GIUSTIZIA INSIEME

Processo Penale " class="voce">

La lotta alla criminalità organizzata e il sequestro di dispositivi, sistemi informatici o telematici o memorie digitali

di Giovanni Melillo

28 maggio 2025

Memoria illustrativa del Procuratore Nazionale Antimafia e Antiterrorismo sulle novità contenute nella proposta di legge AC 1822, approvata dal Senato della Repubblica il 10 aprile 2024, relativa alla modifica del codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali.

Reputo doveroso rassegnare le considerazioni che seguono, in ragione dell'allarme per l'efficacia delle indagini in materia di criminalità organizzata e di sicurezza cibernetica che genera la considerazione di alcuni dei contenuti della proposta di legge AC 1822, approvata dal Senato della Repubblica il 10 aprile 2024.

Come noto, la proposta legislativa in oggetto prevede una innovativa procedura per i sequestri di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute (art. 254-*ter* c.p.p.)

Le soluzioni prefigurate per non pochi e rilevanti aspetti destano profonda preoccupazione.

Naturalmente, non è in discussione la necessità di deciso rafforzamento delle garanzie difensive, ma la capacità di individuare forme di adeguata protezione dei diritti senza minare ingiustificatamente la capacità di risposta repressiva dei più gravi fenomeni criminali.

In generale, credo di essere stato fra i primi a porre in sede parlamentare il tema di un deciso avanzamento degli equilibri fra esigenze delle indagini e diritti della persona, attraverso la previsione di nuove e più elevate garanzie individuali e della stessa funzione difensiva.

Mi riferisco alla mia audizione dinanzi alla Commissione giustizia del Senato del 31 gennaio 2023. In quella sede, infatti, sottolineavo come vi fosse:

"un evidente ritardo normativo nel prendere atto della profonda necessità di innalzamento delle garanzie legali collegate alla tutela dei dati personali che confluiscono nei sistemi digitali: un ritardo evidente, direttamente collegato al da tempo sopravvenuto rilievo eccezionale dei dati personali diversi da quelli oggetto della tradizionale captazione delle comunicazioni: ma tale da imporre, come è stato detto, "la formulazione di un nuovo apparato normativo dagli orizzonti più vasti". La stessa nozione codicistica di "intercettazione", intesa quale captazione clandestina dei flussi di comunicazione in atto fra due soggetti, entra in crisi nell'era digitale, non valendo ad abbracciare e disciplinare unitariamente fenomeni diversi, ma caratterizzati comunemente dalla sottrazione alla sfera di privatezza delle persone di dati di straordinario rilievo giuridico e sociale. È questo un punto cruciale per cogliere la radice di tensioni che la giurisprudenza mostra di non saper risolvere e che probabilmente non può risolvere, come dimostra la sofferenza visibile nell'impiego delle tradizionali categorie del documento e della corrispondenza per individuare la cornice normativa di attività invasive per le quali si rivela la necessità di rafforzamento delle garanzie individuali. Una sofferenza ancor più grande, perché palesemente sostenuta dalla consapevolezza che soltanto il legislatore può definire il punto di equilibrio fra efficienza delle indagini e tutela della riservatezza e delle altre libertà fondamentali; è forse giunto il momento di riconoscere che vi è un deficit di effettività del principio di legalità processuale e delle correlate garanzie difensive che può essere colmato senza pregiudizio per le esigenze di accertamento dei reati più gravi e in coerenza con l'intervento legislativo del 2017; mi riferisco alle possibilità di acquisizione occulta di chat pregresse e comunque di contenuti dei dispositivi di comunicazione telematica mediante captatore in funzione on line search o alle possibilità di ispezione, perquisizione e sequestro di archivi informatici, quali quelli contenuti anche in un semplice smartphone, derivanti dall'inquadramento giurisprudenziale di queste attività come attività "atipiche" di ricerca della prova: è giunto il momento, di "valorizzare, nel settore delle indagini digitali, il principio di proporzionalità quale parametro di legittimità per le attività investigative"... , ciò che oggi non è, se, come sovente accade, è dato sequestrare uno smartphone o altro dispositivo analogo con provvedimento adottabile procedendo per qualsivoglia reato: in ipotesi, anche per semplici contravvenzioni ovvero comunque per delitti di scarsa gravità. In pratica, si tratta di

innalzare il valore del principio di libertà di comunicazione prevedendo l'intervento del Giudice e l'introduzione di rigorose condizioni di proporzionalità ed adeguatezza dell'agire investigativo, così legando l'esercizio del potere di acquisizione dei dati personali a rigidi presupposti, definiti da adeguati limiti edittali e da altre tassative specificazioni e, non ultimo, a più rigorosi e perciò controllabili oneri motivazionali; soprattutto, è necessario prevedere che i dati siano trattati come quelli delle intercettazioni, confluendo nell'Archivio delle Intercettazioni: soltanto così i dati irrilevanti a fini di giustizia potranno restare segregati e sfuggire ad ogni diffusione sterminatrice della reputazione, dell'onore e della vita delle persone."

Dunque, non può che trovare apprezzamento una disciplina che, per non pochi versi consolidando risultati intanto conseguiti in via interpretativa dalla giurisprudenza della Corte di Cassazione, prevede che le acquisizioni dai dispositivi informatici e telematici siano distinte tra rilevanti ed irrilevanti e, per le seconde, proprio come già previsto per le intercettazioni telefoniche, se ne disponga la conservazione, con diritto di accesso solo ai soggetti interessati al procedimento e senza estrazione di copie se non attraverso una procedura governata dal giudice.

L'allarme per la sorte delle indagini che il mio ufficio ha la responsabilità di coordinare nasce da ben altro.

Una prima ragione di grave preoccupazione nasce dalla constatazione della inutile pesantezza delle procedure per l'acquisizione, in fase di indagini, dei contenuti digitali.

Infatti, il testo normativo in esame, dispone che tale attività venga svolta attraverso ben tre provvedimenti di sequestro, dei quali due disposti dal GIP ed uno dal pubblico ministero.

Si prevede infatti che si debba adottare:

a) un primo sequestro - disposto dal GIP su richiesta del PM - relativo all'intero dispositivo;

b) un secondo sequestro - disposto dal PM - sui contenuti estratti che non abbiano carattere di comunicazioni informatiche o telematiche;

c) un terzo sequestro - ancora disposto dal GIP su istanza del PM - relativo ai contenuti estratti dal dispositivo che assumano natura di comunicazioni.

A questa lunga teoria di atti si dovrà inoltre aggiungere un ulteriore sequestro - di natura preventiva, disposto dal GIP su richiesta del PM - qualora il dispositivo, una volta estratti i contenuti rilevati, non possa essere restituito, perché contenente dati o informazioni la cui detenzione integra il reato (ad esempio materiale pedopornografico), ovvero perché suscettibili

di confisca obbligatoria o facoltativa all'esito del giudizio, in quanto utilizzato per la commissione del reato (come accade per il dispositivo utilizzato per commettere i reati di *stalking* ex art. 612-*bis* c.p. o di *revenge porn* ex art. 612-*ter* c.p., ma come accade anche per i gravi delitti cibernetici con riguardo a dispositivi e infrastrutture utilizzati per attacchi ad infrastrutture critiche).

Appare certo che questa proliferazione di interlocuzioni con il GIP per ogni dispositivo sequestrato, oltre a ritardare oltremodo le indagini, procurerà un aggravio insostenibile per uffici spesso onerati da ritardi superiori alla durata delle indagini preliminari nel vaglio delle richieste cautelari per indagini di criminalità organizzata.

Poco male, si dirà, se da questo passa necessariamente una più elevata tutela dei diritti individuali.

Ma forse sarebbe opportuno considerare l'impatto reale di una catena processuale così concepita.

Un duplice, anzi di regola triplice intervento del giudice delle indagini preliminari equivale ad introdurre un potente moltiplicatore dei casi di incompatibilità del giudice, insostenibile soprattutto negli uffici di minori dimensioni.

Un'architettura procedimentale così complessa per giungere alla acquisizione dei dati contenuti in dispositivi in sistemi informatici e telematici, ulteriormente appesantita nel caso in cui si tratti di estrarre contenuti comunicativi, appare sbilanciata rispetto al regime che disciplina le medesime acquisizioni di documenti in formato cartaceo anziché digitale, tanto da offrire, a chi avesse l'accortezza di documentare le proprie attività criminali solo su supporto digitale (si pensi alle scritture contabili o alle corrispondenze d'azienda) una tutela rafforzata nei confronti delle attività di indagine rispetto a chi tale scelta avveduta non abbia assunto.

Si potrebbe persino ironizzare sulla capacità del testo approvato dal Senato a divenire un vero e proprio incentivo alla digitalizzazione delle attività illecite o quantomeno della loro documentazione.

Ma anche l'amaro sorriso dell'ironia si spegne dinanzi alla considerazione della brutalizzazione delle esigenze di contrasto della criminalità mafiosa e delle minacce alla sicurezza cibernetica che inevitabilmente deriverà da altri contenuti del disegno di legge, se approvato nella sua attuale formulazione.

Prima di considerare tali aspetti, appare doveroso, in omaggio ad elementari canoni di lealtà istituzionale, segnalare che l'eccessiva onerosità pratico-organizzativa e ordinamentale prima sottolineata potrebbe ridursi grandemente senza sacrificio per le istanze di maggior tutela delle corrispondenze acquisibili tramite analisi dei dispositivi.

Sul punto conviene dunque segnalare che il regime attualmente delineato potrebbe modificarsi prevedendo che il sequestro previsto dall'art. 1, comma 1, della proposta, relativo all'intero dispositivo, possa estendersi anche ai contenuti non comunicativi estratti all'esito dell'analisi e quindi, assorbire in sé anche l'ipotesi disciplinata al comma 12, prima parte. Al contempo, una specifica ed ulteriore valutazione, riservata esclusivamente al GIP, potrebbe riguardare i soli contenuti comunicativi ritenuti rilevanti per le indagini come già previsto dalla seconda parte dello stesso comma 12.

Sempre in funzione di semplificazione ed alleggerimento della procedura, si potrebbe altresì prevedere, in relazione alla disciplina dettata per la restituzione del dispositivo analizzato (cfr. comma 11 dell'articolo 1 del testo), che il sequestro originario possa essere mantenuto, con eventuale reiezione dell'istanza di parte volta alla restituzione, in tutti i casi nei quali il dispositivo possa essere oggetto di confisca facoltativa o obbligatoria all'esito del giudizio e nei casi in cui contenga dati o programmi dei quali sia vietata la detenzione.

Operando queste modifiche si potrebbe ricondurre l'intera disciplina in una dimensione di sostenibilità, senza alcun nocumento oggettivo ai diritti di libertà ed inviolabilità delle comunicazioni private che si intende qui tutelare.

Il barocco nell'arte ha prodotto capolavori straordinari, ma nell'amministrazione della giustizia le architetture normative che ne imitano la tendenza alla sovrabbondanza formale possono generare effetti disastrosi.

Non soltanto nella dimensione processuale nazionale.

L'introduzione del nuovo regime produrrà conseguenze non di certo positive anche sulla rapidità e sull'efficacia della cooperazione giudiziaria internazionale.

In relazione alla domanda di cooperazione degli altri Stati, la laboriosità delle procedure di sequestro e successive analisi dei dispositivi produrrà certamente un significativo allungamento

dei tempi di risposta della giustizia italiana, ciò che risulterà insopportabile con riferimento a quelle indagini, prime tra tutte quelle relative ai crimini informatici, che richiedono una assoluta speditezza al fine di non disperdere l'utilità dei dati investigativi che si vanno acquisendo.

Ad esempio, l'acquisizione di un indirizzo IP, fondamentale per giungere all'individuazione degli autori del crimine, diverrà inutile se conseguita oltre i termini di *data retention* differenti da Stato a Stato e fino ad ora non disciplinati uniformemente da un testo sovranazionale.

Per non parlare, poi, nel caso di esecuzione di un provvedimento di sequestro disposto dalla A.G. estera di un *server* in Italia, della necessità di effettuare, con le modalità della consulenza tecnica irripetibile, la copia forense, così "vincolando" gli ordinamenti esteri a "subire" macchinosi e defatiganti procedimenti, per mettere a disposizione un *device*, che, ad oggi, verrebbe consegnato in tempi rapidi.

Si pensi, soltanto, alla necessità di:

a) notificare gli avvisi, ovviamente da tradurre, anche all'estero;

b) nominare degli interpreti, ove gli interessati esteri intendano partecipare al conferimento dell'incarico.

Ancor più difficile sarà poi giungere ad una acquisizione di *e-evidence* all'estero che risulti all'esito utilizzabile nel processo italiano.

Infatti, la Corte di Giustizia e la giurisprudenza nazionale stabiliscono che, ai fini dell'utilizzabilità, le modalità di acquisizione adottate all'estero non devono essere meno garantite di quelle previste dal diritto interno per la gestione di situazioni analoghe (Corte Giust. UE Grande Sez. 6 ottobre 2020, C-511/18).

Non vi è dubbio che una procedura come quella in esame non abbia analogie con altre discipline straniere.

Sulla sorte reale delle prospettive della cooperazione internazionale peserà grandemente altresì la disposizione - dell'intrinseca irragionevolezza della quale si dirà oltre - dell'art. 1, comma 14, relativa ai limiti di utilizzabilità delle acquisizioni dei contenuti digitali.

Di fatto, per tale via si disperderanno i vantaggi dell'acquisizione di prove legalmente assunte negli ordinamenti di altri Stati, connessi alla possibilità di estendere gli effetti della richiesta di cooperazione giudiziaria a procedimenti diversi e per reati diversi.

Oggi, se una Autorità giudiziaria estera - in esecuzione di una commissione rogatoria o di un ordine di indagine europeo - consegna un *device* sequestrato in quello Stato, senza apporre condizioni sull'utilizzo processuale, l'Autorità giudiziaria italiana può ben utilizzare il contenuto, anche per reati diversi da quello per cui si procede e ben può mettere a disposizione quella memoria digitale anche di altre autorità giudiziarie ove emergano nuovi e diversi reati di competenza di altri uffici.

Domani, ove approvato nella sua attuale formulazione il testo in esame, viceversa, l'Autorità giudiziaria italiana, senza che vi siano condizioni apposte da quella estera, sarà costretta all'utilizzo del materiale di prova faticosamente per le sole fattispecie di reato per cui già procedeva, salvo a reiterare la medesima domanda, con inutile dispendio di tempo e risorse, in ogni ulteriore procedura interna.

Naturalmente, pur in mancanza dei limiti propri delle clausole di specialità del diritto internazionale penale, ben può il legislatore ancorare l'utilizzabilità dei dati acquisiti a parametri corrispondenti a fondamentali principi di proporzionalità e adeguatezza delle soglie di tutela.

Ma proprio per questa via si giunge al vero punto di crisi dell'intero sistema delle indagini in materia di criminalità organizzata e *cybercrime* generato dall'impianto normativo prefigurato.

Come accennato, il disegno di legge prevede al comma 14 dell'art. 1 l'applicazione di varie disposizioni codicistiche, fra le quali quelle di cui all'art. 270 c.p.p., dettate in tema di utilizzazione delle intercettazioni in altri procedimenti.

Secondo tali disposizioni, i risultati delle acquisizioni non saranno utilizzabili in procedimenti diversi, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.

La stessa, gravemente pregiudizievole disciplina introdotta dal legislatore del 2023 per le intercettazioni, ma con incalcolabili effetti ingiustificatamente nocivi per la tenuta dell'azione di contrasto dei più gravi fenomeni criminali.

Quale sarà questo disastroso impatto, si fa presto ad indicare, passando in rapida rassegna il dettato dell'art. 380 c.p.p., per verificare quali siano alcuni dei delitti rispetto ai quali la documentazione informatica acquisita non costituirebbe più prova in altri procedimenti:

- art. 256 c.p. (procacciamento di notizie segrete concernenti la sicurezza dello Stato)

- art. 314 c.p.: peculato, anche se aggravato dalla finalità di agevolazione di organizzazioni mafiose o commesso avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- artt. 316-*bis* e 316-*ter* c.p., delitti di malversazione di erogazioni pubbliche e indebita percezione di erogazioni pubbliche, disposizioni queste che sanzionano condotte di chi rispettivamente destini risorse pubbliche per finalità diverse per le quali sono state erogate e di chi riceva contributi, sovvenzioni, finanziamenti dallo Stato presentando documenti falsi o atti equipollenti, anche se aggravati dalla finalità di agevolazione di organizzazioni mafiose o commessi avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 318, 319, 319-*ter*, corruzione, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 321 c.p., corruzione in atti giudiziari, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose (eccettuato il caso, assai raro, di fatto da cui deriva una ingiusta condanna superiore ad anni cinque di reclusione);

- art. 326 c.p.: rivelazione di segreto di ufficio, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- artt. 353 e 353-*bis* c.p., in tema di turbata libertà degli incanti e turbata libertà di scelta del contraente, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 356 c.p., frode nelle pubbliche forniture, anche aggravata dalla finalità agevolatrice di mafia o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- artt. 378 e 379 c.p., delitti di favoreggiamento personale o reale, anche se aggravati dalla finalità di agevolazione di organizzazioni mafiose o commessi avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 386 c.p., procurata evasione, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 390 c.p., procurata inosservanza di pena, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 391-*ter* c.p., introduzione indebita di cellulari e altri dispositivi idonei a effettuare comunicazioni in istituti penitenziari, anche aggravato dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 415-*bis* c.p., rivolta all'interno di un istituto penitenziario, anche aggravata dalla finalità di agevolazione di organizzazioni mafiose o commessa avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 416 c.p., direzione, organizzazione e partecipazione ad associazioni per delinquere, anche se aggravate dalla finalità di agevolazione di organizzazioni mafiose o avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 416, comma 6, c.p., direzione, organizzazione e partecipazione ad associazioni per delinquere finalizzate alla commissione di reati in materia di immigrazione illegale, salvo che il reato non sia aggravato dalla finalità di reclutare persone da destinare alla prostituzione o comunque allo sfruttamento sessuale o lavorativo ovvero riguardi l'ingresso di minori da impiegare in attività illecite al fine di favorirne lo sfruttamento ovvero dalla finalità di trame profitto, anche indiretto;

- art. 416 c.p., direzione, organizzazione e partecipazione ad associazione per delinquere finalizzata alla commissione di reati in materia di contraffazione di marchi, segni distintivi, brevetti, modelli e disegni nonché di introduzione nello Stato e commercio di prodotti con segni falsi, anche se aggravate dalla finalità di agevolazione di organizzazioni mafiose o avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 416 c.p., partecipazione ad associazione criminosa diretta a commettere reati di sfruttamento sessuale di minori, compresa la violenza sessuale ai danni di minori degli anni diciotto;

- art. 452-*quaterdecies* c.p., attività organizzate per il traffico illecito di rifiuti, anche se si tratta di rifiuti ad alta radioattività e se aggravate dalla finalità di agevolazione di organizzazioni mafiose o commesse avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.

- art. 517-*quater* c.p., contraffazione di indicazioni geografiche o denominazione di origine dei prodotti agroalimentari, anche se aggravata dalla finalità di agevolazione di organizzazioni mafiose;

- art. 600-*quater* c.p., detenzione di materiale pedopornografico;

- art. 612-*ter* c.p., diffusione illecita di immagini o video sessualmente espliciti (c.d. *revenge porn*);

- art. 615-*ter* c.p., accesso abusivo ad un sistema informatico o telematico, anche se commesso da pubblico ufficiale o da incaricato di pubblico servizio o quando dal fatto derivi la distruzione o il

danneggiamento dei sistemi, anche se di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico;

- artt. 648-*ter* e 648-*ter* c.p., delitti di riciclaggio e di impiego in attività economiche e finanziarie di beni e altre utilità provenienti da delitto;

- delitti di detenzione e porto di un'arma comune da sparo, anche se aggravati dalla finalità di agevolazione di organizzazioni mafiose o avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- art. 86 d.lgs. 26 aprile 2024, n. 141, direzione, organizzazione e partecipazione ad associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri, anche se aggravate dalla finalità di agevolazione di organizzazioni mafiose o avvalendosi delle condizioni di cui all'art. 416-*bis* c.p.;

- tutti gli altri numerosi delitti che, se pur commessi con finalità di agevolazione mafiosa ovvero avvalendosi delle condizioni di cui all'art. 416-*bis* c.p., non abbiano soglie edittali tali da rientrare nel novero di quelli suscettibili di arresto obbligatorio in flagranza.

Tali indicative esemplificazioni offrono misura visibile del sacrificio delle istanze di contrasto dei fenomeni criminali ai quali si riferiscono.

Naturalmente, si tratta di materia tipicamente affidata alla responsabilità politica propria dell'attività legislativa, ma della quale appare doveroso far risaltare gli effettivi contorni più chiaramente di quanto riesca a rendere la tecnica del rinvio alla disposizione che regola l'utilizzabilità delle intercettazioni in altri procedimenti mediante ulteriore rinvio alla disciplina dei casi di arresto obbligatorio nella flagranza del reato.

È appena il caso di sottolineare che anche le medesime limitazioni alla circolazione della prova acquisita mediante intercettazioni di così gravi delitti o, per lo meno, in ogni caso, di quelli commessi al fine di agevolare le associazioni mafiose o avvalendosi delle condizioni di cui all'art. 416-*bis* c.p. introdotte nella conversione del d.l. 90/2023 meriterebbero nuova e più attenta considerazione, per il loro disastroso impatto sulla sorte delle indagini in materia di criminalità organizzata.

Ma è del tutto evidente che la riproduzione di quelle medesime limitazioni all'acquisizione dei dati digitali contenuti in dispositivi e sistemi informatici e telematici appare destinata ad ingigantirne la portata paralizzante delle investigazioni, anche in materia di criminalità organizzata, che la realtà impone invece di proiettare verso le strutture e le attività criminali che ormai trovano nello spazio virtuale la loro ordinaria dimensione, a partire da quelle che si

nutrono di criptovalute o ormai si svolgono nel metaverso.

Si tenga in considerazione il dato per cui l'art. 270 c.p.p. è una disposizione dettata a tutela delle garanzie di cui all'art. 15 Cost. (cfr. Corte costituzionale, sentenza n. 63 del 1994).

In altri termini, vi è una precisa necessità, di rilievo costituzionale, secondo la quale il decreto del giudice non deve divenire una sorta di autorizzazione in bianco, in forza della quale i risultati delle intercettazioni possano circolare liberamente al di fuori del recinto processuale in cui essi sono stati acquisiti.

Ma questa esigenza non pare riconoscibile nel caso in esame, nel quale la prova acquisita è costituita da documenti informatici, che vengono appresi in un'unica soluzione, nel rispetto di principi di pertinenza e di proporzionalità.

Un'acquisizione che, secondo il nuovo statuto processuale, è ben più articolata rispetto alle stesse attività in materia di intercettazione, atteso che sono previsti fino a tre diversi decreti dell'autorità giudiziaria, tutti ancorati alla necessità di scrutinio della sussistenza di rigorosi presupposti.

La scelta prefigurata attraverso l'espresso richiamo all'art. 270 del codice di rito non sembra giustificata. Certamente non lo è nella dimensione accolta nel testo approvato dal Senato.

In primo luogo, il richiamo alla citata disposizione pare esteso sia ai contenuti di natura comunicativa che a quelli di natura non comunicativa, rinvenuti nei dispositivi sequestrati.

Ma soltanto, i primi possono essere latamente assimilabili ai contenuti di una captazione; i secondi vanno comunque equiparati a meri documenti digitali.

Non è dato comprendere la ragione per la quale le esigenze di tutela della riservatezza delle comunicazioni debbano meccanicamente estendersi a un ambito del tutto avulso dal concetto di comunicazione.

In secondo luogo, attesa l'applicabilità dell'intero complesso normativo non solo agli *smartphone*, ma a qualsiasi dispositivo o sistema telematico caduto in sequestro, ne consegue che, rispetto, ad esempio, a un *server*, che ha l'ordinaria funzione di acquisire e trasmettere dati, qualsiasi elemento informatico in esso contenuto subirebbe lo stesso limitato regime di utilizzazione, producendo un effetto assolutamente abnorme.

Peraltro, che tale sistema di ridotta circolazione sia esorbitante anche rispetto agli obiettivi di tutela che il legislatore intende perseguire con questa riforma lo si desume dal raffronto con la

recente disciplina della acquisizione dei dati del traffico telefonico.

Si rammenti in proposito che la Corte costituzionale (sentenza n. 170/2023) ha evidenziato la natura comunicativa dei cd. tabulati, affermando come "*non possa ravvisarsi una differenza ontologica tra il contenuto di una conversazione o di una comunicazione e il documento che rivela i dati estrinseci di queste, quale il tabulato telefonico…*". E tuttavia, la recente modifica del regime di acquisizione dei tabulati telefonici, pur prevedendo l'intervento del giudice, come intende fare oggi il legislatore, non ha in alcun modo limitato l'utilizzazione probatoria dei risultati acquisiti ai sensi dell'art. 270 c.p.p.

Non vi è dubbio che il raffronto tra le due discipline rende evidente la irragionevolezza delle limitazioni di natura investigativa che si intendono introdurre oggi, attraverso il disegno di legge in esame.

Si rischia, all'evidenza, un pericoloso arretramento dell'azione di contrasto della criminalità mafiosa, in sostanziale spregio dell'impegno, asseritamente da tutti inteso come prioritario e inderogabile, a non indebolire gli strumenti investigativi utilizzabili per arginare la pericolosità di gruppi criminali che hanno ormai nello spazio virtuale il loro fondamentale cardine organizzativo.

In ogni caso, quand'anche si volesse mantenere la limitazione alla circolazione dei dati acquisiti in altri procedimenti al fine di non depotenziare il contrasto alla criminalità organizzata e alle minacce di natura cibernetica, sarebbe necessario prevedere che detto divieto di utilizzo non si applichi per tutti i reati di cui all'art. 51, comma 3-*bis* e 3-*quater*, c.p.p. e a quelli previsti nell'art. 371-*bis*, comma 4-*bis*, c.p.p.

In modo del tutto omogeneo con quanto già previsto in altra parte dell'articolato (art 254-*ter*, comma 10, c.p.p.), dove ci si è premurati di porre una apposita deroga processuale anche per i reati anzidetti, altrimenti svuotata di gran parte del suo reale valore.

Le considerazioni fin qui svolte non esauriscono i profili di criticità dei contenuti del disegno di legge, dovendo riservarsi le ultime osservazioni agli aspetti di maggiore ed ingiustificato appesantimento procedurale.

Il testo della novella prevede altresì che *"Nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, dispone con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici o di memorie digitali, 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 criterio di proporzione. Il decreto che dispone il sequestro è immediatamente trasmesso, a cura della cancelleria, al pubblico ministero, che ne cura l'esecuzione ."

Appare, invero, assai discutibile la delimitazione delle condizioni del sequestro dei dispostivi o sistemi informatici necessari per la prosecuzione delle indagini attraverso la formula "*in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta".*

Quid iuris, infatti, qualora il sequestro sia necessario non tanto per individuare le circostanze e di tempo e di luogo del fatto o per definire le modalità della condotta criminosa, ma per identificare gli autori del fatto?

Si pensi al caso in cui dall'utilizzo di videoriprese sia possibile definire, in termini di certezza assoluta, le circostanze di tempo e di luogo del fatto reato per cui si procede (ad esempio una rapina) e le modalità della condotta criminosa (due persone armate e travisate), ma non sia possibile identificare gli autori del fatto e questa identificazione necessiti anche dell'acquisizione di un *device* che possa contenere elementi utili per l'identificazione (videoriprese di sopralluoghi sui luoghi effettuati nei giorni precedenti).

L'identificazione degli autori non sembra possa ricomprendersi nel concetto di *modalità della condotta*, se non attraverso un'applicazione analogica della norma, come tale contrastante con il principio secondo il quale disposizioni eccezionali non possano essere applicate oltre i casi e i modi previsti dalla legge.

Ed ancora: se si vuole verificare se i soggetti indiziati di una determinata rapina ne abbiano commesse altre, il sequestro non sarebbe parimenti possibile, poiché non sono individuate le circostanze di tempo e di luogo dei fatti che radicano l'esigenza di proseguire le indagini.

Parimenti per identificare i fornitori di un ingente carico di stupefacenti ovvero gli autori di reati informatici, laddove siano già acclarate le modalità fattuali, i tempi e luoghi della attività criminosa.

Qualora il fatto sia esattamente ricostruito nella sua dinamica spazio/temporale e siano stati identificati gli autori, inoltre, può certamente accadere che il sequestro del dispositivo rivesta una indubbia utilità per rafforzare la piattaforma indiziaria acquisita a carico degli indagati.

In questo caso come conciliare le finalità di rafforzamento indiziario con le strettoie della disciplina normativa?

Proprio al fine di evitare queste difficolta, il legislatore del 1988, disciplinando all'art. 267 c.p.p. i presupposti a fronte dei quali è possibile autorizzare operazioni di intercettazione telefonica ed ambientale, ha stabilito che le stesse siano possibili qualora *assolutamente indispensabili* (o quantomeno *necessarie* per i reati ricompresi nell'art. 13 d.l. 152/1991) ai fini della prosecuzione delle indagini, senza ulteriori limitazioni.

In altre parole, per le intercettazioni, strumento questo ben più invasivo del sequestro di apparecchi informatici, la legge si limita a prevedere il requisito della assoluta indispensabilità ai fini della prosecuzione delle indagini, che, se da un lato, appare più rigoroso in termini generali (assoluta indispensabilità ai fini della prosecuzione delle indagini, rispetto a necessità per la prosecuzione delle indagini), dall'altro, però non indica in maniera espressa quali siano le esigenze che il mezzo di ricerca della prova mira a soddisfare.

Si segnala, pertanto, l'opportunità di eliminare dalla proposta di formulazione dell'art. 254-*ter*, comma 1, c.p.p. la dizione "*in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta*", sostituendola con quella: *necessari per la prosecuzione delle indagini,*

Appare, infine, doveroso rimarcare ulteriori aspetti critici.

Il dovere di assicurare il preventivo contraddittorio nella formazione della copia forense (art 254-*ter*, comma 6, c.p.p.) può risultare potenzialmente foriero di indebita dilatazione dei tempi di trattazione dei procedimenti e di aggravio di adempimenti, dovendosi notificare alle parti la data e l'ora del conferimento di incarico.

Ulteriori difficoltà operative il sequestro incontrerebbe allorquando debba essere effettuato in esecuzione di domande di assistenza internazionale, atteso che le notifiche dovrebbero essere fatte anche all'estero, previa traduzione degli avvisi nella lingua conosciuta dai soggetti cui devono essere notificati gli stessi. Non vi è dubbio che il rispetto di questa macchinosa procedura potrebbe creare non pochi ostacoli alla tempestiva risposta alla richiesta di assistenza formulata dalla autorità estera.

In particolare, al sesto comma dell'art. 254-*ter* c.p.p. si prevede, inoltre, che, entro 5 giorni dal deposito del verbale di sequestro, abbia inizio la procedura di formazione della duplicazione del contenuto del materiale informatico sequestrato attraverso la creazione di una copia immodificabile.

Giova, ai fini critici che si intende rassegnare, descrivere la scansione essenziale della relativa procedura:

a) avviso alle persone sottoposte a indagini, ai soggetti ai quali sono stati sequestrati i supporti, a quelli che avrebbero diritto alla restituzione e alle persone offese del giorno, delle modalità di conferimento dell'incarico di consulenza tecnica, mutuando dalla disciplina dell'art. 360 c.p.p.;

b) possibilità di duplicare anche dati, informazioni e programmi accessibili da remoto dal dispositivo in sequestro;

c) facoltà per le parti di nominare propri consulenti, di partecipare allo svolgimento delle operazioni e di formulare osservazioni e riserve;

d) restituzione dei supporti all'esito della formazione della copia forense, salvo che il sequestro sia stato disposto a fini preventivi.

Il disegno di legge opportunamente prevede delle deroghe alle disposizioni dettate dai commi 6, 7 e 8, laddove si proceda in relazione ai delitti previsti dagli artt. 406, comma 5-*bis*, c.p. e 371-*bis*, comma 4-*bis* c.p.p., ovvero quando ci sia il pericolo per vita o l'incolumità di una persona, per la sicurezza dello Stato, ovvero pericolo di concreto pregiudizio per le indagini in corso, o un pericolo attuale di cancellazione dei dati o delle informazioni.

In sostanza, negli anzidetti casi non è previsto il contraddittorio sulle modalità di duplicazione dei supporti, salva ovviamente l'osservanza di cautele per garantire che la copia formata sia conforme all'originale e sia ovviamente immodificabile.

Nonostante la clausola semplificatrice prima richiamata, l'impianto procedurale prefigurato appare oltremodo macchinoso e pregiudizievole per l'efficacia delle indagini.

Si pensi alla difficoltà ed alle lungaggini che derivano dalla necessità di procedere alla comunicazione dell'avviso di fissazione del conferimento dell'incarico di duplicazione, qualora il procedimento risulti iscritto a carico di numerosi indagati, alcuni dei quali magari residenti all'estero (si pensi, a meso titolo di esempio, ad articolati procedimenti penali in tema di criminalità economica transazionale, o in materia di riciclaggio transazionale o ancora di immigrazione clandestina), procedura che determina una inevitabile dilatazione dei tempi, difficilmente compatibile con i rigorosi termini delle indagini preliminari.

O ancora ai procedimenti penali con una pluralità di persone offese (ad esempio truffe a danno di un numero elevato di persone), alle quali è necessario dare avviso della data di fissazione del conferimento dell'incarico.

A fronte di queste ipotesi, tutt'altro che remote, la deroga prevista dall'art. 254-*ter*, comma 10, appare difficilmente applicabile, con il concreto rischio che le procedure di comunicazione dell'avviso consumino totalmente i termini di indagine preliminare.

Si tenga conto che la procedura proposta nella novella legislativa è parzialmente sovrapponibile a quella prevista dall'art. 360 c.p.p.

Bisogna però ricordare che la procedura ex art. 360 c.p.p. costituisce una eccezione alla procedura ordinaria di accertamento tecnico, cioè quella disciplinata dall'art. 359 c.p.p., come tale applicabile solo in caso in cui l'accertamento "*riguardi persone, cose o luoghi il cui stato è soggetto a modificazione*".

Non si comprende, in altre parole, perché a fronte di un accertamento tecnico, la duplicazione forense del contenuto del *device*, che attiene ad un oggetto che non presenta alcun rischio di modificazione (il dispositivo, infatti, è sotto sequestro e, qualora ricorra il rischio di sua modificazione o cancellazione, è possibile optare per la procedura semplificata ex comma 10) si debba seguire una procedura articolata, complessa, complicata e del tutto contraria alle naturali esigenze di speditezza investigativa.

Se la garanzia per tutte le parti processuali è costituita da quanto previsto dal successivo comma 9, a norma del quale "*La duplicazione avviene su adeguati supporti informatici mediante una procedura che assicuri la conformità del duplicato all'originale e la sua immodificabilità*" allora è difficile comprendere i motivi che inducono il legislatore a fare ricorso per la mera duplicazione forense (che si ricorda è solo un procedimento tecnico) ad una procedura complicata e che non fornisce garanzie di sicurezza maggiori rispetto a quella ordinaria.

Si rammenti che la formazione della cd. copia forense è considerata dalla Corte di cassazione una procedura che non richiede il contraddittorio anticipato.

Questo perché si tratta di attività meccaniche, che non richiedono alcuna complessa elaborazione intellettuale da parte dell'ausiliario del PM (cfr. Cass., Sez. II, 07/02/2023, n. 17984).

In conclusione, una procedura come quella prefigurata è destinata a creare un notevole e inutile appesantimento delle attività investigative, senza correlativo, reale rafforzamento delle garanzie.

Infine, va segnalato che il comma 12 dell'art. 1 del disegno di legge, nel regolare le attività consequenziali alla formazione della copia forense, detta prescrizioni che destano non poche perplessità.

Come detto, il sequestro informatico viene autorizzato dal GIP con decreto motivato, in relazione alla necessità di proseguire le indagini in relazione a circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del principio di proporzionalità.

Quindi, l'acquisizione del "contenitore" informatico presuppone un controllo giurisdizionale che, oltre a vagliare la ricorrenza del *fumus* del reato, deve altresì scrutinare le esigenze investigative poste a fondamento della mozione del pubblico ministero.

Se questo è il quadro, non appare comprensibile la esigenza che il PM emetta un provvedimento di sequestro, all'esito delle analisi del materiale informatico, su quelle informazioni, dati e programmi strettamente pertinenti al reato in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del principio di proporzionalità.

L'irragionevolezza di ciò si può cogliere se si correla quella previsione sia con la disciplina generale dei sequestri che con quella delle intercettazioni.

Infatti, laddove il pubblico ministero emetta un decreto di perquisizione e contestuale sequestro di quanto eventualmente rinvenuto, non è dato sapere a monte che cosa nello specifico verrà reperito nella disponibilità del soggetto attinto dal mezzo di ricerca della prova.

Però, una volta eseguito il provvedimento e reperito materiale pertinente con il provvedimento, non è necessario un nuovo decreto.

Si pensi al caso di una indagine nei confronti di un indiziato di pedofilia:

a) se il PM dispone perquisizione e sequestro, nel caso di reperimento di foto e altra documentazione fisica (bigliettini, lettere, manoscritti) che dimostrino il tema di accusa, non deve procedere a nuovo sequestro;

b) se il PM chiede al GIP la emissione di un sequestro informatico e vengono trovate le stesse foto, gli stessi bigliettini, lettere e manoscritti nella memoria del telefono (poiché esse erano state scansite ovvero fotografate e poi conservate nell'archivio del supporto), deve procedere a un nuovo sequestro, peraltro con presupposti non previsti per il sequestro fisico (stretta pertinenza con il reato, in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di proporzionalità e necessità).

Vi è poi un'altra considerazione.

Si è detto che il sequestro informatico presuppone uno scrutinio giurisdizionale in punto di *fumus* e di esigenze investigative.

Alla stessa stregua, *mutatis mutandis*, del regime delle intercettazioni, nel quale il mezzo di ricerca della prova presuppone un vaglio del giudice che procede.

Ebbene, nel caso delle intercettazioni, all'esito delle analisi effettuate dalla polizia giudiziaria, non viene emesso alcun provvedimento di sequestro del materiale pertinente al tema di prova (le tracce audio, video e telematiche rilevanti).

Semplicemente, il PM utilizza quel materiale a fini cautelari e, al momento antecedente all'esercizio dell'azione penale (avviso 415-bis c.p.p.; richiesta di giudizio immediato), deposita un elenco di tracce informatiche rilevanti, acquisendo dall'archivio riservato, atti giudiziari (decreto intercettivi e mozioni) e di polizia giudiziaria (annotazioni e informative), che afferiscano le tracce telematiche di cui all'elenco.

Tutto ciò, senza fare alcun provvedimento di sequestro.

Peraltro, il giudizio di rilevanza delle tracce intercettive non prevede alcuna stretta pertinenza al reato in relazione "*alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione*".

È sufficiente che vi sia un legame funzionale tra il materiale intercettivo e il reato per cui si procede, evitando inutili moltiplicazioni di adempimenti formali privi di reale idoneità a porsi a presidio dei diritti delle persone coinvolte nelle indagini,

Infine, qualche riflessione merita il riferimento ai presupposti in base ai quali il giudice può disporre il sequestro di dati inerenti a comunicazioni, conversazioni o a corrispondenza informatica inviata o ricevuta, presupposti che secondo la norma sono i seguenti;

- stretta pertinenza al reato *in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta.*

- limiti di ammissibilità di attività di intercettazione (art. 266 c.p.p.);

- presupposti dell'attività di intercettazione (art. 267, comma 1, c.p.p.).

Ne deriva che tutti gli elementi comunicativi rinvenuti all'interno di *device* sequestrato non potranno essere utilizzati qualora:

- attengano a fatti reato per cui non è ammissibile l'attività di intercettazione telefonica/ambientale;

- oppure, anche se relativi a fatti reato per cui è possibile l'attività di intercettazione, non sussistano gravi indizi della commissione del reato per cui si procede e l'acquisizione non sia assolutamente indispensabile alla prosecuzione delle indagini (salva la diversa disciplina prevista per i procedimenti per cui è applicabile l'art. 13 DL 152/91).

La conseguenza è del tutto evidente.

Per certe tipologie di reati per i quali non sussistono i limiti edittali di pena previsti dall'art. 266, comma 1 c.p.p., (pena della reclusione superiore nel massimo a cinque anni, salvo alcune limitate deroghe) si rischia di creare una sorta di inespugnabile cassaforte , al cui interno collocare dati cd. comunicativi che non potranno mai essere acquisiti in quanto relativi a reati puniti con la semplice pena dell'ammenda, della multa, dell'arresto o, infine, della reclusione, inferiore o corrispondente nel massimo a cinque anni.

Gli esempi sono molteplici e tutti facilmente declinabili.

Si pensi, ad esempio, a tutte le fattispecie di reati che così profondamente agitano la nostra sensibilità e incidono sulle nostre comunicazioni sociali, tra cui tutte le fattispecie di truffa, magari ai danni di persone fragili, (art. 640, comma 2, c.p.) o ai reati di accesso abusivo ai sistemi informatici (art. 615 ter, comma 1, c.p.) e frode informatica (anche nella fattispecie aggravata di cui all'art. 640 ter, comma 2, c.p.), oppure alla maggior parte dei reati tributari posti a presidio di primari interessi economici dello Stato (artt. 3, 4 e 5 d.lgs.. 74/2000); ed ancora a tutti i reati societari (2621 c.c. e seguenti), ai reati colposi tra cui il disastro colposo), ai reati posti a tutela del delicato lavoro svolte delle forze dell'ordine (art. 336 e 337 c.p.) per finire al reato che tutela le nostre frontiere, quello di favoreggiamento dell'immigrazione clandestina (art. 12, comma 5 e 5-*bis*, d.lvo 286/98). Ma gli esempi potrebbero continuare all'infinito.

Così come infinite appaiono le possibilità che una riforma di questa portata, nei limiti descritti, possa, al di là di ogni lodevole intenzione, determinare l'apertura di pericolosi spazi di sostanziale impunità di gravi fenomeni criminali.

Una conclusione tanto amara quanto realistica, in mancanza di necessarie correzioni.