FORNARI E ASSOCIATI

STUDIO LEGALE

FOCUS

SEQUESTRO DI DISPOSITIVI INFORMATICI E DI DATI TRA EFFICIENZA INVESTIGATIVA E DIRITTI FONDAMENTALI

fornarieassociati.com

Milano • Roma • Bari

Agosto 2025

I. PREMESSA

Il **sequestro** di **telefoni cellulari, PC** e altri **dispositivi e sistemi informatici o telematici**, con conseguente estrazione della copia forense del relativo contenuto, rappresenta ormai una prassi costante nelle indagini penali contemporanee.

Gli inquirenti ben sanno che il sequestro del telefono cellulare e del PC dell'indagato – o di soggetti terzi che con questi abbiano rapporti – consente di avere accesso a una **vasta mole di informazioni**, in potenza determinanti per lo sviluppo delle indagini preliminari.

Il contraltare, tuttavia, è che in assenza – sino ad oggi – di una specifica e rigorosa disciplina normativa, il sequestro di tali dispositivi ha spesso comportato una **indiscriminata apprensione di ingenti quantità di dati informatici**, ivi compresi quelli attinenti alla **sfera privata e personale del titolare**.

Se, infatti, la disciplina dell'attività di intercettazione di conversazioni o comunicazioni prevede un *iter* autorizzativo relativamente articolato a tutela dei diritti fondamentali dei soggetti coinvolti nell'indagine, il sequestro di cui trattasi permette – attraverso la semplice lettura delle comunicazioni, scambiate tramite e-mail o applicazioni di messagistica istantanea, archiviate nella memoria dei dispositivi – di ottenere **dati di pari valore investigativo**, ma con un **livello di garanzie decisamente inferiore.**

Analizzando la questione da quest'angolo visuale, risulta evidente come l'assenza di adeguati presidi di carattere procedurale nell'acquisizione del contenuto di dispositivi e sistemi informatici o telematici esponga la collettività ad illegittime intrusioni nella sfera più intima e riservata dell'individuo.

Tale criticità risulta ulteriormente esasperata dalla preoccupante frequenza con cui i ***mass media*** **reperiscono e diffondono**, sin dalle fasi embrionali dei procedimenti penali, **estratti degli atti di indagine** selezionati non già per la loro rilevanza e il loro interesse pubblico, bensì in funzione del rispettivo **potenziale sensazionalistico e *clickbait***.

La problematica non è sfuggita al legislatore euro-unitario, che già dal 2016 ha imposto agli Stati Membri l'adozione di norme a garantire la protezione delle persone fisiche riguardo al trattamento dei dati personali da parte delle autorità in ambito penale.

Segnatamente, la **Direttiva UE 2016/680**, attuata nell'ordinamento interno con il **D.lgs. n. 51/2018**, prevede all'art. 4, rubricato "*principi applicabili al trattamento di dati personali*", che il **trattamento** da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali avvenga:

- in **modo lecito e corretto**;

- per **finalità determinate, esplicite e legittime**;

- in **modo non incompatibile con tali finalità**;

e abbia ad oggetto:

- **dati personali adeguati, pertinenti e non eccedenti rispetto alle finalità** del trattamento.

Ebbene, risulta di palmare evidenza come l'attuale quadro normativo domestico *non* dia effettiva e piena attuazione ai principi di matrice sovranazionale, posto che:

- la **disciplina della c.d. perquisizione informatica**, contenuta all'art. 247, comma 1-*bis* c.p.p., **manca di presidi specifici**, in particolare per quanto concerne l'adeguatezza e la pertinenza dei dati acquisiti;

- la disciplina del sequestro dei dati contempla solo l'ipotesi delle operazioni effettuate presso i fornitori di servizi informatici, telematici e di telecomunicazione;

- nonostante le significative modifiche introdotte dalla L. n. 48/2008 – che ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica, nota come Convenzione di Budapest – l'ordinamento continua a non contemplare disposizioni procedurali sufficientemente rigorose e garantiste in merito alla delicata fase dell'estrazione dei dati, lasciando che questa avvenga anche in assenza di contraddittorio e con modalità che non assicurano la conformità dei dati acquisiti rispetto agli originali.

Nella lettura della Suprema Corte, l'estrazione dei dati archiviati su supporto informatico sequestrato non costituirebbe infatti un accertamento tecnico irripetibile (da esperirsi in contraddittorio ai sensi dell'art. 360 c.p.p.) trattandosi di "*operazione meramente meccanica, riproducibile per un numero indefinito di volte*". Ciò *"poiché non **esiste, ad oggi, uno standard prestabilito per la metodologia di trattamento ed analisi delle prove informatiche***", talché "*l'eventuale alterazione dei dati informatici – e, quindi, la loro inutilizzabilità – a seguito di operazioni effettuate sugli hard disk o su altri supporti informatici, costituisce oggetto di un accertamento di fatto da parte del giudice di merito che, se congruamente motivato, non è suscettibile di censura in sede di legittimità*" (Cass. Pen., sez. V, n. 24998/2015).

In altri termini, ogni vizio tecnico relativo alla fase esecutiva dell'estrazione dei dati sarebbe suscettibile di intaccare solo l'efficacia probatoria dei dati estratti, e non invece la loro utilizzabilità.

In questo panorama, l'indifferibile **necessità di una specifica**

regolamentazione della materia emerge anche dall'interpretazione recentemente fornita dalla **Corte di Giustizia dell'Unione Europea** della nozione di ***trattamento*****:** in particolare, con la sentenza emessa nell'ottobre 2024 nel **caso C-548/21**, la Corte ha riconosciuto tale "***anche un tentativo di accesso ai dati contenuti in un telefono cellulare, da parte dell'autorità di polizia ai fini di una indagine in materia penale***".

Ciò premesso, appare meritoria – pur con alcune riflessioni critiche che verranno esposte sinteticamente nel prosieguo – **l'iniziativa legislativa n. 1822 "Zanettin-Bongiorno"**, approvata dal Senato nel mese di aprile 2024 e attualmente al vaglio della Camera.

Tale proposta prevede l'inserimento dell'**art. 254-*ter* c.p.p.**, volto a disciplinare, in maniera puntuale e sistematica, il "***sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute***", delineando un *iter* procedurale di chiara impronta garantista, in parte mutuato dal sistema previsto per le intercettazioni.

II. IN ATTESA DELLA RIFORMA: LE LINEE GUIDA SUI SEQUESTRI INFORMATICI ADOTTATE DALLA PROCURA DELLA REPUBBLICA DI ROMA

Il 9 giugno 2025, preso atto dell'esistenza di **contrasti interpretativi** su alcuni aspetti rilevanti della disciplina in materia di sequestri informatici – anche alla luce della citata pronuncia della Corte di Giustizia – la **Procura della Repubblica di Roma** ha adottato, in attesa della conclusione dei lavori parlamentari sul nuovo art. 254-*ter* c.p.p., delle **linee guida** senz'altro utili a orientare gli interpreti e gli operatori del diritto.

Muovendo da un'attenta ricognizione degli orientamenti giurisprudenziali formatisi negli ultimi anni, e dimostrando una notevole sensibilità rispetto alla delicatezza dei contrapposti interessi in gioco, la Procura compie un pregevole sforzo di **contemperamento tra le esigenze di efficienza dell'attività investigativa e il rispetto dei principi sanciti dalla normativa europea.**

In particolare:

- preso atto dell'esistenza di orientamenti contrastanti, a livello tanto nazionale quanto sovranazionale, circa la possibilità che il Pubblico Ministero possa o meno procedere senza una previa autorizzazione del Giudice al sequestro di un dispositivo telefonico mobile, la Procura opta

per la soluzione interpretativa meno restrittiva, riservandosi pertanto la **facoltà di disporre il sequestro e procedere all'analisi dei dispositivi sequestrati in autonomia**;

- considerato che il **decreto di sequestro** può essere sottoposto ad impugnazione sia dinanzi al Tribunale del Riesame che alla Corte di cassazione, esso deve contenere, per garantire l'adeguatezza e la proporzionalità del provvedimento, **un'esplicita indicazione**:

  i. delle **cose da ricercare** all'interno dei dispositivi;

  ii. del **nesso di pertinenzialità** tra le cose da ricercare e i fatti oggetto dell'indagine;

  iii. dei **criteri** da utilizzare per la ricerca del materiale rilevante all'interno dei **dispositivi.**

- la Procura individua **criteri tecnici e procedurali** volti a garantire l'**autenticità** dei dati, il **contraddittorio sui criteri di ricerca** degli stessi e la **riservatezza** dei medesimi una volta raccolti.

Il fatto che si sia avvertita l'esigenza di predisporre linee guida operative rappresenta un chiaro indice della consapevolezza, da parte degli inquirenti, delle carenze regolative che ad oggi connotano uno degli snodi nevralgici delle indagini preliminari.

Benché lo sforzo interpretativo/creativo dei Procuratori della capitale appaia tecnicamente apprezzabile e indubbiamente animato dai migliori propositi, risulta evidente come l'intervento organico del legislatore nazionale sia ormai imprescindibile.

La tutela dei diritti fondamentali degli indagati e dei terzi coinvolti nei procedimenti penali, così come l'esatta osservanza della normativa sovranazionale, non possono infatti essere rimessi alla sola iniziativa degli inquirenti.

III. L'ART. 254-*TER* C.P.P.: ANALISI SCHEMATICA DELLA NUOVA DISPOSIZIONE

Come accennato in premessa, il nuovo art. 254-*ter* c.p.p., attualmente al vaglio della Camera, è destinato a regolare il microcosmo dei **sequestri probatori** di dispositivi e sistemi informatici o telematici, dei dati e della corrispondenza in essi contenuti, approntando un *iter* procedurale in parte mutuato dal sistema previsto per le intercettazioni.

Per ragioni di sintesi, in questa sede ci si soffermerà sulle sole previsioni che appaiono di maggiore interesse.

Il **primo comma** della disposizione prevede che il Pubblico Ministero, qualora determinati dispositivi, sistemi informatici o telematici ovvero memorie digitali siano "***necessari per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del principio di proporzionalità***", richiede al **Giudice per le Indagini Preliminari** l'emissione di un decreto di sequestro motivato, che sarà poi trasmesso ed eseguito a cura del Pubblico Ministero stesso.

Il **quarto comma** delinea invece le condizioni in cui Pubblico Ministero o Polizia Giudiziaria possono procedere **autonomamente** al sequestro. Se infatti la "***situazione di urgenza***" rende impossibile attendere il provvedimento del Giudice, il sequestro è disposto:

- dal Pubblico Ministero, con decreto motivato;
- dalla Polizia Giudiziaria, che trasmette al Pubblico Ministero il relativo verbale entro 48 ore.

Entro le 48 ore successive all'emissione del decreto o dalla ricezione del verbale, il Pubblico Ministero chiede dunque al Giudice la **convalida** del sequestro e l'emissione del decreto di cui al primo comma, il tutto **a pena di perdita di efficacia** del sequestro stesso (come previsto dal successivo **quinto comma**).

Così effettuato il sequestro del dispositivo, la norma disciplina il successivo ***iter* di selezione e apprensione dei dati** in esso contenuti.

La **prima fase** si sostanzia nella **duplicazione** integrale del contenuto del dispositivo.

Segnatamente, il Pubblico Ministero procede a:

- fissare una data per il **conferimento dell'incarico** per la duplicazione, che deve avvenire **entro 15 giorni** dal deposito del verbale di sequestro;
- **avvisare, entro 5 giorni dal deposito del verbale di sequestro, i soggetti interessati** (indagato, destinatario del sequestro e avente diritto alla restituzione, persona offesa dal reato e relativi difensori), i quali hanno facoltà di nominare consulenti tecnici;
- con l'eventuale **partecipazione** di difensori e consulenti tecnici – facoltà espressamente prevista dall'**ottavo comma** – si svolgono le **operazioni di duplicazione**, che:
  - **i.** possono avere ad oggetto sia i dati contenuti sul dispositivo sequestrato che quelli accessibili da remoto;
  - **ii.** devono avvenire su adeguati supporti informatici,

mediante una procedura che assicuri la **conformità** rispetto all'originale e l'**immodificabilità** della copia (**nono comma**);

- l'**undicesimo comma** prevede che, una volta effettuata la duplicazione, il Pubblico Ministero dispone **l'immediata restituzione all'avente diritto** del dispositivo, del sistema o della memoria digitale, a meno che non ne venga disposto il sequestro preventivo ai sensi dell'art. 321 c.p.p.

Gli avvisi e la partecipazione delle parti alle operazioni di duplicazione dei dati *non* sono invece previsti nei casi di cui al **decimo comma**, ossia:

- nei procedimenti per alcuni specifici gravi titoli di reato;
- in caso di pericolo per la vita o l'incolumità di una persona;
- in caso di pericolo per la sicurezza di Stato;
- in caso di pericolo di concreto pregiudizio per le indagini in corso;
- in caso di pericolo attuale di cancellazione o dispersione dei dati, delle informazioni o dei programmi.

Una volta realizzata la copia forense del dispositivo sequestrato, si avvia una **seconda fase** inerente al **sequestro dei dati, delle informazioni e dei programmi "*strettamente pertinenti al reato*"**, in relazione alle circostanze di tempo e di luogo del fatto e delle modalità della condotta, nel rispetto dei **criteri di necessità e proporzione**, come disposto dal **dodicesimo comma**.

A ciò procede **il Pubblico Ministero con decreto motivato**, in esito all'analisi del contenuto del duplicato.

Tuttavia, qualora i dati di interesse probatorio siano **inerenti a "*comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute*"**, il Pubblico Ministero richiede l'emissione del decreto al **Giudice per le Indagini Preliminari**, il quale provvede nel rispetto dei presupposti e dei limiti previsti dalla **disciplina delle intercettazioni**.

Per quanto concerne l'utilizzabilità dei dati, trova applicazione – in quanto compatibile – la normativa relativa alle intercettazioni telefoniche, con i relativi limiti di circolazione in altri procedimenti.

Una volta sequestrati, i dati sono riversati su un ulteriore **supporto idoneo** che viene poi acquisito al fascicolo (**comma tredicesimo**), mentre il **duplicato informatico** del dispositivo viene conservato presso la Procura in un luogo che ne garantisca la **sicurezza** e la **assoluta riservatezza** (**comma sedicesimo**).

Tuttavia, agli **interessati** è riconosciuta la facoltà di chiedere al Giudice la **distruzione** dei dati, delle informazioni e dei programmi contenuti nel duplicato laddove essi non siano necessari per il procedimento (**comma diciassettesimo**).

IV. LE NOVITÀ DA ACCOGLIERE CON FAVORE

La proposta legislativa in analisi ha il pregio di introdurre una serie di presidi processuali nel microcosmo dei sequestri informatici, delineando una cornice normativa a tutela di diritti fondamentali quali il **diritto al rispetto della vita privata**, alla **protezione dei dati personali** e alla **libertà e segretezza delle comunicazioni**.

L'obiettivo, certamente encomiabile, è quello di **colmare un vuoto regolatorio** che, fino ad oggi, ha reso necessaria la salvaguardia di tali diritti attraverso la supplenza della giurisprudenza e il ricorso alle prassi operative – pur apprezzabili, ma non sempre uniformi – delle Procure.

Il testo risulta dunque meritevole di apprezzamento nella parte in cui rimedia a significative lacune di tutela, valorizzando alcuni principi cardine individuati dalla giurisprudenza nazionale e sovranazionale, tra i quali spiccano quelli di **necessità e proporzione**, posti quale **architrave dell'intera proposta normativa**.

Altrettanto pregevole risulta la chiara volontà del legislatore di sottoporre ad un **vaglio giurisdizionale** quella che ad oggi risulta, di fatto, una delle fasi più incisive dell'attività di indagine.

Del pari apprezzabili sono, a parere di chi scrive, la **dettagliata regolamentazione** della fase dell'estrazione della copia forense e l'introduzione del relativo **contraddittorio**, nonché la previsione che all'interno del fascicolo processuale confluisca solo il materiale ritenuto "*strettamente pertinente al reato*", sulla base degli appositi parametri previsti *ex lege.*

V. I PROFILI CRITICI DELLA RIFORMA

Pur riconoscendo i lodevoli intenti che animano la Riforma, i commentatori hanno evidenziato numerosi possibili margini di miglioramento.

Seguendo l'ordine dell'art. 254-*ter* c.p.p., che allo stato deterrebbe il non invidiabile primato di articolo più lungo del codice di procedura, si può infatti notare che:

- i **presupposti** che legittimano il sequestro di un dispositivo appaiono fortemente **indefiniti:** il richiamo alle "*circostanze di tempo e di luogo del fatto e alle modalità della condotta*", infatti, risulta di difficile interpretazione. Seguendo un approccio rigoristico, si potrebbe paradossalmente arrivare

a sostenere che, qualora circostanze del fatto e modalità della condotta siano pacifiche, non sarebbe possibile sequestrare un dispositivo informatico – e ciò a prescindere dalla pertinenza e dall'utilità dei dati in esso contenuti rispetto ad altri aspetti dell'indagine, come, ad esempio l'individuazione dell'identità dei soggetti coinvolti;

- realisticamente, si imporrebbe un **doppio, o addirittura triplo, coinvolgimento del Giudice** per le Indagini Preliminari per ogni singolo dispositivo sequestrato, posto che:

  i. il sequestro del dispositivo viene disposto dal Giudice;

  ii. il successivo (prevedibile) sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza in esso contenuti deve essere disposto, nuovamente, dal Giudice;

  iii. laddove ricorrano i presupposti per disporre il sequestro preventivo del dispositivo ovvero dei dati contenuti al suo interno, il Giudice interverrà con apposito provvedimento ai sensi dell'art. 321 c.p.p.;

- ***non*** è previsto il **coinvolgimento né del difensore né dei consulenti** nella fase della **selezione dei dati** visionati dal Pubblico Ministero sulla copia forense del dispositivo; tale fase, peraltro, peraltro, ***non*** risulta scandita da **precisi termini procedurali**;

- ***non*** **è chiaro il perimetro applicativo dei limiti di utilizzabilità previsti dalla disciplina delle intercettazioni** (richiamati dal comma quattordicesimo): in particolare, è dubbio se essi riguardino esclusivamente i dati inerenti a comunicazioni, conversazioni e corrispondenza, ovvero se si applichino all'intero contenuto dei dispositivi sequestrati – compresi dati che nulla hanno a che fare con comunicazioni, conversazioni, o corrispondenza (ragioni di collocazione sistematica farebbero propendere per la prima interpretazione, ma il dato normativo non fornisce indicazioni univoche in tal senso, lasciando dunque spazio a incertezze applicative);

- la Procura rimane in possesso della **copia integrale del contenuto dispositivo per l'intera durata del processo**, indipendentemente dalla relativa utilità;

- ***non*** risulta vi sia una chiara **sanzione processuale** in caso di **mancato rispetto della procedura**

delineata, posto che non si rinviene una esplicita previsione di inutilizzabilità dei dati raccolti o prodotti in violazione del dettato normativo.

VI. CONCLUSIONI

Gli operatori del diritto concordano sulla necessità di un intervento legislativo in materia di acquisizione probatoria del contenuto dei dispositivi informatici, e la proposta di legge in esame offre interessanti spunti di riflessione per individuare un **equilibrato bilanciamento tra i delicati interessi in gioco**.

Ciò posto, si auspica che la discussione parlamentare sull'art. 254-*ter* c.p.p. conduca all'adozione di una procedura che, tutelando il diritto alla riservatezza dei cittadini, risulti al contempo più snella e definita nei suoi parametri e confini.

Contatti

Giuseppe Fornari
Founder Partner

g.fornari@fornarieassociati.com

Francesca Procopio
Associate

f.procopio@fornarieassociati.com

Pietro Frazzica
Trainee Lawyer

p.frazzica@fornarieassociati.com

Milano
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

Roma
Piazza Adriana 5
T: +39 0622201000
E: roma@fornarieassociati.com

Bari
Via Principe Amedeo 25
T: +39 080 918 4280
E: bari@fornarieassociati.com

Fornari e Associati

www.fornarieassociati.com