TANTO TUONÒ CHE PIOVVE: IL NUOVO SEQUESTRO DI DISPOSITIVI INFORMATICI

Andrea Chelo

Premessa

Del tutto assente, più che inadeguata, può oggi definirsi la disciplina processuale relativa al sequestro di apparecchiature elettroniche/informatiche, vieppiù quelle utilizzate per le comunicazioni come *smartphone*, *tablet* e computer. Non si sta esagerando per enfatizzare un concetto: ci si sta limitando a descrivere lo stato dell'arte, avuto riguardo agli strumenti processuali disponibili e all'attuale rilevanza che i dispositivi in questione rivestono nella vita di ogni giorno, con conseguente vulnus alla sfera della *privacy* individuale

talvolta al di fuori da ogni legittima proporzione.

La Corte di Giustizia dell'Unione europea e la Corte costituzionale ancor più di recente, con le loro pronunce, hanno enfatizzato taluni aspetti del diritto alla *privacy* e alla riservatezza delle comunicazioni, fornendo le indicazioni per riconoscergli una tutela effettiva. È per questa ragione che l'attuale iniziativa del legislatore di porre rimedio alla lacuna normativa deve essere colta con entusiasmo e favore, nella speranza che essa sia condotta con rigore metodologico, al fine di evitare che venga alla luce una disciplina inadeguata allo scopo che si prefigge.

La Commissione giustizia del Senato ha, infatti, avviato l'esame dei disegni di legge n. S 690[1] e n. S 806[2]; si tratta di due proposte di legge miranti, entrambe, ad introdurre nel codice di procedura penale l'art. 254-*ter* c.p.p.: una nuova norma che dovrebbe disciplinare il sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali.

Per quanto può rilevarsi dall'iter reso noto attraverso il sito istituzionale del Senato, la trattazione dei due disegni di legge procede in parallelo: circostanza più che positiva, considerato che – anticipando un giudizio sui testi – nessuno dei due disegni di legge pare risolvere, da solo, le problematiche più frequenti incontrate in materia. È auspicabile, pertanto, che nella discussione parlamentare congiunta delle due proposte si trovi un accordo per una soluzione che, mutuando gli aspetti positivi di ognuno dei due testi, rappresenti un corretto equilibrio tra esigenze investigative e tutela della *privacy*.

Lo scenario di riferimento.

Sia le relazioni introduttive dei due disegni di legge che il dossier elaborato dall'Ufficio Studi del Senato e messo a disposizione dei componenti delle Camere chiariscono la delicatezza dello scenario di riferimento[3], ovvero del contesto nel quale la soluzione legislativa dovrà trovarsi ad operare.

Oggi, però, vi è un dato fondamentale, venuto in evidenza successivamente alla presentazione dei due disegni di legge, che ha davvero stravolto la materia[4]: in data 27 luglio 2023, con una sentenza dal contenuto dirompente rispetto allo *status quo*, la Corte costituzionale ha chiarito che i messaggi *e-mail* o di messaggistica istantanea sono da considerarsi corrispondenza – e non mero documento[5] – anche quando

sono stati già ricevuti e letti dal destinatario e sono, pertanto, tutelati, dall'art. 15 Cost.; più precisamente, la Corte ha concluso che, «analogamente all'art. 15 Cost., quanto alla corrispondenza della generalità dei cittadini, anche, e a maggior ragione, l'art. 68, terzo comma, Cost. tuteli la corrispondenza dei membri del Parlamento – ivi compresa quella elettronica – anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico"»[6].

La sentenza della Corte ha così lasciato il riflettore puntato su un'attività già di per sé estremamente delicata, perché profondamente invasiva della sfera della riservatezza dell'individuo: il sequestro di uno strumento che, per l'uso per il quale è stato concepito, è veicolo ma anche contenitore di corrispondenza. Nonostante ciò, la soluzione proposta dal giudice delle leggi ha risolto un problema ma ne ha creato un altro: la Corte, infatti, riconoscendo la sequestrabilità del dispositivo finalizzata ad acquisire i messaggi in esso contenuti e affermando la necessità della sola autorizzazione della Camera di appartenenza ai fini dell'acquisizione dei messaggi trasmessi dal parlamentare o da lui ricevuti, ha attribuito alla corrispondenza una tutela *sui generis*, che, come vedremo, si palesa incompleta alla luce della portata dell'art. 15 Cost., del quadro normativo sovranazionale e della disciplina codicistica. Circostanza, questa, che dimostra, davvero, l'imprescindibilità di un intervento normativo in materia.

Se, infatti, le *e-mail* già lette o le *chat* di messaggistica istantanea costituiscono corrispondenza tutelata dall'art. 15 Cost., quest'ultima disposizione, con la sua doppia riserva, di legge e di giurisdizione, impone non solo l'intervento dell'autorità giudiziaria – ciò che nell'ottica interna si è finora salvaguardatocon il provvedimento di sequestro del pubblico ministero – ma anche la necessità che la limitazione della libertà della corrispondenza avvenga «con le garanzie stabilite dalla legge»[7]; e l'attenzione, a nostro modo di vedere, deve soffermarsi proprio su quest'ultima riserva, che, essendo assoluta, esige una disciplina dettata dal legislatore con normativa primaria[8], ad oggi ancora assente. D'altronde, come sempre affermato dalla dottrina, il riferimento, nella citata disposizione costituzionale, alle "garanzie" deve essere interpretato «nel senso che la previsione legislativa debba accompagnare all'individuazione dei casi e modi (art. 13 Cost.) le garanzie tecniche e giuridiche idonee a limitare l'esercizio della libertà fondamentale e tutelare i protagonisti del rapporto comunicativo»[9].

È evidente, allora, che se la limitazione della libertà e segretezza della corrispondenza può avvenire solo nei limiti indicati dalla legge quanto a casi, modi e garanzie, manca, oggi, nel sistema una disposizione specifica

finalizzata ad individuare casi, modi e garanzie dell'intervento statuale incidente sui messaggi *e-mail* e di messaggistica istantanea già letti e ricevuti.

Se è vero, infatti, che, «nel caso di sequestro probatorio informatico il "vero" oggetto del sequestro non è tanto il dispositivo elettronico (il "contenitore") – il quale, di per sé, non ha di norma alcun interesse per le indagini – quanto piuttosto i suoi dati (il "contenuto"), nella parte in cui risultano utili alle indagini stesse»[10] non può ritenersi sufficiente, a soddisfazione della riserva di legge, la sola previsione codicistica del sequestro probatorio[11] di cui all'art. 253 c.p.p.

È chiaro, pertanto, che manca, nell'attuale sistema, la necessaria e consapevole modulazione dell'atto invasivo che solo il legislatore, per dettato costituzionale, è chiamato a compiere in relazione ad uno strumento processuale che non si limita ad incidere sulla proprietà o sul possesso, ma sulla segretezza della corrispondenza e non di meno sulla libertà della stessa; non possiamo disconoscere, infatti, che l'ampiezza della libertà di comunicare deriva, in parte, dalla stessa segretezza che alla comunicazione è garantita.

Ma nello scenario di riferimento emergono altre problematiche.

La prima ruota attorno alla possibilità o meno di ritenere sufficiente un provvedimento del pubblico ministero per incidere sul diritto alla riservatezza delle comunicazioni garantito dall'art. 15 Cost. Fino a poco tempo fa, il provvedimento del giudice era stato ritenuto imprescindibile per incidere sul diritto in maniera subdola, come accade nelle intercettazioni[12]; da poco più di due anni, però, sulla scia delle indicazioni fornite della Corte di giustizia dell'Unione, il legislatore italiano è stato costretto a modificare la normativa in materia di accesso ai tabulati telefonici e telematici. Con il d.l. 30 settembre 2021, n. 132, convertito dalla l. 23 novembre 2021, n. 178[13] , è stato, infatti, modificato l'art. 132 d.lgs. 30 giugno 2003, n. 196, anche noto come "codice della *privacy*", stabilendo, a differenza che in passato, che i dati esterni delle comunicazioni e quelli di ubicazione siano acquisiti, entro il termine di conservazione imposto dalla legge, «previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private»[14].

Per l'effetto, vacilla anche l'attribuzione in capo al pubblico ministero del sequestro di corrispondenza su un apparato che la contiene: che senso avrebbe, anche in riferimento all'art. 3 Cost., affidare al giudice l'acquisizione dei dati esterni della comunicazione e al pubblico ministero, invece, quella del contenuto?

La seconda problematica attiene, invece, all'individuazione delle finalità dell'atto investigativo e dei casi nei quali è possibile compierlo. In materia di tabulati, ad esempio, l'acquisizione può avvenire esclusivamente qualora essi siano «rilevanti per l'accertamento dei fatti» e «se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi». È evidente, dunque, che se l'acquisizione di dati esterni richiede una motivazione rafforzata e l'atto non è, comunque, ammesso in riferimento a reati di minore gravità, analoghe previsioni dovrebbero sovrintendere il compimento di un'attività investigativa ben più invasiva, come quella dell'acquisizione del "contenitore" della corrispondenza e, dunque, della corrispondenza stessa.

La terza problematica è relativa, poi, alla conservazione dei dati. Oramai, a tutela della *privacy*, in materia di intercettazioni il legislatore ha istituito l'archivio riservato, ove vengono custodite, garantendo la massima riservatezza, le comunicazioni intercettate. È evidente, dunque, che se anche i messaggi di messaggistica istantanea o le *e-mail* già scambiati costituiscono corrispondenza e risultano tutelati, anch'essi, dall'art. 15 Cost., il loro contenuto debba necessariamente essere custodito con i medesimi accorgimenti e non confluire indiscriminatamente, come accade oggi, nel fascicolo processuale.

La quarta problematica attiene, infine, a due aspetti tra loro intimamente legati: l'individuazione di ciò che è rilevante tra il materiale oggetto di sequestro e la tempestiva restituzione dell'apparato all'avente diritto.

Oggi, lo *smartphone*, il *tablet*, il *notebook* rappresentano vere e proprie appendici della persona: vengono utilizzati per gli scopi più diversi e rappresentano, talvolta, l'unico accesso al domicilio informatico del soggetto. Privare a lungo nel tempo un individuo di questi apparati rappresenta, dunque, una misura eccessiva e sproporzionata se la loro acquisizione è funzionale solo a carpirne il contenuto[15]. Si pensi, ad esempio, che lo *smartphone* è lo strumento utilizzato il più delle volte per il riconoscimento e l'autorizzazione a distanza in operazioni dispositive bancarie: privare una persona della sua disponibilità, dunque, significa impedirle di esercitare i propri legittimi diritti, senza che la limitazione soddisfi una qualche esigenza per l'accertamento laddove si protragga pur essendosi proceduto[16].

Diventa allora essenziale prevedere delle tempistiche per la creazione di una copia forense dell'apparato, disponendo, poi, l'immediata restituzione dello stesso[17].

Ma deve anche operarsi la selezione di quanto oggetto di acquisizione: la vita privata di un individuo non può essere violata se non nei limiti in cui la violazione è necessaria per l'accertamento[18] e se quest'ultimo si palesa come dovuto. Pertanto, non è fondamentale prevedere solo la creazione di una copia forense, ma anche la selezione del materiale acquisito[19], con distruzione di quanto non sia rilevante per le legittime esigenze investigative[20].

I progetti del legislatore: il d.d.l. n. S 690.

È alla luce di questo scenario che il legislatore interviene sulla materia, proponendo – in ambo i disegni di legge – l'inserimento di una nuova disposizione: l'art. 254-*ter*c.p.p.[21]

Ognuno dei testi ha dei punti di forza, dalla cui combinazione potrebbe emergere una disciplina efficiente.

Il d.d.l. n. S 690 introduce un art. 254-*ter* c.p.p. che dovrebbe regolamentare il sequestro di uno «strumento elettronico», così definito nella rubrica, che nel corpo della disposizione diventa, però, anche «strumento informatico»: a prescindere dalla differenza di significato tra le due definizioni[22], il riferimento allo strumento informatico rende evidente, che non solo lo *smarthpone*, ma un qualsiasi strumento che possa essere considerato tale – un computer, un *tablet*, ma anche una memoria digitale – sarà soggetto a questa disciplina.

Nello specifico, si prevede che, qualora il pubblico ministero abbia il fondato motivo di ritenere che un tale apparato contenga dati o documenti pertinenti al reato necessari per l'accertamento dei fatti, debba richiedere al giudice l'autorizzazione a disporne il sequestro e il giudice debba provvedere su tale richiesta[23] nelle quarantotto ore successive; la decisione dovrà essere adottata con decreto motivato al ricorrere di gravi indizi di reato, da valutarsi ai sensi dell'art. 203 c.p.p., o di sufficienti indizi, qualora le indagini siano relative ad un delitto di criminalità organizzata.

Ovviamente, nei casi di urgenza – cioè in quei casi in cui sussista un fondato motivo di ritenere, come in materia di intercettazioni, che dal ritardo possa derivare grave pregiudizio alle indagini – il provvedimento di sequestro può essere adottato direttamente dal pubblico ministero, con decreto motivato, che deve essere comunicato immediatamente e comunque non oltre quarantotto ore al giudice: entro quest'ultimo termine

(quarantotto ore dal provvedimento), infatti, il giudice deve decidere sulla convalida con decreto motivato. Ovviamente, nell'ipotesi in cui il decreto non venisse convalidato entro il termine stabilito, il sequestro perderebbe immediatamente efficacia.

La norma si premura, poi, di indicare che il sequestro deve essere eseguito personalmente dal pubblico ministero ovvero da un ufficiale di polizia giudiziaria da questi delegato[24]; e che, se l'interessato è presente, deve essergli consegnata copia del decreto di sequestro.

Il nuovo art. 254-*ter* c.p.p. si occupa, inoltre, di disciplinare la fase successiva al sequestro, ovvero quella di estrazione di una copia forense, conservazione della stessa, restituzione dell'apparato all'avente diritto ed estrazione dei dati rilevanti dalla copia, con distruzione di quelli in relazione ai quali non sussiste un interesse investigativo.

Si prevede, infatti, che il pubblico ministero ordini l'effettuazione di una copia del contenuto dello «strumento elettronico» (così nuovamente definito nel testo della norma) su adeguato supporto, attraverso una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità, nonché la tutela degli stessi. Tali operazioni di copia devono essere svolte nel più breve tempo possibile e comunque non oltre settantadue ore dal momento in cui il sequestro è stato eseguito o convalidato[25], con immediata restituzione all'avente diritto, al termine delle operazioni, delle cose sequestrate, salva la necessità di confisca ai sensi degli artt. 240 e 240-*bis* c.p.

Ovviamente, la copia in questione è relativa a tutto il contenuto del dispositivo sequestrato, dovendosi, pertanto, procedere alla selezione dei dati rilevanti per le indagini in corso: a tal fine, la copia dovrà essere immediatamente trasmessa al pubblico ministero per essere conservata nell'archivio riservato istituito ai sensi dell'art. 269, comma 1, c.p.p.[26] per il tempo strettamente necessario ad operare la selezione. Una volta che quest'ultima sarà stata eseguita, a tutela della riservatezza e su richiesta degli interessati il pubblico ministero dovrà procedere alla distruzione della copia stessa.

Segue: il d.d.l. n. S 806

Anche il d.d.l. n. S 806 è finalizzato ad introdurre, nel sistema codicistico, un nuovo art. 254-*ter* c.p.p.; dalla rubrica ben articolata, («Sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali») si

comprende che oggetto della disposizione è il sequestro, ancora una volta, di un'ampia categoria di apparati, che non si limita ai telefoni cellulari ma spazia fino a qualsiasi "contenitore" di dati, come una memoria digitale.

L'impostazione della nuova disciplina, stando al testo del d.d.l.[27], segue quella tradizionale dei sequestri, con qualche novità legata alla particolarità dei dati contenuti nei dispositivi in questione. Si prevede, infatti, che l'autorità giudiziaria – e, dunque, nella fase delle indagini, il pubblico ministero – disponga il sequestro di «dispositivi e sistemi informatici, smartphone e memorie digitali», con proprio decreto motivato, che deve espressamente indicare sia «le ragioni che rendono necessario il sequestro in relazione al nesso di pertinenza fra il bene appreso e l'oggetto delle indagini», sia «le operazioni tecniche» da svolgere sull'apparato e i criteri che verranno utilizzati «per selezionare, nel rispetto del principio di proporzione, i soli dati effettivamente necessari per il prosieguo delle indagini»[28]. In buona sostanza, è imposta una motivazione rafforzata circa l'utilità del sequestro a fini investigativi e la sua proporzionalità sempre in funzione della prosecuzione delle indagini.

L'atto, giusta la previsione del provvedimento dell'autorità giudiziaria, si palesa come delegabile; ma il d.d.l. procede anche all'interpolazione dell'art. 354 c.p.p., che descrive un'attività di iniziativa della polizia giudiziaria, sicché pare emergere uno scenario composito.

Considerato che, ai sensi della già citata disposizione, in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici è ammessa l'«immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità», il legislatore si premura ora di precisare che la copia realizzata deve essere «immediatamente trasmessa al pubblico ministero affinché, ove lo ritenga necessario, proceda ad attivare senza ritardo e, comunque, nelle 48 ore successive, le procedure di selezione dei dati di eventuale interesse investigativo previste dall'articolo 254-*ter*, commi 3 e seguenti», dovendo, in caso contrario, il pubblico ministero, procedere all'immediata restituzione della copia informatica all'avente diritto.

In buona sostanza, la nuova disposizione, più che disciplinare una nuova ipotesi di sequestro di pertinenza dell'autorità giudiziaria, assume la funzione di individuare regole precise per l'esecuzione della copia, la selezione dei dati, e la restituzione all'avente diritto del dispositivo[29].

Da un lato, infatti, si prevede che, nel caso in cui vi sia pericolo che il contenuto dei dispositivi possa essere cancellato, alterato o modificato, l'autorità giudiziaria adotti le misure tecniche e impartisca le prescrizioni necessarie ad assicurarne la conservazione e a impedirne a chiunque l'analisi e l'esame fino all'espletamento, in contraddittorio con gli interessati, delle operazioni di selezione dei dati, disponendo, se del caso, la duplicazione integrale dei suddetti dispositivi su adeguati supporti informatici mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

Quanto alla selezione, poi, la nuova disposizione prevede che, entro cinque giorni dal sequestro, il pubblico ministero avvisa la persona sottoposta alle indagini, la persona alla quale la cosa è stata sequestrata, la persona alla quale la cosa dovrebbe essere restituita e la persona offesa dal reato e i relativi difensori del giorno, dell'ora e del luogo fissato per l'affidamento dell'incarico (verosimilmente di copia del supporto, se non effettuata, e selezione dei dati) da espletare nelle forme degli accertamenti tecnici irripetibili (senza la possibilità di fare riserva di incidente probatorio), con facoltà di nominare consulenti tecnici. Questi ultimi e i difensori hanno diritto di assistere al conferimento dell'incarico e di partecipare alle operazioni di selezione ed estrazione dei dati, da effettuare eventualmente mediante l'utilizzo di parole chiave, formulando eccezioni o riserve, anche sui criteri utilizzati.

Sicuramente innovativa è la previsione, contenuta nel nuovo art. 254-*ter* c.p.p., secondo cui è possibile sollevare questioni concernenti il rispetto dei princìpi di necessità e di proporzione nella selezione e nell'apprensione dei dati ovvero l'apprensione di dati sensibili che devono essere decise, in prima istanza, entro 48 ore dal pubblico ministero con decreto motivato. In questa ipotesi, il provvedimento adottato è sottoposto a convalida, entro le 48 ore successive, dal giudice per le indagini preliminari, con decreto motivato: la decisione può convalidare tutto o parte del provvedimento del pubblico ministero, e può eventualmente limitare gli effetti solo ad alcuni dei dati selezionati; ma può anche disporre la restituzione all'avente diritto del dispositivo informatico e dell'eventuale copia informatica nel frattempo realizzata.

Il decreto di convalida può essere impugnato con riesame, anche nel merito, ai sensi dell'art. 324 c.p.p.: l'impugnazione può essere proposta dalla persona nei cui confronti sono svolte le indagini, dal suo difensore, dalla persona alla quale le cose sono state sequestrate e da quella che avrebbe diritto alla loro restituzione, entro dieci giorni dalla notifica del decreto, ovvero dalla diversa data in cui si è avuta conoscenza dell'avvenuto sequestro.

Una volta che la convalida è intervenuta, il pubblico ministero dispone che, in contraddittorio con i difensori

e gli eventuali consulenti nominati, si proceda alla duplicazione dei soli dati selezionati nel contraddittorio delle parti ovvero indicati dal giudice per le indagini preliminari nel decreto di convalida; la duplicazione deve avvenire su un autonomo e idoneo supporto informatico con procedure che assicurino la conformità della copia ai dati fonte e l'immodificabilità della medesima. In ogni caso, a duplicazione eseguita, il dispositivo informatico o l'eventuale copia integrale del medesimo che fosse stata *medio termine* eseguita in condizioni di urgenza per preservarne il contenuto, devono essere immediatamente restituiti all'avente diritto.

Chiude la disposizione uno specifico divieto probatorio, secondo il quale i dati informatici appresi dal pubblico ministero senza il rispetto delle formalità dettate sono inutilizzabili.

Un po' di considerazioni...de iure condendo

A fronte di due soluzioni normative dai contenuti così diversi, volte, però, a costruire una disciplina per la stessa materia, riteniamo opportuno – in quella che sostanzialmente è una prima lettura tutta da approfondire – individuare gli aspetti che ci sembrano i punti di forza di ognuno dei disegni di legge, sfruttando i quali potrebbe, magari, costruirsi una norma più performante, capace, cioè, di regolamentare adeguatamente l'attività in questione.

A tal fine, però, non può perdersi d'occhio lo scenario di riferimento che abbiamo ricostruito in premessa: infatti, se quella del legislatore è la risposta ad un'esigenza, è bene che l'esigenza stessa venga ben inquadrata per essere adeguatamente soddisfatta.

E allora, ciò che dovremmo aspettarci dalla nuova disciplina è che essa consenta di ritenere rispettate la riserva di legge e quella di giurisdizione, prevedendo casi, modi e garanzie del sequestro che, in ultima analisi, attinga la corrispondenza, con attribuzione del relativo potere al giudice, unica autorità caratterizzata da terzietà e imparzialità. Ma la disciplina dovrebbe, altresì, prevedere, nel contraddittorio, la tempestiva esecuzione della copia forense, la selezione dei dati utili e la distruzione di quelli non rilevanti; e, appena possibile, la tempestiva restituzione dell'apparato all'avente diritto.

Cercando di confrontarci con i testi normativi, dovrebbe, però, farsi innanzitutto chiarezza sull'oggetto da sottoporre a sequestro che nel d.d.l. n. S 690 è indicato talvolta come "strumento informatico", talaltra come "strumento elettronico", laddove il d.d.l. n. S 806 parla, invece, di "dispositivi e sistemi informatici, smartphone e memorie digitali": si tratta di compiere, insomma una scelta di fondo, tra un

riferimento più generale o uno più preciso. Quand'anche si adottasse un riferimento generale, capace di ricomprendere una più ampia pluralità di apparati, è bene, però, che esso sia generale e non, semplicemente, impreciso.

Un dato però è certo. La norma che entrambi i disegni di legge mirano ad introdurre si applicherà non solo al sequestro di "corrispondenza" ma, data l'ampiezza della categoria di apparati oggetto della misura ablativa e la loro eterogeneità, anche al sequestro di dati che non costituiscono espressione di comunicazioni. Si tratta, allora, di comprendere come operare: se costruire una norma sempre rispettosa dell'art. 15 Cost., oppure una norma che introduca una nuova ipotesi di sequestro e che, nell'eventualità in cui esso cada – indirettamente – sulla corrispondenza, fornisca solo in tal caso le garanzie che l'art. 15 Cost. impone.

Noi riteniamo che la scelta su come operare debba essere influenzata dalla consapevolezza che sugli apparati in questione vi è l'altissima probabilità – in relazione ad alcuni apparati addirittura la certezza – di rinvenire un contenuto che possa essere qualificato, seguendo le citate indicazioni della Corte costituzionale, come corrispondenza. Pertanto, qualora si volesse a tutti i costi introdurre una norma che ricomprendesse apparati così differenti tra loro, anche per funzione[30], non potrebbe farsi a meno di alzare l'asticella delle garanzie per evitare che talune situazioni meritevoli di particolare tutela ne rimangano prive.

Analizzando sotto questo profilo i due disegni di legge, è evidente che la soluzione del d.d.l. n. S 690 è certamente concepita per offrire una tutela ampia ed effettiva, risultando più simile a quella riconosciuta in materia di intercettazioni che in ambito di mero sequestro (seppur priva di sanzione). Tale disegno di legge, infatti, soddisfa appieno la riserva di giurisdizione, individuando nel giudice il soggetto che deve autorizzare il sequestro, con decreto motivato, e prevedendo, altresì, la possibilità di ricorrere, nei casi d'urgenza, al sequestro da parte del pubblico ministero da sottoporre a convalida: ciò che già si verifica in materia di intercettazioni e di acquisizione dei tabulati telefonici. La nuova disposizione, per vero, dovrebbe essere migliorata sotto il profilo della riserva di legge: è totalmente assente, infatti, l'indicazione dei casi in cui procedere all'acquisizione degli apparati *de quibus*, mentre, ad esempio, non solo le intercettazioni prevedono limitazioni alla loro esecuzione – per finalità e reati da accertare – ma la stessa acquisizione dei tabulati risulta legata al reato per il quale si procede.

La soluzione adottata dal d.d.l. n. S 806, invece, non convince: è, infatti, affidata all'autorità giudiziaria – e dunque al pubblico ministero – la decisione sul sequestro, salva la possibilità di sollevare «questioni concernenti il rispetto dei princìpi di necessità e di proporzione nella selezione e nell'apprensione dei dati»

che verranno decise dapprima dallo stesso organo inquirente con decreto motivato, che sarà poi sottoposto a convalida da parte del giudice per le indagini preliminari. Posto che le questioni sono affidate alla parte e da essa dipendono, è difficile riuscire a comprendere, nell'ottica dell'art. 3 Cost., per quale ragione nell'ipotesi di acquisizione del "contenuto delle comunicazioni" (come nel caso del sequestro) l'autorizzazione possa promanare dal pubblico ministero, laddove, invece, solo il giudice può oggi disporre l'acquisizione dei tabulati, ovvero di "dati esterni alle comunicazioni".

È, invece, sicuramente condivisibile l'indicazione data in quest'ultimo disegno di legge circa il contenuto della motivazione del decreto che dispone il sequestro, il quale deve indicare espressamente «*a)* le ragioni che rendono necessario il sequestro in relazione al nesso di pertinenza fra il bene appreso e l'oggetto delle indagini; *b)* le operazioni tecniche da svolgere sul bene appreso e i criteri che saranno utilizzati per selezionare, nel rispetto del principio di proporzione, i soli dati effettivamente necessari per il prosieguo delle indagini». Nell'ottica di un corretto bilanciamento tra opposte esigenze e all'insegna del principio di proporzionalità, un miglioramento potrebbe aversi se il sequestro fosse, però, agganciato all'esistenza di indizi di reato, come fa il d.d.l. n. S 690: esso prevede, infatti, che la decisione sia adottata con «decreto motivato qualora sussistono gravi indizi di reato», ovvero «sufficienti indizi» nell'ipotesi in cui le indagini siano relative ad un delitto di criminalità organizzata.

Quanto poi all'aspetto relativo all'effettuazione della copia, il d.d.l. n. S 690 prevede, in termini condivisibili, che la copia venga effettuata entro un termine predefinito seppure di natura ordinatoria, che è individuato «nel più breve tempo possibile e comunque non oltre settantadue ore dal momento in cui il sequestro è stato convalidato»[31]; meno rigido nelle tempistiche ma più attento al contraddittorio è, invece, sul punto, il d.d.l. n. S 806, secondo il quale la copia forense è eseguita nelle forme di cui all'art. 360 c.p.p.

Infine, il d.d.l. n. S 806, prevedendo una causa di inutilizzabilità nell'ipotesi di violazione delle "formalità" introdotte, offre una ricaduta concreta sul piano processuale nell'ipotesi di violazione che, invece, il d.d.l. n. S 690, purtroppo, non offre.

Conclusioni.

Insomma, i disegni di legge che il legislatore sta valutando non convincono appieno; o meglio, come detto in premessa, considerati autonomamente non riescono a fornire piena soddisfazione alle esigenze che intenderebbero soddisfare.

Ci sembra che il problema stia nel fatto che si stia tentando di creare una disciplina da applicarsi a situazioni eterogenee, considerato che solo la corrispondenza rientra nell'alveo dell'art. 15 Cost. e non, invece, qualsiasi documento informatico nativo digitale o meno che possa essere archiviato in una memoria di massa.

Sarebbe, dunque, necessaria una disciplina differenziata per l'ipotesi di sequestro di apparati che possono essere utilizzati per la comunicazione rispetto a quella del sequestro che incide su apparati che sono destinati alla sola archiviazione: nel primo caso, infatti, deve essere riconosciuta, *ab origine*, la piena tutela che l'art. 15 Cost. assicura alle comunicazioni; nel secondo caso, invece, salva l'ipotesi che i dati archiviati riguardino corrispondenza, è sufficiente venga riconosciuta una valutazione di proporzionalità del sacrificio della *privacy* individuale, con limitazione dell'acquisizione di dati a quelli effettivamente rilevanti per l'indagine in corso.

In entrambi i casi, però, gli apparati sequestrati dovrebbero essere restituiti immediatamente dopo l'esecuzione della copia e la selezione: in caso contrario, infatti, ci si troverà di fronte ad una lesione inutile e sproporzionata dei diritti dell'individuo[32], essendogli impedito di disporre di una *res* comunque inutile all'accertamento; e soprattutto, i dati non utili acquisiti in copia dovranno essere prontamente distrutti, dopo essere stati conservati, però, in modalità riservata.

Concludendo, viene anche da chiedersi, però, quale sarà l'impatto della nuova previsione.

Riteniamo che le conseguenze siano numerose e importanti: l'introduzione di una norma che preveda il sequestro degli apparati elettronici/informatici – o anche, semplicemente, degli apparati di comunicazione – in casi predeterminati e con provvedimento del giudice non fa altro che confermare che il sequestro di tali dispositivi è stato finora disposto ed eseguito in spregio alla riserva di legge e di giurisdizione imposta dall'art. 15 Cost. e dalla giurisprudenza europea; dunque: *praeter legem e contra Constitutionem*. Non solo: l'entrata in vigore della nuova normativa dovrebbe porre fine a quelle attività di *online surveillance* che, per il tramite dell'art. 189 c.p.p., sono state finora eseguite sui dispositivi informatici utilizzati per le comunicazioni: un'attività certamente non rispettosa, ancora una volta, della riserva di legge e di giurisdizione dell'art. 15 Cost.

Per le stesse ragioni non è da escludere, poi, che il legislatore possa pensare ad una norma di diritto transitorio, così come avvenuto in materia di tabulati. Non che la soluzione ci aggradi, perché la lesione del diritto è comunque avvenuta e l'unica sua conseguenza dovrebbe essere l'inutilizzabilità; d'altronde, per

utilizzare le parole sempre attuali del Giudice delle leggi, «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito»[33]. Stiamo, dunque, a vedere.

---

[1] Si tratta del disegno di legge d'iniziativa del senatore Scarpinato, comunicato alla presidenza il 9 maggio 2023, relativo alla "introduzione dell'articolo 254-*ter* del codice di procedura penale recante norme in materia di sequestro di strumenti elettronici".

[2] Si tratta del disegno di legge d'iniziativa dei senatori Zanettin e Bongiorno, comunicato alla presidenza il 19 luglio 2023, recante "modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali".

[3] Per un approfondimento, volendo, cfr. A. Chelo, *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, in *Dir. pen. e proc.*, 2022, p. 1583 e ss.

[4] Di esso si rinviene esclusivamente una fugace traccia nella conclusione del citato *dossier*.

[5] Come noto la giurisprudenza di legittimità è sempre stata incline a ritenere che i messaggi *de quibus* fossero da considerare come documento. Sul punto cfr., ad esempio, Cass., Sez. VI, 22 agosto 2022, n. 31364, inedita, che richiama un costante orientamento già fatto proprio da Cass., Sez. VI, 12 novembre 2019, n. 1822, in *C.E.D. Cass*., n. 278124, secondo cui ai messaggi whatsapp e sms rinvenuti in un telefono cellulare sottoposto a sequestro non sarebbe applicabile la disciplina dettata dall'art. 254 c.p.p., in quanto tali testi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito (per questa affermazione cfr., ancor prima, Cass., Sez. III, 25 novembre 2015, n. 928, in *C.E.D. Cass*., n. 265991); né, secondo la giurisprudenza, l'attività di acquisizione può inquadrarsi in un'attività di intercettazione, la quale postula, per sua natura, la captazione di un flusso di comunicazioni in corso, là dove i dati presenti sulla memoria del telefono acquisiti *ex post* costituiscono mera documentazione di detti flussi. I giudici di legittimità, infatti, hanno costantemente ritenuto che i messaggi *whatsapp*, così come gli sms conservati nella memoria di un apparecchio cellulare,

abbiano natura di documenti ai sensi dell'art. 234 c.p.p., con l'ulteriore conseguenza di dover ritenere detti testi legittimamente acquisiti ed utilizzabili ai fini della decisione ove ottenuti mediante riproduzione fotografica a cura degli inquirenti. Nello stesso senso cfr. anche Cass., Sez. VI, 28 maggio 2019, n. 28269, in *C.E.D. Cass.*, n. 276227, relativa al sequestro di un server contenente messaggi di posta elettronica e Cass., Sez. V, 21 novembre 2017, n. 1822, in *C.E.D. Cass.*, n. 272319, relativa al sequestro di un cellulare contenente sms e messaggi whatsapp.

[6] Così Corte cost. 27 luglio 2023, n. 170, in *Giur. cost.*, 2023, IV, p. 263 e ss.

[7] Sulla portata della riserva *de qua* cfr. P. Barile – E. Cheli, voce *Corrispondenza (libertà di),* in *Enc. Dir.,* vol. X, Milano 1962, p. 743 e ss.; V. Italia, *Libertà e segretezza della corrispondenza e delle comunicazioni,* Milano 1963, *passim*; A. Pace, sub *Art. 15,* in *Commentario della Costituzione,* a cura di G. Branca-A. Pizzorusso, Bologna 1977, p. 105 e ss.; C. Troisio, voce *Corrispondenza (Libertà e segretezza della),* in *Enc. giur.,* vol. IX, 1988, p. 80 e ss.; P. Caretti, voce *Corrispondenza (libertà di),* in *D. disc. pubbl.,* vol. IV, 1989, p. 200 e ss.

[8] È, infatti, riservata alla normativa secondaria la sola regolamentazione di aspetti strettamente esecutivi.

[9] Così L. Califano, *La libertà e la segretezza delle comunicazioni*, in *www.lamagistratura.it,* che richiama sul punto le precedenti considerazioni di A. Pace, sub *Art. 15,* in *Commentario della Costituzione,* cit., p. 106. Secondo M. Mazziotti di Celso, *Lezioni di diritto costituzionale,* vol. II,Milano, 1985, 261, la previsione costituzionale imporrebbe, oltre alle ordinarie garanzie di riserva di legge e di giurisdizione, che altre garanzie debbano essere istituite dalla legge. Sul tema cfr. anche L. Filippi, *L'intercettazione di comunicazioni*, Milano, 1997, p. 43 e ss.

[10] Così sostiene la stessa Corte nella citata sentenza, rifuggendo da una "truffa delle etichette" ed anzi invitando, con schietta concretezza, a focalizzare l'attenzione sui messaggi stessi, imponendo di riconoscere agli stessi l'ordinaria tutela che la Costituzione appresta alla corrispondenza.

[11] Infatti, l'art. 253 c.p.p. è norma troppo generica per poter dare soddisfazione alla riserva di legge di cui all'art. 15 Cost.; l'art. 254 c.p.p., poi, disciplina un'ipotesi differente – il sequestro «presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni» – che non può essere utilizzata, in

chiave estensiva, per legittimare un'apprensione che avviene in condizioni del tutto diverse. Per un approfondimento sulle ragioni per le quali non è possibile ritenere sufficienti le due disposizioni citate, sia consentito il rimando a A. Chelo, *Davvero legittimo il sequestro di messaggi e-mail e WhatsApp già letti?*, in *Giur. cost.*, 2023, IV, p. 296 e ss.

[12] Secondo Corte cost. 24 gennaio 2017, n. 20, il diverso grado di materializzazione del mezzo comunicativo utilizzato avrebbe storicamente orientato il legislatore verso modalità differenti di ricerca della prova, secondo scelte che non possono essere ritenute irragionevoli: il sequestro, per la comunicazione realizzata attraverso un mezzo cartaceo, in linea con gli strumenti tradizionali per l'acquisizione di cose pertinenti al reato; l'intercettazione, invece, per la comunicazione realizzata attraverso mezzi visivi, acustici o elettronici.

[13] Per un commento alla disciplina introdotta con il citato d.l., cfr. G. Battarino, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021 n. 132*, in *www.questionegiustizia.it*; C. Cardinale, *La nuova disciplina di acquisizione dei tabulati telefonici*, in *www.rivistapenaleitaliana.it*; F. Demartis, *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Dir. pen. proc.* 2022, p. 299 ss.; L. Filippi, *La nuova disciplina dei tabulati: il commento "a caldo"*, in *www.penaledp.it*; Id., *Tabulati telefonici e telematici e rispetto della vita privata*, in *www.dirittodidifesa.eu*; A. Malacarne, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *www.sistemapenale.it*; F. Rinaldini, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza Penale Web*, 2021, p. 10.

[14] Il legislatore ha anche previsto che, qualora ricorrano ragioni di urgenza e vi sia fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero possa disporre l'acquisizione dei dati con decreto motivato da sottoporre a convalida del giudice.

[15] A queste conclusioni è giunta da tempo anche la giurisprudenza: secondo Cass., Sez. VI, 2 novembre 2022, n. 44010, in *Dir. di internet*, 2023, n.1, p. 129 con commento di F. Cerqua, *La durata ragionevole del sequestro probatorio informatico*, una volta realizzata la copia forense, lo smartphone deve essere immediatamente restituito, venendo meno le esigenze di indagine che giustificano la protrazione del sequestro. In precedenza, Cass., Sez. VI, 14 novembre 2018, n. 4857, inedita, aveva affermato che, poiché il dispositivo elettronico è un mero contenitore, la cui acquisizione è strumentale all'acquisizione dei dati utili per

l'indagine, la legittimità del sequestro del primo è legata alla temporaneità dello spossessamento, finalizzata esclusivamente all'estrazione di una copia forense del contenuto.

[16] D'altronde, il contemperamento tra le contrapposte esigenze dell'autorità inquirente e del privato può essere assicurato attraverso un sequestro delle cose contenenti i dati da esaminare – o, se possibile, solo di questi ultimi – che si protragga solo per il tempo strettamente necessario al compimento di tale verifica.

[17] Non deve dimenticarsi che proprio il fattore tempo è un parametro di valutazione della correttezza di un sequestro, a norma dell'art. 1 del Protocollo addizionale n. 1 alla Convenzione E.D.U.: in questo senso cfr., ad esempio, Corte E.D.U., 7 giugno 2007, Smirnov c/ Russa, n. 71362/01; Corte E.D.U., 19 giugno 2014, Draghici c/ Portogallo, n. 43620/10.

[18] Secondo così Cass., Sez. VI, 11 novembre 2016, n. 53168, in *C.E.D. Cass.*, n. 268489, l'autorità giudiziaria, al fine di esaminare un'ampia massa di dati potenzialmente rilevanti per le indagini, può disporre un sequestro dai contenuti molto estesi, provvedendo, tuttavia, nel rispetto del principio di proporzionalità ed adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti; con la conseguenza che, in caso di mancata tempestiva restituzione, l'interessato potrà presentare la relativa istanza e far valere le proprie ragioni, se necessario, anche mediante i rimedi impugnatori offerti dal sistema.

[19] Secondo Cass., Sez. VI, 27 ottobre 2021, n. 38460, in *www.processopenaleegiustizia.it*, è illegittimo, per violazione del principio di proporzionalità ed adeguatezza, il sequestro a fini probatori di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione dei relativi criteri. Corollario della declaratoria di illegittimità del provvedimento è la restituzione all'avente diritto di tutte le copie forensi illegittimamente eseguite ed eventualmente ancora a disposizione del pubblico ministero.

[20] Da ultimo, sul punto, cfr. Cass., sez. II, 15 dicembre 2023, n. 50009, in *www.processopenaleegiustizia.it*, secondo cui, in tema di sequestro probatorio di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti, che consente la restituzione del dispositivo, non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede, sicché il pubblico ministero è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano sequestrati a persone

estranee al reato, e provvedere, all'esito, alla restituzione della copia integrale agli aventi diritto. In precedenza, nello stesso senso, cfr. Cass., Sez. VI, 4 marzo 2020, n. 13156, inedita, secondo cui 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.

[21] Per un pronto riscontro si riproduce, di seguito, il testo della nuova disposizione, così come proposto nel disegno di legge: «1. Il pubblico ministero, quando abbia fondato motivo di ritenere che uno strumento informatico contenga dati o documenti pertinenti al reato necessari per l'accertamento dei fatti, richiede al giudice competente l'autorizzazione a disporre il sequestro. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato qualora sussistono gravi indizi di reato. Nella valutazione dei gravi indizi di reato si applica l'articolo 203. 2. In deroga a quanto disposto dal comma 1, la convalida è data, con decreto motivato, quando il sequestro dello strumento elettronico è necessario per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata in ordine al quale sussistano sufficienti indizi. Nella valutazione dei sufficienti indizi si applica l'articolo 203. 3. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone il sequestro con decreto motivato, che è comunicato immediatamente e comunque non oltre quarantotto ore al giudice competente. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato entro il termine stabilito, il sequestro perde di efficacia. 4. Al sequestro provvede il pubblico ministero personalmente ovvero un ufficiale di polizia giudiziaria delegato. 5. Copia del decreto di sequestro è consegnata all'interessato se presente. 6. Il pubblico ministero ordina la copia del contenuto dello strumento elettronico su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità, nonché la tutela degli stessi. 7. Le operazioni di cui al comma 6 devono essere svolte nel più breve tempo possibile e comunque non oltre settantadue ore dal momento in cui il sequestro è stato convalidato. Al termine delle operazioni le cose sequestrate sono restituite a chi ne abbia diritto, salvo i casi in cui si debba procedere ai sensi degli articoli 240 e 240-*bis* del codice penale. 8. La copia dei dati è immediatamente trasmessa al pubblico ministero per la conservazione nell'archivio di cui all'articolo 269, comma 1, per il tempo strettamente necessario alla selezione dei dati rilevanti per le indagini relativamente al reato per il quale si procede. Una volta effettuate le operazioni di selezione, a tutela della riservatezza e su richiesta degli interessati, il pubblico ministero provvede alla distruzione della copia dei dati.»

[22] Come noto, mentre l'elettronica si concentra sull'*hardware* e sui componenti fisici di un apparato che rendono possibile l'elaborazione delle informazioni, l'informatica è la disciplina che si concentra sul

software e sul trattamento delle informazioni.

[23] Impropriamente il testo fa riferimento ad una convalida, che, quale atto decisorio presuppone, però, l'esistenza di un provvedimento già adottato.

[24] Trattandosi di attività che può essere compiuta esclusivamente su delega, non sarà mai ammesso l'intervento da parte di un agente, neppure nei casi di assoluta necessità e urgenza. Ciò è consentito, infatti, stando al contenuto dell'art. 113 norme att. c.p.p., solo con riferimento agli atti previsti dagli artt. 352 e 354, commi 2 e 3, c.p.p.

[25] La norma, quanto alla decorrenza del termine, fa riferimento solo alla convalida ma è evidente che, nell'ipotesi in cui il sequestro sia disposto dal giudice, il termine non possa che decorrere dalla sua esecuzione, che avviene in un momento successivo.

[26] Il d.d.l. n. S 690, infatti, prevede anche un'interpolazione dell'art. 89-*bis*, comma 1, norme att. c.p.p., disciplinante l'archivio delle intercettazioni, nel quale, dopo la modifica, saranno «custoditi i verbali, gli atti e le registrazioni delle intercettazioni a cui afferiscono nonché la copia dei dati di strumenti elettronici».

[27] Per un pronto riscontro si riproduce, di seguito, il testo della nuova disposizione, così come proposto nel disegno di legge: «Art. 254-*ter*. (Sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali) - 1. Al sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali l'autorità giudiziaria può procedere mediante decreto motivato che indichi espressamente: a) le ragioni che rendono necessario il sequestro in relazione al nesso di pertinenza fra il bene appreso e l'oggetto delle indagini; b) le operazioni tecniche da svolgere sul bene appreso e i criteri che saranno utilizzati per selezionare, nel rispetto del principio di proporzione, i soli dati effettivamente necessari per il prosieguo delle indagini. 2. Nel caso in cui vi sia pericolo che il contenuto dei dispositivi possa essere cancellato, alterato o modificato, l'autorità giudiziaria adotta le misure tecniche e impartisce le prescrizioni necessarie ad assicurare la conservazione e a impedirne a chiunque l'analisi e l'esame fino all'espletamento, in contraddittorio con gli interessati, delle operazioni di selezione dei dati di cui al comma 3; a tale fine l'autorità giudiziaria può disporre che si proceda alla duplicazione integrale dei suddetti dispositivi su adeguati supporti informatici mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. 3. Entro cinque giorni dal sequestro il pubblico ministero avvisa la persona sottoposta alle indagini, la persona alla quale la cosa è

stata sequestrata, la persona alla quale la cosa dovrebbe essere restituita e la persona offesa dal reato e i relativi difensori del giorno, dell'ora e del luogo fissato per l'affidamento dell'incarico da espletare ai sensi dell'articolo 360 e della facoltà di nominare consulenti tecnici. I difensori e i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico e di partecipare alle operazioni di selezione ed estrazione dei dati, da effettuare eventualmente mediante l'utilizzo di parole chiave, formulando eccezioni o riserve, anche sui criteri utilizzati. Non si applica la disposizione di cui al comma 4 dell'articolo 360. 4. Sulle eventuali questioni concernenti il rispetto dei princìpi di necessità e di proporzione nella selezione e nell'apprensione dei dati ovvero l'apprensione di dati sensibili, il pubblico ministero decide entro 48 ore con decreto motivato. Entro le 48 ore successive il giudice per le indagini preliminari, con decreto motivato, convalida in tutto o in parte il provvedimento del pubblico ministero, eventualmente limitandone gli effetti solo ad alcuni dei dati selezionati, ovvero dispone la restituzione all'avente diritto del dispositivo informatico e dell'eventuale copia informatica nel frattempo realizzata. 5. Contro il decreto di convalida, la persona nei cui confronti sono svolte le indagini e il suo difensore, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre, entro dieci giorni dalla notifica del decreto, ovvero dalla diversa data in cui l'interessato ha avuto conoscenza dell'avvenuto sequestro, richiesta di riesame anche nel merito a norma dell'articolo 324. 6. Dopo la convalida, il pubblico ministero dispone che, in contraddittorio con i difensori e gli eventuali consulenti nominati, si proceda alla duplicazione dei soli dati selezionati nel contraddittorio delle parti ovvero indicati dal giudice per le indagini preliminari nel decreto di convalida, su un autonomo e idoneo supporto informatico con procedure che assicurino la conformità della copia ai dati fonte e l'immodificabilità della medesima. Una volta eseguita la copia dei dati di interesse, il dispositivo informatico o l'eventuale copia integrale del medesimo, eseguita a norma del comma 2, sono immediatamente restituiti all'avente diritto. 7. I dati informatici appresi dal pubblico ministero senza il rispetto delle formalità previste dal presente articolo sono inutilizzabili».

[28] Sarebbe opportuno valutare se il riferimento all'«oggetto delle indagini» o alla necessarietà «per il prosieguo delle indagini» possano comportare l'impossibilità di procedere al sequestro *de quo* dopo l'esercizio dell'azione penale, così come accade in materia di intercettazioni".

[29] La norma cerca, cioè, di dare soddisfazione al principio di proporzione: come affermato dalla giurisprudenza, questo principio, «certamente ancorato alla disciplina delle cautele personali nel procedimento penale ed alla tutela dei diritti inviolabili, ha nel sistema una portata più ampia in quanto travalica il perimetro della libertà individuale per divenire termine necessario di raffronto tra la compressione dei diritti quesiti e la giustificazione della loro limitazione»: così Cass., Sez. VI, 22 settembre

2020, n. 34265, in *www.sistemapenale.it*. È proprio in quest'ottica che la Corte ha affermato che quando il sequestro riguarda delle memorie fisiche è necessario procedere quanto prima alla realizzazione di una copia integrale delle stesse, al fine della loro immediata restituzione. Solo successivamente su tale copia potrà operarsi la selezione del contenuto, al fine di acquisire i soli dati utili ai fini delle indagini e distruggere i restanti: anche quest'ultima copia integrale, infatti, può essere trattenuta solo per il tempo strettamente necessario all'operazione di selezione. Per un commento alla sentenza citata, cfr. M. Pittiruti, *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *www.sistemapenale.it*

[30] È evidente la differenza esistente tra uno *smartphone* e una memoria digitale: il primo è uno strumento di comunicazione e all'occorrenza di archiviazione; il secondo solo di archiviazione. Nel primo è certo che si troveranno tracce di una comunicazione, nel secondo vi è solo la possibilità.

[31] È opportuno precisare che si tratta di un termine ordinatorio riferito, verosimilmente, all'inizio delle operazioni di copia. È vero che, in tema di sequestro probatorio avente ad oggetto dispositivi informatici o telematici, la finalizzazione dell'ablazione del supporto alla sua successiva analisi, strumentale all'identificazione e all'estrazione dei dati 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. È altrettanto vero, però, che sempre secondo la giurisprudenza, la ragionevole durata di questo termine deve essere valutata in rapporto alle difficoltà tecniche di apprensione dei dati; e queste ultime devono ritenersi accresciute nel caso di mancata collaborazione dell'indagato che non fornisca le chiavi di accesso alle banche dati contenute nei supporti sequestrati: così Cass., Sez. II, 23 marzo 2023, n. 17604, in *C.E.D. Cass*., n. 284393.

[32] Cass., Sez. Un., 19 aprile 2018, n. 36072, in *C.E.D. Cass.*, n. 273548, ha evidenziato che «la portata precettiva degli artt. 42 Cost. e 1 del primo Protocollo addizionale della Convenzione Edu richiede che le ragioni probatorie del vincolo di temporanea indisponibilità della cosa, anche quando la stessa si identifichi nel corpo del reato, siano esplicitate nel provvedimento giudiziario con adeguata motivazione, allo scopo di garantire che la misura, a fronte delle contestazioni difensive, sia soggetta al permanente controllo di legalità - anche sotto il profilo procedimentale - e di concreta idoneità in ordine all'*an* e alla sua durata, in particolare per l'aspetto del giusto equilibrio o del ragionevole rapporto di proporzionalità tra il mezzo impiegato, ovvero lo spossessamento del bene, e il fine endoprocessuale perseguito, ovvero l'accertamento del fatto di reato».

[33] L'espressione è tratta da un memorabile *obiter dictum* del Giudice delle leggi, mai abbastanza seguìto dalla giurisprudenza e in realtà neppure adeguatamente coltivato, in seguito, dalla stessa Corte costituzionale: così Corte cost. 6 aprile 1973, n. 34.