PROCURA DELLA REPUBBLICA

DIREZIONE DISTRETTUALE ANTIMAFIA
TORINO

Ufficio del Procuratore della Repubblica

Prot. nr. 62/25/INT.

OGGETTO: Linee guida in materia di acquisizioni digitali e copie forensi

1. Premessa

Le prove informatiche e digitali hanno acquisito una rilevanza cruciale nelle indagini moderne per una pluralità di fattori:

- **ubiquità dei dispositivi digitali:** la maggioranza degli individui utilizza dispositivi digitali come *smartphone*, *computer* e *tablet*, che possono contenere informazioni rilevanti per le indagini e che porta con sé in ogni suo spostamento;
- **tracce digitali:** gli utenti lasciano tracce digitali attraverso le loro attività *online* e *offline*, come *email*, messaggi, cronologia di navigazione e dati di geolocalizzazione;
- **analisi avanzata:** le tecniche di analisi forense permettono di estrarre, analizzare e interpretare dati nascosti o cancellati, aiutando a ricostruire i fatti di reato.

In particolare, con riguardo alle acquisizioni di dati informatici, riveste centrale importanza la c.d. **copia forense**, alla luce anche degli interventi della Corte Costiruzionale che hanno portato il legislatore a prevedere una normativa ad hoc sulla materia. E' infatti in corso di approvazione avanti alla Camera dei deputati il DDL 806 (già approvato dal Senato) sul sequestro di dispositivi, sistemi informatici o memorie digitali. Negli atti che accompagnano il DDL 806 si legge che "L'intervento legislativo era doveroso per assicurare alle comunicazioni tramite smartphone e dispositivi informatici le stesse garanzie assicurate alla captazione di comunicazioni nelle intercettazione". Nell'articolato è poi previsto che se il sequestro dovrà essere esteso a dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviata o ricevuta si dovrà applicare la disciplina delle intercettazioni e che la conservazione del duplicato informatico dovrà avvenire in luogo protetto presso la Procura della Repubblica fino alla sentenza o al decreto penale di condanna non più soggetti ad impugnazione.

La copia forense, detta anche "*imaging forense*" o "*duplicazione forense*" è il processo informatico attraverso cui viene formata una replica esatta di tutti i dati presenti su un dispositivo

digitale, come un *computer*, uno *smartphone* o un disco rigido. Caratteristiche tipiche di questo processo di duplicazione sono:

- **integrità delle prove**: la copia forense garantisce che i dati digitali siano copiati esattamente nello stato in cui sono, senza alterazioni;
- **genuinità dei dati**: attraverso tecniche specifiche come l'*hash*, si garantisce che i dati originali e le loro copie siano identici e che non vi siano state modifiche durante il processo di copia;
- **supporto alle indagini**: la copia forense, attraverso la creazione di un duplicato appunto, permette agli investigatori di analizzare i dati senza rischiare di alterare le prove originali.

Ebbene, ciò chiarito sotto il profilo tecnico, la copia forense dei dati contenuti su un dispositivo digitale ha, nel corso degli anni, sollevato questioni di carattere **operativo** e **giuridico**.

Scopo della presente circolare è proprio quello di fornire agli operatori e, in particolare, ai Sostituti dell'Ufficio e al personale di P.G., indicazioni in ordine alle modalità di effettuazione e conservazione delle copie forensi, sulla scorta dei principi di diritto enucleati dalla Corte di Cassazione.

2. La copia forense: inquadramento giuridico ed operativo

Ciò posto, l'effettuazione delle copie forensi può, innanzitutto, seguire differenti percorsi pratici.

Infatti, nel caso frequente di **perquisizione disposta dal P.M. ed estesa al materiale informatico,** si possono verificare due scenari:

a) la copia forense viene effettuata dalla P.G. delegata **direttamente *in loco***,
b) in caso di impossibilità contingente (per condizioni di tempo e di luogo o per l'elevato numero di supporti), la P.G. delegata procede al **sequestro dei supporti** ed alla **successiva** attività di copia forense.

Ebbene, mentre l'ipotesi di cui al punto a) non appare particolarmente problematica, trattandosi di attività esecutive della perquisizione, demandate alla P.G. nell'ambito del medesimo atto investigativo, maggiori interrogativi solleva l'ipotesi *sub* b).

In particolare, gli operatori si sono a lungo interrogati sulla natura **ripetibile** o **irripetibile** dell'atto in questione (copia forense), con conseguente necessità o meno di coinvolgere, nelle forme di cui all'art. 360 c.p.p., la difesa dell'imputato e le altre parti[1].

Ebbene, la Suprema Corte di Cassazione ha, a più riprese, affermato la **natura ripetibile** dell'attività di duplicazione dei dati contenuti in supporto digitale: «*L'estrazione di dati archiviati in un supporto informatico, quale è la memoria di un telefono cellulare,* ***non costituisce accertamento tecnico irripetibile*** *... con la conseguenza che né la mancata adozione di tali modalità [previste dalla legge 48/2008], né, a monte, la mancata interlocuzione delle parti al riguardo comportano l'inutilizzabilità dei risultati probatori acquisiti, ferma la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti*» (cfr. da ultimo, Sez. 1, n. 38909 del 10/06/2021, Centofanti, Rv. 282072;

[1] Deve chiarirsi che non sono ammesse modalità di effettuazione della copia forense ulteriori rispetto ai "canali" di cui all'art. 359 e 360 c.p.p. e, quindi, "**ibride**" (sviluppatesi nella prassi), che prevedano il coinvolgimento della difesa ad opera della sola P.G. delegata.

in senso conforme, Sez. 2, n. 29061 del 01/07/2015, Posanzini, Rv. 264572; Sez. 1, n. 14511 del 05/03/2009, Stabile Aversano, Rv. 243150).

Tale ripetibilità, si noti bene, appare condizionata al **mantenimento del vincolo probatorio sul supporto** cosicché di ripetibilità si potrà discorrere fintanto che il supporto originale (ad esempio *smartphone*) permanga in sequestro.

A fronte di supporti originali particolarmente delicati per la natura (personale) degli stessi o per i soggetti coinvolti (ad esempio, società quotata), ove sia ipotizzabile una rapida istanza di dissequestro da parte dei soggetti interessati, potrebbe risultare opportuna l'attivazione della procedura *ex* art. 360 c.p.p., con conseguente effettuazione della copia forense in contraddittorio e successivo dissequestro dei supporti originali.

Una volta realizzata, attraverso i due canali descritti, la copia forense, si pone il tema della **selezione del materiale investigativo di interesse**, attività di solito demandata alla P.G. e in relazione alla quale la Suprema Corte ha, nel corso del tempo, formulato plurimi principi di diritto, a tutela *in primis* dei diritti di riservatezza delle parti coinvolte nel processo penale.

In particolare, il sequestro (anche di dati informatici) deve essere **proporzionato** e **non può avere portata esplorativa**; di conseguenza, non può rimanere sotto sequestro (e per quanto di interesse non può essere versato in atti) il contenuto integrale della copia forense ma soltanto i *files* di stretto interesse investigativo: "*In tema di sequestro probatorio, l'acquisizione indiscriminata di un'intera categorie di beni, nell'ambito della quale procedere successivamente alla selezione delle singole "res" strumentali all'accertamento del reato, è consentita a condizione che il sequestro non assuma una valenza meramente esplorativa e che il pubblico ministero adotti una motivazione che espliciti le ragioni per cui è necessario disporre un sequestro esteso e onnicomprensivo...(Fattispecie, in cui la Corte ... ha ritenuto esplorativo e sproporzionato il sequestro indistinto di tutte le mail, personali e della società, riferibile ad un soggetto terzo estraneo al reato, trasmesse e ricevute nei dieci anni precedenti)* (Sez. 6, n. 34265 del 22/09/2020, Aleotti, Rv. 279949; cfr. in termini, da ultimo, Sez. 6, n. 1286 del 20/11/2024, Bozzano, Rv. 287421).

Pertanto, la realizzazione della copia forense realizza soltanto una "**copia-mezzo**" che può essere trattenuta in sequestro **solo entro un termine ragionevole di tempo**, sufficiente all'estrazione dei *files* di interesse investigativo e alla creazione di una "**copia-fine**" che rimarrà in atti e farà parte del compendio probatorio: "*In tema di sequestro probatorio di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede ...*" (Sez. 6, n. 34265 del 22/09/2020, Aleotti, Rv. 279949); ed ancora: "*In tema di sequestro probatorio, la finalizzazione dell'ablazione del supporto alla sua successiva analisi, strumentale all'identificazione e all'estrazione dei "files" rilevanti per le indagini, implica che la protrazione del vincolo, nel rispetto dei principi di proporzionalità e di adeguatezza, debba essere limitata al tempo necessario all'espletamento delle operazioni tecniche, dovendosi, tuttavia, rapportare la sua ragionevole durata alle difficoltà tecniche di apprensione dei dati, da ritenersi accresciute nel caso di mancata collaborazione dell'indagato, che non fornisca le chiavi di accesso alle banche dati contenute nei supporti sequestrati*" (Sez. 3, n. 36776 del 04/07/2024, Ferrero, Rv. 286923).

In sostanza: "*In tema di sequestro probatorio di contenitori informatici, il Pubblico Ministero:*

a) *può trattenere la copia integrale solo per il tempo strettamente necessario per selezionare, tra la molteplicità delle informazioni in essa contenute, quelle che davvero assolvono alla funzione probatoria sottesa al sequestro;*
b) *è tenuto a predisporre una adeguata organizzazione per compiere la selezione in questione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano stati sequestrati a persone estranee al reato per cui si procede;*
c) *compiute le operazioni di selezione, la c.d. copia-integrale deve essere restituita agli aventi diritto*" (così Sez. 6, n. 37349 del 14/06/2022, La Rosa, non massimata).

Nella ricostruzione operata dalla Suprema Corte, pertanto, la c.d. copia-mezzo, una volta terminate le operazioni di selezione, si presta ad essere restituita all'interessato o distrutta.

Su quest'ultimo profilo deve, tuttavia, rilevarsi che la restituzione *tout court* della copia-mezzo, ritualmente acquisita (in assenza quantomeno di una copia integrale di c.d. sicurezza, cfr. *infra*):

- comporta la **perdita del duplicato "originale"** del supporto, con conseguente impossibilità per le parti private di indicare eventuale contenuto di interesse nonché impossibilità di eventuale verifica successiva in relazione alla procedura di estrazione dei dati;
- rischia di tradursi in un ***vulnus* per la difesa e per le parti in generale**; infatti, la selezione del materiale investigativo di interesse effettuata all'inizio o nel corso delle indagini preliminari potrebbe rivelarsi non esaustiva alla luce delle risultanze dibattimentali. In altre parole, non è ipotesi remota l'insorgenza di nuovi elementi in fasi successive alle indagini, con necessità di verifica da effettuarsi sul contenuto della copia-mezzo ed individuazione di eventuali ed ulteriori *files* di interesse. Del resto, per quanto le indagini si chiudano con la notifica dell'avviso *ex* art. 415-*bis* c.p.p., vige nel procedimento penale il principio di **continuità dell'acquisizione della prova**, scandito da plurime disposizioni:
  - **art. 419, c. 3, c.p.p.** – attività suppletiva di indagine, successiva all'esercizio dell'azione penale;
  - **art. 430 c.p.p.** – attività integrativa di indagine, nel corso del dibattimento;
  - **art. 507 c.p.p.** – assunzione di prove assolutamente necessarie per la decisione in dibattimento;
  - **art. 603 c.p.p.** – rinnovazione dell'istruttoria dibattimentale nel giudizio di appello.

Al fine di contemperare gli interessi delle parti coinvolte alla riservatezza dei propri dati e le istanze difensive e probatorie sopra rappresentate, ed alla luce di quanto rilevato in premessa in ordine al fondato richiamo alle norme che disciplinano la materia delle intercettazioni, appare, pertanto necessario prevedere:

- la formazione di un'ulteriore **"copia di sicurezza"** della copia-mezzo,
- il mantenimento fino *"alla sentenza non più soggetta a impugnazione"* della "**copia di sicurezza**" all'interno di un **archivio informatico**, creato *ad hoc* (cfr., per le specifiche tecniche, la parte n. 3) e collocato presso l'Ufficio di Procura, in maniera analoga a quanto previsto in materia di intercettazioni telefoniche (ove, non a caso, appare avvertita dal legislatore la necessità di mantenere la disponibilità dell'integrale compendio intercettivo, ai fini del pieno contraddittorio con le difese, fino al passaggio in giudicato della sentenza, cfr. artt. 268, 269 c.p.p.).

In questo modo:

- la c.d. **copia-fine** viene trasfusa in apposito supporto che rimarrà all'interno del fascicolo, con facoltà delle parti di visionare ed estrarre copia del contenuto, nei modi ordinari consentiti dalla fase procedimentale;

- la c.d. **copia-mezzo** viene consegnata a richiesta alla parte (che dovrà però sostenere il costo del supporto informatico) alla parte o, preferibilmente, distrutta mediante totale cancellazione dei dati dal supporto/*hardware* acquistato dall'Ufficio (così suscettibile di riutilizzo);
- la c.d. **copia di sicurezza** viene custodita, presso la Procura della Repubblica, nell'archivio informatico, *ad hoc* creato in seno all'Ufficio, con accesso **registrato** e **nominativo** e facoltà per le parti di:
    - accedere e visionare il contenuto,
    - indicare eventuali ed ulteriori *files* di rilievo,
    - chiedere l'acquisizione nelle forme previste dei suddetti *files* al fascicolo e la relativa copia.

Istanze delle parti, queste, in relazione alle quali il Sostituto Procuratore titolare del procedimento /processo penale provvederà, con provvedimento motivato, richiamando la presente circolare.

Della creazione e della custodia della "copia di sicurezza", nonché delle facoltà di accesso di cui sopra, sarà dato avviso all'interessato al momento di consegna /cancellazione della "copia-mezzo"

3. L'archivio riservato delle copie forensi

Con riguardo all'archivio informatico *ad hoc* in precedenza indicato, si precisa quanto segue.

La gestione del sistema di archiviazione è demandata ad un apposito *software* che permette il *backup* dei dati ed il successivo *restore* degli stessi.

L'utilizzo dei nastri magnetici al posto degli *hard disk* permette una conservazione più sicura e fornisce garanzie di riservatezza e integrità per un periodo di tempo maggiore; infatti, le cassette LTO, a differenza degli *hard disk*, non dispongono di parti elettriche ed elettromeccaniche sottoposte a sollecitazioni di corrente, con il conseguente rischio minimo di rottura rispetto ad un *hard disk* ordinario[2].

La corrispondenza dell'integrità dei dati memorizzati e la loro immodificabilità è garantita dalla verifica delle impronte di *hash* che vengono eseguite automaticamente nel momento della produzione delle varie copie.

Tutto l'archivio viene gestito, sotto il diretto controllo del Procuratore della Repubblica o del Procuratore della Repubblica Aggiunto delegato, tramite un apposito *database* che permetta l'immediata identificazione e ubicazione delle copie forensi di un determinato procedimento.

4. Le istruzioni

Si dispone, pertanto, che l'attività di ricerca di prove digitali e di successiva effettuazione di copie forensi sia scandita dai seguenti passaggi:

[2] La peculiarità degli LTO è la non immediata disponibilità dei dati in quanto dopo la registrazione sulle cassette il *restore* degli stessi comporta dei tempi di elaborazione variabili da 1 a 3 giorni in funzione della quantità dei dati da recuperare. Tempistica ritenuta comunque accettabile nell'economia generale del processo di conservazione e sicurezza.

1) emissione del **decreto di perquisizione informatica e sequestro**, con particolare attenzione:
   - alla **perimetrazione soggettiva** (persone sottoposte ad indagini / terzi), **oggettiva** e **temporale** dell'oggetto della ricerca;
   - alla **valorizzazione** di tutti gli elementi oggetto di prova *ex* art. 187 c.p.p. (tra cui rientrano, ad esempio, anche le circostanze rilevanti ai fini degli artt. 133 e 133-*bis* c.p.);

   inserendo, nei casi più delicati ed ove possibile, l'indicazione, con clausola di salvezza, di **parole-chiave;**
2) formazione della **"copia mezzo"** che può essere effettuata direttamente dal personale interno (a mezzo delega di indagine) o essere recapitata dall'esterno (PG esterna o consulente nominato *ex* art. 359 c.p.p.);
3) salvataggio della **"copia mezzo"** su apposito supporto (*hard disk* singolo o *server*);
4) esecuzione di una **ulteriore "copia di sicurezza"** da depositare nella libreria a nastro/archivio *ad hoc* descritto al par. 3);
5) emissione di **delega tempestiva** da parte del P.M.;
6) **selezione,** da parte da parte del Pubblico Ministero titolare del procedimento penale e/o della P.G. delegata, dei dati di interesse investigativo presenti nella "copia mezzo" e creazione della **"copia fine"**, trasfusa in apposito supporto da conservare nel fascicolo del procedimento penale in indagine;
7) consegna alla parte legittimata richiedente (che dovrà, però, sostenere il costo del supporto informatico) della **"copia mezzo"** o, preferibilmente, distruzione/cancellazione dei relativi dati (al più tardi, al momento di chiusura delle indagini preliminari);
8) mantenimento nell'archivio *ad hoc* della "**copia di sicurezza"**, con accesso nominativo e registrato e facoltà per le parti private di visionare il contenuto, di indicare eventuali *files* ulteriori di rilievo e di chiederne l'acquisizione al fascicolo, con autorizzazione del P.M. procedente.
9) informazione alla parte, al momento della consegna della copia-mezzo o della distruzione/cancellazione dei dati ivi contenuti, del mantenimento della c.d. "*copia - sicurezza*" e della posssibilità di accedere e visionare il contenuto, di indicare eventuali ed ulteriori *files* ritenuti rilevanti e di chiedere l'acquisizione, nelle forme previste, dei suddetti *files* al fascicolo e la relativa copia.

La presente circolare ha efficacia immediata, con riserva di eventuali e successive disposizioni all'esito del primo periodo di applicazione.

Si comunichi ai Procuratori dela Repubblica Aggiunti, ai Sostituti Procuratori, al Sig. Dirigente amministrativo, al Funzionario Responsabile del Servizio Intercettazioni, al Responsbaile della Sezione Informatica.

Torino , 14 aprile 2025

IL PROCURATORE DELLA REPUBBLICA
Giovanni Bombardieri