



PROCURA DELLA REPUBBLICA PRESSO IL TRIBUNALE DI SASSARI

APPENDICE ALLA DIRETTIVA IN MATERIA DI ACQUISIZIONE DI DATI DIGITALI

PROTOCOLLO OPERATIVO PER LA POLIZIA GIUDIZIARIA

Disposizioni per l'acquisizione di dati digitali da dispositivi informatici

DISPOSIZIONI PRELIMINARI

Tutte le operazioni di acquisizione di dati digitali descritte nel presente protocollo si svolgono nell'ambito e con **le forme della perquisizione**, con le garanzie previste per tale atto dagli artt. 247, 250 e 251 c.p.p. **nonché – allorché lo scopo della perquisizione sia l'acquisizione di comunicazioni – a mezzo APP (Whatsapp, Messenger, Telegram ecc.) dell'art. 353 c.p.p. (sequestro di corrispondenza).**

Nessuna operazione di acquisizione, estrazione o analisi di dati digitali può essere avviata in assenza di decreto di perquisizione informatica firmato dal pubblico ministero, salvo i casi di urgenza disciplinati alla § 2. In tal caso, si dovrà operare in osservanza dell'art. 353 c.p.p., richiedendo autorizzazione al pubblico ministero di turno urgenze.

La persona sottoposta a perquisizione e il suo difensore, ove presenti, hanno diritto di assistere a tutte le operazioni, comprese quelle di estrazione della copia forense. Tale diritto deve essere comunicato espressamente prima dell'inizio delle operazioni e la comunicazione deve essere documentata nel verbale.

Distinzione tra messaggi archiviati e comunicazioni in corso. Il riferimento all'art. 353 c.p.p. nelle disposizioni che precedono riguarda esclusivamente i messaggi e le comunicazioni già memorizzati sul dispositivo o sull'account (corrispondenza archiviata). L'acquisizione di comunicazioni in corso, ovvero il monitoraggio in tempo reale di flussi comunicativi tramite APP di messaggistica, è soggetta al diverso e più restrittivo regime delle intercettazioni di comunicazioni (artt. 266 e ss. c.p.p.) e richiede autorizzazione del Giudice per le indagini preliminari. In caso di dubbio sulla qualificazione dell'attività da compiere, la polizia giudiziaria sospende le operazioni e si raccorda immediatamente con il pubblico ministero.

Trattamento dei dati personali di terzi. I dispositivi digitali contengono frequentemente dati personali di soggetti terzi estranei al procedimento (contatti, fotografie, conversazioni, documenti). In conformità al principio di minimizzazione di cui all'art. 5, par. 1, lett. c), del Regolamento UE 2016/679 (GDPR) e alle disposizioni del d.lgs. 51/2018 (trattamento dati a fini di giustizia penale), la polizia giudiziaria limita l'acquisizione ai soli dati pertinenti e necessari rispetto agli scopi dell'indagine, come definiti nel decreto di perquisizione. I dati

di terzi non pertinenti non possono essere estratti nella copia-fine, né consultati, né conservati, salvo specifica autorizzazione del pubblico ministero. Il verbale deve dare atto delle misure adottate per garantire il rispetto di tale principio.

§ 1 — RICOGNIZIONE DEI DISPOSITIVI

Quando procede, la polizia giudiziaria individua tutti i dispositivi digitali presenti: telefoni cellulari, computer, tablet, supporti di memoria esterni, chiavette USB e qualsiasi altro apparato suscettibile di contenere dati digitali.

Nessun dispositivo deve essere acceso, sbloccato o manipolato prima che siano stati predisposti gli strumenti tecnici necessari a garantire l'integrità dei dati.

Qualora dal dispositivo risulti accessibile un account in cloud (Google Drive, iCloud, servizi di messaggistica o altri), la polizia giudiziaria adotta le seguenti misure nell'ordine indicato:

- (i) attiva, ove disponibile, la modalità aereo o disconnette il dispositivo dalla rete, al fine di impedire sincronizzazioni o cancellazioni remote, senza modificare alcuna credenziale;
- (ii) richiede immediatamente al pubblico ministero l'emissione di un ordine di conservazione ai sensi dell'art. 254-bis c.p.p. da notificare al provider, nonché — ove necessario — di un decreto di sequestro dei dati in cloud;
- (iii) qualora il pubblico ministero, valutata l'urgenza, autorizzi espressamente la modifica delle credenziali, la polizia giudiziaria annota nel verbale la motivazione, le credenziali originali (ove note) e quelle sostituite.

In ogni caso è vietata la modifica delle credenziali di accesso in assenza di autorizzazione del pubblico ministero.

§ 2 — PROCEDURA IN CASO DI URGENZA

Quando la perquisizione del contenuto delle memorie digitali non può essere eseguita sul posto per mancanza degli strumenti tecnici necessari o delle competenze specialistiche richieste, la polizia giudiziaria procede come segue.

Sequestro cautelativo del dispositivo. Il dispositivo è posto sotto sequestro ai sensi dell'art. 354, comma 2, c.p.p., adottando tutte le misure tecniche necessarie a conservare i dati e a impedirne l'alterazione o l'accesso non autorizzato. Il sequestro è comunicato al pubblico ministero entro quarantotto ore ai sensi dell'art. 355 c.p.p., per la convalida e per l'adozione del relativo decreto.

Perquisizione differita delle memorie. La perquisizione del contenuto del dispositivo sequestrato è eseguita successivamente, sulla base di apposito decreto del pubblico ministero. Non è consentita alcuna analisi, anche parziale, del contenuto del dispositivo prima del ricevimento del decreto.

Forme della perquisizione differita. La perquisizione delle memorie digitali, ancorché eseguita in momento successivo al sequestro del dispositivo, segue le regole ordinarie della perquisizione. In particolare:

- a) la persona nei cui confronti la perquisizione è disposta deve essere avvisata per iscritto con congruo anticipo della data, dell'ora e del luogo delle operazioni, con l'avviso che ha facoltà di farsi assistere da un difensore di fiducia (art. 250 c.p.p.);

- b) copia del decreto di perquisizione deve essere consegnata alla persona interessata prima dell'inizio delle operazioni (art. 251 c.p.p.);
- c) la persona interessata e il suo difensore hanno diritto di assistere a tutte le operazioni di estrazione della copia forense;
- d) le misure tecniche di cui all'art. 247, comma 1-bis, c.p.p. devono essere adottate per tutta la durata delle operazioni;
- e) le operazioni sono documentate con verbale redatto nelle forme previste dall'art. 251 c.p.p., contenente tutti gli elementi indicati al §6 del presente protocollo.
- f) Qualora le operazioni di perquisizione non si esauriscano nella giornata, le operazioni vengono sospese dando atto della sospensione a verbale. Le parti presenti sono avvisate del giorno dell'ora e del luogo fissato per la prosecuzione delle operazioni.

Al termine della perquisizione delle memorie digitali il dispositivo originale è restituito all'avente diritto previa autorizzazione del pubblico ministero, salvo che ricorra una delle ipotesi che ne escludono la restituzione indicate alla disposizione 7 della direttiva.

§ 3 — SCELTA DELLA MODALITÀ DI ESTRAZIONE

La polizia giudiziaria procede secondo le modalità indicate nel decreto di perquisizione, nell'ordine di preferenza di seguito indicato.

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. Si procede quindi all'estrazione della copia fine, all'analisi degli artefatti individuati e la trasmissione delle evidenze acquisite all'A.G. (VDS §5 - ESTRAZIONE DELLA COPIA-FINE E TRASMISSIONE).

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 pubblico ministero. L'estrazione della copia forense è eseguita nei giorni immediatamente successivi, in laboratorio, 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. Si procede quindi all'estrazione della copia fine, all'analisi degli artefatti individuati e la trasmissione delle evidenze acquisite all'A.G. (VDS §5 - ESTRAZIONE DELLA COPIA-FINE E TRASMISSIONE).

Modalità 3 — Perquisizione informatica diretta sul dispositivo

In alternativa alle modalità precedenti, previo consenso esplicito della persona sottoposta a perquisizione e del suo difensore ove presente, la polizia giudiziaria può procedere a perquisizione informatica direttamente sul dispositivo, adottando tutte le cautele tecniche

necessarie. Il consenso deve essere documentato nel verbale con l'indicazione nominativa dei soggetti che lo hanno prestato. La polizia giudiziaria annota 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. **AVVERTENZA TECNICA:** la perquisizione diretta sul dispositivo originale comporta inevitabilmente l'alterazione di alcuni metadati (in particolare i timestamp di ultimo accesso ai file e le voci di log del sistema operativo). La Modalità 3 deve pertanto essere adottata solo in via residuale, quando le Modalità 1 e 2 non siano praticabili, e la scelta deve essere motivata nel verbale con indicazione delle ragioni tecniche o operative che la giustificano. Gli operatori devono documentare nel verbale quali strumenti sono stati utilizzati e quali azioni sono state compiute sul dispositivo, al fine di consentire la successiva ricostruzione delle eventuali alterazioni introdotte.

§ 4 — MODALITÀ TECNICHE DI ESTRAZIONE

L'estrazione della copia forense deve avvenire nel rispetto delle seguenti regole tecniche:

- a) impiego obbligatorio di strumenti di write-blocking, hardware o software, che impediscano qualsiasi scrittura sul dispositivo originale durante le operazioni; non è consentito procedere all'estrazione in assenza di write-blocker di alcun tipo;
- b) calcolo e annotazione nel verbale del valore hash del dispositivo originale prima dell'inizio delle operazioni e del valore hash della copia al termine delle stesse, con verifica della corrispondenza tra i due valori a garanzia dell'integrità e dell'immodificabilità della copia; in caso di impossibilità tecnica di calcolare l'hash sull'originale, la circostanza deve essere espressamente motivata nel verbale;
- c) documentazione fotografica o video dello stato fisico del dispositivo al momento del rinvenimento, prima di qualsiasi manipolazione, con strumento che registri automaticamente data e ora; le immagini sono allegate al verbale o conservate unitamente agli atti del procedimento;
- d) annotazione nel verbale della denominazione, della versione e dell'aggiornamento di tutti gli strumenti hardware e software utilizzati per l'acquisizione, con attestazione che gli stessi erano validati al momento dell'uso.

Le modalità tecnico-operative di dettaglio relative a ciascuna delle regole di cui sopra, nonché le procedure per i dispositivi cifrati, per i dati volatili e per tutte le ulteriori casistiche, sono disciplinate dall'allegato tecnico alla presente Appendice, al quale si rinvia integralmente.

§ 5 — ESTRAZIONE DELLA COPIA-FINE E TRASMISSIONE

L'analisi del contenuto della copia-mezzo non può essere avviata in assenza di specifica delega del pubblico ministero che specifica le parole da cercare o i criteri per la ricerca delle tracce del reato.

In base alla delega, la polizia giudiziaria procede alla perquisizione della memoria ed estrae dalla copia-mezzo la sola copia forense selettiva (*copia-fine*), contenente i dati di interesse investigativo individuati secondo i criteri e le parole chiave indicati nel decreto di perquisizione.

Qualora nel corso della perquisizione della memoria emergano dati di interesse investigativo non direttamente contemplati dal decreto di perquisizione, la polizia giudiziaria ne dà immediata comunicazione al pubblico ministero. Detti dati non possono essere acquisiti senza un autonomo decreto di sequestro emesso dal pubblico ministero o – a seguito di sequestro di iniziativa – di autorizzazione ex art. 353 comma 2 c.p.p..

I dati selezionati nella copia-fine devono essere riversati su supporto durevole idoneo al volume dei dati: hard disk esterno o supporto flash dedicato al procedimento, ovvero — per volumi contenuti — supporto ottico (DVD o Blu-ray). Il supporto deve essere dedicato esclusivamente al procedimento, previamente formattato e verificato (processo di sanificazione), e il valore hash del contenuto riversato deve essere calcolato e annotato contestualmente al riversamento. Il supporto viene conservato presso il comando / ufficio di appartenenza in luogo sicuro e ad accesso riservato.

La copia-fine è trasmessa al pubblico ministero tramite portale NDR, mediante invio su APP. Prima della trasmissione la polizia giudiziaria verifica che il valore hash del file da trasmettere corrisponda a quello annotato nel verbale.

Al termine delle operazioni di selezione la polizia giudiziaria notizia il pubblico ministero e attende istruzioni in merito alla restituzione o alla conservazione della copia-mezzo.

§ 6 — REDAZIONE DEL VERBALE

Il verbale delle operazioni, redatto con le forme previste per la perquisizione dagli artt. 250 e 251 c.p.p., deve contenere obbligatoriamente:

- data, ora e luogo di inizio e termine delle operazioni;
- estremi del decreto di perquisizione in esecuzione del quale si procede;
- descrizione del dispositivo (marca, modello, numero seriale o altro elemento identificativo);
- modalità tecnica adottata per l'estrazione e strumenti impiegati;
- valore hash della copia estratta (MD5 o SHA-256);
- attestazione dell'avviso dato alla persona interessata circa la facoltà di farsi assistere da un difensore di fiducia, con indicazione dell'esito;
- generalità della persona presente e del difensore, ove presenti;
- nel caso di ricorso alla Modalità 3: indicazione nominativa dei soggetti che hanno prestato il consenso;
- eventuali riserve o osservazioni formulate dalla persona o dal difensore;
- esito delle operazioni con elenco dettagliato dei singoli file riversati nella *copia-fine* e indicazione del supporto sul quale la copia è stata estratta.

§ 7 — RESTITUZIONE DEI DISPOSITIVI E DELLA COPIA-MEZZO

Il dispositivo originale è restituito all'avente diritto non appena completata l'estrazione della copia-mezzo, salvo che:

- a. contenga dati di cui è vietata la detenzione o che costituiscano corpo di reato;
- b. si renda necessario adottare un sequestro preventivo ai sensi dell'art. 321 c.p.p.;
- c. sia stato emesso un autonomo decreto di sequestro del dispositivo.

La copia-mezzo non è restituita né cancellata fino a quando non siano decorsi i termini per la proposizione del riesame avverso il decreto di sequestro dei dati, salva diversa disposizione del pubblico ministero.

La restituzione o la cancellazione della copia-mezzo è disposta dal pubblico ministero con provvedimento motivato, secondo quanto previsto alla disposizione 9 della direttiva. In assenza di istruzioni, la polizia giudiziaria conserva la copia-mezzo in luogo sicuro e riservato e ne attende la richiesta.

§ 8 — DIVIETI

È in ogni caso vietato:

1. acquisire dati digitali in assenza di decreto del pubblico ministero, salvo i casi di urgenza disciplinati alla Capitolo §2 e § 3;
2. aprire, leggere o visionare messaggi, e-mail o comunicazioni di qualsiasi tipo senza autorizzazione scritta del pubblico ministero;
3. procedere all'analisi del contenuto di un dispositivo sequestrato in urgenza prima del ricevimento del decreto del pubblico ministero;
4. acquisire dati ulteriori rispetto a quelli contemplati dal decreto di perquisizione e non ad essi connessi senza un autonomo decreto di sequestro;
5. restituire o cancellare la copia-mezzo prima del decorso dei termini per il riesame e senza istruzioni del pubblico ministero;
6. conservare copie di dati sui sistemi dell'ufficio di appartenenza senza istruzioni del pubblico ministero;
7. trasmettere, mostrare o comunicare i dati estratti a soggetti diversi dal pubblico ministero titolare del procedimento;
8. modificare, cancellare o spostare file sul dispositivo originale.

DISPOSIZIONE FINALE

Qualsiasi situazione non prevista dal presente protocollo, o che susciti dubbi in ordine alle modalità operative da adottare, deve essere segnalata immediatamente al pubblico ministero titolare del procedimento prima di procedere. Non è consentita alcuna iniziativa autonoma in deroga alle presenti disposizioni.

Il presente protocollo costituisce parte integrante della direttiva in materia di acquisizione di dati digitali adottata dalla Procura della Repubblica di Sassari.

Sassari, 08/04/2026

Il Procuratore della Repubblica
Armando Mammone



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