Camera, 4 ottobre 2024, Causa C-548/21), nonché, da ultimo, Cass. pen., Sez. 2, n. 40451 del 13 novembre 2025.

La particolare delicatezza delle problematiche coinvolte, che toccano la tutela della riservatezza e dei dati sensibili, la genuinità della prova, il diritto di difesa e il diritto al contraddittorio, hanno indotto il legislatore a predisporre una disciplina organica, oggetto del DDL 806, attualmente in corso di esame davanti alla Camera dei Deputati. In attesa dell'eventuale introduzione di tale disciplina, considerata l'urgenza di dettare linee operative uniformi e rilevato che su tale materia sono intervenute, anche di recente, diverse decisioni di legittimità tra loro non sempre concordi, si dettano le seguenti disposizioni, incidenti su aspetti che concernono la correttezza dell'esercizio dell'azione penale e il rispetto del principio del giusto processo.

Va premessa, anzitutto, una rassegna delle diverse problematiche e delle indicazioni che si ricavano dalle fonti giurisprudenziali.

1. Principio di proporzionalità e motivazione

La Corte di cassazione ha affermato, con ripetute pronunce, che il sequestro dei dati digitali deve rispettare il **principio di proporzionalità** e la **rigorosa motivazione** delle ragioni di acquisizione dei dati medesimi. Il decreto del pubblico ministero, ove intenda accedere al vaglio del contenuto dei dispositivi e non limitarsi alla mera acquisizione dell'apparecchio quale strumento di comunicazione, deve illustrare le ragioni per cui è necessario disporre un sequestro esteso e onnicomprensivo o, in alternativa, le specifiche informazioni oggetto di ricerca, indicando i criteri di selezione del materiale informatico archiviato nel dispositivo, la giustificazione della perimetrazione temporale dei dati di interesse e i tempi entro cui verrà effettuata tale selezione, con conseguente restituzione anche della copia informatica dei dati non rilevanti (Cass. pen., Sez. 6, n. 1286/2025; Sez. 6, n. 17312/2024; Sez. 6, n. 6623/2021).

Di regola, il provvedimento di sequestro - o di convalida del sequestro eseguito d'iniziativa dalla polizia giudiziaria - deve indicare e motivare le informazioni oggetto di ricerca, i criteri

di selezione del materiale, la perimetrazione temporale dei dati e i tempi entro i quali dovrà essere effettuata la selezione, **restando quindi esclusa ogni attività meramente esplorativa**. Ove siano indispensabili l'acquisizione e la verifica integrale dei dati contenuti in una memoria informatica, di ciò dovrà essere data rigorosa motivazione.

Ulteriore rigore è dovuto quando il sequestro sia eseguito nei confronti di un **soggetto terzo estraneo al reato** e quando i dati oggetto di sequestro abbiano natura di **dati personali**, nel qual caso dovranno essere rispettati i principi di necessità, finalità, pertinenza e non eccedenza, in conformità con la sentenza Corte cost. n. 20/2019 e con la Direttiva (UE) 2016/680, attuata con D.Lgs. n. 51/2018.

2. Dati a carattere comunicativo

I messaggi elettronici - e-mail, SMS, WhatsApp e simili - conservati nella memoria di un dispositivo digitale costituiscono **corrispondenza ai sensi dell'art. 15 Cost.** anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo o per altra causa, non abbiano perso ogni carattere di attualità, trasformandosi in un mero documento storico (Corte cost. n. 170/2023; Cass. Sez. U, n. 23756/2024, Giorgi; Cass. Sez. 2, n. 25549/2024, Tundo). La loro acquisizione deve avvenire secondo le forme previste dall'art. 254 c.p.p. per il sequestro della corrispondenza, sulla base di un provvedimento motivato dell'autorità giudiziaria che rispetti il principio di proporzionalità, definisca i dati oggetto di ricerca e dia conto delle ragioni che giustificano la compressione del diritto alla libertà e segretezza della corrispondenza.

La tutela prevista dall'art. 15 Cost. non richiede che il provvedimento emani necessariamente da un giudice: l'espressione "autorità giudiziaria" include il pubblico ministero (Cass. Sez. U, n. 23756/2024; Cass. Sez. 5, n. 8376/2025). Tale conclusione è tuttavia oggetto di un crescente orientamento contrario, esaminato al paragrafo 3.

Pertanto, la polizia giudiziaria che agisce su delega, eseguita l'estrazione dalla memoria digitale, dovrebbe trasmettere i dati a carattere comunicativo al pubblico ministero senza aprirli e senza prenderne comunque conoscenza, ai sensi degli artt. 254, comma 2, e 353, comma 1, c.p.p.. Ove vi sia il fondato motivo di ritenere che da quei dati possano ricavarsi notizie che rendono necessario procedere con urgenza ad ulteriori attività di indagine, il pubblico ministero può autorizzare la polizia giudiziaria all'apertura e lettura immediata dei dati, come previsto dall'art. 353, comma 2, c.p.p..

Autorizzazione che dovrà essere comunque conferita allorché la Polizia giudiziaria proceda di iniziativa in situazione di urgenza.

3. Acquisizione dei dati ed estrazione delle copie: modalità tecniche e regole processuali

3.1 Modalità tecniche

La legge 18 marzo 2008, n. 48, ha modificato la disciplina dei mezzi di ricerca della prova al fine di garantire l'integrità e la genuinità del dato informatico. La **perquisizione** - intesa come apprensione materiale del dispositivo e ricerca in esso delle tracce del reato - e la **estrazione della copia forense** - quale operazione tecnica distinta retta da proprie regole - costituiscono fasi autonome, ancorché frequentemente contestuali nell'esecuzione. L'estrazione della copia non è un atto della perquisizione, ma la modalità esecutiva del

sequestro dei dati: essa trae la propria base normativa dagli artt. 244, comma 2, 247, comma 1-bis, e 354, comma 2, c.p.p., nonché, ove delegata successivamente, dall'art. 359 c.p.p.

3.2 Ripetibilità dell'estrazione e necessità del contraddittorio

L'estrazione di copia dei dati digitali **non costituisce accertamento tecnico irripetibile** ai sensi dell'art. 360 c.p.p. L'operazione è ripetibile fintanto che resti in sequestro il supporto originale o ne siano comunque garantite la conservazione e l'intangibilità dei relativi dati digitali. La mancata adozione delle modalità tecniche prescritte dalla l. 48/2008 non determina di per sé l'inutilizzabilità del dato (Cass. Sez. 1, n. 38909/2021; Cass. Sez. 2, n. 40451/2025).

Nondimeno, il contraddittorio nell'estrazione è necessario, non in quanto imposto dalla qualificazione dell'atto come irripetibile, bensì perché costituisce la principale garanzia contro future contestazioni sull'autenticità e l'integrità dei dati estratti. A tale fine, l'estrazione della copia forense deve essere eseguita nell'ambito e con le garanzie dell'attività di perquisizione, in presenza dell'indagato o di un suo delegato, con redazione di verbale che documenti le modalità tecniche dell'estrazione, gli strumenti impiegati e i valori hash di verifica della copia.

Il ricorso alle forme dell'art. 360 c.p.p. rimane facoltativo e risulta opportuno nei soli casi in cui non sia assicurabile la conservazione del supporto originale fino a una successiva estrazione.

3.3 Organo competente a disporre l'accesso

La questione è attualmente oggetto di un contrasto non risolto in seno alla Cassazione. Con Cass. Sez. 5, n. 8376/2025 è stato ritenuto che il PM costituisce organo idoneo ad autorizzare l'accesso ai dati, escludendo la necessità di un provvedimento del giudice. Con Cass. Sez. 6, n. 13585/2025 è stato invece affermato che il controllo preventivo richiesto dalla sentenza della Corte di Giustizia (Grande Camera, C-548/21/2024) non può essere esercitato dal PM, stante la sua natura di parte processuale. Da ultimo, Cass. Sez. 2, n. 40451/2025 ha espressamente dichiarato di non condividere la pronuncia della Sez. 5 e ha ritenuto condivisibile l'orientamento della Sez. 6, chiarendo che la nozione di "organo amministrativo indipendente" richiede la terzietà rispetto all'organo richiedente l'accesso, requisito che il PM non soddisfa. La stessa pronuncia ha tuttavia accertato che la Direttiva 2016/680/UE è priva di efficacia diretta nell'ordinamento interno e che la normativa interna non può essere disapplicata.

Sul piano applicativo attuale, il PM conserva quindi il potere di disporre l'accesso ai dati. In considerazione della vulnerabilità sistemica di questo assetto, il provvedimento di accesso deve essere sorretto da motivazione particolarmente rigorosa quanto a necessità, proporzionalità e perimetrazione.

4. Conservazione e selezione dei dati digitali

In applicazione del principio ricavato dall'art. 253 c.p.p., ove l'oggetto del sequestro abbia un contenuto esteso, la copia integrale dei dati deve essere restituita una volta trascorso il tempo necessario per selezionare, nella massa dei dati, i soli rilevanti e pertinenti a fini probatori (Cass. Sez. 6, n. 34265/2020). Va distinto tra **copia-mezzo** - la copia integrale dei

dati digitali, trattenibile al solo scopo di selezionare i dati pertinenti e rilevanti - e **copia-fine** nella quale vengono riversati i dati all'esito della selezione.

Sono soggetti a sequestro e al conseguente deposito, con facoltà per le parti di acquisirne copia, i soli dati oggetto di selezione in quanto ritenuti, ai sensi dell'art. 253 c.p.p., cose pertinenti al reato necessarie per l'accertamento dei fatti.

5. Restituzione della copia-mezzo e bilanciamento fra diritto alla riservatezza e diritto di difesa

Ove si proceda a un'estesa acquisizione della memoria digitale in vista della successiva selezione, la restituzione della copia-mezzo comporta il rischio della perdita processuale di tutti i dati diversi da quelli riversati nella copia-fine. Se è vero che l'esercizio dell'azione penale segna la conclusione delle indagini preliminari, è anche vero che nel processo penale la prova assume carattere di continuità, considerata la possibilità di attività di indagine suppletiva (art. 419, comma 3, c.p.p.), integrativa del pubblico ministero o del difensore (art. 430 c.p.p.), dell'assunzione di nuove prove anche d'ufficio da parte del giudice (art. 507 c.p.p.), e di rinnovazione dell'istruzione dibattimentale in appello (art. 603 c.p.p.).

Un bilanciamento ragionevole tra le esigenze potenzialmente confliggenti - diritto alla riservatezza da un lato e diritto alla prova di tutte le parti dall'altro - può essere realizzato, in via di interpretazione analogica, sul modello di quanto previsto in materia di intercettazioni dall'art. 269 c.p.p. Va in ogni caso esclusa la conservazione dei dati non rilevanti e non necessari protratta oltre il tempo effettivamente richiesto dalle esigenze della prova.

Tanto premesso,

visto l'art. 2 della circolare CSM sull'organizzazione degli uffici di Procura,

SI DETTANO LE SEGUENTI DISPOSIZIONI

1. Decreto del pubblico ministero e organo competente

Il sequestro probatorio di dati informatici e dei relativi supporti è disposto con decreto del pubblico ministero, motivato nel rispetto del principio di proporzionalità secondo quanto indicato al paragrafo. Il provvedimento di accesso alla memoria digitale sarà motivato con il massimo rigore in relazione a proporzionalità, finalità e perimetrazione dei dati.

1-bis. Autorizzazione del GIP nei procedimenti di particolare gravità

Nei procedimenti aventi ad oggetto reati di particolare gravità o delicatezza, i sostituti procuratori titolari valutano l'opportunità di richiedere al GIP, prima di disporre l'accesso al contenuto della memoria digitale, un provvedimento autorizzatorio. Pur non essendo prevista allo stato una procedura specifica a tal fine, tale richiesta può essere formulata con richiesta di autorizzazione atipica fondata sugli artt. 189 e 328 c.p.p. Il provvedimento del GIP, ove ottenuto, consolida la legittimità dell'acquisizione rispetto alle eccezioni difensive prevedibili alla luce dell'evoluzione giurisprudenziale descritta al paragrafo 3.3.

2. Contenuto del decreto di sequestro

Nel caso di sequestro di una memoria informatica contenuta in locale o accessibile da remoto dal dispositivo oggetto del sequestro, il pubblico ministero indica con adeguata motivazione quali siano le informazioni e i dati oggetto di ricerca, quale sia il nesso tra questi e i fatti oggetto del procedimento, nonché - salva la necessità, con rigorosa motivazione, di acquisizione integrale della memoria - i limiti temporali dell'acquisizione dei dati e i criteri da utilizzare per la ricerca degli elementi nella fase di selezione, nel rispetto dei principi di adeguatezza e proporzionalità. Particolare rigore è dovuto nel caso in cui il sequestro sia eseguito nei confronti di un terzo estraneo al reato.

3. Dati digitali a carattere comunicativo

I messaggi elettronici di qualsiasi tipo conservati nella memoria di un dispositivo digitale costituiscono corrispondenza ai sensi dell'art. 15 Cost. e sono soggetti alle garanzie previste dall'art. 254 c.p.p., fintanto che conservino carattere di attualità e di interesse per i corrispondenti. La loro acquisizione richiede un provvedimento motivato del pubblico ministero che rispetti il principio di proporzionalità, definisca i dati oggetto di ricerca e dia conto delle ragioni che giustificano la compressione del diritto alla libertà e segretezza della corrispondenza. In considerazione dell'evoluzione giurisprudenziale descritta al paragrafo 3.3, la motivazione del provvedimento sarà redatta con particolare rigore.

La polizia giudiziaria, qualora sia stata incaricata di eseguire la sola copia forense del dispositivo, la trasmette al pubblico ministero senza aprirla e senza prenderne comunque conoscenza, ai sensi degli artt. 254, comma 2, e 353, comma 1, c.p.p.

Qualora vi sia il fondato motivo di ritenere che dal contenuto dei dati comunicativi possano emergere notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, il pubblico ministero può autorizzare la polizia giudiziaria all'apertura e lettura immediata dei dati, ai sensi dell'art. 353, comma 2, c.p.p., con provvedimento motivato che individua i soli dati la cui cognizione immediata è necessaria per le finalità indicate.

Nel caso in cui i dati a carattere comunicativo siano acquisiti presso un soggetto terzo estraneo al reato si applicano le garanzie rafforzate previste dall'art. 254 c.p.p. nella sua integralità.

4. Sequestro d'iniziativa della polizia giudiziaria

Ove la necessità del sequestro dei dati si manifesti in occasione di un'attività di iniziativa della polizia giudiziaria, sarà dato avviso al pubblico ministero ai fini dell'adozione del relativo decreto, salvo il caso di urgenza ai sensi dell'art. 354, comma 2, c.p.p.

In caso di urgenza, qualora non sia possibile procedere alla perquisizione delle memorie per mancanza di mezzi tecnici o di competenze specialistiche, la polizia giudiziaria pone sotto sequestro il dispositivo ai sensi dell'art. 354, comma 2, c.p.p. e ne dà comunicazione al PM entro quarantotto ore ai sensi dell'art. 355 c.p.p. La successiva perquisizione del contenuto delle memorie avviene sulla base di apposito decreto del pubblico ministero e nel rispetto delle forme ordinarie della perquisizione previste dagli artt. 247, 250 e 251 c.p.p.

5. Apertura dei dati in caso di urgenza

Ove l'esecuzione del sequestro sia delegata alla polizia giudiziaria, il pubblico ministero può autorizzare l'apertura immediata delle memorie, come previsto in caso di urgenza

dall'art. 353 c.p.p., qualora vi sia il fondato motivo di ritenere che dal contenuto della memoria digitale possano emergere notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo.

6. Estrazione della copia forense: modalità operative

L'estrazione della copia forense dei dati digitali non costituisce accertamento tecnico irripetibile ai sensi dell'art. 360 c.p.p. e viene eseguita dalla polizia giudiziaria quale fase esecutiva della perquisizione, con le garanzie previste per tale atto, in contraddittorio con la persona sottoposta a perquisizione e, ove presente, con il suo difensore. Il verbale documenta le modalità tecniche dell'estrazione, gli strumenti impiegati e i valori hash di verifica della copia.

Ove l'organo procedente non disponga di risorse tecniche adeguate, si avvale del supporto del personale specializzato dei rispettivi uffici di appartenenza. La nomina di tecnici informatici come ausiliari ai sensi dell'art. 348, comma 4, c.p.p. potrà avvenire previa autorizzazione del P.M. titolare delle indagini, solo in caso di operazioni in cui necessitano competenze con elevata specializzazione (es.: sequestro di file conservati su cloud di grandi aziende a cui non è possibile accedere con write blocker fisici).

L'esecuzione avviene secondo le seguenti modalità, indicate in ordine di preferenza:

Modalità 1 — Estrazione sul posto. Ove tecnicamente possibile, la polizia giudiziaria estrae la copia forense integrale del dispositivo (*copia-mezzo*) direttamente nel corso della perquisizione, alla presenza della persona sottoposta a perquisizione e del suo difensore, ove presente. Al termine dell'estrazione il dispositivo originale è restituito all'avente diritto.

Modalità 2 — Sequestro con estrazione differita. Qualora non sia possibile procedere all'estrazione sul posto per la particolare complessità tecnica delle operazioni, la polizia giudiziaria sequestra il dispositivo e ne dà immediata comunicazione al PM. L'estrazione della copia forense è eseguita nei giorni immediatamente successivi sempre con le forme della perquisizione. La persona sottoposta a perquisizione e il suo difensore devono essere avvisati per iscritto con congruo anticipo, con indicazione di data, ora e luogo delle operazioni e con l'avviso che possono assistere e nominare un consulente tecnico di parte. Al termine delle operazioni il dispositivo originale è restituito all'avente diritto.

Modalità 3 — Ispezione informatica speditiva. In alternativa alle modalità precedenti, previo consenso esplicito della persona sottoposta a perquisizione e del suo difensore ove presente (consenso documentato nel verbale con l'indicazione nominativa dei soggetti che lo hanno prestato) la polizia giudiziaria può procedere a una perquisizione informatica direttamente sul dispositivo, adottando tutte le cautele tecniche necessarie e annotando nel verbale tutti i contenuti di interesse rilevati secondo i criteri indicati nel decreto. Ove le operazioni siano ritenute adeguate rispetto alle esigenze di indagine, non si procede al sequestro del dispositivo.

7. Estrazione della copia-fine e restituzione del supporto

Nei casi di cui alle Modalità 1 e 2, una volta acquisita la copia-mezzo nelle forme descritte, la polizia giudiziaria procede alla perquisizione della memoria e all'estrazione della copia forense selettiva (*copia-fine*), contenente i soli dati di interesse investigativo, che devono essere riversati su supporto durevole (CDROM, DVD, Bluray).

La perquisizione si opera effettuando ricerche mediante le parole chiave e i criteri di selezione indicati nel decreto di perquisizione.

Al termine di questa operazione la polizia giudiziaria notizia questo Ufficio, che impartisce disposizioni in merito alla conservazione o restituzione della copia-mezzo secondo quanto previsto alla disposizione 9.

Il pubblico ministero, presa visione del verbale, dispone con autonomo decreto il sequestro dei dati emersi durante la perquisizione e non direttamente contemplati dal decreto di perquisizione.

Il dispositivo originale è restituito all'avente diritto non appena completata l'estrazione della copia-mezzo, salvo che contenga dati di cui è vietata la detenzione, che costituiscano corpo di reato, o che si renda necessario adottare un sequestro preventivo ai sensi dell'art. 321 c.p.p. ovvero che sia stato emesso autonomo decreto di sequestro. In tal caso, si provvede alla cancellazione della copia mezzo solo decorsi i termini per la proposizione del riesame.

8. Selezione dei dati e garanzie tecniche

La selezione dei dati sulla copia-mezzo è effettuata ad opera della stessa polizia giudiziaria, ove disponga di adeguate risorse tecniche, ovvero con l'ausilio di un consulente informatico. La selezione è effettuata nel rispetto delle migliori regole tecniche, in modo da garantire l'integrità dei dati e delle copie. La copia-fine così formata è acquisita al fascicolo del procedimento, mediante invio dei dati estratti su APP tramite portale NDR.

9. Conservazione della copia-mezzo e regime della copia di sicurezza

Completata l'estrazione della copia-fine, il magistrato titolare del procedimento valuta la necessità della conservazione della copia-mezzo alla luce delle esigenze di prova, della fase del procedimento e dell'ampiezza dell'oggetto delle indagini, adottando uno dei seguenti provvedimenti motivati.

9.1 Restituzione immediata. Ove la fase di selezione debba ritenersi definitivamente conclusa e la conservazione della copia-mezzo risulti palesemente non necessaria (in particolare quando il procedimento abbia un oggetto circoscritto, il numero degli indagati e delle ipotesi di reato sia limitato e la selezione sia avvenuta nel contraddittorio con le parti, sia decorso il termine per il riesame) il magistrato titolare dispone, con provvedimento motivato, la restituzione della copia-mezzo all'avente diritto, previo pagamento del costo del supporto informatico.

In subordine, ove la restituzione non sia materialmente possibile o non sia desiderata dalla parte, dispone la cancellazione mediante distruzione integrale dei dati.

9.2 — Conservazione come copia di sicurezza. Ove permanga la necessità di garantire il contraddittorio nella fase di selezione – in particolare quando la selezione sia avvenuta senza contraddittorio, ovvero in una fase iniziale delle indagini con oggetto ancora non sufficientemente definito, o possano sopravvenire nuovi indagati, nuove persone offese o ulteriori ipotesi di reato – il magistrato titolare dispone, con provvedimento motivato, la conservazione della copia-mezzo quale copia di sicurezza, con modalità tali da assicurarne l'assoluta riservatezza, in forme analoghe a quelle previste per la sezione documentale dell'archivio riservato destinato alle intercettazioni. In tal caso:

- a) al fascicolo delle indagini preliminari è acquisita la sola copia-fine contenente i dati oggetto di selezione;

- b) al soggetto che avrebbe diritto alla restituzione della copia-mezzo è dato avviso della sua conservazione quale copia di sicurezza e della facoltà di accesso ad essa, nonché del diritto di ricorrere agli ordinari mezzi di impugnazione e di chiedere la distruzione dei dati che risultino manifestamente non necessari per il procedimento;
- c) è riconosciuto alle parti il diritto di accesso nominativo e registrato alla copia di sicurezza, previa apposita istanza, con facoltà di esaminarne i contenuti (senza estrarne copia) di indicare dati ulteriori rispetto a quelli già riversati nella copia-fine e di chiederne l'acquisizione, nonché di chiedere la distruzione dei dati manifestamente non necessari, in conformità con quanto previsto in via analogica dall'art. 269, comma 2, c.p.p.;
- d) la copia-mezzo è conservata, nella descritta forma riservata, almeno fino al momento della richiesta di archiviazione o dell'esercizio dell'azione penale, salvo che, in base a elementi sopravvenuti, risulti palesemente venuta meno ogni ragione che ne giustifichi l'ulteriore conservazione, nel qual caso il magistrato titolare dispone con provvedimento motivato la restituzione o la distruzione mediante cancellazione integrale dei dati;
- e) nelle fasi successive all'esercizio dell'azione penale, ogni decisione sulla conservazione della copia-mezzo è rimessa al giudice, cui sarà rappresentata l'opportunità di mantenerne la conservazione fino alla sentenza irrevocabile o comunque fino al momento in cui tale conservazione risulti palesemente non più necessaria.

9.3 Dati di cui è vietata la detenzione. La restituzione della copia-mezzo è in ogni caso esclusa quando il dispositivo o la copia contengano dati di cui è vietata la detenzione o che costituiscano corpo di reato, ovvero quando la disponibilità dei dati consenta il protrarsi o la reiterazione del reato. In tali casi si procede con richiesta al giudice di sequestro preventivo ai sensi dell'art. 321 c.p.p.

9.4 Rimedi impugnatori. L'intera materia dell'acquisizione, conservazione e restituzione dei dati digitali e dei relativi supporti resta soggetta alle disposizioni degli artt. 257 e 263 c.p.p. in materia di sequestro e agli ordinari rimedi impugnatori ivi previsti.

Si dispone che la presente direttiva sia diramata ai magistrati dell'Ufficio e trasmessa, per quanto di competenza, alla Polizia di Stato, all'Arma dei Carabinieri, alla Guardia di Finanza e agli ulteriori organi di polizia giudiziaria operanti nel circondario, nonché al responsabile dell'Ufficio Intercettazioni.

Si dispone la trasmissione della presente direttiva al Procuratore generale presso la Corte d'appello per opportuna conoscenza.

Sassari, 08/04/2026

Il Procuratore della Repubblica



ARMANDO MAMMONE
MINISTERO DELLA GIUSTIZIA
08.04.2026 10:37:18 GMT+01:00

Fanno parte integrante della presente direttiva:

- protocollo operativo per le attività di polizia giudiziaria in caso di perquisizione di memorie informatiche;
- allegato tecnico disciplinante le modalità esecutive sui dispositivi elettronici;

- modulistica per la compilazione degli atti di repertamento (disponibile anche sul sito internet della Procura)