La sentenza di cui ad oggetto, nella sua asciuttezza espressiva, riafferma, e ne ha ben donde!, princìpi inconcussi: 1) tra le *res adprehensae* ed il reato oggetto di accertamento deve sussistere un nesso di pertinenzialità nel verso che le prime debbono rappresentare il corpo del reato oppure cose, beni o strumenti, finanche informatici, che servirono o furono destinate a commettere il predetto o che ne costituiscono prezzo, prodotto o profitto (o, ancora, un valore economico equivalente a tale prodotto o profitto); 2) non è dato acconsentire, di regola, all'accesso indiscriminato, "in bianco" verrebbe da dire, alle cose, ai beni, agli oggetti, ai dati di cui ad un determinato "contenitore" vietandosi quindi un "mandato esplorativo" a sequestrare ("poniamo tutto sotto sigillo ché qualcosa di funzionale per le indagini di certo troveremo" …): è dunque interdetto ciò che nei sistemi anglosassoni, con immaginifica e felice locuzione, viene a qualificarsi come *fishing expedition* – ovviamente sono contemplate eccezioni: si pensi, ad esempio, ad un "magazzino", poco rileva ora se cartaceo o virtuaceo, destinato alla gestione di supporti audiovisivi "piratati" oppure alla conservazione/archiviazione di materiale illecito.

Altrimenti detto, altresì per le misure cautelari reali (e, per estensione, finanche per il sequestro probatorio come regolato dagli artt. da 253 a 264 c.p.p.), hanno valenza i princìpi di proporzionalità, di adeguatezza, di gradualità, esplicitamente declinati "solo" per le misure cautelari personali *ex* art. 275 c.p.p., nel senso che il giudice deve a proposito motivare sulla impossibilità di conseguire il medesimo risultato attraverso ulteriori, e meno invasivi, strumenti cautelari (ovvero l'organo di *jus dicere* deve fornire conto delle ragioni per cui, a fronte di una determinata *tranche de vie*, debbasi, putacaso, procedere al sequestro dell'intera documentazione contabile, cartacea o virtuacea che sia, di un'azienda in luogo di una selezionata apprensione di *n* "faldoni" tra quelli disponibili).

In giurisprudenza, con estrema chiarezza sul punto, è dato avvalersi di Cass., Sez. VI, 19 febbraio 2021, P., ad oggetto la perquisizione ed il sequestro, non "selezionati", di dati risultanti da un *tablet* e da un telefono cellulare nella disponibilità del ricorrente giusta il cui insegnamento, «[p]er quanto non possa dirsi di per sé illegittimo il sequestro del dispositivo in luogo dell'estrazione immediata del suo contenuto, ove sussistano specifiche difficoltà tecniche, nondimeno deve rilevarsi che in casi siffatti il vincolo risulta soltanto strumentale rispetto all'acquisizione mirata di dati in esso

contenuti, risultando altrimenti di per sé privo di giustificazione, non potendosi procedere ad un'acquisizione di carattere meramente esplorativo. Ciò comporta che il vincolo deve essere *ab origine* commisurato, anche sul piano temporale, a quell'esigenza di estrapolazione e che nel contempo deve essere assicurato un canone di selezione in assenza del quale il vincolo risulta nel suo complesso ingiustificato per difetto di proporzionalità».

Ciò appurato, emergono all'attenzione dell'interprete due quesiti di non breve momento: 1) che cosa possa identificarsi oggetto del sequestro ovvero se esso debba di necessità "cadere" su di un *quid* fisico oppure se possa riguardare finanche beni immateriali (*res quae tangere non potest*) di cui, prototipicamente, rappresentano un'esemplificazione i dati informatici conservati in *x devices* di utilizzo comune; 2) se, a fronte dell'estrazione di copia del *quid* da sequestrare, la restituzione dell'originale al legittimo reclamante faccia venire meno ogni interesse ad impugnare il decreto che aveva disposto la misura cautelare *de qua*. Se, giusta il primo interrogativo, la risposta appare pacifica alla luce delle interpolazioni apportate al codice di rito penale stante la ratifica "interna" della Convenzione di Budapest sulla criminalità informatica, ratifica operata con l. 18 marzo 2008, n. 48, in tema di perquisizione e di sequestro (v., a mero "florilegio", gli artt. 247, co. 1 *bis*, 248, co. 2, 254, co. 1 e 2, 254 *bis*, 256, co. 1, 259, co. 2, 260, co. 1 e 2, 352, co. 1 *bis*, 353, co. 2 e 3, 354, co. 2, c.p.p.) è proprio sul secondo "corno" che viene ad innestarsi la problematica di cui alla cosiddetta "copia forense". Ma procediamo con ordine.

Il dubbio circa la "trattenibilità" presso gli uffici requirenti di una copia di dati informatici, nel caso di specie estratti dal *personal computer* dell'interessato alla restituzione, viene a porsi per la prima volta, salvo errori ed/omissioni di chi scrive, in un "arresto" del 2015 (Cass., Sez. VI, 24 febbraio 2015, R.) in cui, a margine di un'indagine per segreto di ufficio, si disponeva la perquisizione della postazione fisica di lavoro del R. (giornalista non indagato per la fattispecie penale di cui sopra) nonché del suo *pc* ad esito della quale venivano "appresi" quattro messaggi di posta elettronica dalla *mailbox* di riferimento onde, eventualmente, accedere alle generalità della "gola profonda" che aveva riferito al suddetto i fatti oggetto di indagine. Il Tribunale del Riesame, adìto dall'instante, rispondeva "picche" alla domandata restituzione assumendo che si fosse in presenza di mero trattenimento di copia del materiale

individuato con la perquisizione restando l'originale nel pieno possesso del R. Venendone, a logica conseguenza, che «tale acquisizione di copia non è stata ritenuta un sequestro probatorio e, quindi, si è escluso che vi sia un provvedimento impugnabile – in ogni caso andrebbe ritenuto materiale ormai restituito alla parte con conseguente venire meno dell'interesse al ricorso».

Premesso che, una volta venuto meno l'interesse alla restituzione di quanto in sequestro per essere stato già restituito, non permane un diritto alla decisione sul riesame del sequestro perché tale impugnazione è mirata esclusivamente alla tutela del diritto sul bene (così Cass., Sezioni Unite, 7 maggio 2008, T.), la Suprema Corte di legittimità, solo astrattamente, nondimeno, come a breve avremo agio di osservare, valorizza il principio di diritto testé espresso chiosando come l'intervenuta restituzione dell'originale del *quid* non soddisfi, in sé e per sé, le coordinate di cui alla pronunzia T. nella misura in cui l'estrazione di copia del dato informatico (ed il suo trattenimento presso gli uffici della Procura) susciti una perdurante perdita del diritto su di una *res*, materiale od immateriale che sia, in capo al ricorrente.

In altri termini, «non si può ritenere che vi sia stata una effettiva restituzione quando la parte sia stata comunque privata del valore in sé del dato …» legittimamente adducendosi, allora, che «la disciplina delle "copie" di documenti *ex* art. 258 c.p.p. non comporta affatto che qualsiasi acquisizione di copia, con restituzione (o mancata apprensione), dell'originale, integri una situazione di "*non sequestro*" e, quindi, di inesistenza di un diritto al sindacato innanzi al Tribunale del Riesame per la restituzione della copia del documento, anche cartaceo» non fosse altro perché, «in tutti quei casi in cui il valore del documento deriva proprio dalla esclusione dell'accesso di altri…, non si può ritenere che il trattenimento di copia risolva il tema del diritto alla restituzione. Chi ha subito lo spossessamento ha ragione di contestare tale perdita della esclusiva disponibilità che rappresenta il valore in sé del documento». A compendio finale si può ordunque affermare che «la restituzione degli atti originali …, previa estrazione di copie, comporti 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 … La risposta data dal Tribunale (del Riesame: *n.d.a.*), di non esservi bene in sequestro per essere stata

disposta "*solo*" la estrazione di copia non è, quindi, corretta, non essendo stato considerato se il dato in sé sia stato "*sottratto*" alla disponibilità della parte» (questo, ed i precedenti, tratti "escerpiti" dalla sentenza R.).

Nell'evenienza di specie, ed al postutto – e con ciò diamo conto del correlato avverbiale "astrattamente" di cui *supra* –, né il Tribunale del Riesame né, soprattutto, il R. nel presentato ricorso individuano, con la dovuta puntualità, l'oggetto di acquisizione dal *computer* riferendosi, genericamente, alla «"*stampa di alcune email rinvenute sulla posta elettronica del giornalista*"» ed al fatto che «a tali messaggi erano allegati dei documenti, anch'essi acquisiti in copia» non facendosi riguardo veruno alle generalità del supposto informatore: di modo che R. dimostrando, con tale genericità, di non avere alcun interesse concreto all'ottenimento di materiale di sua spettanza non può che vedere dichiarato il rigetto del ricorso (altrimenti detto, egli non ha "argomentato" con sufficiente puntualità quella "perdita valutabile" che, a dire della "terza istanza", legittima la restituzione della copia).

Ad ogni buon conto, il principio "esaltato" nel 2015 è stato recentemente sottoscritto dalla Suprema Corte di legittimità (Cass., Sez. VI, 27 ottobre 2021, D.G.) in un intervento ad oggetto le ultime "luci della ribalta" ovverossia le cosiddette "copie forensi" (o, per equivalenti semantici, "copie conformi", "copie *bitstream*", "copie *bit* a *bit*", "immagini forensi") in un laconico *decisum* (il Considerato in Diritto "copre", all'incirca, una paginetta il che dovrebbe, allora, giustificare lo spazio, *prima facie* eccessivo, assegnato a quanto precede).

Con "**copia forense**" (d'ora in innanzi, per convenzione linguistica, ci avvarremo di tale locuzione o dell'omologo inglese "*bitstream image*") si fa riguardo al risultato dell'acquisizione di documenti in formato digitale mediante la procedura di duplicazione *bitstream image* idonea a garantire un "clone" identico all'originale ovvero ad una copia *bit* a *bit* (il termine *bit* indica l'unità di misura delle informazioni che costituiscono un sistema informatico) di tutto il contenuto di un supporto che "clona", e ciò rappresenta un significativo momento di "devianza" rispetto alla semplice copia di un *file* o di un *hard disk*, finanche le zone di spazio "libero" (ovvero anche quelle zone del disco che non contengono alcun *file* direttamente visibile all'utente: le cosiddette "aree non allocate").

Invero, quando rimuoviamo definitivamente un *file* salvato nel nostro *file system*, in realtà non facciamo altro che "etichettare" una porzione del dispositivo di memorizzazione – quella in cui risiede il *file* eliminato – come "spazio libero". Così motivandosi "comunichiamo" al sistema operativo che, se necessario, quella porzione di spazio può essere utilizzata per nuovi *files*, o per nuovi dati, e quindi sovrascritta con informazioni diverse. Pur tuttavia, dopo l'eliminazione, e ad ogni effetto, il dato rimosso rimane esattamente dove si collocava subito prima della sua cancellazione.

La copia forense, quindi, non replica in esclusiva i *files* memorizzati nello spazio delineato dagli investigatori come occupato, ma anche tutto il cosiddetto "spazio libero" giacché questo potrebbe o, a contraltare, non potrebbe contenere dati sensibili – ad esempio il contenuto della posta elettronica, della cronologia *Internet*, delle immagini, dei documenti – che possono essere recuperati grazie a *hardwares* ed a *softwares* dedicati od a *toolbox* – insieme di strumenti *softwares* per facilitare lo sviluppo di applicazioni derivate più complesse – "personalizzati" dagli stessi tecnici forensi o da ulteriori professionisti. In estrema sintesi, allora, poter avere accesso alle "aree non allocate" garantisce il recupero di *files* cancellati o di informazioni ormai non più disponibili all'utilizzatore del sistema.

La copia forense non si limita ai supporti di archiviazione dati quali *hard disk*, *CDROM*, *pendrive* ma si estende ai dati memorizzati su di un *cloud* – ovvero su di uno spazio di archiviazione *online* che permette di effettuare *backup* e di salvare dati senza necessità di un supporto materiale che, invero, può smarrirsi o rompersi. Attraverso la copia *bitstream* l'investigatore "congela" i dati nella loro forma originale per utilizzarli in Tribunale come documenti probatori.

La copia forense così ottenuta deve "manifestare" un impatto nullo sulla fonte originale di cui si ottiene il "duplicato" alla luce di quanto indicato dalla legge n. 48 del 2008, la quale prescrive che le attività di acquisizione forense dei dati devono venire svolte "*adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*" (cfr. artt. 8 e 9 l. cit.): perciò è necessario che l'operatore segua dettagliatamente e minuziosamente le procedure di acquisizione e di custodia dell'elemento probatorio per evitare di "inquinare" i supporti di interesse; la copia forense sarà conforme allorquando risulterà identica all'originale, il che deve essere garantito o per mezzo dell'impronta *hash* (algoritmo matematico che "mappa" i

dati in una stringa binaria di dimensione fissa), onde permettere di mostrare eventuali modifiche, o con l'utilizzo di un *write blocker* (strumento *hardware* che permette l'accesso ai dati digitali presenti su di un supporto di memorizzazione prevenendo scritture ed alterazioni dei dati) onde impedire, giustappunto, di "sovrascrivere" sul supporto di riferimento, nonché immodificabile (le eventuali modifiche apportate devono potersi identificare tramite il calcolo di funzioni matematiche quali l'*hash* sul dato originale e su quello acquisito); *last but not least*, e proprio per "mandare ad effetto" quest'ultimo obiettivo, si dovrà procedere a redigere apposito verbale in modo da poter "reggere" eventuali opposizioni su metodi, strumenti o tecniche utilizzate riportando dati relativi alla cosiddetta "catena di custodia (o di conservazione") dei reperti (con ciò intendendosi la documentazione cronologica, o la traccia cartacea, che mostra il sequestro, la custodia, il controllo, il trasferimento, l'analisi e la disposizione di elementi di prova, materiali od immateriali che siano) ed ai vari calcoli di valori *hash* che garantiscono l'integrità dei dati nei vari passaggi.

Rebus sic stantibus, stante la complessità del "fenomeno" e la pervasività di accesso al dato riservato affetto da siffatto "volano acquisitivo", bene ha fatto il giudice di legittimità, con la sentenza D.G., quantunque per tramite di un'argomentazione a dir poco succinta, a ribadire quanto summenzionato. Nella vicenda di interesse, difatti, il Tribunale del Riesame di Napoli aveva annullato il provvedimento di perquisizione e sequestro con cui il Procuratore della Repubblica presso il medesimo Tribunale aveva provveduto al sequestro di due telefoni cellulari nella disponibilità dell'interessata senza, nondimeno, trarre le dovute conseguenze evincibili dal prefato annullamento. Invero, a seguito della dichiarata illegittimità di quel provvedimento, si era provveduto sì a restituire le *res ablatae*, ovverossia i *devices* "fisici" di cui ad oggetto, ma nulla si era disposto in ordine alle estratte copie forensi delle memorie contenenti i dati registrati nonostante fosse il Tribunale medesimo a deplorare l'assenza di informazioni circa l'avvenuta esecuzione di quelle e circa l'individuazione dei criteri di selezione nell'analisi e nell'estrapolazione dei dati. «[I]l Tribunale avrebbe dovuto contestualmente pronunciarsi sulla relativa legittimità, non trincerandosi dietro una inesistente insindacabilità non prevista né dalla legge né desumibile dal sistema. Costituiscono, infatti, inevitabili corollari della affermata illegittimità totale di un provvedimento di sequestro afferente ad un dispositivo elettronico tanto l'illegittimità

del sequestro della massa (indistinta: *n.d.a.*) dei dati informatici ivi contenuti, in assenza di preventiva selezione o di indicazione dei relativi criteri, quanto la restituzione all'avente diritto di tutte le copie forensi illegittimamente eseguite ed eventualmente ancora a disposizione del Pubblico Ministero».

A morale conclusiva: non sarà sfuggito all'osservatore più attento come le pronunce *de quibus* non facciano cenno veruno sul versante dell'utilizzo di quei dati, come "appresi", nel "recinto" processuale. Certo: soccorreranno le disposizioni rintracciabili, in ordine sparso, nel codice di procedura penale in tema di prove acquisite in violazione dei divieti stabiliti dalla legge. Pur tuttavia, proprio l'incessante – "ingovernato" come da titolo del presente contributo – avvicendarsi di *new technology*, la cui regolazione è vieppiù affidata allo *jus praetorium*, dovrebbe allertare sull'improcrastinabilità di una riforma organica del codice di procedura penale. "Mettere seriamente le mani" sull'articolato del 1988 si rivela, a nostro modo di vedere, ormai indifferibile: necessita un *corpus 2.0* che realizzi un vero e proprio "giusto processo telematico" contestualizzando i valori fondanti di cui all'art. 111 Cost. alla realtà dell'oggi, tanto più considerando che la "tradizionale" prova dichiarativa ('storico-narrativa' nell'insegnamento Corderiano) mostra palesi tratti di sofferenza nel contesto del *brave new world* processuale.

Le occasioni non mancano … e più di una è venuta meno ad ipotetici disegni riformistici. Giusta quest'ultimo profilo la più sensibile Accademia, non molto tempo addietro, si doleva dell'impostazione "miope" che aveva guidato il riformatore nel "plasmare" i contenuti della normativa in tema di intercettazioni di flussi comunicativi mancando, in quel frangente, il coraggio per modulare *ab imis* un processo "tecnologico". Oggi, a "tenere banco", è la cosiddetta riforma Cartabia – dalle generalità della facente funzioni di Ministro della Giustizia (l. 27 settembre 2021, n. 134, recante "*Delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*"): il provvedimento, caratterizzato da due soli articoli, al primo delega il Governo alla modifica "*del codice di procedura penale, delle norme di attuazione del codice di procedura penale, del codice penale e della collegata legislazione speciale nonché delle disposizioni dell'ordinamento giudiziario in materia di progetti organizzativi delle Procure della Repubblica, per la revisione del regime sanzionatorio*

dei reati e per l'introduzione di una disciplina organica della giustizia riparativa e di una disciplina organica dell'ufficio per il processo penale" stante 28 commi ispirati al conseguimento dell'efficienza del rito penale. Il riscontrato *focus* potrebbe invero fare "bene sperare": nondimeno le disposizioni di cui all'articolo 2, di immediata precettività, non paiono incoraggiare. Si mediti, solo per fare un esempio, su di uno degli "snodi centrali" della riforma ovvero sulla "*Improcedibilità per superamento dei termini di durata massima del giudizio di impugnazione*", come disciplinata dal, di nuovo conio, art. 344 *bis* c.p.p.: ispirato da un "afflato" di velocizzazione economicistica del rito, e non certo da ideali di razionalizzazione, ragionata (anche, se non soprattutto, giusta i tempi processuali) di sistema, l'avverbio numerale di cui a quell'articolo non pare garantire quegli obiettivi il cui intendimento, *supra*, si è voluto perseguire.

Comunque sia si è solo agli esordi del percorso di delegazione (che si concluderà, verosimilmente, entro un anno dall'entrata in vigore della l. n. 134 del 2021 – fatti salvi ulteriori due anni a far termine dalla data di entrata in vigore dell'ultimo decreto legislativo adottato per eventuali integrazioni e/o correzioni): non resta che attendere, *more solito*, nell'auspicio che, una volta tanto, la speranza non sia vana.