40963-17

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

SEZIONI UNITE PENALI

Composta da

Giovanni Canzio - Presidente -
Giovanni Conti
Domenico Gallo
Maurizio Fumo
Francesco M. Silvio Bonito
Fausto Izzo
Maria Vessichelli
Luca Ramacci - Relatore -
Gaetano De Amicis

Sent. n. sez. 18
CC – 20/07/2017
R.G.N. 50286/2016

ha pronunciato la seguente

SENTENZA

sul ricorso proposto da
Andreucci Carlo, nato a Terni il 27/06/1964

avverso la ordinanza del 2/12/2016 del Tribunale di Terni;
visti gli atti, il provvedimento impugnato e il ricorso;
udita la relazione svolta dal componente Luca Ramacci;
lette le richieste del Pubblico Ministero, in persona del Sostituto Procuratore generale Delia Cardia, che ha concluso chiedendo il rigetto del ricorso.

RITENUTO IN FATTO

1. Il Tribunale di Terni, sezione per il riesame delle misure cautelari, con ordinanza del 2 dicembre 2016 ha confermato il decreto con il quale, il 16/11/2016, il Pubblico Ministero presso il medesimo Tribunale aveva convalidato il sequestro disposto d'iniziativa dalla polizia giudiziaria, all'esito della perquisizione personale e locale eseguita nei confronti di Carlo Andreucci, in relazione ai reati di turbata libertà degli incanti e turbata libertà del procedimento di scelta del contraente (artt. 353 e 353-*bis* cod. pen.) ed avente ad oggetto, tra l'altro, il computer personale dell'indagato, successivamente restituitogli previa estrazione di copia integrale dei dati informatici memorizzati.

2. Avverso tale pronuncia l'indagato ha proposto ricorso per cassazione tramite il proprio difensore di fiducia.

Osserva il ricorrente, con il primo motivo, che il computer personale non può essere equiparato ad un documento o ad un gruppo di documenti, bensì ad un intero archivio o libreria in senso fisico, in considerazione della elevata capacità di conservazione dei dati, con la conseguenza che il sequestro dell'intero apparato sarebbe contrario al principio di proporzionalità, oltre che a quanto disposto dall'art. 258, comma 4, cod. proc. pen.

Il sequestro di un intero sistema informatico, nozione nella quale rientra anche il computer ad uso personale, sarebbe inoltre escluso dalle disposizioni del codice di rito, come modificate dalla legge 18 marzo 2008, n. 48, sulla criminalità informatica.

Lamenta, inoltre, la mera apparenza della motivazione in ordine alla sussistenza del vincolo di pertinenzialità tra il reato ed i beni sequestrati, aggiungendo che l'avvenuta restituzione del computer, previa estrazione di copia dei dati, prima ancora della richiesta di riesame, non avrebbe fatto venir meno il suo interesse alla verifica della legittimità del provvedimento, mediante il quale si sarebbe proceduto ad un indiscriminato ampliamento del mezzo di ricerca della prova, tale da snaturarne la finalità, con conseguente intrusione nella sfera personale attraverso l'acquisizione di tutto il materiale informatico posseduto e riguardante la sua professione e non anche mediante un provvedimento espressamente finalizzato all'individuazione di quanto strettamente necessario ai fini probatori.

Con un secondo motivo di ricorso deduce che il provvedimento impugnato sarebbe del tutto privo di motivazione in ordine alle ragioni per le quali i giudici del riesame non avrebbero ritenuto rilevanti le argomentazioni sviluppate dalla difesa.

3. Il ricorso è stato assegnato alla Sesta Sezione penale, la quale ha preliminarmente dato atto di un precedente contrasto, risolto con una pronuncia resa nel 2008 dalle Sezioni Unite, alla quale si erano successivamente adeguate le Sezioni semplici, con la quale, in relazione ad una fattispecie di sequestro di un computer e di alcuni documenti, si era affermato che, una volta restituita la cosa sequestrata, la richiesta di riesame del sequestro, o l'eventuale ricorso per cassazione contro la decisione del tribunale del riesame, è inammissibile per sopravvenuta carenza di interesse, che non è configurabile neanche qualora l'autorità giudiziaria disponga, all'atto della restituzione, l'estrazione di copia degli atti o documenti sequestrati; ciò in quanto il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni. (Sez. U, n. 18253 del 24/04/2008, Tchmil, Rv. 23939701).

La Sezione rimettente pone tuttavia in luce il formarsi di una recente, diversa, linea interpretativa che, considerando i contenuti delle disposizioni introdotte con la legge n. 48 del 2008, riconosce anche al "dato informatico" in tuttaviaquanto tale, e non solo al supporto che lo contiene, la caratteristica di oggetto del sequestro, poiché la sua riproduzione si risolve in un "clone" identico ed indistinguibile dall'originale. Con la conseguenza che i dati informatici acquisiti mediante l'integrale riproduzione di quelli presenti sulla memoria del computer rimangono sotto sequestro anche se il supporto fisico di memorizzazione sia restituito: permane, sul piano del diritto sostanziale, una perdita autonomamente valutabile per il titolare del dato, venendo meno la disponibilità esclusiva della "informazione".

Da ciò conseguirebbe che la restituzione del computer, previa estrazione di copia informatica o riproduzione su supporto cartaceo dei dati in esso contenuti, non fa venire meno l'interesse a coltivare i ricorsi per riesame e per cassazione.

4. E' stata emessa ordinanza di rimessione alle Sezioni Unite ed il Primo Presidente, con decreto del 9 maggio 2017, ha fissato per la data odierna la trattazione del ricorso in camera di consiglio.

5. Il Procuratore generale ha sollecitato il rigetto del ricorso, pur riconoscendo la sussistenza di un interesse del ricorrente a impugnare il provvedimento nonostante l'avvenuta restituzione del materiale sequestrato, previa estrazione di "copia forense", escludendo, però, la sussistenza della carenza motivazionale evocata.

Il Procuratore generale ha depositato altresì memoria, con la quale, sulla scorta della giurisprudenza della Corte EDU, ha espresso le ragioni dell'adesione

all'indirizzo secondo il quale permane un interesse all'impugnazione anche dopo la restituzione del computer e del dato "originale", qualora l'autorità inquirente ne abbia estratto copia, pur ribadendo l'infondatezza, nel merito, del ricorso.

CONSIDERATO IN DIRITTO

1. La questione di diritto per la quale il ricorso è stato rimesso alle Sezioni Unite può essere così enunciata:

"*Se sia inammissibile, per sopravvenuta carenza di interesse, il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti*".

2. La Sezione rimettente ha posto in evidenza i diversi indirizzi interpretativi venutisi a formare dopo la pronuncia delle Sezioni Unite n. 18253 del 2008, Tchmil, dalla quale occorre dunque prendere le mosse ed i cui contenuti vanno sommariamente richiamati.

3. Osservando come, in una precedente pronuncia (Sez. U, n. 230 del 20/12/2007, dep. 2008, Normanno, Rv. 237861), si fosse già condiviso il maggioritario orientamento, secondo il quale la restituzione del bene priva di interesse concreto l'impugnazione, con conseguente inammissibilità del ricorso, la sentenza Tchmil, previa disamina dei contenuti degli artt. 258 e 262 cod. proc. pen., rileva l'autonomia del provvedimento acquisitivo della copia rispetto al sequestro probatorio, osservando anche come tale acquisizione possa avvenire, ad esempio, all'esito di perquisizione non seguita da sequestro, consegna spontanea o adempimento al dovere di esibizione.

Tale provvedimento, inoltre, viene indicato come frutto di autonoma determinazione discrezionale – ben potendo gli originali essere restituiti senza che ne sia stata estratta copia – che richiede una giustificazione della rilevanza probatoria dell'acquisizione, la quale non potrebbe esaurirsi nella menzione dell'esistenza di un pregresso provvedimento con cui si è resa temporaneamente indisponibile, a fini probatori, la cosa oggetto di copia, venendone tuttavia esclusa l'autonoma impugnabilità mediante riesame o altre forme di gravame in forza del principio di tassatività delle impugnazioni.

Viene inoltre considerato anche l'ulteriore aspetto relativo all'eventuale permanere, a fronte dell'avvenuta restituzione, di un interesse ad impedire comunque l'ingresso della copia nel patrimonio probatorio utilizzabile, cosicché l'eventuale annullamento del sequestro all'esito dell'esame travolgerebbe il

presupposto di validità del conseguente provvedimento di acquisizione probatoria, rendendolo a sua volta invalido. Si obietta, tuttavia, che, anche a voler riconoscere una dipendenza tra sequestro probatorio ed estrazione di copia tale da comportare una propagazione della nullità, deve volgersi l'attenzione al fatto che il riesame proposto con un sequestro ancora in atto risponde all'interesse, immediato ed attuale, alla restituzione; il che non avviene con riferimento alle copie estratte, delle quali non è in atto l'utilizzazione, la quale non è neppure certa, dipendendo dalla strategia delle parti nel successivo giudizio e dalle decisioni del giudice del processo, che non sarebbero, peraltro, in alcun modo condizionate dall'esito del giudizio incidentale del riesame.

Si è altresì escluso che la questione possa assumere rilievo con riferimento alla utilizzabilità di un elemento probatorio illegittimamente acquisito nell'eventuale applicazione di una misura cautelare, che pure non sarebbe condizionata dall'esito del riesame del sequestro, stante l'autonoma valutazione sulla legittimità, utilizzabilità e significatività dei mezzi di prova demandata al giudice della misura cautelare, ribadendosi, in definitiva, che il giudicato nel procedimento incidentale riguarda solo il vincolo imposto dal provvedimento e ordinariamente non produce alcun effetto diverso, esaurendo completamente il proprio ambito con la pronuncia su quel vincolo.

4. Alla decisione si sono adeguate le Sezioni semplici con successive pronunce (tra le molte, Sez. 2, n. 29019 del 30/06/2010, Fontana, Rv. 248143; Sez. 6, n. 29846 del 24/04/2012, Addona, Rv. 253251; Sez. 1, n. 43541 del 08/10/2013, Poltrone, Rv. 257357; Sez. 3, n. 27503 del 30/05/2014, Peselli, Rv. 259197; Sez. 3, n. 24928 del 25/09/2014, Cenni, non mass.), alcune delle quali riguardanti specificamente ipotesi di sequestro di computer e documenti informatici.

5. Successivamente, altre pronunce si sono contrapposte all'indirizzo ormai consolidato.

In particolare, in una prima decisione (Sez. 6, n. 24617 del 24/02/2015, Rizzo, Rv. 264093) si è riconosciuto che costituisce sequestro probatorio l'acquisizione, mediante estrazione di copia informatica o riproduzione su supporto cartaceo, dei dati contenuti in un archivio informatico visionato nel corso di una perquisizione legittimamente eseguita ai sensi dell'art. 247 cod. proc. pen., quando il trattenimento della copia determina la sottrazione all'interessato della esclusiva disponibilità dell'informazione.

La pronuncia, riguardante l'acquisizione, a seguito di perquisizione, di quattro messaggi di posta elettronica prelevati e stampati previo accesso al

sistema mediante le credenziali fornite dallo stesso titolare dell'indirizzo, pone in evidenza come anche il singolo *personal computer* non possa essere equiparato ad un documento o ad un gruppo di documenti, bensì ad un intero archivio o deposito o libreria in senso fisico, in ragione delle enormi potenzialità di archiviazione di grandi masse di dati, escludendo pertanto la possibilità di un indiscriminato sequestro del computer, con estrazione di copia dell'intero contenuto, difettando, in tal caso, la necessaria individuazione della cosa da acquisire ed il collegamento tra la cosa ed il reato da dimostrare, violandosi, inoltre, le regole in tema di proporzionalità del sequestro.

Viene inoltre rilevata la esplicita esclusione della possibilità di procedere, di norma, al sequestro di interi sistemi informatici alla luce di quanto disposto dalla legge 18 marzo 2008, n. 48, e richiamando i contenuti degli artt. 247, comma 1-*bis*, e 352, comma 1-*bis*, cod. proc. pen., che tale legge ha introdotto. Non si esclude tuttavia la possibilità del sequestro di un intero sistema se il provvedimento è proporzionato rispetto alle esigenze probatorie o quando l'accertamento riguardi l'intero sistema (come nel caso di utilizzazione del computer per archiviazione di materiale illecito o per la duplicazione abusiva di supporti audiovisivi), tenendo peraltro conto della possibilità di un trasferimento fisico delle apparecchiature per l'effettuazione della perquisizione in luogo e con modalità adeguate, come nel caso in cui si presenti la necessità di disporre di personale tecnico, ad esempio per superare le barriere di protezione del sistema.

Richiamando quindi la sentenza Tchmil delle Sezioni Unite ed osservando come la stessa sia stata assunta antecedentemente alla vigenza delle nuove disposizioni introdotte con la legge n. 48 del 2008, si osserva che in quella decisione non si era affrontato il tema della estrazione di copia del dato informatico e della perdurante perdita di un diritto su una cosa che potrebbe conseguirne.

Attraverso l'analisi della legge citata, la sentenza Rizzo individua il dato informatico come oggetto del sequestro, riconoscendogli la qualifica di "cosa", trovando conferma a tale assunto nel disposto degli artt. 635-*bis* e 635-*ter* cod. pen., nonché in quelle disposizioni del codice di rito che a tale dato attribuiscono un valore del tutto assimilabile a quello di un oggetto "fisico" (artt. 248, 254, 254-*bis*, 256, 260 cod. proc. pen.).

Viene poi rilevato che la sostanziale identità tra originale e copia, significativamente individuata, nel linguaggio comune, come "clone", non consentirebbe di ritenere che vi sia stata una effettiva restituzione di quanto in sequestro quando l'interessato sia stato comunque privato del valore in sé del dato, rappresentato dalla sua esclusiva disponibilità.

Ritenendo quindi che l'art. 258 cod. proc. pen. non sembra voler disciplinare

il caso in cui il documento trasferisca il proprio valore anche sulla copia, si sostiene che «la restituzione degli atti originali, cartacei o digitali, previa estrazione di copie» determina «il venir meno del sequestro solo laddove non permanga una perdita valutabile per il titolare del bene originale. Perdita che deve essere considerata sul piano di un diritto sostanziale e non deve invece essere considerata quanto al semplice interesse a che la data cosa non faccia parte del materiale probatorio» (come afferma la già citata sentenza delle SS.UU.)».

6. Altra decisione (Sez. 3, n. 38148 del 23/6/2015, Cellino, Rv. 265181) evidenzia la «assoluta peculiarità della nozione di documento informatico/dato informatico» e, richiamando le argomentazioni sviluppate nella sentenza Rizzo, riconosce la sussistenza di un interesse attuale a richiedere il controllo giurisdizionale sulla legittimità del sequestro, perché la restituzione dei supporti di archiviazione, previo trattenimento di copia dei dati informatici estratti, non comporta il venir meno del vincolo (ad essa si è successivamente conformata Sez. 5, n. 25527 del 27/10/2016, dep. 2017, Storari, Rv. 269811).

7. Su una posizione in un certo senso intermedia si colloca, invece, una successiva pronuncia (Sez. 2, n. 40831 del 09/09/2016, Iona, Rv. 267610) che, pur seguendo il solco tracciato dalla sentenza Tchmil, riconosce, tenendo conto delle argomentazioni sviluppate dalla sentenza Rizzo, la permanenza di un interesse all'impugnazione quando sia dimostrato il valore autonomo dei dati copiati, perché il trattenimento della copia determina la sottrazione all'interessato della esclusiva disponibilità dell'informazione, risolvendosi in un vero e proprio "sequestro di informazione", autonomamente apprezzabile.

8. Ciò posto, occorre in primo luogo individuare la natura del "dato informatico", verificando se lo stesso abbia caratteristiche particolari che lo differenziano rispetto ad altri dati raccolti ed archiviati con diverse modalità.

Va peraltro considerato come tale operazione richieda un'ulteriore premessa, finalizzata a ben delineare l'oggetto del discorso, prendendo in considerazione le diverse possibili componenti di quello che può definirsi, in concreto, un "sistema informatico".

Deve tuttavia osservarsi che il risultato di tale analisi non potrà che essere limitato agli aspetti strettamente necessari per la soluzione della questione di diritto.

9. Un sistema informatico, in linea generale, è costituito dalle componenti

hardware e *software*, le prime rappresentate, secondo la comune definizione, dal complesso di elementi fisici non modificabili, (quali circuiti, unità di memoria, parti meccaniche etc.) cui si aggiungono periferiche di ingresso (ad. es. tastiera, *scanner* etc.) e di uscita (es. *monitor*, stampante) ed altri componenti comuni (*modem*, masterizzatore, cavi) e le seconde costituite, sempre secondo la comune accezione, dall'insieme di istruzioni e procedure necessarie per il funzionamento stesso della macchina (*software* di base) o per farle eseguire determinate attività (*software* applicativo) e costituiti da programmi o dati memorizzati su specifici supporti.

La Convenzione di Budapest, ratificata dalla legge n. 48 del 2008, definisce il sistema informatico come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati», tenendo quindi conto anche della possibile interazione di più dispositivi.

Va dunque distinto, per quel che qui interessa, il "contenitore" rispetto al "contenuto", dovendosi quindi valutare l'oggetto di un eventuale provvedimento di sequestro, il quale, come correttamente ricordato nella sentenza Rizzo, può riguardare, sussistendone la necessità, l'intero sistema (come nel caso in cui l'apprensione sia necessaria per esaminare grosse quantità di dati, pur essendo necessario – come ricorda Sez. 6, n. 53168 del 11/11/2016, Amores, Rv. 268489 – la immediata restituzione decorso il tempo ragionevolmente utile per gli accertamenti legittimamente in corso) ovvero il singolo dato, che ha certamente una sua identità fisica, essendo modificabile e misurabile.

10. Dunque anche la componente *software* di un sistema informatico, avendo una sua consistenza compiutamente individuabile, può pacificamente ritenersi suscettibile di sequestro (come peraltro già riconosciuto, con riferimento a "siti *web*" o singole "pagine telematiche", da Sez. U, n. 31022 del 29/01/2015, Fazzo, Rv. 264089), seppure con le specifiche modalità dettate dalla legge.

Va peraltro osservato, a tale proposito, che la distinzione tra le diverse componenti di un sistema informatico di cui si è appena detto non è stata sempre chiara al legislatore, il quale, nell'art. 491-*bis* cod. pen., definiva, ad esempio, come "documento informatico", qualunque «supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli», così sostanzialmente sovrapponendo il "documento", entità del tutto autonoma, con il "supporto" che lo contiene.

A tale anomalia, segnalata dalla dottrina, si è successivamente rimediato attraverso la soppressione del periodo ad opera dell'art. 3, comma 1, lett. *b*), della legge n. 48 del 2008, dovendosi ora fare riferimento alla definizione di

"documento informatico" contenuta nell' art. 1, lett. *p*), d.lgs. 7 marzo 2005, n. 82 («documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti») già in precedenza fornita, sotto diversa forma, dapprima dal d.P.R. 10 novembre 1997, n. 513, e, successivamente, dal d.P.R. 28 dicembre 2000, n. 445.

La differenza è ora ben presente anche in altre disposizioni, come, ad esempio, negli artt. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* cod. pen., che distinguono il danneggiamento dell'integrità dei dati dal danneggiamento dell'integrità di un sistema.

11. La distinzione tra intero sistema e dati è altresì rinvenibile nelle disposizioni del codice di rito modificate dalla legge n. 48 del 2008, come, ad esempio, negli artt. 247, comma 1-*bis* e 352, comma 1-*bis.*

Detta distinzione tra i dati ed il sistema che ne consente l'archiviazione o l'elaborazione (o, meglio, tra componenti *hardware* e *software* di un sistema) è dunque evidente non soltanto sotto un profilo prettamente tecnico, ma anche nell'uso dei termini effettuato dal legislatore, così come è altrettanto evidente che a dati, programmi ed informazioni viene comunque riconosciuta quella individualità fisica di cui si è detto, sanzionandone il danneggiamento (artt. 635-*bis* e 635-*ter* cod. pen.) e specificando le modalità esecutive delle perquisizioni (248, comma 2, 352, comma 1-*bis*, cod. proc. pen.), dei sequestri (art. 256, comma 1, 259, comma 2, 260, comma 2, cod. proc. pen.) e degli accertamenti urgenti (art. 354, comma 2, cod. proc. pen.).

12. Deve a questo punto considerarsi che la nozione di "dato informatico", sebbene riferibile, per quel che qui rileva, ai «dati, programmi ed informazioni» di cui alle norme appena richiamate e, più in generale, alla componente *software* di un sistema, risulta comunque non chiaramente definita se non per l'ampia indicazione dell'oggetto fisico, il quale, tuttavia, può assumere conformazioni diverse, potendo, ad esempio, riguardare un insieme di istruzioni formulate in uno specifico linguaggio e finalizzate alla esecuzione di determinate operazioni (come nel caso del programma applicativo), un mero insieme di informazioni come quelle conservabili su carta, il risultato dell'elaborazione di più informazioni o operazioni, la rappresentazione di atti, fatti o dati giuridicamente rilevanti (nella forma, quindi, del documento elettronico), la riproduzione per immagine di atti o documenti cartacei etc.

Sempre la Convenzione di Budapest definisce come dato informatico «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di

consentire ad un sistema computerizzato di svolgere una funzione».

In dottrina si è fatto rilevare come la terminologia utilizzata dal legislatore non sia sempre corrispondente alla definizione offerta dalla Convenzione, essendosi ad esempio, nella frode informatica (art. 640-*ter* cod. pen.) e nel danneggiamento, affiancato, al termine "dato" anche quelli di "informazione" e "programma", che sono in esso ricompresi.

13. Oggetto di un eventuale sequestro, in definitiva, può anche essere il dato informatico così come in precedenza individuato.

Secondo il rapporto esplicativo adottato dal Comitato dei ministri del Consiglio d'Europa (punto 197), il termine "sequestrare", in base alla convenzione «significa prendere il mezzo fisico sul quale i dati o le informazioni sono registrati oppure fare e trattenere una copia di tali dati o informazioni. "Sequestrare" include l'uso o il sequestro di programmi necessari ad accedere ai dati che si stanno sequestrando. Allo stesso modo in cui si usa il termine tradizionale "sequestrare", il termine "assicurare in modo simile" è incluso per indicare gli altri modi nei quali i dati intangibili possono essere portati via, resi inaccessibili o il suo controllo e in altro modo escluso per il sistema informatico».

Alla luce di quanto sinora riportato, sembra possa rilevarsi che la peculiarità del dato informatico sia data esclusivamente dalle sue caratteristiche fisiche e dalle modalità di conservazione e di elaborazione, mentre non si rilevano rilevanti differenze rispetto al contenuto, quando rappresentativo di fatti, atti, idee, sequenze di espressioni, etc., il quale può essere conservato anche altrove, ad esempio sulla carta.

14. Di tale particolarità si è fatto evidentemente carico il legislatore con le modifiche apportate al codice penale ed al codice di rito con la più volte menzionata legge n. 48 del 2008.

Ed infatti, l'art. 244, comma 2, cod. proc. pen. prevede, ad esempio, la possibilità di adottare, riguardo ai rilievi ed alle operazioni tecniche da effettuare in relazione a sistemi informatici o telematici, misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

L'art. 247, comma 1-*bis*, cod. proc. pen. prevede analoghi accorgimenti nel consentire la perquisizione di un sistema informatico o telematico, anche se protetto da misure di sicurezza, quando vi è fondato motivo di ritenere che in essi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato (analoga possibilità di perquisizione è riconosciuta alla polizia giudiziaria dall'art. 352, comma 1-*bis*, cod. proc. pen.).

L'art. 254-*bis* cod. proc. pen., nel disciplinare il sequestro di dati informatici

presso fornitori di servizi informatici, telematici e di telecomunicazioni, consente all'autorità giudiziaria di stabilire, per esigenze legate alla regolare fornitura dei servizi, che l'acquisizione avvenga mediante copia dei dati su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità, ordinandosi, in questo caso, al fornitore dei servizi, di conservare e proteggere adeguatamente i dati originali.

L'art. 256, comma 1, cod. proc. pen. estende l'obbligo di consegna all'autorità giudiziaria richiedente ai «dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto».

L'art. 260, comma 2, cod. proc. pen., che originariamente stabiliva la possibilità di estrarre copia dei documenti e far eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, prescrive ora che quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità, potendosi, in tali casi, disporre la custodia degli originali anche in luoghi diversi dalla cancelleria o dalla segreteria.

L'art. 354, comma 2, cod. proc. pen., nel disciplinare gli accertamenti urgenti da parte della polizia giudiziaria, prevede, riguardo ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, l'adozione di misure tecniche o l'imposizione delle prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso, stabilendo altresì che, ove possibile, la medesima polizia giudiziaria provveda alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

15. Come si evince dal contenuto delle disposizioni appena richiamate, esse fanno riferimento a dati, informazioni e programmi nella loro essenza fisica e senza riferimento ai contenuti, prevedendo la possibilità di ricercarli mediante perquisizione del sistema informatico o telematico che li potrebbe contenere.

Altro elemento comune che si rinviene nelle citate disposizioni è il riferimento alla possibilità di estrazione di copie dei dati secondo procedure, peraltro non tipizzate (cfr. Sez. 3, n. 37644 del 28/5/2015, R., Rv. 265180), che ne assicurino la conformità all'originale e la immodificabilità.

Invero, come emerge con chiarezza dal complesso delle disposizioni codicistiche dianzi richiamate, l'estrazione della copia con modalità tali da assicurarne la conformità all'originale e la sua immodificabilità è prevista allo scopo di preservare il dato acquisito isolandolo dal sistema che lo contiene, impedendone la successiva elaborazione, trasformazione o eliminazione, sempre

possibile anche senza il diretto intervento di un operatore, ad esempio, se precedentemente programmata.

Si tratta, in altre parole, di un riferimento alla c.d. copia-immagine, che riproduce il dato duplicato nelle stesse condizioni in cui si trova al momento della sua acquisizione, poiché ciò che può rilevare, per le finalità di indagine che giustificano l'apprensione, non è necessariamente il solo contenuto informativo del dato, ma il dato stesso e il suo stato in un determinato periodo, potendo, ad esempio, con riferimento ad un semplice *file*, risultare di interesse investigativo la data di creazione, quella di apertura, di esecuzione o dell'ultima modifica, la proprietà, i permessi, eventuali codici di controllo, la posizione all'interno di una determinata cartella o gruppo di cartelle etc.

L'acquisizione della copia con le modalità indicate, peraltro, consente l'estrazione di ulteriori copie immagine e la loro successiva manipolazione per i necessari accertamenti tecnici senza l'inevitabile trasformazione o modifica delle condizioni originali che si avrebbe operando diversamente, rendendo peraltro detti accertamenti ripetibili successivamente.

In tali casi, dunque, i dati individuati attraverso la perquisizione vengono sottoposti a sequestro.

Va anche osservato che la concreta esecuzione delle attività finalizzate all'acquisizione del dato va calibrata secondo le specifiche esigenze del caso (oltre che nell'ovvio rispetto del principio di proporzionalità), poiché la acquisizione, ad esempio, del mero contenuto testuale di un documento conservato in formato elettronico richiede modalità diverse e presenta minore complessità rispetto alle attività di acquisizione del dato da effettuarsi mantenendolo inalterato o su un computer acceso e funzionante, per evitare, ad esempio, che lo spegnimento disperda informazioni sulla connessione o l'accesso ad una rete o ad un determinato sistema remoto, oppure nel caso in cui la sola ricerca del dato possa alterarne i contenuti.

16. Nel fare riferimento a tali casi si è sostenuta, in dottrina ed anche nella giurisprudenza richiamata, la sostanziale identità tra l'estrazione della copia dei dati informatici ed il sequestro. Ma tale assunto, se posto in termini così drastici, non pare pienamente condivisibile e richiede alcune precisazioni.

Le disposizioni in precedenza richiamate sono finalizzate all'individuazione delle concrete modalità di estrazione e conservazione in considerazione delle caratteristiche delle cose da sequestrare e della suscettibilità delle stesse a repentine trasformazioni o, come nel caso dell'art. 254-*bis* cod. proc. pen., all'assicurazione della continuità del servizio.

Significativo, a tale proposito, risulta l'art. 260 cod. proc. pen., il quale, così

come dispone che l'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, altrettanto prevede, per ciò che concerne i dati informatici, stabilendo le specifiche modalità di copia e distinguendo quest'ultima dagli originali, la cui custodia può essere disposta anche in luoghi diversi.

17. I riferimenti alla copia dei dati ed al mantenimento della loro originaria integrità introdotti dalla legge n. 48 del 2008 riguardano le cosiddette copie-immagine (la cui integrità ed identità all'originale è assicurata dalla funzione crittografica di "*hash*" alla stregua di un'impronta) ed è evidente, dal momento che, riguardando la legge suddetta la criminalità informatica, l'acquisizione e conservazione del dato informatico deve assicurare la possibilità di successive analisi nello stato e nelle condizioni nelle quali esso si trovava all'interno del sistema attraverso la creazione, appunto, di un "clone".

Può peraltro verificarsi l'ipotesi in cui tale necessità non sia avvertita, essendo sufficiente la mera copia del contenuto del dato informatico mediante estrapolazione dello stesso in una copia priva delle suddette caratteristiche.

Una simile distinzione è presente nel d.lgs. n. 82 del 2005 (Codice dell'amministrazione digitale) laddove, nell'art. 1, oltre a distinguere, al comma 1, il "documento informatico" dal "documento analogico" (rispettivamente, nel comma 1, lettere *p* e *p-bis*) a seconda che la rappresentazione di atti, fatti o dati giuridicamente rilevanti sia o meno inserita in un documento elettronico che ne contiene la rappresentazione informatica, definisce, nella lett. i-*quater,* la "copia informatica" di documento informatico («il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari») e la distingue dal "duplicato informatico" di cui alla lettera i-*quinquies* («il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario»), operando, peraltro, una analoga distinzione tra "copia informatica di documento analogico" e "copia per immagine su supporto informatico di documento analogico", laddove la prima è «il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto» e la seconda «il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto».

Va tuttavia posto in evidenza che, sulla base delle disposizioni in precedenza esaminate e delle diverse esigenze investigative che rendono necessario il

sequestro, la distinzione tra "copia-immagine" (o "clone") e semplice copia non sembra sufficiente per definire i termini della questione, dovendosi anche distinguere i casi in cui la apprensione riguardi, essenzialmente, il dato informatico in relazione al suo contenuto, in quanto rappresentativo di atti o fatti, dunque quale vero e proprio documento, la cui particolarità è data soltanto dalle modalità di acquisizione e conservazione.

18. In definitiva, alla luce delle considerazioni sopra esposte, riguardo ai dati ed ai sistemi informatici possono verificarsi diverse situazioni, in precedenza individuate, rispetto alle quali il sequestro probatorio, secondo le diverse necessità, può colpire il singolo apparato, il dato informatico in sé, ovvero il medesimo dato quale mero "recipiente" di informazioni.

Se, per quanto riguarda la prima ipotesi, è indubbio che l'interesse ad ottenere la restituzione va riferito all'intero apparato o sistema in quanto tale, perché specifico oggetto del sequestro, nella seconda, invece, la materiale apprensione riguarda il dato come cristallizzato nel "clone" identico all'originale e, perciò, da esso indistinguibile, perché riversato nella "copia immagine" solo per preservarne l'integrità e l'identità alle condizioni in cui si trovava al momento del prelievo e consentire successive verifiche o accertamenti tecnici.

In tale caso l'interesse alla restituzione riguarda, appunto, il dato in sé e non anche il supporto che originariamente lo conteneva o quello sul quale è trasferito il "clone", sicché la mera restituzione del supporto non può considerarsi come esaustiva restituzione della cosa in sequestro; e ciò trova conferma anche nella ricordata definizione di "sequestro" offerta dalla convenzione di Budapest.

Diverso è invece il caso in cui un atto o un documento si presenti sotto forma di dato informatico, non rilevando, in tali casi, il dato in sé, bensì quanto in esso rappresentato, come avviene per i documenti cartacei, ben potendosi distinguere, in tali casi, le copie dall'originale, che in questo caso sarà rappresentato dal documento elettronico originariamente formato ed univocamente identificabile.

19. Se questa è, dunque, la distinzione che deve operarsi, è evidente che nei primi due casi ipotizzati non può trovare applicazione l'art. 258 cod. proc. pen., che riguarda espressamente i documenti, mentre tale disposizione andrebbe considerata quando il dato informatico può essere ricondotto entro la nozione di atto o documento, nel qual caso andrebbero apprezzate le conclusioni cui è pervenuta la sentenza Tchmil.

Occorre però rilevare, a tale proposito, che la sentenza Tchmil non ha affatto preso in esame l'ipotesi, sulla quale parte della giurisprudenza successiva ha

focalizzato l'attenzione, in cui il documento, sia esso informatico o di altro tipo, «trasferisca il proprio valore anche sulla copia», venendo così in gioco l'interesse alla «disponibilità esclusiva del "patrimonio informativo"» cui fa riferimento l'ordinanza di rimessione, poiché esso non verrebbe meno con la mera restituzione fisica di quanto oggetto di sequestro.

20. E' indubbio che, in tali casi, la restituzione non può considerarsi risolutiva, dal momento che la mera reintegrazione nella disponibilità della cosa non elimina il pregiudizio, conseguente al mantenimento del vincolo sugli specifici contenuti rispetto al contenitore, incidente su diritti certamente meritevoli di tutela, quali quello alla riservatezza o al segreto.

Vanno a tale proposito considerate le indicazioni fornite dalla Corte EDU, che anche le pronunce successive alla sentenza Tchmil hanno valorizzato, concernenti non soltanto il fattore tempo come parametro di valutazione della correttezza di un sequestro (come ricordato da Sez. 6, n. 53168 del 2016, Amores, cit. la quale richiama Corte EDU 07/06/2007, Smirnov c. Russia, nonché Corte EDU 19/06/2014, Draghici c. Portogallo), ma anche il diritto alla libertà di espressione di cui all'art. 10 CEDU, in particolare, la tutela della segretezza delle fonti giornalistiche (Sez. 6, n. 24617 del 2015, Rizzo, cit., richiama Corte EDU, Grande Camera, 14/09/2010, Sanoma Uitgevers, B.V. contro Paesi Bassi, ma v. anche Corte EDU 19/01/2016, Gulcu c. Turchia), nonché, con riferimento all'art. 8 della Convenzione, il diritto al rispetto della vita privata e familiare (Corte EDU, 22/5/2008, Ilya Stefanov c. Bulgaria; 02/04/2015, Vinci Construction et GTM Génie Civil et Services c. Francia).

La Corte EDU ha tenuto dunque in considerazione la inevitabile incidenza degli atti di indagine aventi ad oggetto dati sensibili e, in un caso, ha espressamente evidenziato, riconoscendo la legittimità del procedimento, in una ipotesi di sequestro di documenti e *file* estratti da computer aziendali, la necessità di un pieno contraddittorio quanto ai documenti acquisiti e la possibilità di impugnare il sequestro davanti ad un giudice.

Può in definitiva ritenersi che, in tali casi, nonostante la restituzione del supporto sul quale il dato è contenuto, permanga comunque un interesse all'impugnazione del provvedimento ablativo per la verifica della sussistenza dei presupposti applicativi.

Deve tuttavia trattarsi di un interesse concreto ed attuale, specifico ed oggettivamente valutabile sulla base di elementi univocamente indicativi della lesione di interessi primari conseguenti alla indisponibilità delle informazioni contenute nel documento, la cui sussistenza andrà dimostrata, non potendosi ritenere sufficienti allo scopo generiche allegazioni.

21. Deve conseguentemente affermarsi il seguente principio di diritto:

"*E' ammissibile il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un computer o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l'interesse, concreto e attuale, alla esclusiva disponibilità dei dati*".

22. Venendo all'esame dei motivi di ricorso, va osservato, con riferimento alla prima doglianza, che secondo quanto rilevato nel provvedimento impugnato, il Pubblico Ministero non ha disposto, come affermato dal ricorrente, il sequestro indiscriminato dell'intero computer, avendo invece proceduto a perquisizione personale, veicolare e locale finalizzata al sequestro di atti e documenti che i giudici del riesame hanno motivatamente ritenuto pertinenti ai reati per i quali si procede.

Per ciò che concerne specificamente gli archivi informatici, il Tribunale ha chiaramente posto in evidenza come il Pubblico Ministero avesse disposto la sola "perquisizione mirata" degli stessi, cui ha fatto seguito l'estrazione dei dati significativi e l'immediata restituzione degli archivi all'avente diritto senza pregiudizio per la fruizione del sistema informatico.

Quanto all'acquisizione delle copie, va rilevato che trattasi di materiale verosimilmente di natura documentale, rispetto al quale il ricorrente non ha indicato quale fosse l'interesse alla esclusiva disponibilità delle informazioni in essi contenute, limitandosi a riferimenti del tutto generici a non meglio precisate «intrusioni nella sfera personale» che il sequestro del materiale «attinente alla professione» avrebbe determinato.

Per ciò che concerne, invece, il secondo motivo di ricorso, lo stesso è inammissibile perché deduce un vizio di motivazione denunciandone l'illogicità, mentre, secondo quanto stabilito dall'art. 325 cod. proc. pen., il ricorso per cassazione avverso l'ordinanza emessa in sede di riesame dei provvedimenti di sequestro preventivo e probatorio è proponibile solo per violazione di legge.

Il ricorso deve pertanto essere rigettato, con le consequenziali statuizioni indicate in dispositivo.

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali.

Così deciso il 20/7/2017.

Il Componente estensore
Luca Ramacci

Il Presidente
Giovanni Canzio

SEZIONI UNITE PENALI
Depositato in Cancelleria
il - 7 SET. 2017
IL CANCELLIERE
Stefania Faiella