

IL SEQUESTRO DEI DISPOSITIVI DI ARCHIVIAZIONE DIGITALE*

Katia La Regina



L'evoluzione tecnologica ha trasformato, innanzitutto, le cadenze di impiego dei tradizionali mezzi di ricerca della prova. Per questo aspetto, basti considerare che nelle indagini tradizionali, quantomeno di regola, la perquisizione o l'ispezione precedono il sequestro mentre, al contrario, nel caso delle investigazioni informatiche o comunque nel caso di indagini che investono dispositivi elettronici e per la comunicazione a distanza, è frequente che questo rapporto si inverta, nel senso che prima si sequestra il *device* per procedere poi alla sua ispezione o perquisizione.

L'esigenza di una rinnovata riflessione sulle ricadute dell'accentuata autonomia del sequestro - anche nell'ottica di quelle dinamiche di presupposizione logico-giuridica che, nei rapporti con la perquisizione, sono

state valorizzate per la ricostruzione del perimetro della invalidità derivata – è, tuttavia, solo una delle questioni che si pongono sul tappeto.

Il fronte più delicato è, infatti, quello che investe i vuoti di un settore alla cui dirompente evoluzione il legislatore non ha saputo offrire risposte adeguate. Una regolamentazione scarsamente congruente rispetto alle potenzialità espressive dell'agire investigativo, del resto, inesorabilmente conduce il sistema a sbilanciarsi sulle esigenze dell'accertamento, a tutto discapito dei diritti di difesa e di riservatezza.

Non pare un caso, dunque, che quello del sequestro di dispositivi di archiviazione digitale sia un settore in cui il principio di proporzionalità – che è presente nelle analisi della giurisprudenza europea e, seppure con declinazioni talvolta discutibili^[1], nella giurisprudenza nazionale^[2] – non riesce a permeare efficacemente l'attuale tessuto normativo.

Non ci sono regole per il governo dei dati acquisiti e, prima ancora, non sono posti limiti alla pervasività dello strumento investigativo: basti pensare che oggi è consentito sequestrare uno *smartphone* o un qualunque altro dispositivo elettronico in relazione a qualunque tipologia di reato, ancorché di scarsissimo allarme sociale; non vi è alcuna possibilità di sottrarre, tanto alle investigazioni quanto al processo, ciò che non è pertinente e rilevante e non è prevista alcuna forma di tutela della riservatezza dei dati acquisiti per il tramite del sequestro, al contrario di quanto possa dirsi in materia di intercettazioni^[3].

Perché questo parallelismo? È chiaro che ci sia una differenza tra l'intercettazione e il sequestro di dispositivi elettronici: ovviamente la differenza c'è, tra l'altro, sotto il profilo dinamico della comunicazione. Pare altrettanto indiscutibile, tuttavia, che tali difformità non sbiadiscono la possibilità di intravedere una connessione sul versante della portata offensiva: quando si sequestra uno *smatphone*, un *tablet*, un *computer* o, comunque, un *device* dalle funzioni similari, si consente l'acquisizione di una mole enorme di conversazioni, di documenti e di dati, anche risalenti nel tempo e anche relativi a terzi del tutto estranei al procedimento. Di conseguenza - a prescindere dalle modalità esecutive e dalle indiscutibili differenze tra i due atti - è chiaro che gli interessi in gioco siano gli stessi e che la molteplicità di interessi costituzionali di riferimento sia la stessa e, prima di tutto, sia riconducibile all'art. 15 Cost.

In assenza di una regolamentazione, tuttavia, molto spesso si assiste ad una invasione totale nel patrimonio comunicativo e personale dell'interessato; una invasione che, peraltro, non solo rischia di consentire il superamento delle norme di garanzia delle intercettazioni - captatore compreso - ma che pone evidenti

rischi di trasfigurazione del sequestro in uno strumento puramente esplorativo e, come tale, preordinato alla ricerca della notizia di reato e all'avvio di nuove o ulteriori indagini.

Immaginare la costruzione di itinerari suscettibili di circoscrivere azioni così invasive significa, pertanto, non poter prescindere dall'introduzione di una disciplina che contempra l'espressa definizione dei presupposti del sequestro nella cornice del principio di proporzionalità.

L'intervento del legislatore, di conseguenza, dovrebbe dirigersi su un duplice fronte, funzionale a ricondurre l'azione investigativa nel perimetro di quella riserva di legge che la Costituzione postula per l'incidenza su un diritto inviolabile: individuazione di un catalogo di reati attraverso cui perimetrare le possibilità di impiego del mezzo e rigorosi oneri motivazionali strutturati nell'ottica dell'indispensabilità.

Sotto il profilo procedurale, poi, del tutto auspicabile è l'innesto di un segmento dedicato alla verifica del rispetto di queste condizioni. In tal senso, sarebbe particolarmente opportuno valorizzare il ruolo del giudice per le indagini preliminari e, correlativamente, potenziare gli itinerari che garantiscano l'effettività del suo controllo. La verifica, in altri termini, non dovrebbe essere calibrata solo sul perimetro ritagliato dal pubblico ministero perché, senza un ampliamento dell'orizzonte conoscitivo del g.i.p. – sulla scia, peraltro, di quello che la Riforma Cartabia ha garantito in materia di iscrizioni (art. 110-ter disp. att. c.p.p.) - è veramente difficile pensare che il giudice non si appiattisca sulla prognosi di pertinenza dei dati e dei documenti espressa dall'unico organo che possiede un quadro completo delle investigazioni.

Sul fronte delle copie forensi, la relativa esecuzione potrebbe assurgere alla considerazione di atto investigativo autonomo che, in quanto suscettibile di incidere in maniera sostanziale sui profili legati all'attendibilità dell'accertamento, andrebbe circondato di adeguate garanzie di partecipazione e di difesa: si pensi, ad esempio, ad una partecipazione assicurata per il tramite di consulenti o, in caso di urgenza, ad una videoripresa che garantisca quantomeno un contraddittorio postumo^[4].

Sempre restando sul medesimo versante, si potrebbe cominciare a trattare le copie forensi come si trattano i risultati delle intercettazioni: si potrebbe far confluire i dati in un archivio riservato ad esempio. Un archivio apposito o lo stesso archivio delle intercettazioni ma, in quest'ultimo caso, bisognerebbe disporre di un archivio adeguato in termini di capienza perché le possibilità di immagazzinamento dei dati non sono illimitate e già sono stati segnalati da più parti problemi di sostenibilità gestionale.

Infine, si potrebbe istituire una procedura in contraddittorio sulla falsariga di quella prevista in materia di intercettazioni, per lo stralcio, davanti al giudice, di ciò che non è rilevante.

Alcuni di questi spunti si ritrovano nelle riflessioni legislative più recenti.

Nel mai sopito dibattito in materia di intercettazioni - e a valle dell'indagine conoscitiva che la Commissione Giustizia del Senato ha condotto su questo tema - si è, infatti, aperta una breccia anche per l'individuazione delle garanzie funzionali a circoscrivere la portata invasiva del sequestro di dispositivi elettronici.

In questo senso si muove, in primo luogo, il disegno di legge n. 806, presentato d'iniziativa dei senatori Zanettin e Bongiorno.

Innanzitutto, il d.l. - esattamente come l'ulteriore proposta cui si darà conto a breve - punta all'inserimento di una norma apposita nel codice di rito, l'art. 254-ter, per la disciplina del sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali.

Si prevedono, in particolare, i profili che devono essere oggetto di specifica motivazione da parte del p.m., sia sotto il profilo del nesso di pertinenza tra il bene appreso e l'oggetto delle indagini, sia in relazione alla tipologia di operazioni tecniche da svolgere per eseguire la selezione dei dati; si prevede, inoltre, che questa selezione sia circoscritta ai soli dati effettivamente necessari per il prosieguo delle indagini.

In questo contesto, l'analisi e l'esame dei dati viene impedita fino all'espletamento delle operazioni di selezione; queste ultime, infatti, devono essere svolte in contraddittorio con gli interessati e i difensori. Lo schema prescelto è quello degli accertamenti tecnici irripetibili, con la conseguenza anche di risolvere l'annosa questione circa la doverosità, per l'acquisizione della *digital evidence*, della attivazione del congegno di cui all'art. 360 c.p.p. Questo meccanismo, pertanto, diviene funzionale alla selezione dei dati rilevanti e correlativamente alla duplicazione dei soli dati selezionati.

Nonostante, nelle sue linee complessive, si tratti di una proposta da cui certamente non resta estraneo il tema del necessario equilibrio tra le esigenze difensive e quelle dell'accertamento, restano diverse zone d'ombra.

In primo luogo, si assiste ad una marginalizzazione del ruolo del g.i.p., la quale si scorge, peraltro, dallo sbarramento alla possibilità di sollevare riserva di promuovere incidente probatorio perché, nel richiamare la disciplina di cui all'art. 360 c.p.p., si fa espressa esclusione del comma 4.

Che al g.i.p. venga ritagliato un ruolo di secondo piano, del resto, emerge anche dalla scelta di affidare al p.m. la decisione sulle questioni concernenti il rispetto dei principi di necessità e di proporzione nella selezione dei dati: in questo contesto, infatti, è il *dominus* che decide entro quarantotto ore e il g.i.p. deve esprimersi sulla convalida del provvedimento entro le successive quarantotto ore. Tuttavia, non c'è traccia di messa a disposizione del giudice di elementi di valutazione diversi dal provvedimento decisorio del p.m.; di conseguenza, l'impressione è che, nella traduzione operativa, possa agevolmente prendere vita quello stesso simulacro di controllo che caratterizza la verifica di una intercettazione urgente, rispetto alla quale è ben noto che la convalida non rappresenti affatto il controllo di legittimità di un atto compiuto in sostituzione ma, piuttosto, la sanatoria di un atto illegittimo.

In questa proposta, infine, non si fa riferimento all'archivio e ciò in quanto, una volta eseguita la copia dei dati di interesse, il dispositivo e l'eventuale copia integrale - che può essere disposta, ai sensi del comma 2 del progetto di norma, prima e senza contraddittorio, quando vi è pericolo che il contenuto dei dispositivi possa essere cancellato, alterato o modificato - sono immediatamente restituiti all'avente diritto.

Diversa, anche dal punto di vista dei valori sottostanti, è la prospettiva che viene riversata nella seconda proposta di legge, la n. 690, presentata dal Senatore Scarpinato, la quale - e nonostante conduca la copia forense nell'archivio riservato delle intercettazioni - appare, invece, molto più attenta alle esigenze dell'accertamento piuttosto che ai diritti individuali.

Qui lo schema è presentato come una sorta di ibrido tra il procedimento di sequestro, le disposizioni relative all'acquisizione dei dati del traffico telefonico e le intercettazioni.

In sintesi: al p.m. serve l'autorizzazione del giudice per procedere al sequestro ma nei casi di urgenza può provvedere di propria iniziativa, salvo successiva convalida; sia nel caso di azione autorizzata che nell'ipotesi di atto compiuto d'iniziativa non è prevista la sottoposizione al giudice del fascicolo o comunque di materiale ulteriore rispetto al provvedimento del p.m.

Come nel d.l. n. 806, anche in questa proposta manca l'indicazione di un catalogo di reati anche se, a

differenza della prima, nella n. 690 si è seguita la strada delle intercettazioni e si istituisce un doppio regime: servono gravi indizi di reato per la generalità dei reati e sufficienti indizi per quelli attinenti alla criminalità organizzata.

Nel progetto dell'On. Scarpinato, inoltre, non c'è contraddittorio con gli interessati: qui è il pubblico ministero che, in solitaria, stabilisce l'area di ciò che è rilevante e di ciò che non lo è. Lo dimostra anche il fatto che, a conclusione delle operazioni e comunque non oltre settantadue ore (termine peraltro non presidiato da sanzione), si restituisce solo il dispositivo e non la copia forense, la quale però viene indirizzata nell'archivio riservato.

Gli interessati appaiono sulla scena solo una volta concluse le operazioni di selezione dei dati rilevanti, perché possono richiedere – non è chiarito in che modo, in che tempi e con quali possibili sviluppi procedurali nel caso di disaccordo con il p.m. – la distruzione di quanto non rilevante per le indagini.

Entrambi i progetti sono in fase di esame da parte della Commissione giustizia, quindi, non resta che attendere auspicabili ulteriori sviluppi per comprendere che valore assegna il legislatore al principio di legalità processuale.

** Contributo tratto dalla relazione svolta nell'ambito del convegno "Per uno statuto dei nuovi mezzi di ricerca della prova di fronte alla società digitale", tenutosi in Roma in data 22.9.2023.*

[1] Così, per limitarci a qualche esempio, per l'affermazione secondo cui deve ritenersi legittimo e non in contrasto con i principi di proporzionalità, adeguatezza e proporzione, il sequestro di un intero personal *computer* quando sia giustificato da difficoltà tecniche di estrapolare, con riproduzione mirata, gli elementi contenuti nella memoria, v. Cass. pen., Sez. V, 17.5.2019, n. 38456, rv. 2777343; per la considerazione della mancata fornitura delle chiavi di accesso come comportamento che influisce sulla valutazione della legittimità della protrazione del vincolo, state l'accresciuta difficoltà di accesso ai dati di interesse investigativo, v. Cass. pen., Sez. II, 23.3.2023, Casale, n. 17604, non massimata.

[2] Cfr., tra le più significative, Cass. pen., Sez. VI, 22.9.2020, n. 34265, rv. 279949, che in tema di sequestro probatorio di dispositivi informatici o telematici, ha stabilito che «una volta creata la c.d. copia originale, essa non rileva in sé come cosa pertinente al reato in quanto essa contiene un insieme di dati indistinti e magmatici rispetto ai quali nessuna funzione selettiva è stata compiuta al fine di verificare il nesso di strumentalità tra *res*, reato ed esigenza probatoria. La c.d. copia integrale, cioè, contiene l'insieme dei dati contenuti nel contenitore (pc., tablet, telefono), ma non soddisfa affatto l'esigenza indifferibile di porre sotto sequestro solo il materiale digitale che sia pertinente rispetto al reato per cui si procede e che svolga una necessaria funzione probatoria. Ne deriva ... che la c.d. copia integrale costituisce solo una copia mezzo, cioè una copia che consente di restituire il contenitore, ma che non legittima affatto il trattenimento dell'insieme di dati appresi. La copia integrale consente di fare, dopo il sequestro, ciò che naturalmente avrebbe dovuto essere fatto prima, cioè la verifica di quali, tra i dati contenuti nel contenitore, siano quelli pertinenti rispetto al reato. La c.d. copia integrale è una copia servente, una copia "mezzo" e non una copia "fine". Ne deriva che, restituito il contenitore, il Pubblico Ministero 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. L'avvenuta selezione delle *res* pertinenti impone la restituzione della copia integrale il cui trattenimento realizzerebbe, diversamente, una elusione ed uno svuotamento della portata dell'art. 253, co. 1, c.p.p. che legittima il sequestro probatorio solo delle cose "necessarie" per l'accertamento dei fatti. Ne consegue che il Pubblico Ministero: a) non può trattenere la c.d. copia integrale dei dati appresi se non per il tempo strettamente necessario alla loro selezione; 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». A partire da queste indicazioni alcune Procure hanno impartito specifiche direttive volte al riconoscimento, anche per il sequestro di dispositivi elettronici, degli stessi criteri di proporzionalità e di adeguatezza che operano in relazione alle misure cautelari personali; in questo senso, per tutte, cfr. la nota di indirizzo organizzativo della Procura Generale di Trento del 22.10.2021, sulla quale v. L. Filippi, *Sequestro dispositivi elettronici: nota della Procura Generale di Trento*, in questa *Rivista*, 19.11.2021.

[3] Queste sottolineature si ritrovano diffuse in tutte le audizioni svolte nell'ambito dell'indagine conoscitiva in materia di intercettazioni condotta, a partire dal 12 gennaio 2023, dalla Commissione giustizia del Senato. Tra queste, si ricorda il contributo del Procuratore Nazionale Antimafia Giovanni Melillo, che può leggersi su www.giustiziainsieme.it, 3 febbraio 2023.

[4] Per uno spunto in tal senso, da ultimo, v. C. Scaccianoce, *Prova tecnica e contraddittorio nel processo*

penale, Palermo, 2023, 73.