Cass., pen., sez. VI, 21/05/2024, n.31180, in *Cass. Pen., 2024, 11, 3417*

RIFLESSIONI A MARGINE DELLA SENTENZA CORTE CASS., SEZ. VI, 21 MAGGIO 2024, N. 31180, IN ORDINE ALLE MODALITA' DI ACQUISIZIONE, AI FINI PROBATORI, NELLA FASE DELLE INDAGINI PRELIMINARI, DELLE CONVERSAZIONI CONTENUTE SU UN DISPOSITIVO DI TELEFONIA MOBILE IN USO ALL'INDAGATO.

Enrico Ranieri *[1]

SOMMARIO: 1.- Le (interessanti ed attuali) questioni affrontate dalla sentenza Cass., sez. VI, 21 maggio 2024, n.31180. 2.- La genesi della vicenda e la (grave) ipoteca sulla legittimità dell'operato degli organi inquirenti. 3.- Sulla legittimità della attività del magistrato del pubblico ministero che abbia ignorato i *dicta* del Tribunale del riesame. 4. - L*'overruling* in ordine alla qualificazione giuridica della messagistica *washapss*. 5. - Natura della nullità riconosciuta dalla Corte e conseguenze. 6. – Osservazioni conclusive.

1.- Le (interessanti ed attuali) questioni affrontate dalla sentenza Cass., sez. VI, 21 maggio 2024, n.31180.

La sentenza in commento[2], affrontando e risolvendo diverse questioni, seppur connesse e conseguenziali, appare particolarmente interessante per diverse ragioni.

Essa, invero, offre importanti spunti di riflessione su varie tematiche, attuali e di non poco rilievo.

In primo luogo, induce a soffermarsi sul tema delle modalità e dei limiti che connotano il potere della polizia giudiziaria quando, nel corso di una indagine – agendo di propria iniziativa o su delega del magistrato del pubblico ministero - intenda acquisire il contenuto di conversazioni contenute in un applicativo presente su un telefono cellulare in uso ad una persona sottoposta alle indagini.

Vi è, poi, l'ulteriore questione, strettamente connessa alla prima, relativa alla legittimità del provvedimento del magistrato del pubblico ministero che - ad onta di una ordinanza di annullamento, da parte del Tribunale del riesame, di un precedente provvedimento di sequestro probatorio del dispositivo e della relativa copia forense – disponga una ispezione informatica, al fine di acquisire, comunque, contestualmente all'esecuzione dell'ordine di restituzione di quanto sequestrato, i dati contenuti proprio nel dispositivo precedentemente sequestrato.

Ancora, la decisione in commento si lascia apprezzare per aver precisato la natura che, ai fini della corretta individuazione della disciplina codicistica da applicare, debba essere riconosciuta al contenuto della messagistica rinvenuta su un dispositivo elettronico e, infine, per essersi espressa sulla tipologia e sul grado della invalidità conseguente alla violazione dei principi di diritto (ri)affermati in sentenza.

Andiamo per ordine.

[1]*Ricercatore di Procedura Penale e professore aggregato di Diritto dell'esecuzione penale presso Università degli Studi di Salerno.

[2] Cass., sez. VI, 21 maggio 2024, n. 31180, in *Cass, pen.*, 2024, 11, 3417.

2.- La genesi della vicenda e la (grave) ipoteca sulla legittimità dell'operato degli organi inquirenti.

La complessa vicenda cautelare (prima reale e, poi, personale), che ha trovato approdo nella emissione della sentenza in commento, da parte della Corte di cassazione, prende il via dalla emissione, da parte del Tribunale del riesame, di una ordinanza con la quale veniva annullato, per difetto di motivazione, un decreto di sequestro probatorio, emesso dal magistrato del pubblico ministero, di telefoni cellulari in uso agli indagati, al fine di procedere alla estrazione – mediante copia forense – dei dati (in particolare messaggistica) in essi conservati.

L'annullamento si giustificava in ragione della natura generica (*id est*: meramente apparente) della motivazione, ovvero della finalità meramente esplorativa del ricorso al mezzo di ricerca della prova e del conseguente sequestro di tutti i dati contenuti sui dispositivi mobili.

Al riguardo, merita di essere ricordato che, nelle ipotesi di provvedimenti di perquisizione e sequestro, previsti dagli artt. 250 e 252 c.p.p., le cose da ricercare e da sottoporre, eventualmente, a sequestro, devono connotarsi come "corpo del reato" o "cose pertinenti al reato", con la conseguenza che la motivazione dei provvedimenti che dispongono le perquisizioni ed i sequestri, ai sensi dell'art. 247 c.p.p., deve non solo contenere l'indicazione, sia pure sommaria ed approssimativa, delle fattispecie criminose per le quali si procede (non potendosi, il magistrato del pubblico ministero, limitare alla mera enunciazione degli articoli di legge asseritamente violati) ma, altresì, la indicazione delle ragioni per le quali, rispetto a quelle fattispecie, provvisoriamente contestate e sommariamente descritte, le cose da ricercare e, eventualmente, da sequestrare, assumano rilevanza quale "corpo di reato" o di "cosa pertinente al reato"[3].

Sicchè, ove mai dal testo della motivazione del decreto non emerga la necessaria delimitazione dell'oggetto del sequestro, idonea a consentire la verifica, sia in ordine al rapporto di pertinenzialità tra quanto sequestrato e la fattispecie di reato (provvisoriamente) contestata all'indagato, sia in ordine alle relative finalità probatorie perseguite, il provvedimento ablativo finirebbe per assumere, semplicemente, una non consentita finalità "esplorativa" ed "onnivora", in palese violazione del criterio di proporzionalità tra contenuto del provvedimento ed esigenze di accertamento dei fatti per i quali si procede.

Costituisce, ormai, *ius receptum*, il principio per il quale, anche in materia di misure cautelari reali, debbano essere rispettati i principi di adeguatezza e proporzionalità, al fine di arginare il rischio di interventi indebitamente invasivi, destinati a limitare anche la garanzia convenzionale, desumibile dall'art. 10 CEDU[4], atteso che «in tema di sequestro di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede»[5].

Chiarita, per quanto detto, la natura illegittima di un provvedimento di sequestro probatorio del magistrato del pubblico ministero, comportante un'ablazione onnivora, del tutto sproporzionata e scollegata da una reale finalità probatoria - oltretutto, priva di qualsivoglia delimitazione temporale e circostanziale - occorre verificare se - e con quali limiti - gli organi inquirenti possano, di nuovo,

[3] Cfr., sul tema, Cass., sez. VI, 20 maggio 1998, in *Cass. pen.*, 1999, 575.

[4] In tale prospettiva, così come è vietata l'acquisizione di un intero archivio di documentazione cartacea di un'azienda (Cass., Sez. VI, 26 settembre 2019, n. 43556, in *Diritto & Giustizia* 2019, 25 ottobre), altrettanto deve dirsi per la indiscriminata acquisizione, in difetto di specifiche ragioni, di un dispositivo quale un *personal computer*, del tutto equiparabile ad uno *smartphone*, contenente una massa indistinta di dati informatici (Cass., sez. VI, 19 gennaio 2018, n. 9989, in *Guida al diritto*, 2018, 16, 75; Id., sez. VI, 24 febbraio 2015, n. 24617, in *Cass. pen., 2016, 1, 286*).

[5] Cass., sez. VI, 22 settembre 2020, *Rv.279949*; Id., sez. VI, 4 marzo 2020, n. 13165, in *Diritto & Giustizia 2020, 29 aprile.*

legittimamente acquisire, agli atti del procedimento, proprio quei dati di cui era stata disposta la restituzione all'avente diritto.
Anche in relazione a tale interessante tema, la vicenda – che ha portato alla emanazione della sentenza in commento - offre utili spunti di riflessione, dal momento che la polizia giudiziaria, in occasione della restituzione all'indagato – in esecuzione dell'ordinanza di annullamento del Tribunale del riesame - della copia forense del contenuto del cellulare, dava esecuzione ad un decreto di ispezione informatica, emesso, nelle more, dal magistrato del pubblico ministero e, all'esito delle operazioni, sottoponeva, di iniziativa, a sequestro probatorio – poi convalidato dall'Organo inquirente - una serie di conversazioni, rinvenute sull'applicazione *washapss*, ritenute di interesse investigativo.
Tanto premesso, gli snodi procedimentali della vicenda inducono, innanzitutto, a porsi qualche interrogativo in ordine alla individuazione dei corretti addentellati normativi, idonei a legittimare l'attività degli organi inquirenti.
Risulta, in particolare, interessante chiarire come possa essere qualificata, alla luce dell'ordito normativo codicistico, l'attività della polizia giudiziaria, la quale, dopo aver ispezionato, per attività delegata, la copia forense da restituire all'indagato, abbia poi proceduto alla preventiva estrapolazione e al successivo sequestro di conversazioni ivi rinvenute.
Sembra fuori discussione che, ove mai la polizia giudiziaria avesse agito ai sensi e nei limiti di cui all'art. 352 c.p.p., la perquisizione e, si badi, il conseguente sequestro - non trattandosi di corpo del reato, ma al limite di una "traccia" o "cosa pertinente" ad una ipotesi di reato che, peraltro, aveva trovato la sua genesi proprio negli esiti della precedente, illegittimità, attività investigativa - sarebbero da considerarsi posti in essere in violazione di legge, difettando il fondamentale requisito minimo di legalità, costituito, espressamente, dalla "flagranza del reato", unica condizione, in forza della quale è consentita all'organo di polizia, l'adozione di atti che, diversamente, sarebbero riservati alla Autorità giudiziaria.
Né sembra che l'iniziativa della polizia giudiziaria si possa giustificare in forza del disposto dell'art. 354 c.p.p., atteso che ci si troverebbe, comunque, al cospetto di una attività palesemente illegittima, per evidente difetto dei presupposti, atteso che, solo in via del tutto eccezionale e residuale, il Legislatore del 1988 ha inteso consentire alla polizia giudiziaria il compimento di attività (*id est*: atto omologo alla ispezione) che - per la capacità di limitare, in modo ancor più incisivo della perquisizione, diritti di indubbio rilievo costituzionale (dignità, riservatezza, pudore ..ecc) – di regola sono riservate alla Autorità giudiziaria, attraverso il precipuo mezzo di ricerca della prova denominato ispezione.
Ed infatti, e non a caso, l'art. 354, comma 2 c.p.p. subordina la legittimità dell'accertamento ispettivo, di iniziativa, della polizia giudiziaria alle tassative condizioni (peraltro richieste in modalità cumulativa e non alternativa) che vi sia «pericolo che le cose, le tracce e i luoghi (…) si alterino o si disperdano o comunque si modifichino» e che «il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini».
Ne discende che l'esame della copia dell'apparato telefonico cellulare in uso all'indagato non possa essere qualificato come perquisizione *ex* art. 352 c.p.p. - dato che la polizia giudiziaria non ha agito nella flagranza del reato o nel caso di evasione o negli altri casi di cui all'art. 352, comma 2 c.p.p. - né come ispezione di cose - posto che la copia di un telefono cellulare non è qualificabile come traccia o altro effetto materiale del reato, come previsto dall'art. 244, comma 1 c.p.p. - né come attività urgente e "innominata" di polizia giudiziaria di cui all'art. 348 c.p.p., finalizzata all'assicurazione delle fonti di prova mediante la raccolta di ogni elemento utile alla ricostruzione del fatto e all'individuazione del colpevole e, neppure, come accertamento urgente sulle cose di cui all'art. 354, comma 2 c.p.p., dal momento che, allorquando la polizia giudiziaria ha esaminato le conversazioni presenti sul telefono cellulare in uso all'indagato, il magistrato del pubblico ministero

aveva già assunto la direzione delle indagini (tanto che lo stesso aveva emesso il decreto di ispezione informatica).
Il tutto, senza sottovalutare che, in ogni caso, ci si trova al cospetto di un'apprensione di "documenti informatici", la cui definizione è contenuta nel d. lgs. 7 marzo 2005, n. 82, art. 1, lett. p), secondo cui è «documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».
Ebbene, secondo il rapporto esplicativo adottato dal Comitato dei ministri del Consiglio d'Europa della Convenzione sulla criminalità informatica di Budapest il 23 novembre 2001, ratificata dalla l. n. 48 del 2008 (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», includendo, nella accezione, l'uso o il sequestro di programmi necessari ad accedere ai dati che si stanno ablando.
In altri termini, l'interesse tutelato è riferibile al "contenuto" (conversazioni *whatsapp*) e non al "contenitore", non dovendosi dimenticare che, in ogni caso, l'integrale ed indiscriminata apprensione della totalità del patrimonio informatico contenuto all'interno di un *device*, è stata ripetutamente censurata dalla giurisprudenza, che non ha evitato di sottolineare che «così come è vietata l'acquisizione di un intero archivio di documentazione di un'azienda»[6], altrettanto è a dirsi per «l'indiscriminata acquisizione di un dispositivo quale un *personal computer* ovvero uno *smartphone*»[7], senza mancare, ancora, di specificare che «è illegittima la misura applicata su una massa indistinta di dati informatici senza selezione e senza indicazione dei criteri di estrazione dal dispositivo sequestrato», e che «è illegittimo, per violazione del principio di proporzionalità e adeguatezza, il sequestro a fini probatori di un dispositivo elettronico che conduca, in difetto di specifiche ragioni, alla indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione degli eventuali criteri di selezione»[8]

3. - Sulla legittimità della attività del magistrato del pubblico ministero che abbia ignorato i *dicta* del Tribunale del riesame.

In ogni caso, la legittimità del sequestro di iniziativa della polizia giudiziaria, sul versante della successiva verifica, resterebbe, come è noto, "garantita" e "coperta" dall'intervento di un provvedimento di convalida da parte dello stesso magistrato del pubblico ministero.[9]
Sicchè, il *Kern* della questione è stabilire se, pur in presenza di una ordinanza di annullamento, da parte del Tribunale del riesame, di un provvedimento di sequestro probatorio, il magistrato del pubblico ministero mantenga il potere di estrarre copia del materiale oggetto del sequestro annullato e – in virtù del sequestro d'iniziativa (convalidato) della polizia giudiziaria - di utilizzarlo probatoriamente.
È agevolmente immaginabile che, in caso di risposta positiva al quesito innanzi posto, la pronuncia di annullamento del sequestro da parte del Tribunale del riesame costituirebbe una sanzione *inutiliter data* ed il magistrato del pubblico ministero potrebbe comunque fare ricorso ad un facile espediente elusivo per aggirare le garanzie di rito, rendendole in concreto inoperanti, con pregiudizio per gli interessati.
La Corte di cassazione, con la sentenza in commento, ha chiarito che l'Autorità inquirente, dopo una ordinanza del Tribunale del riesame, di annullamento del decreto di sequestro probatorio del cellulare,

[6] Cass., sez. VI, 26 settembre 2019, Scarsini, in *Mass. Uff.*, n. 277211.
[7] Cass., sez. VI, 19 gennaio 2018, Lillo, in *Mass. Uff.*, n. 272536; Id., sez. VI, 24 febbraio 2015, Rizzo, *ivi*, n. 264092.
[8] Cass., sez. VI, 28 settembre 2021, Di Gennaro, non mass.
[9] Cfr., sul tema, Cass., sez. VI, 12 dicembre 2012, n. 49884, in *CED Cass. 2012*, nonché Corte cost., 3 ottobre 2019, n. 219, in *Giur. Cost.*, 2019, 5, 2581.

non può riacquisire i dati in esso rinvenuti, mediante decreto di ispezione informatica e conseguente sequestro da parte della polizia giudiziaria.
La Corte, infatti, scrive che «la patologia deriva proprio dalla violazione del provvedimento giurisdizionale cui è conseguita una illegittima violazione della sfera di riservatezza al di fuori dei presupposti declinati dall'art. 15 Cost. Tale disposizione stabilisce infatti che la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili e che la loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge. Nel momento in cui la competente Autorità giudiziaria - ossia il Tribunale del riesame - ha accertato l'assenza di idonea motivazione a fondamento del sequestro probatorio operato dal magistrato del pubblico ministero, disponendone l'annullamento e ordinando la restituzione dei beni appresi agli aventi diritto, è evidente che l'ulteriore compressione della sfera costituzionalmente tutelata, attuata tramite la ispezione informatica, si pone fuori dal rispetto del perimetro delle garanzie derivanti dall'art. 15 Cost.» [10]
Le argomentazioni della Suprema Corte non possono che meritare ampia condivisione.
Ed invero, tenuto conto che, nel corso delle indagini preliminari, all'esito della pronuncia con cui il Tribunale del riesame aveva dichiarato la nullità del decreto di sequestro dei dispositivi mobili in uso agli indagati, il magistrato del pubblico ministero, prima di procedere alla immediata restituzione della copia forense - atto dovuto - aveva disposto di trattenere i beni e procedere *sua sponte* alla relativa ispezione, non ci si può non preliminarmente soffermare sugli ormai consolidati principi giurisprudenziali che ammettono la riproposizione di un provvedimento ablativo sulla medesima *res* – essendo tali decreti caratterizzati ciascuno da una propria autonomia e indipendenza – purché ci sia adeguata ed esaustiva motivazione in ordine ai presupposti legittimanti e alle cadenze temporali. Nondimeno, va rimarcato che la *ratio* sottostante il citato orientamento risiede nel fatto che l'indagato – la cui sfera soggettiva viene violata per finalità procedimentali – ha sempre la possibilità di sindacare la legittimità del provvedimento ablativo in virtù dell'art. 257 c.p.p.; medesima facoltà, tuttavia, non è riconosciuta al soggetto destinatario di attività ispettiva, non essendo tale atto sindacabile in sede di riesame, dal momento che l'attività ispettiva non comporta il sequestro della *res*.
Del resto, non può sfuggire il differente oggetto su cui vertono i due diversi mezzi di ricerca della prova (ispezione e sequestro): il sequestro probatorio è finalizzato all'apprensione del corpo del reato o delle cose pertinenti al reato, vale a dire delle cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne rappresentano il prodotto, il prezzo o il profitto; al contrario, nel caso di attività ispettiva, a norma degli artt. 244 e ss. c.p.p., il mezzo in questione è destinato all'apprensione di tracce ovvero effetti materiali del reato, con la conseguenza che tale istituto, più che essere deputato all'acquisizione di fonti probatorie di rilievo, è invece preordinato al recepimento di materiale indiziante sul quale poi orientare la successiva attività investigativa.
Per la verità e l'ortodossia del diritto processuale penale, ogni qualvolta l'attività di ispezione informatica non si limiti ad una mera attività descrittiva del sistema informatico, ma viene compendiata nella rappresentazione fotografica (tramite *screenshot*) delle conversazioni *whatsapp* visionate e selezionate sulla copia forense, si concretizza – tradendo i limiti della ispezione – in una vera e propria perquisizione informatica, *ex* art 247, comma 1-*bis* c.p.p., tenuto conto della ontologica attività dinamica di "ricerca" nel "domicilio informatico" dell'indagato.

[10] Da ciò discende, sempre secondo la Corte, la inutilizzabilità delle *chat* che non possono essere quindi valutate neppure in sede cautelare. Al riguardo, cfr. Cass, Sez. un., 21 giugno 2020, n. 16, Tammaro, *Rv. 216246-01*; Id., sez. IV, 18 maggio 2005, n. 31304 , *Rv. 231739 - 01*; Id., sez. III, 27 settembre 2023, n. 44926, Bianchini, *Rv. 285316-02*.

Per vero, l'art. 244, comma 2 c.p.p. contempla la possibilità, per l'Autorità giudiziaria, di disporre l'ispezione «anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e la loro inalterabilità».

Nondimeno, l'ispezione informatica deve essere limitata all'osservazione del "sistema informatico", descrivendolo nei suoi particolari – al fine, per esempio, di rilevare la presenza di eventuali collegamenti a periferiche, di tracciare tutti gli accessi alla rete, di attestare la presenza di *software* in funzione, di accertare la presenza di programmi di messagistica, ecc…. – evitando qualsiasi possibilità di alterazione e, dunque, qualsiasi interferenza con la disciplina di cui all'art. 360 c.p.p.

L'assunto, del resto, trova ampia conferma nella disposizione di cui al comma 1-*bis* dell'art. 247 c.p.p., secondo cui «quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione», nonché nella disposizione di cui all'art. 352 c.p.p. la quale, al comma 1-*bis*, prevede che «nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previste, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione, procedono alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, se hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

Diversamente opinando, gli esiti del mezzo di cui all'art. 244 c.p.p. sostituirebbero, nei fatti, quelli di un sequestro probatorio e, conseguenzialmente l'organo inquirente, vanificando *i dicta* di un organo giurisdizionale (nel caso di specie, del Tribunale del riesame), non vedrebbe "dispersi" gli esiti investigativi illegittimamente acquisiti: in sintesi, ci troveremmo al cospetto di una illegittima eterogenesi dei fini e degli effetti dell'attività ispettiva.

Del resto, ad ulteriore riprova del precedente assunto, sarebbe sufficiente richiamare la circostanza che lo stesso Legislatore, nel delineare il discrimine tra i due mezzi di ricerca della prova, abbia individuato quale oggetto dell'attività ispettiva il solo "sistema informatico o telematico" nella sua interezza, a differenza di quanto invece stabilito per la perquisizione informatica, in forza della quale oggetto di ablazione possono essere i "dati, informazioni o programmi" contenuti nello stesso, ragion per cui l'opinare diversamente comporterebbe la confusione/sovrapposizione dei due istituti, con la conseguente perdita delle rispettive specificità.

In altri termini, l'ispezione consente una conoscenza indiretta – tramite l'efficacia rappresentativa dell'annotazione o del verbale redatti dalla polizia giudiziaria – dell'informazione acquisita mediante l'osservazione, operando quale strumento di convincimento del giudice, laddove, viceversa, l'attività di perquisizione deve essere compiuta seguendo le migliori tecniche di ricerca informatiche, tenendo conto, altresì, della finalizzazione dell'attività al successivo sequestro probatorio, mettendo in campo competenze in termini di apprensione e conservazione del dato informatico.

Quanto evidenziato costituisce, sicuramente, la ragione per la quale, ad avviso della Corte, nella vicenda *de qua*, l'attività ispettiva si sia tradotta in un mero aggiramento sia del provvedimento di annullamento del Tribunale del riesame che della specifica disciplina della perquisizione informatica e delle sottese garanzie difensive.

Ma vi è di più.

4.- L*'overruling* in ordine alla qualificazione giuridica della messagistica *washapss*.

La Corte, nella sentenza in commento, si è anche diffusamente soffermata su un altro tema, di particolare interesse, già affrontato, di recente, sia dalla Consulta che dalla Corte di Cassazione a Sezioni unite.

La sentenza ha, infatti, ribadito che, alla luce della sentenza della Corte costituzionale n. 170 del 2023[11] e di quanto deciso dalle Sezioni unite della stessa Corte[12], le *chat* costituiscono non "mera documentazione", acquisibile *ex* art. 234 c.p.p., ma "corrispondenza informatica" che, quindi, può essere acquisita solo in forza di un provvedimento di sequestro *ex* art. 254 c.p.p. Così come ha ulteriormente specificato che, di certo, il principio affermato dalla Corte costituzionale, di portata generale, non trova applicazione esclusivamente all'ambito applicativo delle guarentigie apprestate dall'art. 68 Cost. in favore del parlamentare.

A sostegno, la Consulta – nella sentenza n. 170 del 2023 - ha stabilito che lo scambio di messaggi elettronici, *e-mail, sms, whatsapp* e simili - costituisce, di per sé, una forma di corrispondenza agli effetti degli artt. 15 e 68, comma 3 Cost., atteso che quello di "corrispondenza" è concetto ampiamente comprensivo, atto ad inglobare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, realizzata in modo diverso dalla conversazione in presenza. Ne consegue, secondo la Consulta, che la tutela accordata dall'art. 15 Cost. - che assicura a tutti i consociati la libertà e la segretezza «della corrispondenza e di ogni altra forma di comunicazione», consentendone la limitazione «soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» - prescinde dalle caratteristiche del mezzo tecnico utilizzato ai fini della trasmissione del pensiero, «aprendo così il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata»[13]

Non può non conseguirne che la garanzia si estende, necessariamente, ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento del varo della Carta costituzionale[14].

Ha precisato, ancora, la Consulta che la posta elettronica, i messaggi inviati tramite l'applicazione *whatsapp* (appartenente ai sistemi di cosiddetta messaggistica istantanea) rientrano, dunque, a pieno titolo, nella sfera di protezione dell'art. 15 Cost., apparendo del tutto assimilabili a lettere o biglietti chiusi. La riservatezza della comunicazione, che, nella tradizionale corrispondenza epistolare, è garantita dall'inserimento del plico cartaceo o del biglietto in una busta chiusa, in ipotesi di posta elettronica o di altra modalità di corrispondenza telematica, è garantita dal fatto che la posta elettronica viene inviata a una specifica casella di posta, accessibile solo al destinatario tramite procedure che prevedono l'utilizzo di codici personali. Difatti, un messaggio *whatsapp*, spedito tramite tecniche che assicurano la riservatezza, è accessibile solo al soggetto che abbia la disponibilità del dispositivo elettronico di destinazione, normalmente protetto anch'esso da codici di accesso o altri meccanismi di identificazione. Argomentazioni chiare, in base alle quali si deve concludere che, in linea generale, la messaggistica a mezzo *chat* costituisce "corrispondenza" rientrando dunque nella disciplina costituzionale dell'art. 15 Cost.

Le argomentazioni della Corte di cassazione, in ordine alla portata generale dei *dicta* della Consulta, non possono che meritare ampia condivisione.

Per vero, la Corte costituzionale, nella sentenza n. 170 del 2023, ha nitidamente affermato che «degradare la comunicazione a mero documento quando non più in itinere, è soluzione che, se confina in ambiti angusti la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, sempre più ridotti, di corrispondenza cartacea, finisce addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente – o, comunque sia, senza uno iato temporale apprezzabile – la ricezione».

[11] Cfr. Corte cost., 27 luglio 2023, n.170, in *Giur. cost.*, 2024, 5, 2154.

[12] Cfr., al riguardo, Cass., Sez un., 29 febbraio 2024, n.23755, in *Cass, pen.*, 2024, 9, 2553 e Id., 29 febbraio 2024, n. 23756, in *Cass. pen.*,2024, 9, 2575.

[13] Cfr. Corte cost., 12 gennaio 2023, n. 2, in *Foro it.*, 2023, 2, I, 321.

[14] Cfr. Corte cost, 24 gennaio 2017, n.20, in *Giur. cost*, 2017, 2, 917.

In sintesi, anche le comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea devono essere considerate, a pieno titolo, "corrispondenza" in forza dell'*overruling* (rispetto a precedenti prese di posizione da parte del Giudice di legittimità), determinatosi per effetto delle recenti pronunce della Corte costituzionale[15], della Corte di giustizia[16] e prima ancora della Corte EDU[17], che avevano ricondotto entro la disciplina delle intercettazioni telefoniche e dell'inviolabilità della corrispondenza anche l'acquisizione delle *chat* e, in genere, delle conversazioni telematiche.
L'utilizzo delle *chat* acquisite illegittimamente nel procedimento penale si porrebbe, in caso contrario, come una violazione dei principi costituzionali e della normativa sovranazionale (art. 13, § 1, della direttiva 95/46/CE) che consente deroghe e limiti alla riservatezza delle comunicazioni (art. 5 della direttiva 95/46/CE) solo qualora la restrizione integri una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica.
La naturale, necessaria, conseguenza è che, per procedere al sequestro della messaggistica *whatsapp* o del contenuto di altre forma di comunicazione telematica, è necessario procedere ai sensi dell'art. 254 c.p.p. e non ai sensi dell'art. 234 stesso codice.

5. - Natura della nullità riconosciuta dalla Corte e conseguenze.
Resta, a questo punto, da valutare quale sia la natura della invalidità che investe gli esiti della attività di ablazione del contenuto della messaggistica *whatsapp* o del contenuto di altre forma di comunicazione telematica, avvenuta in violazione dei principi e delle regole in epigrafe richiamati.
Sulla scorta dei richiamati principi, la Corte, con la sentenza in commento, ha ritenuto che gli elementi indiziari derivanti dalla (illegittima) ispezione informatica siano affetti da inutilizzabilità "patologica"; di qui, la loro inutilizzabilità anche nella fase delle indagini preliminari e, vieppiù, a fini cautelari[18].
Costituisce, difatti, ormai, *ius receptum* – secondo il Giudice di legittimità - il principio per il quale rientrano nella categoria delle prove sanzionate dall'inutilizzabilità "patologica", non solo le prove oggettivamente vietate, ma anche quelle formate o acquisite in violazione dei diritti soggettivi tutelati dalla legge e, a maggior ragione, quelle acquisite in violazione dei diritti costituzionalmente garantiti.
Per corroborare l'assunto, la Corte richiama, altresì, i *dicta* della Consulta, cristallizzati nella sentenza n. 34 del 1973[19], che ha ravvisato l'esistenza di divieti probatori ricavabili in modo diretto dal dettato costituzionale, enunciando il principio per cui le «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito».
Si tratta, in sintesi, di un esplicito richiamo – ove mai ve ne fosse stato bisogno - alla categoria delle prove cosiddette "incostituzionali", cioè di quelle prove ottenute attraverso modalità, metodi e comportamenti realizzati in violazione dei fondamentali diritti del cittadino garantiti dalla Costituzione, da considerarsi perciò inutilizzabili nel processo penale[20].

[15] Cfr. Corte cost., 27 luglio 2023, n.170, *cit.*

[16] Il riferimento è alla decisione del 7 settembre 2023 in causa C-162/22, A.S. vs. Lituania.

[17] Il riferimento è alla decisione del 9 marzo 2021, in causa Eminağaoğlu vs. Turchia.

[18] Cfr. Cass, Sez. un., 21 giugno 2020, n. 16, Tammaro, cit.; Id., sez. IV, 18 maggio 2005, Bossi, *Rv. 231739 - 01*; Id. sez. III, 27 settembre 2023, n. 44926, Bianchini, *Rv. 285316-02*.

[19] Cfr. Corte cost. 6 aprile 1973, n. 34, in *www.cortecostituzionale.it.*

[20] Cfr. Cass., sez VI, 11 gennaio 2023, n. 15836, Berera, *Rv. 284590 - 01*, che ha affermato il principio secondo cui in tema di acquisizione di dati contenuti in tabulati telefonici, non sono utilizzabili nel giudizio abbreviato i dati di geolocalizzazione relativi a utenze telefoniche o telematiche, contenuti nei tabulati acquisiti dalla polizia giudiziaria in assenza del decreto di autorizzazione dell'Autorità giudiziaria, in violazione dell'art. 132, comma 3 d. lgs. 30 giugno

In effetti, nel caso di specie, la patologia della accertata invalidità conseguiva alla violazione del provvedimento giurisdizionale (*id est*: ordinanza di annullamento del Tribunale del riesame) cui era conseguita una illegittima violazione della sfera di riservatezza, al di fuori dei presupposti declinati dall'art. 15 Cost. Tale ultima sovraordinata disposizione, infatti, stabilisce che la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili e che la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge. Ne deriva che, avendo il Tribunale del riesame accertato l'assenza di idonea motivazione a fondamento del sequestro probatorio operato dal magistrato del pubblico ministero, disponendone l'annullamento e ordinando la restituzione dei beni appresi agli aventi diritto, l'ulteriore compressione della sfera costituzionalmente tutelata, attuata tramite la ispezione informatica, si era posta al di fuori del rispetto del perimetro delle garanzie derivanti dall'art. 15 Cost.

L'assunto della Corte è, ancora una volta, ampiamente condivisibile.

Si è, difatti, certamente, in presenza di una attività investigativa affetta da inutilizzabilità c.d. "patologica", essendosi sostanziata in un'acquisizione di elementi di prova *contra legem*, il cui impiego, per granitica giurisprudenza, è vietato in modo assoluto non solo nel dibattimento ma in qualsiasi altra fase del procedimento, ivi compresa quella delle indagini preliminari, dell'udienza preliminare, delle procedure incidentali cautelari e quelle negoziali di merito.

Il principio, per vero, è stato già ripetutamente affermato dal massimo consesso giurisdizionale: in tema di tabulati telefonici[21]; sulle conseguenze della mancata allegazione al giudice per le indagini preliminari o al Tribunale del riesame dei decreti autorizzativi di intercettazioni telefoniche, ai fini della sussistenza dei gravi indizi di colpevolezza[22]; sulla perquisizione invalida e sul conseguente sequestro di corpo del reato o di cose pertinenti al reato[23].

Invero, le Sezioni unite della Suprema corte hanno ripetutamente sottolineato, nella citate decisioni, come nel fenomeno della inutilizzabilità patologica rientrino tanto le prove oggettivamente vietate quanto le prove comunque formate o acquisite in violazione - o con modalità lesive - dei diritti fondamentali della persona, tutelati dalla Costituzione e, perciò, assoluti e irrinunciabili, a prescindere dall'esistenza di un espresso o tacito divieto al loro impiego nel procedimento contenuto nella legge processuale.

Solo per completezza argomentativa, deve essere anche sottolineato che, neppure potrebbe dirsi che, pur ammettendosi la illegittimità della ispezione informatica, l'acquisizione dei dati non sarebbe censurabile, sulla base del principio del "*male captum, bene retentum*".

Ed invero, secondo tale principio[24], oramai consolidato, l'eventuale illegittimità dell'atto di perquisizione compiuto ad opera della polizia giudiziaria non comporterebbe effetti invalidanti sul successivo sequestro del corpo del reato o delle cose pertinenti al reato, che costituisce un atto dovuto a norma dell'art. 253, comma 1 c.p.p.[25]

Nondimeno, a ben vedere, nel caso di specie, è la stessa acquisizione dei dati a risultare illegittima, in quanto effettuata in violazione del provvedimento del Tribunale del riesame che, avendo annullato il sequestro e disposto la restituzione del telefono all'avente diritto, ha privato il magistrato del pubblico ministero del potere di incidere nuovamente sul bene che non avendo natura

2003, n. 196, in quanto prove lesive del diritto alla segretezza delle comunicazioni costituzionalmente tutelato e, pertanto, affette da inutilizzabilità patologica.

[21] Cfr. Cass., Sez. un., 13 luglio 1998, n. 21, in *Cass. pen.*, 1999, 465 ; Id., Sez. un., 23 febbraio 2000, n. 2, in *Giur. it.*, 2001, 1701.

[22] Cfr. Cass., Sez. un., 2 novembre 1996, n. 21, in *Arch. nuova proc. pen.*, 1997, 166.

[23] Cfr. Cass., Sez. un., 27 marzo 1996, n. 5021, in *Foro it.*, 1996, II, 473.

[24] Principio declinato da Cass., Sez. un., 27 marzo 1996, n. 5021, *Rv. 204644*.

[25] Da ultimo, v. Cass., sez. II, 10 gennaio 2020, n. 16065, Giannetti, *Rv. 278996 - 01*.

intrinsecamente criminosa, ma essendo stato, eventualmente, utilizzato per commettere il reato non è neppure soggetto a confisca obbligatoria[26]

6. – Osservazioni conclusive.

La circostanza che la Corte di cassazione, con la sentenza in commento, abbia ancorato – con tutte le doverose conseguenze – la sussistenza della inutilizzabilità patologica degli esiti investigativi, illegittimamente acquisti, alla violazione (*rectius*: aggiramento) della statuizione di annullamento del Tribunale del riesame, induce, comunque, a porsi un ulteriore quesito, ovvero se, nell'ipotesi in cui vi fossero stati, nello stesso procedimento, più indagati, tutti attinti dallo stesso *modus operandi* investigativo – *id est*: essere stato destinatario di un atto illegittimo di ablazione delle conversazioni telematiche rinvenute sul proprio *device* - e qualcuno di essi non avesse, per diverse ragioni, proposto impugnazione al Tribunale del riesame, la inutilizzabilità "patologica" dichiarata dalla suprema Corte si sarebbe potuta estendere anche agli elementi investigativi acquisiti a carico di quest'ultimi.

La risposta al quesito non può che essere positiva, atteso che non sembra possa revocarsi in dubbio che la declaratoria di annullamento, pronunciata dal Tribunale del riesame, abbia prodotto effetti anche nei confronti di altri coindagati , in ossequio al principio di diritto secondo cui «in tema di effetto estensivo della impugnazione in materia cautelare, la frammentazione dei mezzi di impugnazione proposti non preclude l'estensione degli effetti favorevoli della decisione allorchè il vizio del provvedimento cautelare sia così radicale da essere necessariamente comune a tutti gli indagati»[27].

Resta, infine, soltanto, un residuale, possibile, dubbio interpretativo, al fine di evitare un macroscopico errore, che potrebbe essere agevolmente ingenerato da una distonica comparazione dei *dicta* della sentenza in commento con un (ben noto e anche, per la verità, ormai risalente) arresto giurisprudenziale secondo il quale occorrerebbe operare una distinzione, rispetto al perimetro di operatività della inutilizzabilità, tra i dati (tutti illegittimamente acquisiti) comunicativi e i dati non comunicativi[28].

Ebbene, rapportato il citato arresto giurisprudenziale al caso risolto dalla sentenza in commento, si potrebbe ipotizzare che la inutilizzabilità patologica sentenziata dalla Corte, con la sentenza in commento, possa riguardare esclusivamente i soli dati comunicativi, ovvero i dati relativi al traffico, all'ubicazione, alla provenienza ed al contenuto delle comunicazioni informatiche, ma non anche il restante materiale documentale (e non) presente sul *device* dell'indagato (copie di documenti, immagini fotografiche, ecc…) rinvenute all'esito della ispezione dichiarata illegittima.

Una siffatta interpretazione potrebbe essere (erroneamente) indotta da una non attenta e oculata interpretazione di quel filone giurisprudenziale secondo il quale i documenti (e altri mezzi di prova assimilabili, quali immagini fotografiche, ecc…), hanno natura extraprocedimentale, ragion per cui non costituirebbero documentazione, ancorché atipica, dell'attività investigativa[29]. Di tal chè, sarebbero utilizzabili a prescindere dalla dichiarata inutilizzabilità patologica della attività di indagine.

La ipotizzata chiave interpretativa, tuttavia, sembra improponibile, se non altro perché si porrebbe in contrato con i *dicta* della sentenza in commento la quale, chiaramente, ha sentenziato la

[26] Cfr. Cass., sez. VI, 7 luglio 2003, n. 34088, Lomartire, *Rv. 226687 – 01*.

[27] Cfr. Cass., sez. VI, 8 gennaio 2021, n. 10809, in *CED Cass. pen.*, 2021.

[28] Il riferimento è alla nota sentenza Cass., Sez. un., 28 marzo 2006, n. 26795, *Rv. 234270 - 01*, secondo cui «Le riprese video di comportamenti "non comunicativi" non possono essere eseguite all'interno del "domicilio", in quanto lesive dell'art. 14 Cost.. Ne consegue che è vietata la loro acquisizione ed utilizzazione anche in sede cautelare, e, in quanto la prova illecita, non può trovare applicazione la disciplina dettata dall'art. 189 c.p.p.».

[29] Cass., sez. V, 13 aprile 1999, n. 6887 Gianferrari, *Rv 213606*; Id., sez. V, 16 marzo 1999, n, 5337, Di Marco, *Rv 213183*.

inutilizzabilità patologica di tutto il materiale conoscitivo/investigativo acquisito con la illegittima ispezione informatica. Diversamente opinando, alla luce dei principi costituzionali richiamati dalla suprema Corte (e di quelli di diritto sovranazionale richiamati nel presente contributo) si perverrebbe a risultati aberranti, volti a neutralizzare le garanzie costituzionalmente ancorate a libertà fondamentali, quali quella della segretezza e della riservatezza delle comunicazioni, atteso che, nella società contemporanea, un supporto informatico risulta essere, ancora più del "tradizionale" domicilio, il luogo nel quale trova la massima (e libera) espressione la personalità di ciascun individuo.