

Ma davvero per il sequestro della corrispondenza basta il decreto del P.M.?

di **Leonardo Filippi**

Sommario. 1. La vicenda processuale. – 2. Motivi della decisione. - 3. Osservazioni critiche.

1. La vicenda processuale.

Il Tribunale del riesame aveva rigettato la richiesta di riesame avverso il decreto di perquisizione e sequestro emesso dalla Procura della Repubblica per i delitti di bancarotta fraudolenta patrimoniale e truffa ai danni dello Stato.

Avverso il provvedimento di rigetto, l'indagato aveva proposto ricorso per cassazione, deducendo, tra l'altro, la nullità del sequestro per mancanza di convalida da parte del giudice in violazione dell'art. 355, comma 2, c.p.p. In ordine a tale censura, già avanzata in sede di riesame sul presupposto della genericità del decreto di perquisizione e sequestro, il Tribunale aveva evidenziato come la stessa fosse inammissibile, oltre che destituita di fondamento, in quanto la Procura della Repubblica avrebbe pedissequamente descritto l'oggetto del sequestro e avrebbe individuato tempo e ragioni per le quali si rendeva necessaria la temporanea apprensione dei supporti o strumenti informatici per l'estrazione di copia forense dei contenuti.

Il ricorrente aveva dedotto, invece, che il Pubblico ministero, ex art. 247, c. p. p., avrebbe disposto la perquisizione e sequestro dei supporti informatici con un'indicazione generica. A conferma della necessità della convalida del sequestro da parte del G.I.P., si osserva che recentemente la Corte di giustizia dell'Unione europea, nella causa C-548/21, ha affermato che l'accesso ai dati dei telefoni cellulari deve essere subordinata ad un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente, salvo i casi di urgenza debitamente comprovati.

2. Motivi della decisione.

La sentenza premette che la Suprema Corte, in tema di sequestro probatorio, ha già avuto modo di osservare che l'attività della polizia giudiziaria non necessita di convalida nel caso in cui il decreto del Pubblico ministero disponga, senza ulteriori specificazioni, l'ablazione di dispositivi informatici in uso all'indagato, in quanto, trattandosi di beni correlati alla tipologia del reato per cui si procede, l'indicazione non lascia spazio alla discrezionalità degli operanti (Sez. V, 15.9.2022, n. 38219, Rv. 283800 – 01). Secondo la giurisprudenza, 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. La motivazione deve, cioè, essere 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. In relazione ad un *computer* o altro dispositivo informatico o elettronico, il cui ampio contenuto non è conoscibile preventivamente, il criterio di selezione non può che essere quello della pertinenzialità del dato rispetto al reato ipotizzato ed è pertanto sufficiente che emerga l'ambito – circoscritto – entro il quale deve eseguirsi il sequestro.

Secondo la sentenza, nel caso di specie, non potrebbe giungersi a conclusione diversa dal momento che, come si evince dalla mera lettura del provvedimento impugnato, questo ha descritto l'oggetto del sequestro e individuato tempi e ragioni per le quali si rendeva necessaria la temporanea apprensione dei supporti o strumenti informatici per l'estrazione di copia forense dei contenuti, indicando anche i criteri di selezione. Esso ha, in particolare, precisato le finalità della perquisizione e sequestro, evidenziando che si tratta di ricostruire la vicenda criminosa che si va delineando, segnatamente le modalità di consumazione delle condotte distrattive e di frode, i rapporti tra tutte le parti coinvolte e, in particolare, tra gli amministratori della società e i soggetti che risultano formalmente legali rappresentanti delle società affittuarie all'atto della sottoscrizione dei contratti, gli accordi intercorsi tra gli stessi nelle fasi immediatamente precedenti e successive alla stipula dei contratti di affitto, nonché le comunicazioni, anche mediante strumenti di messaggistica, intercorse tra le medesime parti durante lo svolgersi della procedura di concordato preventiva, tuttora in corso anche a seguito delle relazioni dei commissari giudiziali.

Tali specifiche finalità, unitamente ai criteri dettati per la selezione dei contenuti da porre in sequestro, strettamente connessi alle prime e alla tipologia delle condotte che si reputano già venute in evidenza, consentono di ritenere che il provvedimento del Pubblico ministero non sia affatto generico e non lasci spazio alla discrezionalità degli operanti che devono eseguirlo.

Relativamente, invece, alla necessità della convalida da parte del giudice alla stregua della sentenza della Corte di giustizia U.E. citata nel ricorso (Grande Camera, 4.10.2024, causa C-548/21), la sentenza precisa che tale pronuncia 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". Secondo la Corte, tale ente amministrativo autonomo è certamente individuabile,

quanto all'ordinamento italiano, nella figura del Pubblico ministero, quale autorità giudiziaria che nell'esercizio delle sue funzioni pubbliche procede alle indagini secondo le specifiche regole dettate dal legislatore idonee a garantire anche i diritti dell'indagato.

Rimane solo da precisare che, essendo il sequestro delegato alla polizia giudiziaria con un legittimo provvedimento autorizzativo del Pubblico ministero di perquisizione e sequestro, la sentenza esclude che nella fattispecie in esame assuma rilievo quanto affermato dalla Corte costituzionale con la sentenza n. 170 del 2023 e dalla Suprema Corte a seguito di tale sentenza. Com'è noto, il Giudice delle leggi ha chiarito che «lo scambio di messaggi elettronici – *e-mail*, *SMS*, *WhatsApp* e simili – rappresenta, di per sé, una forma di corrispondenza», e ciò anche nel caso in cui si tratti di messaggi già ricevuti e letti dal destinatario, con l'unica eccezione che, in ragione del tempo trascorso, il messaggio non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico". La suprema Corte, facendo tesoro delle chiare indicazioni della Consulta, ha abbandonato l'orientamento precedente ed ha affermato che i messaggi di posta elettronica, i messaggi *WhatsApp* e gli *SMS* conservati nella memoria di un dispositivo elettronico costituiscono corrispondenza anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo o per altra causa, essi non abbiano perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico", sicché, fino a quel momento, la loro acquisizione deve avvenire secondo le forme previste dall'art. 254 c. p. p. per il sequestro della corrispondenza (Sez. II, 15.5.2024, n. 25549, Rv. 286467) ovvero, quanto al sequestro in questione, con decreto motivato del Pubblico ministero (da ultimo, Sez. VI, 11.9.2024, n. 39548, Rv. 287039 – 01, che ha affermato che in tema di mezzi di prova, sono affetti da inutilizzabilità patologica, in considerazione della loro natura di corrispondenza, i messaggi *WhatsApp* 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).

Tale conclusione è stata condivisa anche dalle Sezioni unite penali, che, risolvendo un contrasto in tema di Ordine europeo di indagine, oltre ad abbracciare le indicazioni della Corte costituzionale sulla nozione di corrispondenza, hanno chiarito che la tutela prevista dall'art. 15 Cost. non richiede che per la limitazione della libertà e segretezza della corrispondenza e, dunque, per la sua acquisizione ad un procedimento penale, sia necessario un provvedimento del giudice (Sez. Un., 29.2.2024, n. 23756, Giorgi, in motivazione, par. 14.2; Sez. Un., 29.2.2024, n. 23755, Gjuzi, in motivazione, par. 11.2).

Ciò in quanto, come emerge anche dalla giurisprudenza della Corte di giustizia (cfr. Corte giust. U.E., 8.12.2020, *Staatsanwaltschaft Wien*, C584/19), il sintagma «autorità giudiziaria» indica una categoria in cui sono compresi sia il giudice che il Pubblico ministero. Di conseguenza, anche sotto tale profilo, alla stregua delle

ulteriori considerazioni di recente sviluppate nella giurisprudenza di legittimità, la sentenza conclude per la non necessarietà del provvedimento di un giudice ai fini del sequestro di dati informatici assimilabili al concetto di corrispondenza – e alla sufficienza, invece, di un provvedimento dispositivo del Pubblico ministero – che nel caso di specie sussiste e, per le ragioni suesposte, presenta contenuti idonei a supportare ciò che è stato poi acquisito in sede di esecuzione da parte della polizia giudiziaria, sicché non necessitava nemmeno alcun provvedimento successivo di convalida né da parte di un giudice né da parte del Pubblico ministero.

3. Osservazioni critiche.

Le argomentazioni svolte nella sentenza in esame non convincono.

Infatti, la materia della corrispondenza è presidiata dall'art. 15 Cost. e quindi dalla doppia riserva di legge e di giurisdizione.

Come si è già detto, la Corte costituzionale ha chiarito che mantengono “la natura di corrispondenza anche i messaggi di posta elettronica e *WhatsApp* già ricevuti e letti dal destinatario, ma conservati nella memoria dei dispositivi elettronici del destinatario stesso o del mittente” (Corte cost. n. 170/2023). Anche la Corte giust. U.E. ha affermato la necessità dell'autorizzazione del giudice o di un'autorità amministrativa indipendente per accedere ai dati contenuti in un telefono cellulare, nonché dell'altrettanto indispensabilità dell'informazione alla persona interessata del tentativo di accedere a tali dati. Infatti la Grande Camera ha affermato che l'art. 4, par. 1, lett. c), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, accertamento, indagine e perseguimento di reati o di esecuzione di sanzioni penali, e alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio, letto alla luce degli artt. 7 e 8, nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che non si oppone a una normativa nazionale che concede alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, a fini di prevenzione, accertamento, rilevazione e perseguimento di reati in generale, a condizione che tale normativa: definisca in modo sufficientemente preciso la natura o le categorie di reati interessati, garantisca il rispetto del principio di proporzionalità, e subordini l'esercizio di tale possibilità, salvo casi di emergenza debitamente giustificati, a un controllo preventivo di un giudice o di un'entità amministrativa indipendente. Inoltre, gli 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, devono essere interpretati nel senso che si oppongono a una normativa nazionale che autorizza le autorità competenti a tentare di accedere ai dati contenuti in un telefono cellulare senza informare la 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 (Corte giust. U.E. (Grande Camera), 4.10.2024, causa C-548/21, cit.).

Perciò, non può condividersi 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.

In giurisprudenza si riconosce che non è consentito alla polizia giudiziaria, in un sistema rigorosamente ispirato al principio di legalità, scostarsi dalle previsioni legislative per compiere atti atipici i quali, permettendo di conseguire risultati identici o analoghi a quelli conseguibili con gli atti tipici, eludano tuttavia le garanzie costituzionali dettate dalla legge per questi ultimi (Sez. VI, 20.11.2024, n.1269/2025, Lato (fattispecie in cui la polizia giudiziaria aveva acquisito dall'indagato, su suo consenso ma senza autorizzazione dell'autorità giudiziaria, lo *screenshot* dei messaggi compromettenti contenuti nel suo cellulare).

Il legislatore, che troppo spesso è distratto, dovrebbe quindi approntare una disciplina particolare per il sequestro del dispositivo in cui sono contenuti messaggi e conversazioni: in questo caso, poiché l'art. 15 Cost. tutela la libertà e la segretezza di "ogni ...forma di comunicazione" la legge dovrebbe prevedere casi e modi di limitazione, la autorizzazione del giudice e, a tutela della riservatezza, la custodia protetta dei contenuti (in questo senso CHELO, *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, in *Dir. pen. e proc.*, 2022, p. 1583). Oggi, infatti, si verifica il paradosso che il provvedimento del giudice è necessario per acquisire dal gestore i dati esterni delle comunicazioni, ma la polizia giudiziaria, sequestrando il *device* di un soggetto, può entrare in possesso del contenuto di tutte le comunicazioni e messaggi (scritti o vocali) da costui intrattenuti, eludendo in questo modo la doppia riserva di legge e di giurisdizione, oltre la riservatezza della persona.

Infine, *last but not least*, deve osservarsi che la disposizione sulla base della quale il Pubblico ministero ha autorizzato perquisizione e sequestro nei locali della società è l'art. 254 c.p.p., il quale, però, li consente soltanto "presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni" e non presso l'indagato o terzi non gestori del servizio di telecomunicazioni e, trattandosi di disposizione speciale che limita una libertà fondamentale, non ammette interpretazioni estensive o analogiche.