LE NUOVE FRONTIERE DEL CONCETTO DI "CORRISPONDENZA" NEL PROCESSO PENALE

Sarah Grieco

Abstract – *Adeguare le vecchie garanzie ai nuovi strumenti della tecnica, garantendo continuità alla protezione dei diritti fondamentali dei cittadini, costituisce una esigenza permanente, oltre che una sfida, per l'ordinamento giuridico nazionale. Le nuove tecnologie di comunicazione, come la messaggistica istantanea, richiedono un aggiornamento della tradizionale concezione di "corrispondenza" nel procedimento penale, al fine di un'effettiva attuazione delle garanzie costituzionali che ne presiedono la libertà e la segretezza. La riflessione prende spunto dalla sentenza della Suprema corte, la n. 31180 del 2024, che sembra aver definitivamente consacrato il* dictum *reso, un anno prima, dalla Corte costituzionale, con la sentenza n. 170 del 2023, riconoscendo dignità di "corrispondenza" alle comunicazioni effettuate, tra soggetti determinati, attraverso i nuovi mezzi telematici, anche*

quando già ricevuti e letti dal destinatario. Dopo una breve panoramica sulla progressiva presa di coscienza del legislatore e della giurisprudenza sulla necessità di "attualizzare" la tutela costituzionale della libertà di corrispondenza, adattandola ai moderni strumenti di comunicazione, si prosegue con una disamina della proposta di legge n. 806/2023, tesa ad introdurre una procedimentalizzazione ad hoc *del sequestro e dell'acquisizione dei dati tratti da strumenti elettronici (*smartphone, personal computer, tablet et similia). *A chiudere l'elaborato alcune osservazioni critiche sulla proposta in esame e sull'impianto generale del sistema.*

Abstract Adapting the old safeguards to the new tools of technology, ensuring continuity in the protection of citizens' fundamental rights, is a permanent requirement and challenge for national legal systems. The new communication technologies, such as instant messaging, require an update of the traditional concept of "correspondence" in criminal proceedings, with a view to the effective implementation of the constitutional guarantees governing freedom and secrecy. The reflection is inspired by the ruling of the Supreme Court, n. 31180 of 2024, which seems to have definitively consecrated the dictum made, a year before, by the Constitutional Court, with the judgment n. 170 of 2023, recognizing the dignity of "correspondence" the communications carried out, between determined subjects, through new telematic means, even when already received and read by the addressee. After a brief overview of the progressive awareness of the legislator and jurisprudence on the need to "update" the constitutional protection of freedom of correspondence, adapting it to modern communication tools, It continues with an examination of the draft law n. 806/2023, aimed at introducing an ad hoc proceduralization of seizure and acquisition of data taken from electronic instruments (smartphone, personal computer, tablet et similia). To conclude, I have a few critical comments on the proposal under consideration and on the general scheme of the system.

***Sommario*: 1. L'evoluzione del concetto di corrispondenza nel processo penale – 2.** L'approdo della Suprema Corte con la sentenza n. 31180 del 2024: un passo ulteriore verso un concetto "moderno" di corrispondenza - 3. Prospettive *de jure condendo:* il disegno di legge sul sequestro di strumenti elettronici - 4. Luci ed ombre dell'impianto riformatore

1. L'evoluzione del concetto di corrispondenza nel processo penale

L'avanzare delle nuove tecnologie è fonte di inevitabili e profondi rivolgimenti, nei diversi rami del diritto, che impongono al legislatore, e all'interprete, un continuo aggiornamento normativo.

Il diritto e la procedura penale costituiscono un terreno privilegiato di questa doverosa attività di adeguamento della disciplina legale al dato tecnologico, tanto più che, ad essere coinvolti, sono beni giuridici di massima rilevanza, quali la libertà personale dell'indagato/imputato e i diritti della persona offesa.

La mancata "attualizzazione" normativa rischierebbe, infatti, di "svuotare" di significato diritti costituzionali, anche di origine antica, che, se continuassero ad essere relegati ai soli strumenti per i quali furono inizialmente pensati, di fatto, oggi, non troverebbero più cittadinanza.

In tale quadro, la tutela della libertà e della segretezza della "corrispondenza" - diritto costituzionale la cui inviolabilità, com'è noto, trova presidio costituzionale nell'art. 15 Cos., con la duplice riserva di legge e di giurisdizione[1] - si colloca in modo del tutto peculiare.[2]

Nel "luogo virtuale" assumono rilievo sia l'art. 13 Cost., con il suo vasto spettro delle libertà morali e della dignità stessa della persona, presupposto di tutti gli altri diritti di libertà, sia i successivi segmenti, indicati negli artt. 14 e 15 Cost., che ne ampliano, rafforzano e perfezionano la portata[3].

In particolare, il dispositivo elettronico, per la sua idoneità a custodire un'enorme mole di dati e il suo innegabile rapporto di continuità spaziale, tra individuo ed oggetto, rappresenta, più di ogni altro bene materiale, l'estensione del corpo umano[4]. I nuovi mezzi telematici, quali la messaggistica sms o le *chat* istantanee (*WhatsApp* su tutte), assurgono ad «*appendici virtuali della persona e luoghi di manifestazione di buona parte delle esperienze umane*»[5], sin dalla prima adolescenza, ed impongono riflessioni e aggiornamenti che il legislatore, proprio in materia penale, ha mostrato, più volte, di cogliere.

Si veda, solo per citare un esempio, l'articolo 616, comma 4 del codice penale, come modificato già con l'art. 5, comma 2, della legge 23 dicembre 1993, n. 547. Sebbene con la specifica ai soli "*fini delle disposizioni di questa sezione*"[6], la nuova formulazione della norma ha precisato che, nel concetto di "corrispondenza", dovesse rientrarvi «*quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione*».

Oltre alla legge sostanziale, anche nel codice di rito si è assistito ad un tentativo di adeguamento dell'originario impianto "predigitale".

L'art. 254 c.p.p., così come riformato dalla legge n. 48/2008[7], in tema di sequestro di corrispondenza, ha

introdotto il riferimento ai fornitori di servizi «*telematici*» e agli oggetti di corrispondenza «*anche se inoltrati per via telematica*». È stata prevista, inoltre, una disposizione specifica, l'art. 254-*bis* c.p.p., rubricata «*Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni*».

L'intento, come si desume dalla lettura del testo normativo, è quello di assicurare la conformità tra i dati acquisiti e quelli originali, così come, del resto, previsto nell'art. 260, 2° co., c.p.p. innovato sempre dal medesimo provvedimento legislativo.

Si tratta, tuttavia, di innovazioni limitate, incapaci di scalfire un impianto ancorato a stilemi sorpassati[8]. La riforma in parola, inoltre, non si è preoccupata di precisare limiti e divieti, né di stabilire un controllo giurisdizionale preventivo o a posteriori effettivo, lasciando sullo sfondo il rischio della prova illecita[9].

L'inadeguatezza del dato normativo non è stata sopperita dal lavoro della giurisprudenza che ha mostrato, sotto diversi aspetti, una scarsa attenzione all'implementazione delle nuove tecnologie di comunicazione.

Con particolare riguardo alla messaggistica digitale (sms e *WhatsApp)*, la Suprema Corte ha adottato una visione di "stampo minimale", attribuendo all'apprensione di tali forme di comunicazione, nel corso delle indagini e in fase istruttoria, anche dibattimentale, la valenza di una mera acquisizione documentale, ai sensi dell'art. 234 c.p.p., precludendo, così, l'accesso alle guarentigie proprie della corrispondenza di vecchio stampo[10], la cui nozione implica un'attività di spedizione in corso o, comunque, avviata dal mittente mediante consegna a terzi per il recapito. Né, d'altra parte, si è ritenuta applicabile la disciplina delle intercettazioni che postula, per sua natura, la captazione di un flusso di comunicazioni in corso, cd. acquisizione dei documenti informatici *on going*, là dove i dati presenti sulla memoria del telefono, acquisiti *ex post*, costituiscono mera documentazione "statica" di detti flussi.[11]

Di qui, l'affermazione del principio di diritto secondo cui l'apprensione della messaggistica, conservata nella memoria di un apparecchio cellulare, non soggiace alle regole stabilite per la corrispondenza né, tantomeno, alla disciplina delle intercettazioni telefoniche; con l'ulteriore conseguenza che, detti testi, possono ritenersi legittimamente acquisiti al processo, ed utilizzabili ai fini della decisione, ove ottenuti mediante riproduzione fotografica a cura degli inquirenti.

L'indirizzo in parola è rimasto pressoché costante anche in tempi assai recenti, con riguardo ai messaggi pubblicati sui profili *social*, in area riservata[12]. La Corte ha ribadito come, nel vigente sistema processuale -

caratterizzato dalla dialettica delle parti, alle quali è attribuito l'onere di allegazione delle prove - il giudice è tenuto a provvedere alle richieste probatorie avanzate dalle parti, sulla scorta dei parametri di ammissibilità enunciati dall'art. 190, comma 1, c.p.p.[13], con una valutazione, in concreto, della sola necessità di acquisire o meno il supporto telematico, o figurativo, sul quale viene apposta la registrazione della conversazioni digitale, oggetto di trascrizione[14].

Ad imporre una profonda rimeditazione del quadro interpretativo, fatto proprio anche dal giudice di legittimità, è stata la posizione espressa dalla Corte costituzionale, con la nota sentenza n. 170/2023[15].

Al concetto di corrispondenza viene attribuita una valenza fortemente inclusiva che deve "tendersi" fino «*ad abbracciare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza*». Pertanto, la tutela accordata dall'art. 15 della Costituzione, garanzia per tutti i consociati di libertà e segretezza «*della corrispondenza e di ogni altra forma di comunicazione*», prescinde dalle caratteristiche del mezzo tecnico utilizzato nella trasmissione del pensiero. La tutela abbraccia 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[16].

Posta elettronica e messaggi inviati tramite l'applicazione *WhatsApp* rientrano, dunque, a pieno titolo, nella sfera di protezione costituzionale, apparendo del tutto assimilabili a lettere o biglietti chiusi.

La Corte, infatti, si sofferma anche sul grado di riservatezza della comunicazione dei nuovi strumenti tecnologici rispetto alla tradizionale corrispondenza epistolare. Alla busta chiusa, in cui inserire il cartaceo, viene sostituita la specifica casella di posta della messaggistica digitale, accessibile solo al destinatario, tramite procedure che prevedono l'utilizzo di codici personali; mentre il messaggio *WhatsApp* è destinato, esclusivamente, al soggetto che abbia la disponibilità del dispositivo elettronico di destinazione, normalmente protetto, anch'esso, da codici di accesso o altri meccanismi di identificazione[17].

Nella pronuncia in parola - di cui, in questa sede, ci si è limitati ad illustrare i soli principi enucleati, in quanto oggetto di numerosi commenti, per i molteplici spunti che ha suscitato[18]- il Giudice delle leggi ha "disancorato" la tutela accordata dall'art. 15 Cost. dalle caratteristiche dello strumento tecnico utilizzato, aprendo, così, il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata, che l'evoluzione tecnologica mette a disposizione a fini comunicativi; ivi inclusi quelli elettronici e

informatici.

In aperto dissenso con la posizione adottata dalla giurisprudenza di legittimità, fino a quel momento, il Giudice delle leggi non lascia spazio a dubbi interpretativi quando afferma 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*».

2. L'approdo della Suprema Corte con la sentenza n. 31180 del 2024: un passo ulteriore verso un concetto "moderno" di corrispondenza

Il disallineamento, fra la tradizionale posizione della Corte di Cassazione e l'avanzato insegnamento della Corte costituzionale, sembrerebbe essersi finalmente colmato, almeno in massima parte, con la sentenza n. 31180 del 2024[19].

Tuttavia, prima di addentrarsi nella disamina della pronuncia, è opportuno richiamare alcune precedenti pronunce, in tema di sequestri di apparecchiatura digitale, che mostrano una maggiore attenzione al sistema di garanzie da approntare, in caso di sequestro di un apparato informatico complesso.

Con riguardo alla protezione della *privacy* dei soggetti indagati, ad esempio, la Suprema Corte[20], con sentenza n. 38460/2021 aveva sancito l'illegittimità del sequestro applicato su di una massa indistinta di dati informatici, senza selezione né indicazione dei criteri di estrazione; con conseguente restituzione all'avente diritto e distruzione di tutte le copie forensi in possesso del giudice, evidenziandone anche la necessità di una sua procedimentalizzazione.

Giova, pure, evidenziare la successiva pronuncia n. 17604 del 2023[21] che stabiliva, sempre relativamente al sequestro probatorio avente ad oggetto un intero *personal computer*, come l'estrapolazione di "singoli" dati, con copia forense, dovesse ritenersi legittima solo se giustificata da difficoltà tecniche che non consentissero, con riproduzione mirata, di estrarre gli elementi contenuti nella memoria. In difetto, l'indiscriminata apprensione di tutte le informazioni ivi contenute, era destinata a rappresentare una chiara violazione del principio di proporzionalità e adeguatezza.

Il principio di proporzionalità, in vista di un adeguato contemperamento delle opposte esigenze, è stato oggetto di una ulteriore pronuncia[22]: la n.44010/2022. I giudici di legittimità evidenziavano l'accezione di proporzionalità non solo in senso "quantitativo", in relazione alla massa di dati a cui accedere, ma anche sotto il profilo temporale, sottolineando l'importanza della rapidità di duplicazione del contenuto digitale, mediante la creazione della cosiddetta copia forense; così da garantire la tempestiva restituzione dell'apparecchio *smartphone*, al cessare delle esigenze di indagine giustificative del sequestro.

Un ultimo "avvicinamento", prima della decisione in commento, si era poi manifestato con le due sentenze gemelle delle Sezioni Unite sull'utilizzo della messaggistica "*Sky ECC*" (in materia di c.d. criptofonini)[23]. Già in quella sede, riprendendo le conclusioni della Consulta, la Suprema Corte aveva qualificato le *chat* non come mera documentazione acquisibile *ex* art. 234 c.p.p., ma come "corrispondenza informatica" che necessitava di un provvedimento di sequestro *ex* art. 254 c.p.p.[24] Quest'ultimo, tuttavia, non doveva provenire necessariamente dal giudice. Il sintagma "autorità giudiziaria", impiegato dall'art. 15 Cost., a parere della Corte, indicava una categoria più amplia, capace di includere tanto il giudice, quanto il pubblico ministero[25].

La sentenza n. 31180 del 2024 si pone sulla scia della tratteggiata ricerca di un equilibrio tra esigenze investigative, diritto alla *privacy* elibertà della corrispondenza dell'indagato[26].

Con il primo motivo di ricorso veniva eccepita l'inutilizzabilità della messaggistica tratta dai dispositivi mobili appartenenti al ricorrente e agli altri indagati, oggetto di sequestro, acquisita, nuovamente, a seguito di un'indebita "ispezione telematica" disposta dal P.M[27]; ciò nonostante l'originario sequestro probatorio fosse stato annullato dal Tribunale del riesame, per carenza di motivazione, con la conseguente restituzione dei cellullari agli aventi diritto. L'organo inquirente, prima della loro riconsegna, aveva, infatti, proceduto ad ispezionare il contenuto dei dispositivi, acquisendone il contenuto e ponendo i dati informatici recuperati alla base della successiva richiesta cautelare a carico dell'indagato.

Il ricorrente denunciava l'assenza di un ulteriore provvedimento di sequestro *ex* artt. 254 c.p.p. che legittimasse la nuova acquisizione dei dati, attesa la qualifica della messaggistica *Whatsapp* quale corrispondenza informatica, anziché mero documento *ex* art. 234 c.p., contrariamente a quanto sostenuto nell'ordinanza impugnata ed in aperto contrasto con quelli che erano i dettami della citata sentenza della Corte costituzionale n. 170 del 2023. L'acquisizione configurava, pertanto, una violazione della sfera di libertà e segretezza della corrispondenza, in quanto posta al di fuori dei presupposti stabiliti dall'art. 15 Cost.,

trattandosi di un provvedimento contrario ad una decisione giurisdizionale; col conseguente venir meno del potere dell'organo inquirente di incidere ulteriormente sul bene, neppure soggetto a confisca obbligatoria. La violazione dei precetti costituzionali, sempre secondo l'impostazione del ricorrente, avrebbe dovuto essere sanzionata con l'inutilizzabilità patologica della messaggistica acquisita, assunta a presupposto dei "gravi indizi di colpevolezza", legittimanti la successiva misura custodiale adottata.

I giudici di legittimità, nell'accogliere la censura, hanno confermato la posizione espressa dalla Corte costituzione circa la natura di "corrispondenza informatica" e, pertanto, la necessità di un provvedimento di sequestro ai fini dell'acquisizione al procedimento; almeno fino a quando, per il decorso del tempo, essa non avesse perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico".

Il *modus procedendi* del P.M. - nel disporre, dopo l'annullamento del sequestro probatorio, un'ispezione telematica, volta ad ottenere i medesimi dati – avrebbe integrato, pertanto, una violazione del provvedimento giurisdizionale, con un tentativo di "neutralizzarne" gli effetti, attraverso l'utilizzo improprio di un atto di ricerca della prova, ritenuto nullo dal Tribunale del riesame reale.

Secondo autorevole dottrina, l'iniziativa investigativa intrapresa dal PM presenta i caratteri non solo dell'illeceità, ma anche dell'illegalità e, finanche, dell'incostituzionalità. Si tratterebbe, infatti, di una prova illecita, in quanto integrativa del reato di cui all'art. 650 c.p., per inosservanza del provvedimento "legalmente dato dall'Autorità per ragione di giustizia"; una condotta che, negli ordinamenti anglosassoni, sarebbe punita come *contempt of Court*, il reato che punisce la disobbedienza o la mancanza di rispetto nei confronti di un tribunale e dei suoi funzionari. L'"ispezione informatica" del contenuto dei telefoni cellulari rappresenterebbe, inoltre, una prova non ammessa dalla legge, la quale prevede la sola ispezione "di luoghi o di cose" ex art. 246 c.p.p. ma non della corrispondenza, qual è il contenuto di un cellulare. L'ispezione effettuata sarebbe stata compiuta anche in spregio del principio di inviolabilità del diritto di difesa, previsto dall'art. 364 c.p.p., che indica l'ispezione tra gli atti ai quali il difensore della persona sottoposta alle indagini ha diritto di assistere, previo avviso[28].

La Corte ha preso, poi, esplicita posizione sulla portata generale del *dictum* affermato dalla Corte costituzionale con la sentenza n. 170. Disattendendo la diversa ricostruzione offerta dal Procuratore Generale - secondo cui il principio espresso dalla Corte costituzionale si sarebbe riferito alle sole guarentigie apprestate dall'art. 68 Cost. in favore del parlamentare, protagonista della vicenda processuale - il Collegio

ha evidenziato come il Giudice delle leggi (par. 4.2 del *Considerato in diritto*) si fosse già espresso, conferendo, al principio di cui sopra, un'applicazione generalizzata che, prescindendo dalla qualifica di parlamentare, si riverberava su tutti i consociati.

Altro importante precipitato della sentenza è, poi, offerto dalla contestazione della tesi, sempre sostenuta dal Procuratore Generale, secondo cui, pur ammettendo l'illegittimità della "ispezione informatica", l'acquisizione dei dati non sarebbe stata censurabile sulla base della regola del *male captum, bene retentum*[29]; principio che ha rappresentato, da sempre, un punto fermo nella giurisprudenza di legittimità.

A partire dalle Sezioni Unite "Sala", n. 5021 del '96[30], la Cassazione, infatti, si è costantemente espressa circa l'eventuale illegittimità dell'atto di perquisizione, compiuto ad opera della polizia giudiziaria, sulla validità del successivo sequestro del corpo del reato o delle cose pertinenti al reato; atto dovuto a norma dell'art. 253, comma 1, c.p.p.[31]. La nullità del provvedimento di perquisizione non si trasmetterebbe a quello di sequestro delle cose rinvenute nel corso della sua esecuzione, né determinerebbe l'inutilizzabilità, a fini di prova delle stesse.

Pur senza sconfessare, *apertis verbis,* tale assunto, la sentenza in commento compie un'operazione di *distinguisching*. Lo fa ponendo in risalto l'illegittimità dell'acquisizione dei dati, effettuata in aperta violazione del provvedimento del Tribunale del riesame. Avendo annullato il sequestro e disposto la restituzione del telefono all'avente diritto, il Pubblico ministero sarebbe stato privato del potere di incidere ulteriormente sul bene. Peraltro, il dispositivo non sarebbe neppure soggetto a confisca obbligatoria[32] - a differenza del "caso Sala" che aveva ad oggetto la confisca della sostanza stupefacente - attesa la sua mancata natura intrinsecamente criminosa, ma strumento, eventualmente, utilizzato per commettere il reato.

Nonostante la "deferenza" che la decisione ancora offre al precedente orientamento, diversi commentatori[33] hanno già rilevato che la pronuncia si pone in netta contraddizione col consolidato principio del *male captum bene retentum.*

La sentenza in commento ha concluso soffermandosi sugli effetti invalidanti della violazione: la natura "patologica" dell'illegittimità avrebbe esplicato i suoi effetti anche nella fase delle indagini e nel giudizio cautelare.

Va, in tal senso, l'espresso richiamo ad una cristallina (sebbene risalente) pronuncia della Corte

costituzionale: la n. 34 del 1973. Quest'ultima, già nella dinamica di un Codice di procedura di stampo ancora semi-inquisitorio, aveva rilevato come, nella categoria delle prove sanzionate dall'inutilizzabilità, dovevano essere annoverate non solo le "prove oggettivamente vietate", ma anche quelle formate, o acquisite, in violazione dei diritti soggettivi tutelati dalla "legge" e, a maggior ragione, come in precedenza detto, dalla Costituzione[34]. In particolare, la Corte costituzionale aveva ravvisato l'esistenza di "divieti" probatori, ricavabili, in modo diretto, dal dettato costituzionale, enunciando il principio per cui «*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*»[35].

Il suddetto principio ha consentito l'elaborazione della categoria delle «*prove cosiddette incostituzionali, cioè di prove ottenute attraverso modalità, metodi e comportamenti realizzati in violazione dei fondamentali diritti del cittadino garantiti dalla Costituzione, da considerarsi perciò inutilizzabili nel processo*»[36].

Derivando la "patologia" in esame proprio dalla violazione del provvedimento giurisdizionale del Tribunale del riesame – che, accertata l'assenza di idonea motivazione, a fondamento del sequestro probatorio operato dal PM, ne aveva disposto l'annullamento e ordinato la restituzione dei beni appresi agli aventi diritto - l'ulteriore compressione della sfera costituzionalmente tutelata, attuata tramite la ispezione informatica, rappresentava un'illegittima violazione della sfera di riservatezza; al di fuori dal rispetto del perimetro delle garanzie derivanti dall'art. 15 Cost.[37].

Da tale assunto, la Corte dichiarava l'inutilizzabilità delle *chat* anche in sede cautelare, richiamando, sul punto, la giurisprudenza sulla non utilizzabilità degli atti probatori affetti dalla cd. "inutilizzabilità patologica"[38] e rinviando al Tribunale del riesame per il nuovo scrutinio della richiesta di misura cautelare, espunte le risultanze probatorie dichiarate inutilizzabili.

Nel solco dell'orientamento della sentenza in commento ne sono succedute, in ordine cronologico, altre dello stesso tenore fra le quali spicca la pronuncia n. 39548 del settembre 2024 [39] che ha affermato, in tema di mezzi di prova, l'inutilizzabilità patologica dei messaggi WhatsApp, in considerazione della loro natura di corrispondenza, allorquando vengono acquisiti, in violazione dell'art. 254 c. p. p., mediante *screenshots* eseguiti dalla polizia giudiziaria, di propria iniziativa e senza ragioni di urgenza, in assenza di decreto di sequestro del Pubblico ministero.

Sempre in tema di messaggistica WhatsApp acquisita mediante *screenshot*, con successiva sentenza, la

n.1269 del 13 gennaio 2025[40], la Corte sottolinea che neppure il consenso dell'indagato potrebbe far «*ritenere legittima l'acquisizione di* chat *dallo* smartphone *in uso dal medesimo*». Né è possibile ricorrere alla disciplina della prova atipica: «*in un sistema ispirato al principio di legalità*», specifica la Corte, in modo assolutamente eloquente, «*non è permesso alla polizia di aggirare espresse previsioni di legge per compiere atti atipici con l'obiettivo di raggiungere lo stesso risultato di quelli tipici. Pertanto neppure qualora il consenso fosse stato reso dalla persona indagata su sollecitazione della polizia giudiziaria, resta imprescindibile per quest'ultima, procedere al sequestro del telefono senza, tuttavia poter accedere al suo contenuto, «onde prevenire rischi di abuso*».

Nonostante il richiamo della Consulta alle garanzie di cui all'art. 15 Cost., i giudici di legittimità, non sembrano, tuttavia, orientati a ritenere necessario un intervento giurisdizionale. Anche nella ultimissima pronuncia n.8376/2025, infatti, i giudici di legittimità, ai fini del sequestro di dati informatici assimilabili al concetto di corrispondenza, ritengono sufficiente il provvedimento dispositivo del pubblico ministero, dotato di adeguata motivazione tale da far emergere, sia pure *per relationem* rispetto alle condotte descritte, l'oggetto del sequestro e la plausibile aspettativa del rinvenimento di ciò che si ricerca, ai fini di prova, proprio attraverso le cose da sequestrare [41].

3. Prospettive *de jure condendo*: il disegno di legge sul sequestro di strumenti elettronici

Il nuovo orientamento sancito dalla Corte costituzionale, e ora consacrato dalla giurisprudenza di legittimità, si scontra con un quadro legislativo ancora fortemente "arretrato" nel quale, nonostante i citati interventi di adeguamento, i moderni strumenti di comunicazione digitale rivestono un ruolo ancillare e residuale, rispetto al fulcro della disciplina legale.

Laddove l'evoluzione della tecnica consegna nuovi strumenti di comunicazione sui quali svolgere operazioni investigative, nel tentativo di dare loro cittadinanza probatoria all'interno dell'ordinamento, tre sembrano essere le prospettive che si presentano all'interprete: ricorrere alla fattispecie probatoria atipica regolata all'art 189 c.p.p.; tentare di ricondurre la novità sotto l'egida di un'ipotesi tipica, oppure, in ultima istanza, attendere la tipizzazione ad opera del legislatore tramite la creazione di una norma *ad hoc*.

L'ultima delle tre soluzioni, indubbiamente, più lenta e complessa, è l'unica a consentire una regolazione senza lasciare spazi eccessivi all'interprete; una discrezionalità che mal si concilia non solo con le garanzie dell'art. 15 Cost. ma col più generale principio di legalità di cui all'art. 111 Cost.

È evidente, infatti, come l'applicazione della disciplina sulla prova atipica – che comprende tutte prove non disciplinate espressamente dal legislatore, la cui ammissibilità è rimessa alla valutazione del giudice - rimandando il contraddittorio richiesto al momento dell'ammissione in giudizio dei risultati probatori, non consentirebbe di dirimere, preliminarmente, la complessa questione relativa ai diritti coinvolti in tali operazioni.

Ugualmente, la disciplina delineata dall'art 253 c.p.p. non può soddisfare la riserva di legge prevista dal dettato costituzionale, in quanto norma troppo generica rispetto ai casi, modi e garanzie che la legge dovrebbe definire[42].

Mancando, nell'attuale sistema, la disciplina dell'"atto invasivo", che solo il legislatore è chiamato a compiere, l'intervento normativo diviene imprescindibile a seguito proprio dell'orientamento consacrato con la sentenza n. 31180 del 2024.

Non sono mancate proposte di adeguamento volte a superare il *gap* normativo.

Nell'attuale legislatura, è in discussione un progetto di legge volto ad introdurre una norma *ad hoc* di disciplina del «*sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute*».

In particolare, il disegno di legge n. 806[43] - che ha assorbito il precedente d.d.l. n.690[44], già oggetto di approvazione, in prima lettera al Senato, il 10 aprile 2024, con l'emendamento 1.100 che sostituisce l'integrale testo originario – è, al momento in cui si scrive, all'esame della II Commissione Giustizia della Camera[45].

L'intervento riformatore, come noto, inserisce una specifica procedura di sequestro degli "strumenti elettronici", all'interno del codice di rito, attraverso un nuovo articolo, il 254-*ter* c.p.p., posto di seguito a quello che disciplina il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.

Centrale è l'articolo 1 che prevede una specifica disciplina piuttosto ampia nel suo oggetto: al fianco dei dispositivi e dei sistemi informatici o telematici, è contemplato anche il sequestro di memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute; facendo intendere,

con tale accezione, ogni supporto di dati, anche quelli non propriamente qualificabili come "comunicazioni". La *voluntas legis* è quella di introdurre una serie di preziose garanzie per vari apparati differenti tra loro, anche per funzione. Tuttavia, l'ampiezza e l'eterogeneità della categoria di "strumenti elettronici", che spazia fino a qualsiasi "contenitore" di dati, così come concepiti nella nuova disciplina, renderebbe auspicabile una disciplina dedicata agli apparati che possono essere utilizzati per la comunicazione, diversa da quella individuata per il sequestro di dispositivi elettronici impiegati per la sola archiviazione dei dati, a partire dalla fase di apprensione del dispositivo anziché limitarsi, come oggi, a quella di sequestro del contenuto degli stessi[46].

L'articolata procedimentalizzazione del sequestro dei dispositivi elettronici - suddivisa in tre distinte fasi (apprensione del dispositivo, copia forense del contenuto con l'analisi dei dati, acquisizione dei soli dati di rilievo investigativo) - riprende, in parte, la normativa sui tabulati telefonici e, in altra parte, quella afferente alle intercettazioni, rispettando a pieno la riserva di giurisdizione.

Il procedimento, infatti, si contraddistingue per due diversi *step* autorizzativi, uno preliminare, disciplinato dal primo comma, che riguarda il sequestro dei dispositivi, ed uno, eventualmente successivo all'analisi del duplicato informatico, disciplinato dal comma 12.

Lo stesso prende avvio con la richiesta dell'organo inquirente di autorizzazione al sequestro dal giudice per le indagini preliminari - anziché dal pubblico ministero, a differenza della versione originaria[47] - qualora gli elementi da acquisire siano *necessari* per la prosecuzione delle indagini («*in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta*») e nel rispetto del criterio di *proporzionalità*, con riguardo alle esigenze investigative.

È d'obbligo, fin d'ora, far rilevare come, l'assenza di un limite espressamente previsto dal legislatore e di una specificazione dei casi e dei modi legittimanti la lesione del diritto, sembra rendere difficilmente superabile il vaglio di costituzionalità della proposta di legge in esame[48].

La riserva di legge, a differenza di quella di giurisdizione, non appare rispettata. Se la massima espansione delle libertà e dei diritti fondamentali, come quello di comunicazione, presuppone un'interpretazione estensiva di tali diritti, da un lato, e restrittiva dei limiti, dall'altro, il sequestro dei dispositivi elettronici deve, necessariamente, essere presidiato da norme processuali volte anche a definire casi, tempi e modi dell'attività investigativa, con una dettagliata motivazione all'interno del decreto che lo dispone; pena

l'illegittimità per violazione della riserva di legge.

È evidente come il generico richiamo ai criteri di *necessità* e *proporzionalità*, previsti dal disegno di legge, non siano in grado di soddisfare tale esigenza.

Il giudice dispone il sequestro con decreto motivato, immediatamente esecutivo, con trasmissione al PM che ne cura, direttamente o per il tramite della polizia giudiziaria, l'esecuzione. Nei soli casi di urgenza, il pubblico ministero può disporre il sequestro, subordinando la convalida ad un momento successivo. Negli stessi casi, prima dell'intervento del pubblico ministero, al sequestro possono procedere ufficiali di polizia giudiziaria, i quali, nelle quarantotto ore successive, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito. Questi, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto di disposizione del mezzo di ricerca della prova, entro quarantotto ore dal sequestro, se disposto dallo stesso pubblico ministero, o dalla ricezione del verbale, se il sequestro è stato eseguito di iniziativa dalla polizia giudiziaria. Dopo l'esercizio dell'azione penale, il sequestro è, invece, disposto dal "giudice che procede" e la duplicazione è eseguita mediante perizia. Copia dell'ordinanza è immediatamente notificata alla persona, alla quale le cose sono state sequestrate (comma 5).

Il sequestro perde efficacia se non sono osservati i termini previsti dal comma 4 o in caso di mancato rispetto del termine di dieci giorni dalla ricezione della richiesta per l'emissione dell'ordinanza.

Con riguardo alla successiva fase della "duplicazione"[49] e analisi del contenuto – di cui ai successivi commi (dal 6 all'11) – si scorge una particolare attenzione al contraddittorio, seppur con alcuni limiti. In particolare la disposizione, in linea con i summenzionati indirizzi giurisprudenziali, prevede sì tempi stringenti per lo svolgimento delle operazioni tecniche[50], ma anche il diritto per i difensori e i consulenti tecnici, eventualmente nominati, di partecipare allo svolgimento delle operazioni di duplicazione e di formulare osservazioni e riserve (comma 8)[51].

Sul punto, attenta dottrina[52] ha osservato come la particolare fragilità e alterabilità dei dati informatici, oggetto di duplicazione[53], avrebbe richiesto l'attivazione dei presidi di cui all'art. 360 c.p.p., tipici degli accertamenti tecnici irripetibili, ivi inclusa la riserva di promuovere incidente probatorio, laddove, invece, l'unico riferimento è alla sola disposizione di cui all'art. 364, comma 2, c.p.p. con l'avviso della nomina del difensore di ufficio, qualora sprovvisto di quello d fiducia.

La duplicazione del contenuto del supporto digitale - di cui, tuttavia, non si stabilisce un perimetro, consentendo, così, un accesso indiscriminato di dati, contrario all'indirizzo giurisprudenziale a cui si è fatto, in precedenza, riferimento (cfr. par.1) - avviene su adeguati supporti informatici mediante una procedura che deve assicurare la conformità del duplicato all'originale e la sua immodificabilità (comma 9)[54]. La normativa non si sofferma, però, sugli aspetti tecnici ed operativi da adottare per rispettare la richiamata garanzia di immodificabilità dei dati, lasciando agli operatori tale scelta e vincolandoli al rispetto del solo contraddittorio.

La proposta di legge introduce, poi, per alcuni particolari delitti, che la duplicazione possa avvenire, in deroga al contradditorio della disciplina generale (disposto nei commi 6, 7 e 8,) con modalità tecniche idonee ad assicurare la conformità del duplicato all'originale e la sua immodificabilità.

Effettuata la duplicazione, viene disposta, senza ritardo, la restituzione dei dispositivi all'avente diritto. La restituzione del patrimonio dei dati, tuttavia, viene posticipata «*fino alla sentenza o al decreto penale di condanna non più soggetti a impugnazione*», con il possibile pericolo di un loro utilizzo esplorativo nonché di rischio di dossieraggio.

Con riguardo al sequestro dei dati, successivo all'analisi del duplicato informatico da parte del PM, l'articolo 254-*ter* delinea due distinte procedure, a seconda della tipologia di elemento da acquisire (comunicativo o non comunicativo), atteso che solo i primi rientrano nell'alveo dell'art 15 della carta costituzionale. Con i dati a contenuto comunicativo, per ottenere il sequestro, sarà necessario rivolgersi, nuovamente, al giudice per le indagini preliminari, che dovrà emettere un nuovo decreto autorizzativo, qualora ravvisi i presupposti delle intercettazioni: i "gravi indizi" (art.267, comma 1 c.p.p.) dei reati di cui all'art. 266 c.p.p. e i "sufficienti indizi" nel caso di procedimenti per reati di criminalità organizzata (art. 13 del d.l. n. 152 del 1991). Qualora i dati non rappresentino comunicazioni sarà sufficiente una valutazione, da parte dello stesso PM, di proporzionalità del sacrificio della *privacy* individuale, con limitazione dell'acquisizione di dati a quelli effettivamente rilevanti per l'indagine in corso[55].

Contro i decreti di sequestro è ammesso riesame, anche nel merito, ai sensi dell'articolo 257 c.p.p.

L'articolo 2 apporta una serie di modifiche al codice di procedura penale in materia di: perquisizione informatica e sequestro conseguente alla perquisizione; divieto di pubblicazione del contenuto dei duplicati; perquisizioni, accertamenti urgenti e sequestri d'iniziativa della polizia giudiziaria; fasi successive al

sequestro informatico.

Infine, l'articolo 3 introduce nelle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, due nuove disposizioni: l'articolo 82-*bis* in materia di attività per la custodia dei supporti contenenti dati, informazioni e programmi sottoposti a sequestro e l'articolo 82-*ter* che disciplina la conservazione dei duplicati informatici.

4. Luci ed ombre dell'impianto riformatore

La ricerca di un equilibrio tra le esigenze investigative e il diritto alla riservatezza rappresenta il pilastro fondamentale di una società democratica.

Il progetto di legge in discussione costituisce, senza dubbio, un deciso passo in avanti verso la tutela "aggiornata" del principio costituzionale di libertà e segretezza della corrispondenza che sembra, così, trovare una nuova "declinazione digitale". Lo stesso si muove nella consapevolezza che i dispositivi informatici di uso corrente, vere e proprie appendici della persona, vengono utilizzati per gli scopi più diversi, rappresentando, talvolta, l'unico accesso al domicilio informatico del soggetto (si pensi, ad esempio, all'utilizzo dello *smartphone*, per il riconoscimento e l'autorizzazione, a distanza, di operazioni bancarie o per la firma digitale).

La privazione, protratta nel tempo, di apparati, nelle cui memorie sono conservate le tracce di comunicazioni e conversazioni tra privati, senza che la stessa abbia una funzione che vada al di là della comprensione del solo contenuto, rappresenta una misura sproporzionata in quanto significa impedire l'esercizio di legittimi diritti, senza che la limitazione soddisfi una qualche esigenza di accertamento.

È indubbio che l'inserimento di una procedimentalizzazione - al di là dei comprensibili timori di chi[56] vede il rischio di un "ingolfamento" del sistema giustizia, in particolare durante la fase delle indagini preliminari – reca con sé il pregio dell'apertura di una "*finestra di giurisdizione*", fino ad oggi preclusa, in linea sia con l'importanza costituzionale dei valori in gioco e dell'impostazione generale della stessa riforma Cartabia, che ha tentato di riportare in equilibrio i rapporti fra Pubblico Ministero e Giudice fin dentro le indagini preliminari, secondo una comune cultura della giurisdizione[57].

Ciò nonostante, non sbaglia chi afferma che il disegno di legge in discussione, da una prima analisi, «*non*

riesce a fornire piena soddisfazione alle esigenze che intenderebbero soddisfare»[58].

In particolare, l'utilizzo di un locuzioni dalla natura eccessivamente generica e indefinita nell'individuare i presupposti applicativi - quali il criterio della *necessità* per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle *modalità* della condotta, nel rispetto del criterio di proporzione – denota un'alea eccessiva che finisce per attribuire ampli (e preoccupanti) margini di discrezionalità all'Autorità Giudiziaria procedente; mettendo in discussione, nuovamente, il principio di tassatività che governa la restrizione delle libertà in discussione.

Tali circostanze si porrebbero in contrasto, non solo con i principi costituzionali, ma anche con le più recenti indicazioni giurisprudenziali della Corte di cassazione, con specifico riferimento all'illegittimità del sequestro a fini probatori di una indistinta massa di dati informatici, con una indiscriminata apprensione di tutte le informazioni ivi contenute, in difetto di specifiche ragioni[59].

Allo stesso modo, si è evidenziato un *vulnus* interpretativo successivo circa la concreta distinzione tra comunicazioni e meri documenti; si pensi, ad esempio, alla classificazione di uno *screenshot* di un dialogo intercorso sull'applicativo *Whatsapp* (anche tramite lo scambio di messaggi "vocali"). La classificazione tra corrispondenza o documento/fotografia si riverbera, automaticamente, sulle modalità procedurali di acquisizione del dato laddove il secondo non può rappresentare una prova digitale, a differenza della prima. Tale difficoltà operativa potrebbe essere superata da un unico regime autorizzativo che contempli garanzie simili a quelle previste per le intercettazioni, con il sequestro disposto dal Giudice su richiesta del PM, solo in presenza di gravi indizi di reato[60]. In tal modo si restringerebbe, a monte, l'accesso ad una copiosa mole di dati privati altamente sensibili, che renderebbe di difficile applicazione pratica la procedura di selezione ad opera del pubblico ministero; oltre a prevenire il rischio di trasformare il sequestro da mezzo di ricerca della prova a mezzo di ricerca di ulteriori notizie di reato a causa proprio dell'enorme mole di dati con cui gli inquirenti verrebbero in contatto. Tale approccio, a ben guardare, sarebbe anche più rispettoso dell'art. 13 Cost. che consente di ricomprendere al suo interno il vasto spettro delle libertà morali e della dignità stessa della persona, attesa l'estensione del corpo umano che, soprattutto, lo *smatphone* rappresenta.

Alcune critiche possono essere mosse anche con riguardo alla previsione della regola del doppio binario per il successivo decreto del sequestro dei dati, con riguardo ai reati previsti dall'art. 13 del D.L. 152/1991, convertito con la legge n. 203/1991. La sostituzione del vaglio delle "gravità" indiziaria con il più debole criterio della "sufficienza", sembra scontrarsi con alcuni capisaldi costituzionali quali la presunzione di non

colpevolezza, la natura personale della responsabilità penale, la tutela delle libertà fondamentali e del principio di uguaglianza. Il procedimento penale deve essere parametrato sulla figura dell'indagato/imputato, prescindendo dalle mere ipotesi di reato, la cui eventuale sussistenza è, appunto, demandata esclusivamente all'accertamento processuale. L'applicazione della regola del doppio binario, rischia, inoltre, di finire sotto la scure del criterio della proporzionalità. Trattandosi di un generalizzato accesso *ex post* alla vita privata del cittadino, la dimensione della gravità indiziaria, in ordine alla sussistenza di un reato, appare decisamente un requisito minimale per giustificare un intervento così invasivo[61].

Quantunque tutto sia perfettibile, non vi è dubbio che la nuova disciplina è il segno tangibile della condizione *praeter legem* e *contra constitutionem* in cui versa il nostro sistema attuale. L'introduzione di una disciplina tassativa del sequestro degli apparati elettronici/informatici – o anche, semplicemente, degli apparati di comunicazione - conferma implicitamente lo stato dell'arte connotato dall'assenza di una benché minima regolamentazione della materia; ciò in spregio della riserva di legge e di giurisdizione imposta dall'art. 15 Cost. e dalla giurisprudenza europea.

Non solo: l'entrata in vigore della nuova normativa dovrebbe porre fine a quelle attività di *online surveillance* che, per il tramite della fattispecie probatoria atipica dell'art. 189 c.p.p., sono state, finora, eseguite sui dispositivi informatici utilizzati per le comunicazioni; un'attività certamente non rispettosa, ancora una volta, della riserva (assoluta) di legge primaria e di giurisdizione imposte dall'art. 15 Cost.[62].

La prospettiva di riforma *de jure condendo* pone le basi normative delle "nuove frontiere" del concetto di corrispondenza digitale che, di fatto, ha soppiantato le precedenti forme di comunicazione. Una nuova realtà che pone sfide inedite nel campo della *privacy,* con importanti ricaduteche meritano, indubbiamente, una più rigorosa disciplina, soprattutto all'interno del procedimento penale.

Un intervento tempestivo del legislatore per colmare il *gap* normativo esistente, assicurando la protezione da esplorazioni invasive ed indiscriminate anche delle nuove forme di conversazioni digitali, appare improcrastinabile.

Orizzonte culturale e parametro di riferimento, *in primis*, per il legislatore, ma anche per gli interpreti, resta il principio di proporzionalità, così com'è destinato a rivestire «*nel sistema una portata più ampia, in quanto travalica il perimetro della libertà individuale per divenire termine necessario di raffronto tra la compressione dei diritti quesiti e la giustificazione della loro limitazione*»[63].

In attesa dell'approvazione del progetto di riforma da parte dell'altro ramo del Parlamento, infine, preme sottolineare come, uno slancio verso l'approvazione della nuova legge, potrebbe giungere dal contesto europeo. La Grande Camera della Corte di giustizia dell'Unione del 4/10/2024, causa C-548/21, riconoscendo che l'accesso da parte della polizia, nell'ambito di un'indagine penale, ai dati personali, conservati in un telefono cellulare, può costituire un'ingerenza grave nei diritti fondamentali dell'interessato, ha affermato l'indispensabilità della preventiva autorizzazione da un giudice o da un'autorità indipendente, salvo in casi di urgenza, debitamente comprovati; ciò proprio a garanzia del rispetto del principio di proporzionalità. Inoltre la Corte ha affermato anche la necessità di una preventiva informazione alla persona interessata, nell'ambito delle procedure nazionali applicabili, dei motivi su cui si basa l'autorizzazione di accesso a tali dati, rilasciata da un giudice o da un'entità amministrativa indipendente, dal momento in cui la comunicazione di tali informazioni non sia più idonea a compromettere i compiti affidati a tali autorità ai sensi di tale direttiva (ai sensi degli artt. 13 e 54 della direttiva 2016/680, letti alla luce dell'art. 47 e dell'art. 52, par. 1, della Carta dei diritti fondamentali).[64]

---

[1] L'art. 15 Cost. stabilisce che la limitazione della libertà e segretezza delle comunicazioni «*può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*». In dottrina è prevalsa la tesi che considera come "assoluta" la riserva di giurisdizione disposta dall'art. 15 C. ed esclude la possibilità di desumere, in via interpretativa, l'applicabilità, in questo campo, dei poteri preventivi di polizia, previsti dai precedenti artt. 13 e 14 C., rispetto alla libertà personale e di domicilio. Sul punto: A. PACE, *sub Art. 15*, in *Commentario della Costituzione*, a cura di G. BRANCA, A. PIZZORUSSO, Bologna 1977, p. 106. Secondo M. MAZZIOTTI DI CELSO, *Lezioni di diritto costituzionale*, vol. II, Milano, 1985, p. 261, la previsione costituzionale, oltre alle ordinarie garanzie di riserva di legge e di giurisdizione, imporrebbe che altre garanzie debbano essere istituite dalla legge. Sul tema cfr. anche L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 43 e ss. Sulla portata della riserva *de qua* cfr. V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni*, Milano 1963, passim; C. TROISIO, voce *Corrispondenza (Libertà e segretezza della)*, in *Enciclopedia giuridica*, vol. IX, 1988, p. 80 e ss.; P. CARETTI, voce *Corrispondenza (libertà di)*, in *Digesto discipline pubblicistiche*, vol. IV, 1989, p. 200 e ss. Sul piano della giurisprudenza costituzionale, la sentenza della Corte cost. n. 2 del 12 gennaio 2023, in *cortecostituzionale.it*, specifica che la tutela *ex* art. 15 Cost. si connota per la "riserva di giurisdizione", da intendersi come «*vaglio dell'autorità giurisdizionale (...) associato alla garanzia del contraddittorio, alla possibile contestazione dei presupposti applicativi della misura, della sua eccessività e proporzione, e, in ultima analisi, consente il pieno dispiegarsi allo stesso diritto di difesa*». Con riferimento, invece, alla giurisprudenza sovranazionale, la Corte EDU ha ricondotto sotto il cono di protezione dell'art. 8

CEDU, ove pure si fa riferimento alla "corrispondenza" *tout court*, i messaggi di posta elettronica e la messaggistica istantanea inviata e ricevuta tramite internet; cfr. Corte EDU, 5 settembre 2017, (*Omissis) C. Romania*; par. 72; Corte EDU, 3 aprile 2007*, (Omissis) C. Regno Unito*, par. 41), gli s.m.s.; Corte EDU, 17-dicembre 2020, (*Omissis) C. Norvegia*.

[2] Per tale intendendosi, secondo le classiche definizioni, la comunicazione dotata del carattere della intersoggettività e della attualità: cfr. P. BARILE, E. CHELI*,* voce *Corrispondenza (libertà di)*, in *Enciclopedia del Diritto*, vol. X, Milano 1962, p. 743 ss.

[3] V. GREVI, *Libertà personale dell'imputato e costituzione*, Giuffrè, Milano, 1976, p. 1; ID., voce *Libertà personale dell'imputato*, in *Enc. dir*., XXIV, Giuffrè, Milano, 1974, p. 333. Con specifico riferimento allo *smartphone*, si rimanda a Corte cost., 12 gennaio 2023, n. 2, in, con nota di F. LOSURDO, *Nucleo essenziale della libertà di comunicazione e riserva di giurisdizione. Esiste un "diritto al mezzo"?* in *Giurisprudenza costituzionale*, 2023, p. 18. La Corte afferma che privare una persona del telefono cellulare equivale, data la "*universale diffusione attuale dello strumento*", a intaccare il "nucleo essenziale" del diritto fondamentale garantito dall'art. 15 Cost. Il primario rilievo assunto dal telefono cellulare nella sfera comunicativa della persona fa sì, in altri termini, che la limitazione del mezzo si converta in una limitazione del diritto fondamentale.

[4] Il concetto di "libertà" si è estesa sino a ricomprendere gli oggetti che abitualmente sono portati sulla persona (come portafogli, portamonete etc.) o ad immediato contatto con essa (come borse, borselli e borsette); cfr. Corte cost., 25 marzo 1987, n. 88, in https://giurcost.org/decisioni/1987/0088s-87.html

[5] P. TROISI, *Le investigazioni digitali sotto copertura*, Cacucci, Bari, 2022, p. 15 et 42.

[6] Si intende la Sezione V del Titolo XII del Libro II del Codice penale, dedicata appunto ai delitti contro la inviolabilità dei segreti (cfr. artt. 616-623-*ter* c.p.).

[7] Legge n. 48 del 18 maggio 2008, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001. La Convenzione impone le cautele necessarie per l'acquisizione e poi l'incorporazione e conservazione genuina delle cd. prove digitali attraverso cinque le garanzie: 1) il dovere di conservare inalterato il dato informatico originale nella sua genuinità (garanzia prevista oggi per le ispezioni e perquisizioni, anche della P.G., negli artt. 244, co.2, 247,

co.1-bis, 352, co.1-bis, 354, co.2, c.p.p.); 2) il dovere di impedire l'alterazione successiva del dato originale (garanzia prevista oggi per le ispezioni e perquisizioni, anche della P.G., negli artt. 244, co.2, 247, co.1-bis, 352, co.1-bis, 354, co.2, c.p.p.); 3) il dovere di formare una copia che assicuri la conformità del dato informatico acquisito all'originale (oggi negli artt. 354, co.2, 354-bis c.p.p., solo però per il sequestro dell'A.G. presso i fornitori di servizi e non presso altri come ad esempio le banche, e si prescrive anche che il supporto deve essere "adeguato"); 4) il dovere di assicurare la non modificabilità della copia del documento informatico (la c.d. catena di custodia, oggi previsto nell'art. 254-*bis* c.p.p. e quindi non per tutti i tipi di sequestro); 5) la garanzia dell'installazione di sigilli informatici sui documenti acquisiti (c.d. *hash*, previsto dall'art. 260 c.p.p. ma come facoltativa per il sequestro). Per un approfondimento sulle modifiche apportate dalla legge n.48/2008 cfr. G. CORASANITI, G. CORRIAS LUCENTE (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Pacini, 2009; v. anche L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Diritto penale e processo*, 6, 2008.

[8] Con particolare riguardo al sequestro di apparati informatici, così si esprime A. CHELO, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in *Questa rivista*, n.1, 2024, p.29: «*Del tutto assente, più che inadeguata, può oggi definirsi la disciplina processuale relativa al sequestro di apparecchiature elettroniche/informatiche, vieppiù quelle utilizzate per le comunicazioni come* smartphone, tablet e computer*. Non si sta esagerando per enfatizzare un concetto: ci si sta limitando a descrivere lo stato dell'arte, avuto riguardo agli strumenti processuali disponibili e all'attuale rilevanza che i dispositivi in questione rivestono nella vita di ogni giorno, con conseguente* vulnus *alla sfera della* privacy *individuale talvolta al di fuori da ogni legittima proporzione*». Sul punto si v. ancora ID, S*equestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma,* in *Diritto penale e processo*, 2022, p. 1583 e ss.

[9] L. COMOGLIO, *L'inutilizzabilità 'assoluta' delle prove incostituzionali*, in *Rivista di diritto processuale,* 2011, p. 30.

[10] Cass. pen., Sez. VI, n. 1822 del 17 gennaio 2020. In particolare, riteneva la Suprema Corte che, ai messaggi *WhatsApp* e SMS, rinvenuti in un telefono cellulare sottoposto a sequestro, non fosse applicabile la disciplina dettata dall'art. 254 c.p.p., non rientrando tali testi nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito; Cass. pen., Sez. III, n. 928 del 25 novembre 2015, tutte in *CED Cassazione.*

[11] Sempre in tema di messagistica *WhatsApp* e della legittimità della sua acquisizione mediante mera

riproduzione fotografica, si veda anche: Cass. pen., Sez. VI, n. 22417 del 16 marzo 2022; Cass. pen., Sez. V, n. 1822 del 21 novembre 2017; Cass. pen., Sez. VI, n. 1822 del 12 novembre 2019, tutte in *CED Cassazione.*

[12] Cass. pen., Sez. V, n. 24824 dell'8 giugno 2023, in *CED Cassazione.* Cfr. anche Cass. pen., Sez. VI, n. 38678 del 21 settembre 2023 in *CED Cassazione,* nella quale si specifica, in tema di prove penali, come i messaggi *WhatsApp* e gli sms, rinvenuti nella memoria di un telefono cellulare, e prodotti *ex* art 234 c.p.p., possono essere utilizzati per fondare un giudizio di condanna, senza che il giudice abbia l'obbligo di giustificarne l'utilizzo, salvo che sulla loro acquisizione od utilizzabilità vi sia contestazione.

[13] In proposito si v. anche Cass. pen., Sez. VI, n. 22417 del 16 marzo 2022; Sez. VI, n. 1822 del 12 novembre 2019, tutte in *CED Cassazione*.

[14] Cass. pen., Sez. V, n. 2658 del 6 ottobre 2021 in *CED Cassazione*.

[15] Corte cost., sentenza n. 170 del 27 luglio 2023, in *www.cortecostituzionale.it* . Il caso, come noto, trae origine dal conflitto di attribuzioni tra poteri dello Stato, sollevato dal Senato della Repubblica nei confronti della Procura della Repubblica presso il Tribunale ordinario di Firenze, in merito alla acquisizione di plurime comunicazioni del senatore Matteo Renzi, disposta dalla Procura del capoluogo toscano, nell'ambito del procedimento penale a carico dello stesso senatore e di altri soggetti, in assenza di una previa autorizzazione da parte del Senato.

[16] Nel medesimo senso si veda anche Corte cost., sentenza n. 20 del 24 gennaio 2017; già in precedenza, con riguardo agli apparecchi ricetrasmittenti di debole potenza; Corte cost., sentenza n. 1030 del 15 novembre 1988. Sulla libertà del titolare del diritto di scegliere liberamente il mezzo con cui corrispondere, cfr. Corte cost., sentenza n. 81 dell'11 marzo 1993, tutte in *cortecostituzionale.it*.

[17] Corte cost., sentenza n. 170 del 27 luglio 2023, *par. 4.2* del *Considerato in diritto*, in *cortecostituzionale.it.*

[18] Cfr. M. BORGOBELLO, I*l concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale*, in *Giurisprudenza penale*, 7-8, 2023; L. FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*, in *Penale Diritto e Procedura (web)*, 6 settembre 2023; A. CHELO, *Davvero legittimo il sequestro di messaggi* 'e mail' *e* 'WhatsApp' *già letti?* in *Giurisprudenza costituzionale*, 4, 2023; S. CURRERI, *La Consulta sui casi Renzi e Ferri: un passo avanti sull'art. 15 Cost. e uno indietro sull'art. 68, comma 3, Cost*., in *Quaderni*

costituzionali, 4, 2023, p. 887; D. CURTOTTI, *La sentenza costituzionale n. 170 del 2023 e le comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2023; N. D'ANZA, *La Corte costituzionale estende ai soggetti non parlamentari l'immunità di cui all'art. 68, comma 3, Cost. con riguardo alla corrispondenza scambiata con membri del Parlamento*, in *Forum costituzionale*, 2023; F.R. DINACCI, *I modi acquisitivi della messaggistica* chat *o* e-mail*: verso letture rispettose dei principi*, in *Archivio penale*, 1, 2024; C. FONTANI, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza,* in *Diritto penale e processo*, 10, 2023, p. 1312; G. GUZZETTA, *La nozione di comunicazione e altre importanti precisazioni della Corte costituzionale sull'art. 15 della Costituzione nella sentenza n. 170 del 2023*, in *Federalismi*, 21, 2023; A. IACOVIELLO, *I riflessi della sentenza n. 170/2023 della Corte costituzionale sulle procedure per il sequestro della corrispondenza elettronica e delle comunicazioni archiviate su dispositivi di tipo informatico e telematico*, in *Nomos. Le attualità nel diritto*, 1, 2024; L. LUPÀRIA DONATI, F. CERQUA, *La versione della Consulta sulla corrispondenza elettronica. Un* bouleversement *in materia di prova digitale?* in *Diritto dell'informazione e dell'informatica*, 4-5, 2023; M.T. MORCELLA, *Ed ora, come si può apprendere la corrispondenza archiviata?* in *Giurisprudenza italiana*, 2024; V. ZENO ZENCOVIC, *La "corrispondenza digitale": notazioni comparate da oltre-Atlantico*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2023. Cfr. da ultimo L. TOMBELLI, *La tutela della corrispondenza tra atipicità della prova e tentativi di riforma,* in *Penale. Diritto e procedura*, 16 gennaio 2025.

[19] Cass. pen., Sez. VI, n. 31180 del 30 luglio 2024, in *CED Cassazione.*

[20] Cass. pen., Sez. VI, n. 38460 del 27 ottobre 2021, in *Quotidiano giuridico*, afferma che: «*… è illegittimo, per violazione del principio di proporzionalità ed adeguatezza, il sequestro a fini probatori di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione dei relativi criteri*».

[21] Cass. pen., Sez. II, n. 17604 del 27 aprile 2023, in *CED Cassazione*: «*…in tema di sequestro probatorio avente ad oggetto dispositivi informatici o telematici, la finalizzazione dell'ablazione del supporto alla sua successiva analisi, strumentale all'identificazione e all'estrazione dei dati rilevanti per le indagini, implica che la protrazione del vincolo, nel rispetto dei principi di proporzionalità e di adeguatezza, debba essere limitata al tempo necessario all'espletamento delle operazioni tecniche, dovendosi, tuttavia, valutare la sua ragionevole durata in rapporto alle difficoltà tecniche di apprensione dei dati, da ritenersi accresciute nel caso di mancata collaborazione dell'indagato che non fornisca le chiavi di accesso alle banche dati contenute nei supporti sequestrati*». Allo stesso modo si v. Cass. pen., Sez. II, n. 50009 del 15 dicembre 2023, in *www.processopenaleegiustizia.it*, secondo cui, sempre in tema di sequestro probatorio di dispositivi informatici o telematici, «*l'estrazione di copia integrale dei dati in essi contenuti, che consente la restituzione del dispositivo, non legittima il trattenimento della totalità delle*

informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede. Il pubblico ministero è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano sequestrati a persone estranee al reato, e provvedere, all'esito, alla restituzione della copia integrale agli aventi diritto». In precedenza, nello stesso senso, cfr. Cass. pen., Sez. VI, n. 13156 del 4 marzo 2020, inedita, in *CED Cassazione*, secondo cui la c.d. copia integrale costituisce solo una copia-mezzo, cioè una copia che consente di restituire il contenitore, ma che non legittima affatto il trattenimento dell'insieme di dati appresi. Da ultimo si v. pure Cass. pen., Sez. VI, n. 222 del 03 gennaio 2024, in *CED Cassazione:* «*l'acquisizione indiscriminata di un'intera categoria di beni, nell'ambito della quale procedere successivamente alla selezione delle singole res strumentali all'accertamento del reato, è consentita a condizione che il sequestro non assuma una valenza meramente esplorativa e che il pubblico ministero adotti una motivazione che espliciti le ragioni per cui è necessario disporre un sequestro esteso e onnicomprensivo, in ragione del tipo di reato per cui si procede, della condotta e del ruolo attribuiti alla persona titolare dei beni, e della difficoltà di individuare ex ante l'oggetto del sequestro*». Sul sequestro probatorio del *personal computer* cfr., anche Cass. pen., Sez. I, n. 2744 del 23 gennaio 2025 in *www.deiustitia.it* con cui la Corte ribadisce il divieto di acquisizione indiscriminata – in difetto di specifiche ragioni – del pc contenente una massa indifferenziata di dati informatici.

[22] Cass. pen. Sez. VI, n. 44010 del 18 novembre 2022, in *leggiditalia.it*afferma: «*nel caso di sequestro di un apparato informatico complesso, quale quello costituito da un telefono cellulare e dalla relativa memoria, deve aversi riguardo, in vista di un adeguato contemperamento delle opposte esigenze, sia alla possibilità di verificare il contenuto a fini di indagini, secondo precise direttrici, sia alla necessità di rispettare il principio di proporzionalità, da intendersi non solo in senso quantitativo, in relazione alla messe di dati, ma anche in senso temporale. Deve infatti valutarsi la possibilità di sottoporre il cellulare ad una rapida duplicazione del contenuto, mediante la creazione di una copia forense, costituente lo strumento per lo svolgimento di ulteriori verifiche, a fronte delle quali l'esigenza della materiale disponibilità del bene sfuma in assenza di specifici elementi di segno contrario, con l'ulteriore conseguenza per cui l'espletamento delle indagini tecniche con creazione di una copia forense costituisce elemento idoneo a far venir meno esigenze di indagine tali da giustificare l'ulteriore mantenimento in sequestro del cellulare e della relativa scheda, in assenza della specifica indicazione di esigenze di segno diverso*».

[23] Cass. pen., Sez. U., n. 23755 del 14 giugno 2024 e Cass. pen., Sez. U., n. 23756 del 14 giugno 2024, entrambe in *CED Cassazione*.

[24] Per un approfondimento cfr., *ex plurimis*, **G. MARRA,** *Le comunicazioni conservate sulle chat sono da considerare corrispondenza. Problematiche attuali e prospettive* **de iure condendo, in** *Giustizia Insieme*, **30 ottobre 2024; M. DANIELE,** *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, **in** *Sistema Penale*, **17 luglio 2024.**

[25] Per l'inclusione del pubblico ministero nella nozione di "autorità giudiziaria" anche nel diritto europeo , cfr. Corte giustizia, Grande Sezione, 08 dicembre 2020, (Omissis), C-584-19: «*L'articolo 1, paragrafo 1, e l'articolo 2, lettera c), della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, deve essere interpretati nel senso che rientra nelle nozioni di «autorità giudiziaria» e di «autorità di emissione», ai sensi delle disposizioni sopra citate, il pubblico ministero di uno Stato membro o, più in generale, la procura di uno Stato membro, indipendentemente dal rapporto di subordinazione legale che potrebbe esistere tra tale pubblico ministero o tale procura e il potere esecutivo di tale Stato membro, e dall'esposizione di detto pubblico ministero o di detta procura al rischio di essere soggetti, direttamente o indirettamente, ad ordini o istruzioni individuali da parte del predetto potere, nell'ambito dell'adozione di un ordine europeo di indagine*».

[26] La vicenda prende le mosse dal ricorso promosso ex art. 311 c.p.p. avverso l'ordinanza del Tribunale del riesame di Napoli, confermativa dell'ordinanza del Gip del Tribunale di Nola, con cui veniva applicata la misura degli arresti domiciliari, nei confronti di un indagato, per i delitti di cui agli artt. 110 e 353 cod. pen., art. 319 cod. pen., artt. 110, 476, 490 cod. pen., artt. 81, 40 cpv., 110 cod. pen. e 21 comma 1 L. n. 646/1982.

[27] L. FILIPPI, *"Mettere il p.m. al suo posto" (ovvero la prova incostituzionale per contempt of court da parte del p.m.*, in *Cassazione Penale*, fasc.11, 2024, 3424 e ss. L'a. parla di un vero e proprio "braccio di ferro" tra il p.m. e il Tribunale

del riesame, il quale, «*investito nuovamente della questione, cedette infine all'ardita tesi dell'organo di accusa che proponeva come indizi di colpevolezza i messaggi acquisiti in esito all' "ispezione informatica*"».

[28] *Ibidem*, p.3424.L'a. – pur definendo la sentenza "apprezzabile" per aver affermato il principio di incostituzionalità della prova assunta *contra sententiam iudicis* - lamenta, tuttavia, una mancata "sensibilità" proprio per gli altri valori costituzionali, di pari rango, lesi nella vicenda dall'iniziativa del p.m., quali, appunto,

la violazione della riserva di legge e la totale elusione del diritto di difesa, oltre al sacrificio della segretezza delle comunicazioni.

[29] Sul tema, v. l'ampio studio di L. ANNUNZIATA, *Questioni probatorie, tra* male captum bene retentum *e* theory of the fruit of the poisonous tree, Pacini editore, Pisa, 2017. V., inoltre, M. PANZAVOLTA, *Contributo allo studio dell'invalidità derivata*, Aras edizioni, Fano, 2012; G. SPANGHER, *'E pur si muove': dal* male captum bene retentum *alle* exclusionary rules, in *Giurisprudenza. costituzionale*, 2001, p. 2821.

[30] Cass. pen., Sez. Un., n. 5021 del 27 marzo 1996. Le Sezioni unite affermarono che il "sequestro conseguente a perquisizione", come recita la rubrica dell'art. 252 c.p.p., presupponeva un vero e proprio rapporto di dipendenza giuridica tra i due mezzi di ricerca della prova e dall'illegittimità della perquisizione, tale da far derivare l'illegittimità del sequestro. Tuttavia, attribuirono, con una argomentazione molto discutibile, effetto sanante al sequestro attraverso il potere-dovere del P.M. di sequestrare il corpo del reato anche a fini probatori. Secondo la Corte era lo stesso ordinamento processuale a considerare del tutto irrilevante il modo con il quale pervenire al sequestro, concludendo che «*convergono nella stessa prospettiva le numerose ed espresse deroghe dall'ordinamento previste in relazione alla disciplina normativa del sequestro del "corpo del reato" (cfr. artt. 235-103-240 c.p.), deroghe tutte riferibili alla necessità primaria di interrompere il protrarsi di una situazione di intrinseca illiceità penale, quando non addirittura la permanenza del reato o gli effetti al reato strettamente connessi*». La conclusione opposta avrebbe condotto all'assurda conseguenza di consentire al giudice la confisca del corpo del reato e, nel contempo, di non tenerne conto ai fini della decisione conclusiva del processo,

[31] Nel solco delle Sezioni Unite, Cass. pen., Sez. II, n. 26819 del 23 aprile 2010; Cass. pen., Sez. II, n. 15784 del 29 marzo 2016 e Cass. pen., Sez. II, n. 15784 del 29 marzo 2017, secondo cui il potere di sequestro non dipende dalle modalità con cui le cose oggettivamente sequestrabili sono state reperite. Per l'affermazione secondo cui la nullità del provvedimento di perquisizione non si trasmette a quello di sequestro delle cose rinvenute nel corso della sua esecuzione, né determina l'inutilizzabilità a fini di prova delle stesse, Cass. pen., Sez. I, n. 23764 del 10 maggio 2011 e Cass. pen., Sez. V, n. 32009 del 12 luglio 2018. Sulla stessa scorta, ancora di recente, si v. Cass. pen., Sez. VI, n. 17437 del 19 marzo 2024; Cass. pen., Sez. II, n. 16065 del 10 gennaio 2020, in *CED Cassazione.* Difforme Cass. pen., Sez. III, n. 50657 dell'8 novembre.2018, in *Diritto.it*. La pronuncia, trattando un caso di perquisizione eseguita senza avviso circa il diritto di assistenza difensiva nonostante la sussistenza di una iscrizione delle persone sottoposte ad indagine ex art. 335 c.p.p., ha riconosciuto che il mancato adempimento ha costituito la violazione di un divieto a tutela del diritto di difesa di chiara pregnanza sostanziale, tale da comportare l'inutilizzabilità patologica di quanto acquisito a seguito

dell'atto. Il finale è dunque nel senso per cui il vizio consistente nella violazione di norme processuali determina la 'illegittimità derivata' della attività 'istruttoria' di seguito espletata, con l'effetto della invalidità del sequestro probatorio. In tema, A. CABIALE, *L'inutilizzabilità 'derivata': un mito a mezza via fra nullità ed esigenze sostanziali*, in *Diritto penale contemporaneo* – Riv. trim., n.4, 2013, p. 112; cfr. anche N. GALANTINI, *L'inutilizzabilità effettiva della prova tra tassatività e proporzionalità,* in *Diritto Penale Contemporaneo - DPC,* 1, 2019, p.67-68.

[32] In proposito la sentenza richiama il precedente di Cass. pen., Sez. VI, n. 34088 del 7 luglio 2003, in *CED Cassazione.*

[33] In questi termini si esprime ad esempio L. FILIPPI, *Quando il PM tenta di eludere l'inutilizzabilità dichiarata dal giudice,* in *www.altalex.it, 26 agosto 2024:* «*Il principio di diritto affermato dalla sentenza è rivoluzionario e travolge il consolidato brocardo* male captum, bene retentum. *Infatti, non vi è alcuna sostanziale differenza tra la fattispecie ora esaminata e quella che fu oggetto della pronuncia S. delle Sezioni unite: in quest'ultima la perquisizione fu dichiarata illegittima perché eseguita in difetto dei presupposti indicati dall'art. 103, comma 3, D.P.R. n. 309/1990, così come nella fattispecie ora esaminata il Tribunale del riesame aveva annullato - per carenza di motivazione - il sequestro probatorio del cellulare dell'indagato. In entrambe le fattispecie, quindi, vi è un* vulnus *alla giurisdizione, o, come si esprime la sentenza in commento, una "violazione del provvedimento giurisdizionale cui è conseguita una illegittima violazione della sfera di riservatezza al di fuori dei presupposti declinati dall'art. 15 Cost.". È vero che nel "caso S." si trattava della detenzione illegittima di 31 grammi di cocaina, che rendeva obbligatorio il sequestro del corpo del reato, mentre nella fattispecie ora all'esame della Corte oggetto del sequestro erano alcuni telefoni cellulari, ma in quest'ultimo caso, a differenza del primo, è in gioco la compressione di un valore costituzionale, il che rende di per sé "incostituzionale" la prova. Pertanto, è stato affermato un nuovo principio di diritto che cozza contro la consolidata giurisprudenza della Corte e impone un nuovo intervento delle Sezioni unite per riconoscere non solo il primato del giudice sul pubblico ministero ma anche l'"inviolabilità" della libertà e segretezza della corrispondenza e delle comunicazioni*»; dello stesso autore v. anche *"Mettere il p.m. al suo posto" (ovvero la prova incostituzionale per* contempt of court *da parte del p.m.*, cit.

[34] Per un approfondimento sulla categoria concettuale della prova incostituzionale cfr. L. TOMBELLI, *La tutela della corrispondenza tra atipicità della prova e tentativi di riforma*, *in Penale. Diritto e Procedura*, 16 Gennaio 2025, p.12-14.

[35] Cfr. Corte cost., sentenza n. 34 del 4 aprile 1973, in *cortecostituzionale.it*: «*Nel nostro ordinamento vige il*

principio secondo il quale le attività compiute in dispregio dei fondamentali diritti del cittadino garantiti dalla Costituzione non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito». Sulla sentenza n. 34/1973 v. V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giurisprudenza costituzionale*, 1974, p. 317.

[36] Cass. pen., Sez. VI, n. 31180 del 30 luglio 2024, in *CED Cassazione*. Sulla stessa linea va citata la recente Cass. pen., Sez. VI, n. 15836 dell'11 gennaio 2023, in *CED Cassazione,* 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 2003, n. 196, in quanto prove lesive del diritto alla segretezza delle comunicazioni costituzionalmente tutelato e, pertanto, affette da inutilizzabilità patologica, non sanata dalla richiesta di definizione del giudizio con le forme del rito alternativo.

[37] Cass. pen., Sez. VI, n. 31180 del 30 luglio 2024, in *CED Cassazione.*

[38] Si v. in particolare, Cass. pen., Sez. Un., n. 16 del 21 giugno 2000; Cass. pen., Sez. IV, n. 31304 del 18 maggio 2005; Cass. pen., Sez. III, n. 44926 del 27 settembre 2023, tutte *in CED Cassazione*, secondo cui il giudice non può valutare, né porre a fondamento della decisione, gli atti probatori viziati da nullità o inutilizzabilità assolute, non risultando derogato il principio della rilevabilità di ufficio, nonché della insanabilità di queste situazioni patologiche, né espressamente né implicitamente, da alcuna norma. Il giudice, pertanto, fatta eccezione per i casi di inutilizzabilità "fisiologica" prevista solo per il dibattimento, non può utilizzare prove affette da inutilizzabilità "patologica"', quella cioè inerenti agli atti probatori assunti *contro legem*, il cui impiego è vietato, in modo assoluto, dall'articolo 191 c.p.p.

[39] Cass. pen., Sez. VI, n. 39548 dell'11 settembre 2024, Rv. 287039.

[40] Cass. Pen., Sez. VI, n. 1269 del 13 gennaio 2025, in www.processopenaleegiustizia.it. Il caso vedeva l'indagato per spaccio di sostanze stupefacenti, incriminato anche grazie al ricorso agli screenshot dei messaggi WhatsApp, acquisiti dalla polizia nel corso di un controllo dell'indagato, dopo aver acquisito il suo consenso all'utilizzo dello *smartphone* e ottenuto il codice di accesso, comunicato dallo stesso imputato, senza avvisarlo della facoltà di farsi assistere da un difensore né della necessità del suo consenso. utilizzati a

suo carico ma inutilizzabili in quanto acquisiti senza il rispetto delle forme previste dagli artt. 253 e 254 c.p.p.

[41] Cass. Pen., Sez. V, n. 8376 del 28 febbraio 2025 in *Giurisprudenza Penale web*, 4, 2025 secondo cui ciò che rileva è che il pubblico ministero adotti una motivazione che espliciti le ragioni per cui è necessario disporre il sequestro, in ragione del tipo di reato per cui si procede, della condotta e del ruolo attribuiti alla persona titolare dei beni, e della difficoltà di individuare *ex ante*, in maniera più specifica, l'oggetto del sequestro. Con commento di L. FILIPPI, *Ma davvero per il sequestro della corrispondenza basta il decreto del P.M.?* in Giurisprudenza penale, 2 aprile 2025. L'a. non condivide l'affermazione, contenuta in sentenza, secondo cui il sintagma «autorità giudiziaria» indica una categoria in cui sono compresi sia il giudice che il Pubblico ministero. Infatti, è vero che il Pubblico ministero è "autorità giudiziaria", ma il garante delle libertà fondamentali è il giudice, come riconosce anche la Corte costituzionale, e non il Pubblico ministero, che è pur sempre una parte, anche se pubblica.

[42] A. PACE, *Problematica delle libertà costituzionali,* vol. II, Padova, Cedam, 1992, 241ss. L'a. interpreta le "garanzie" nel senso che la previsione legislativa debba accompagnare all'individuazione dei casi e modi (art. 13 Cost.) le garanzie tecniche e giuridiche idonee a limitare l'esercizio della libertà fondamentale e tutelare i protagonisti del rapporto comunicativo. In tal senso anche la giurisprudenza della stessa Corte costituzionale che definisce le "garanzie" con le procedure, le modalità e i tempi che compete al legislatore prevedere, nel rispetto della riserva di legge prevista dalla Costituzione; cfr. Corte cost., sentenza n.3 del 19 gennaio 2023, in www.astrid-online.it. Sull'art.15 Cost. in generale Cfr.: F. DONATI*, Art.15,* in *Commentario della Costituzione,* a cura DI R. BIFULCO, A. CELOTTO, M. OLIVETTI, vol. I, Torino, Utet, 2006, 362 e ss.; G. M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza,* in *I diritti costituzionali,* vol. II, a cura di R. NANIA, P. RIDOLA, Torino, Giappichelli, 2006, p. 617 e ss.; A. VALASTRO, *Libertà di comunicazione e nuove tecnologie,* Milano, Giuffrè, 2001; A. PACE, *Art. 15,* in *Commentario della Costituzione,* a cura di G. BRANCA, A. PIZZORUSSO, Bologna – Roma, Zanichelli, 1977; P. CARETTI, voce *Corrispondenza (libertà di),* in *Dig. disc. Pubbl.,* vol. IV, Torino, Utet, 1989, p.200 e ss.; C. TROISIO, voce *Corrispondenza (Libertà e segretezza della),* in *Enc. Dir.,* vol. IX, Roma, Istituto dell'enciclopedia italiana, 1988, p.80 e ss.; V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* Milano, Giuffrè, 1963; P. BARILE, E. CHELI, voce *Corrispondenza (libertà di),* in *Enc. Dir.,* vol. X, Milano, Giuffrè, 1962, p.743 e ss.

[43] Atto Senato n. 806, XIX legislatura, d'iniziativa dei senatori Zanettin e Bongiorno, comunicato alla presidenza il 19 luglio 2023, recante «*Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici,* smartphone *e memorie digitali*», approvato con il nuovo titolo «*Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie*

digitali» in https://www.senato.it/leg/19/BGT/Schede/Ddliter/57327.htm Per un approfondimento del disegno di legge cfr. O. MURRO, S*equestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del D.D.L. A.S. n. 806*, in *Questa rivista,* 12 marzo 2024.

[44] Atto Senato n. 690, XIX legislatura, d'iniziativa del senatore Scarpinato, comunicato alla presidenza il 9 maggio 2023, relativo alla «*Introduzione dell'articolo 254-ter del codice di procedura penale recante norme in materia di sequestro di strumenti elettronici*» in www.senato.it. Per un'analisi comparativa dei due progetti di legge v. A. CHELO, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, cit.

[45] Atto Camera n.1822, XIX legislatura, relatore Andrea Pellicini, relativo a "*Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali*" con esame iniziato il 9 aprile 2025, in www.camera.it.

[46] L. TOMBELLI*, La tutela della corrispondenza tra atipicità della prova e tentativi di riforma*, cit. p.22.

[47] L'originaria scelta di autorizzazione al sequestro del PM non convinceva in quanto appariva in contrasto con l'art 3 Cost., laddove, a seguito del nuovo art. 132 d.lgs. 30 giugno 2003, n. 196, cd. "codice della privacy", così come modificato dal d.l. 30 settembre 2021, n. 132, convertito dalla l. n. 178/ 2021, ha stabilito, a differenza che in passato, che i dati di traffico telefonico e telematico per fini di indagine penali siano acquisiti, solo «*previa autorizzazione rilasciata dal giudice con decreto motivato*». Pertanto non si comprendeva perché mentre l'acquisizione dei "dati esterni alle comunicazioni" richiedesse una riserva di giurisdizione piena, l'acquisizione del "contenuto delle comunicazioni" (come nel caso del sequestro) dovesse accontentarsi dell'autorizzazione del pubblico ministero. Sulla riforma della disciplina di acquisizione dei tabulati telefonici cfr. F. RINALDINI, La *nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza Penale,* 16 ottobre 2021.

[48] O. MURRO, S*equestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del D.D.L. A.S. n. 806*, cit.,p.4

[49] La duplicazione, a differenza della semplice formazione di copia dei file contenuti nella memoria, determina la formazione di un duplicato dei singoli file contenuti nella memoria, ovvero di tutte le zone del disco scritto, anche quelle che non contengono alcun file direttamente visibile all'utente, definite tecnicamente aree non allocate, senza riorganizzazione o compressione di quanto scritto. In questo modo è

possibile il recupero anche di file cancellati o di informazioni ormai non più disponibili all'utilizzatore del sistema.

[50] Tra l'avviso (che deve avvenire entro cinque giorni dal deposito del verbale di sequestro) e la data fissata per il conferimento dell'incarico non può intercorrere, infatti, un termine superiore a dieci giorni.

[51] In tale contesto, entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero avvisa le parti e i difensori del giorno, dell'ora e luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici, nonché dei dati, delle informazioni o dei programmi accessibili da remoto dal dispositivo in sequestro. Le parti sono avvisate della facoltà di nominare consulenti tecnici, con espresso richiamo alla sola disposizione di cui all'art. 364, comma 2, c.p.p.

[52] O. MURRO, S*equestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? Brevi note a margine del D.D.L. A.S. n. 806*, cit.,p.5.

[53] S. DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema Penale*, 8 marzo 2024, p.3. L'a., tracciando la distinzione con *screenshot* delle *chat* o di *files* (video, foto…), che non sostituisce la prova digitale, sottolinea come il documento informatico, in quanto dematerializzato, ovvero esistente a prescindere dal suo supporto e agevolmente trasferibile, è facilmente alterabile e dunque fragile. Si pensi ai casi di apparecchio acceso, specie con software Android: l'accesso al sistema per effettuare la copia potrebbe produrre alterazioni in grado di inficiare la genuinità dei dati utente in esso contenuto. Sul trattamento della prova digitale cfr. anche, tra gli altri, L. CUOMO, *La prova digitale*, in G. CANZIO E L. LUPARIA DONATI (a cura di), *Prova scientifica e processo penale,* Cedam, Padova, 2022, p.623 ss

[54] Ciò avviene: a) nei procedimenti di cui agli articoli 406, comma 5-*bis* (si tratta dei procedimenti per taluno dei delitti indicati nell'articolo 51, comma 3-*bis* e nell'articolo 407, comma 2, lett. a), nn.2 e 7-*bis)* e 371-*bis,* comma 4-*bis* (si tratta dei procedimenti per i delitti di cui agli articoli 615-ter, terzo comma, 635-*ter* e 635-*quinquies* c.p. nonché quando i fatti sono commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, in relazione ai procedimenti per i delitti di cui agli articoli 617-*quate*r, 617-quinquies e 617-*sexies* c.p.); b) quando sussiste un pericolo per la vita o l'incolumità di una persona o la sicurezza dello Stato, ovvero un pericolo di concreto pregiudizio per le indagini in corso, o un pericolo attuale di cancellazione o dispersione dei dati, delle informazioni o dei programmi.

[55] Il P.M., nel caso di dati aventi contenuto non comunicativo, dispone il sequestro dei dati strettamente pertinenti al reato, in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta e, comunque, nel rispetto dei criteri di necessità e proporzione (art.12 Emendamento al Disegno di Legge N. 806)

[56] S. De Flammineis, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sistema penale*, 2024.

[57] Sul punto cfr. la Relazione di G. CANZIO alla Commissione Giustizia del Senato della Repubblica del 20 febbraio 2024, in www.senato.it.

[58] CHELO A., *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, cit., p. 12.

[59] Cfr. le già citate Cass. pen., Sez. VI, n. 38460 del 27 ottobre 2021; Cass. pen., Sez. II, n. 17604 del 17 aprile 2023 entrambe in https://simpliciter.ai/.

[60] Unione Camere penali italiane,*DDL 806 "Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali*", Commissione Giustizia Senato, Audizione 20 febbraio 2024 in www.camerepenali.it, p.2.

[61] Unione Camere penali italiane, *ibidem,* p.3.

[62] CHELO A., *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, cit., p.13.

[63] Così Cass. pen., Sez. VI, n. 34265 del 22 settembre 2020, in *www.sistemapenale.it*.

[64] Corte giust. U.E. (Grande Camera), 4.10.2024, causa C- 548/2. La pronuncia, in particolare, ha concluso che «*non osta a una normativa nazionale che concede alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, a fini di prevenzione, ricerca, accertamento e perseguimento di reati in generale, se tale normativa: definisce in modo sufficientemente preciso la natura o le categorie dei reati in questione, garantisce il rispetto del principio di proporzionalità, e subordina l'esercizio di tale possibilità, salvo in casi di urgenza debitamente comprovati, ad un controllo preventivo di un giudice o di un organo amministrativo*

indipendente».