SISTEMA PENALE

FASCICOLO

6/2025

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2023, p. 5 ss.

6/2025

L'ACQUISIZIONE DELLA MESSAGGISTICA DIGITALE NEL PROCESSO PENALE: TRA CORTOCIRCUITI PROCESSUALI E PROSPETTIVE *DE IURE CONDENDO*

Cass. Sez. VI, 13 gennaio 2025, n. 1269 Pres. Aprile, Rel. Amoroso

di Michele Oddis

Il presente contributo analizza una recente sentenza della Corte di cassazione in tema di acquisizione della messaggistica digitale nel processo penale a seguito delle note prese di posizione della giurisprudenza costituzionale. Sebbene sia apprezzabile una lettura maggiormente rispettosa del principio di segretezza della corrispondenza di cui all'art. 15 Cost. permangono particolari criticità sistematiche con riferimento – in modo particolare – alle carenti garanzie giurisdizionali a presidio delle fasi acquisitive del dato informatico. L'innalzamento delle garanzie procedimentali è alla base del recente disegno di legge S. 806 che mira all'introduzione di un inedito art. 254-ter rubricato «sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute». Tuttavia, l'attuale proposta di riforma risulta ancora contraddistinta da gravi lacune che se non adeguatamente colmate potrebbero compromettere severamente diritti e prerogative dell'indagato.

1. Il caso.

Con la sentenza che si annota la Corte di cassazione si è pronunciata, tra l'altro, sull'utilizzabilità degli *screenshot* relativi a conversazioni effettuate mediante l'applicazione di *mobile messaging Whatsapp* installata all'interno del telefono cellulare in uso all'imputato.

A tale riguardo, la difesa lamentava la mancata declaratoria di inutilizzabilità del suddetto materiale probatorio, trattandosi di prove acquisite *contra legem* e in violazione del principio di segretezza della corrispondenza.

Nel ritenere fondata le censura proposta, i giudici di legittimità hanno sottolineato 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. Ne deriva che «la messaggistica archiviata nei telefoni cellulari non può più essere considerata alla stregua di un mero documento, ma richiede l'assoggettamento alla disciplina dell'art. 254 c.p.p. che impone la necessità di un provvedimento dell'autorità giudiziaria, necessariamente motivato, al fine di giustificare il sacrificio della segretezza della corrispondenza»[1].

La soluzione privilegiata dai giudici di legittimità nella pronuncia in commento recepisce il recente orientamento della Corte costituzionale secondo cui «lo scambio di messaggi elettronici rappresenta, di per sé, una forma di corrispondenza»[2]. È, così, superato il precedente indirizzo giurisprudenziale che qualificava i messaggi *Whatsapp* e gli *sms* conservati nella memoria di un telefono cellulare come prova documentale acquisibile «mediante mera riproduzione fotografica»[3].

2. Dato digitale e prova documentale.

La pronuncia in commento offre lo spunto per alcune considerazioni sui rapporti intercorrenti tra dato digitale e prova documentale.

A tale riguardo, va subito detto che la disposizione di cui all'art. 234 c.p.p. è stata «pensat[a] per strumenti analogici, la cui peculiarità è data da grandezze fisiche che assumono valori continui»[4]. Ciononostante, non sono mancate decisioni orientate a ricomprendere *tout court* nel perimetro applicativo della disposizione in esame anche i

---

[1] Così, testualmente, il § 3 dei "*Considerato in diritto*" della sentenza in commento.

[2] Il riferimento è a Corte cost. 27 luglio 2023, n. 170. Per alcuni commenti v. 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.it*, n. 21/2023, p. 81 ss; P. VILLASCHI, *La posta elettronica e i messaggi WhatsApp sono corrispondenza? Note a margine del ricorso per conflitto di attribuzione tra poteri dello Stato promosso dal Senato della Repubblica in relazione al "caso Renzi"*, *ivi*, n.7/2023, p.234 ss.; E. FURNO, *Libertà di comunicazione e diritto alla riservatezza del parlamentare nelle sentenze nn. 157 e 170 del 2023 della Corte costituzionale in tema di intercettazioni*, *ivi*, n. 25/2023, p. 37 ss.; L. LONGHI, *La libertà e la segretezza delle comunicazioni parlamentari in due recentissime pronunce della Corte costituzionale*, *ivi*, n. 25/2023 p. 58 ss; C. FONTANI, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Dir. pen. proc*. n. 10/2023, p. 1311 ss.; 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*, n. 1/2024.

[3] Da ultimo, Cass., sez. VI, 16 marzo 2022, n. 22417, in *C.E.D. Cass.*, rv. 283319-01 secondo cui «per i dati informatici non valgono i principi elaborati in materia di intercettazioni e di acquisizione di corrispondenza, dovendosi ritenere che i messaggi whatsapp e gli sms conservati nella memoria di un telefono cellulare hanno natura di documenti ai sensi dell'art. 234 c.p.p., sicché è legittima la loro acquisizione mediante mera riproduzione fotografica, non trovando applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 c.p.p.», in senso conforme ex multis Cass, sez. VI, 12 novembre 2019, dep. 2020, n. 1822, in *C.E.D. Cass.*, rv. 278124; Cass., sez. V, 21 novembre 2017, dep. 2018, n.1822, *ivi* rv. 272319).

[4] In questi termini F. ZACCHÉ, *La prova documentale*, Giuffrè, Milano, 2012, p. 26. Sul punto A. VELE, *La prova documentale nel processo penale*, Cacucci, Bari, 2022, p. 51 ss.

dati informatici[5]. Ad avallare simili opzioni esegetiche concorre il dato letterale dell'art. 234 c.p.p., il quale, come noto, ricomprende nel proprio ambito di operatività ogni rappresentazione di fatti, persone o cose, a prescindere dal mezzo utilizzato: se, infatti, «è consentita l'acquisizione di […] documenti che rappresentano fatti, persone, o cose mediante […] qualsiasi mezzo» rientrerebbe in tale categoria anche il documento digitale.

Una simile impostazione, tuttavia, omette del tutto di confrontarsi con le peculiari caratteristiche morfologiche che differenziano il documento "tradizionale" da quello informatico[6]. Nella prima ipotesi, il contenuto informativo è materialmente incorporato su un supporto fisico e, pertanto, «la rappresentazione non esiste senza il supporto fisico sul quale è incorporata»[7], di conseguenza, esiste un «rapporto di immedesimazione che lega contenuto e contenitore»[8]. Nel secondo caso, al contrario, il dato digitale è contraddistinto dall'immaterialità, «nel senso che la rappresentazione esiste indifferentemente dalla scelta del tipo di supporto fisico sul quale il dato informatico è incorporato»[9], giacché esso ben può essere trasferito agevolmente da un supporto all'altro (*hard disk, pen drive* ecc.).

Da tale "ontologica" distinzione discende la necessità di garantire una maggior tutela, nel caso di documento informatico, da eventuali possibilità di alterazione o distruzione[10]. Tale esigenza è stata avvertita anche dal legislatore il quale, con la l. n. 48

---

[5] Da ultimo Cass. pen., Sez. VI, 3 giugno 2022, n. 21624 *non mass.* secondo cui «deve evidenziarsi che i dati di carattere informatico contenuti nel computer, in quanto rappresentativi di cose, alla stregua della previsione normativa di cui all'art. 234 c.p.p. rientrano tra le prove documentali».

[6] Una prima ipotesi definitoria di documento informatico era rinvenibile nell'art. 491-*bis* c.p. introdotto dalla legge n. 547 del 1993 ove lo si identificava come «qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli». Una simile definizione, tuttavia, apriva il varco a problematiche interpretazioni di sistema. Il legislatore, poco avveduto, si era limitato a trasporre acriticamente nel contesto processuale penale una nozione tradizionalmente civilistica di documento mediante la quale è possibile indicare come tale il solo supporto che contiene dati. Come osservato da M. PITTIRUTI, Digital evidence *e procedimento penale*, Giappichelli, Torino, 2017, p. 24, una tale statuizione dogmatica, calata sul piano penale, non coglieva adeguatamente nel segno, in quanto «tutelava il solo supporto fisico e non il dato informatico che invece era proprio quello che andava protetto» confondendo «contenitore (in ipotesi, un personal computer) e contenuto (il file oggetto di attenzione investigativa)». Nel frattempo, il legislatore aveva inteso ideare una seconda definizione che, se sebbene più ampia della definizione del 1993 condivideva con quest'ultima lo stesso coefficiente di indeterminatezza ed inesattezza. Il riferimento è, in questo caso, alla definizione introdotta dall'art. 1 lett. p) del codice dell'amministrazione digitale secondo cui è possibile considerare come documento informatico qualsiasi «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». Soltanto nel marzo del 2008 la prima definizione, quella risalente al 1993 è stata espunta dall'ordinamento, sostituita dalla più dettagliata definizione contenuta all'art. 1 convenzione di Budapest secondo cui per documento informatico deve necessariamente intendersi «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

[7] Così P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, n. 4/2009, p.403.

[8] V. R. DEL COCO, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* in *Proc. pen. giust.*, n. 3/2018, p. 537.

[9] Così P. TONINI, *Documento informatico e giusto processo*, cit., p.403.

[10] In tal senso A. CHELO, *Le prime indagini sulla scena del crimine. Accertamenti e rilievi urgenti di polizia*

del 2008[11], ha inserito nell'apparato codicistico regole *ad hoc* per l'indagine informatica. Il riferimento va all'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[12] oppure alla previsione di particolari procedure volte ad assicurare «la conformità dei dati acquisiti a quelli originali e la loro immodificabilità»[13] nell'ambito delle attività di sequestro di dati informatici.

In considerazioni di tali rilievi, si fa strada il dubbio circa l'effettiva riconducibilità di qualsiasi dato digitale, una volta incorporato in un supporto cartaceo, al contenitore della prova documentale. Simile espediente si risolve, a ben vedere, in una mera «scorciatoia probatoria»[14] per eludere il controllo sull'autenticità delle informazioni, dal momento che l'art. 234 c.p.p. non detta alcuna prescrizione in ordine alla genuinità del dato incorporato nel documento. Accade spesso che pagine *web* o *screenshot* estratti da *social network* siano acquisiti al fascicolo dibattimentale quali prove documentali ai sensi dell'art. 234 c.p.p. attraverso una semplice stampa del *file* originale, solitamente prodotta dalla polizia giudiziaria o dalla persona offesa, senza alcuna garanzia circa l'autenticità e la provenienza dei dati.

Il procedimento così delineato suscita qualche perplessità in ragione delle innumerevoli possibilità di falsificazione del materiale digitale. Ad esempio, per rimanere nell'ambito delle comunicazioni effettuate tramite *whatsapp*, «è nota la possibilità di cancellare dalla *chat* alcuni messaggi di testo o di scaricare apposite applicazioni per la creazione di messaggi falsi che, una volta riportati su supporti cartacei, si sottraggono ad una verifica di falsificazione e possono essere, così, acquisiti a fini processuali»[15]. Analoghe considerazioni valgono per i messaggi sms o le informazioni tratte da rete telematica, ugualmente suscettibili di alterazione.

Indicazioni in merito alle modalità attraverso le quali il dato digitale deve essere acquisito al processo non sembrano neppure rinvenibili all'interno dell'art. 234-*bis* c.p.p.[16], il quale stabilisce che «è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo

---

giudiziaria, Cedam, Milano, 2014, p. 63.

[11] Legge 18 marzo 2008, n. 48 recante «*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*» in *G. U.* 4 aprile 2008 n. 80 – suppl ord. n. 79. Per un commento, L. LUPARIA (a cura di), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime (l. 18 marzo 2008, n. 48), Giuffrè, Milano, 2009.

[12] Cfr. artt. 244, comma 2; 247, comma 1-*bis* nonché artt. 352, comma 1-*bis* e 354, comma 2 c.p.p.

[13] V. artt. 254-*bis*, 354, comma 2, nonché, con formula pressoché analoga, art. 260, comma 2 c.p.p.

[14] In tal senso, M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 25.

[15] V. R. DEL COCO, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* cit. p. 536.

[16] Articolo aggiunto dal d.l. 18 febbraio 2015, n. 7, convertito, con modificazioni, nella l. 17 aprile 2015, n. 43 recante « *Conversione in legge, con modificazioni, del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonche' proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione*» in *G. U.* 20 aprile 2015-serie generale n.91.

consenso, in quest'ultimo caso, del legittimo titolare». Due, in particolare, i rilievi degni di nota.

In primo luogo, a venire in rilievo è la distinzione, operata dalla stessa rubrica della disposizione in esame, tra documenti e dati informatici «quasi a voler sottolineare l'incapacità della prima categoria concettuale di ricomprendere al proprio interno anche la seconda»[17]. Una simile opzione esegetica, tuttavia, si risolverebbe «in un'interpretazione restrittiva dell'art. 234 c.p.p. nonché, in ultima analisi, [in] una interpretazione abrogante della locuzione "qualsiasi altro mezzo di rappresentazione", in contrasto con pressocché unanime dottrina e giurisprudenza»[18].

In secondo luogo, la nuova disposizione sconta il medesimo – inesistente – livello di tutela della genuinità delineato dall'art. 234 c.p.p. in considerazione dell'assenza di qualsiasi riferimento alle cautele procedimentali da adottare al fine di garantire la non alterabilità del dato informatico.

Anche in considerazione di tali rilievi è evidente che un simile quadro normativo risulta inadatto a far fronte alle numerose criticità che possono derivare dall'intersezione tra processo penale e dato digitale.

3. La corrispondenza digitale: verso letture rispettose del principio di segretezza *ex* art. 15 Cost.

Neppure la giurisprudenza di legittimità è stata in grado di fornire opzioni esegetiche idonee a sopperire all'inadeguatezza del sostrato normativo appena descritto. La Corte di cassazione, infatti, si è per lungo tempo attestata su posizioni alquanto recessive, noncurante della necessaria cautela[19] che deve inevitabilmente contraddistinguere ogni approccio al dato informatico.

Vale la pena richiamare quell'orientamento – ormai superato – secondo cui i dati informatici conservati nella memoria di un telefono cellulare «hanno natura di documenti ai sensi dell'art. 234 c.p.p. sicché è legittima la loro acquisizione mediante mera riproduzione fotografica, non trovando applicazione né la disciplina delle intercettazioni, né quella relativa all'acquisizione di corrispondenza di cui all'art. 254 c.p.p.»[20].

Simile opzione esegetica si radica su un duplice ordine di considerazioni.

Da un lato, i giudici di legittimità ritengono ostativa all'applicazione dell'art. 266-*bis* c.p.p. l'assenza di un flusso di comunicazioni in corso[21]; dall'altro lato, invece,

---

[17] V. R. DEL COCO, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* cit. p 536.

[18] In tal senso, M. PITTIRUTI, Digital evidence *e procedimento penale*, cit., p. 28.

[19] Rileva l'esistenza di un principio di cautela nel trattamento del dato informatico G. ZICCARDI, *L'ingresso della* computer forensics *nel sistema processuale italiano: alcune considerazioni informatico-giuridiche*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 177.

[20] Così, da ultimo, Cass., Sez. VI, sent. 8 giugno 2022, n. 22417, in *C.E.D. Cass*. rv. 283319-01.

[21] *Ex multis* Cass. pen., Sez. VI, Sent., 12 novembre 2019 (dep.2020) n. 1822, in *C.E.D. Cass*. rv. 278124-01.

escludono il richiamo alla disciplina dettata dall'art. 254 c.p.p. facendo leva sul rilevo per cui si tratterebbe di dati che non rientrano 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[22].

La conclusione patrocinata, tuttavia, risulta ancorata ad un concetto ormai anacronistico di corrispondenza cartacea trasmessa tramite servizio postale e telegrafico. Difatti, «è indubitabile che la quasi contestualità che contraddistingue, soprattutto nelle comunicazioni telefoniche, i tempi di inoltro e ricezione dei messaggi [..] esiga una calibratura interpretativa volta ad estendere la nozione di corrispondenza a tutti quei dati digitali già pervenuti al destinatario»[23].

Simili ricostruzioni dogmatiche – preconizzate dalla dottrina più avveduta – hanno trovato integrale recepimento in una recente pronuncia della Corte costituzionale. Nel dettaglio, i giudici della Consulta, intervenuti nella risoluzione di un conflitto di attribuzione tra poteri dello stato nella nota vicenda "*Open*", hanno chiarito, tra l'altro, che anche la messaggistica elettronica già ricevuta e letta dal destinatario rientra nel concetto di corrispondenza evocato dall'art. 68, comma 3 Cost.

Nel tracciare il perimetro operativo della garanzia contemplata all'art. 15 Cost., i giudici costituzionali sottolineano che la tutela della segretezza della corrispondenza prescinde dalle caratteristiche del mezzo tecnico impiegato ai fini della trasmissione del pensiero. Di talché, la garanzia dell'art. 15 Cost. si estende ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, «ignoti al momento del varo della Carta costituzionale»[24].

Alla luce di simili rilievi è indubbio che posta elettronica e messaggi inviati tramite l'applicazione *Whatsapp* possano rientrare a pieno titolo nella sfera di protezione dell'art. 15 Cost., essendo del tutto assimilabili a lettere o biglietti chiusi. Se, difatti, nella tradizionale corrispondenza cartacea la riservatezza di quest'ultima è assicurata dall'inserimento in plichi cartacei o buste chiuse, analogamente, nella nuova corrispondenza digitale, la segretezza e la riservatezza vengono assicurate da procedure che prevedono codici di accesso o altri meccanismi di identificazione per l'invio e la ricezione.

Simili considerazioni valgono anche per biglietti elettronici già ricevuti e letti dal destinatario e conservati nella memoria del proprio dispositivo digitale. Difatti, poiché nei casi di comunicazione tramite posta elettronica o altri servizi di messaggistica istantanea manca un rilevante iato temporale tra invio e successiva recezione del messaggio elettronico, degradare la comunicazione a mero documento quando non più *in itinere* è soluzione che azzera la tutela costituzionale prefigurata dall'art. 15 Cost.

---

[22] In tal senso Cass. sez. III, sent. 25 novembre 2015 (dep. 2016), Giorgi, in *C.E.D. Cass*. rv. 265991.

[23] V. R. DEL COCO, *L'utilizzo probatorio dei dati whatsapp tra lacune normative e avanguardie giurisprudenziali,* cit. p 541. Sul punto v. C. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2014, p 41; A. SCALAS, *I confini mobili della* digital evidence*: una necessaria tassonomia per la tutela delle garanzie*, in *Arch. pen. web*., n. 2/2023.

[24] Così, 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,* cit. p.5.

4. Cortocircuiti processuali.

L'impianto tecnico-argomentativo messo a punto dalla Consulta è integralmente recepito dalla sentenza in commento. Segnatamente, i giudici di legittimità sottolineano che lo scambio di messaggi elettronici rappresenta di per sé una forma di corrispondenza anche nel caso in cui siano stati già ricevuti e letti dal destinatario. Conseguentemente, l'apprensione del contenuto dei biglietti elettronici agli atti del procedimento deve avvenire nelle forme del sequestro di corrispondenza, sulla base di un provvedimento motivato del pubblico ministero.

Tale modalità di acquisizione del dato digitale non troverebbe applicazione nel caso di messaggi privi del carattere di attualità per i corrispondenti[25]. L'assenza di tale specifico requisito qualificherebbe il biglietto elettronico come semplice documento, acquisibile anche mediante riproduzione fotografica.

Simili approdi esegetici, pur condivisibili per l'indubbia sensibilità garantista, si prestano a qualche critica.

A destare riserve è, innanzitutto, il secondo passaggio dell'*iter* argomentativo, secondo cui le garanzie costituzionali a presidio della segretezza della corrispondenza si estendono ai soli messaggi conservati nella memoria di un dispositivo elettronico che non abbiano perso il carattere di attualità. Una simile conclusione, infatti, è caratterizzata da un elevato grado di genericità, dal momento che potrebbe essere alquanto arduo, per gli organi inquirenti, stabilire se il messaggio comunicativo, già recepito e appreso dal destinatario, sia da considerarsi "attuale". Non solo. Così facendo, si eleva un concetto estremamente «sfumato»[26] quale l'"attualità" della corrispondenza a vero e proprio spartiacque procedimentale tra due modalità di acquisizione dei biglietti elettronici a cui si riconnettono differenti livelli di tutela: da un lato, il sequestro di corrispondenza – che assicura una maggiore protezione del contenuto comunicativo – dall'altro, il meccanismo acquisitivo della prova documentale.

Accanto ai rilievi appena prospettati, a suscitare perplessità è, altresì, l'assunto secondo cui l'acquisizione agli atti del procedimento di biglietti elettronici ancora "attuali" con le forme del sequestro di corrispondenza dovrebbe necessariamente avvenire sulla base di un decreto motivato del pubblico ministero[27]. A riguardo, sebbene tanto l'art. 254 c.p.p. quanto l'art. 15 Cost. non facciano alcun riferimento espresso alla necessità di un intervento del giudice[28], è proprio la particolare intrusività delle modalità

---

[25] Così, la pronuncia in commento, al § 3 dei *Considerato in diritto*.

[26] V. D. ALBANESE, *La "nuova" corrispondenza nel processo penale, tra recenti sviluppi giurisprudenziali e scenari* de lege ferenda, in *Dir. pen. proc.*, n. 11/2024, p. 1521.

[27] Sulla qualificazione del pubblico ministero come parte *sui generis* v. R. DEL COCO, *La maschera e il volto della consulenza tecnica d'accusa*, in *Proc. pen. giust.*, n. 3/2021, p.669 ss.

[28] Dello stesso avviso Cass. Sez. Un. Sent. 29 febbraio 2024, n.23756, Giorgi, in *C.E.D. Cass*. rv. 286589 e a Cass. Sez. Un. Sent. 29 febbraio 2024, n. 23755, Gjuzi, *C.E.D. Cass*. rv. 286573 per un commento L. MARAFIOTI, *Sezioni Unite e tirannie tecnologiche: diritto di difesa, contraddittorio e "criptofononi"*, in *Diritto di difesa*, 18 settembre 2024.

di investigazione digitale unitamente alla peculiarità del "contenitore" della corrispondenza in esame – vale a dire lo smartphone[29] – a renderlo preferibile. Proprio in considerazione di simili rilievi, è necessario che sia un organo effettivamente terzo ed imparziale rispetto alle indagini a valutare la legittimità e la proporzionalità di ogni limitazione dei diritti fondamentali dell'individuo, analogamente a quanto accade per l'applicazione delle misure cautelari, per l'autorizzazione alle intercettazioni, oppure ancora per l'acquisizione dei tabulati telefonici[30]. Con riferimento al meccanismo acquisitivo da ultimo richiamato vale la pena sottolineare che, a seguito di importanti prese di posizione della giurisprudenza europea[31], il legislatore italiano ha rinnovato l'art. 132 comma 3 del d.lgs. 196 del 2003[32] disponendo che «[…] i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private».

Ora, simili garanzie riservate ai tabulati, devono valere ancor di più rispetto ai dati comunicativi non potendosi ravvisare alcuna differenza ontologica tra contenuto di una conversazione e il documento che rileva dati esteriori a quest'ultima.

Diversamente opinando, verrebbe a crearsi un problematico «cortocircuito sistemico»[33]. Difatti, violerebbe il principio di uguaglianza codificato all'art. 3 della Carta costituzionale «affidare al giudice l'acquisizione di dati esterni della comunicazione e al pubblico ministero, invece, quella del contenuto»[34].

5. Prospettive *de iure condendo*: tra proiezioni garantiste…

Su posizioni analoghe è sembrato attestarsi lo stesso legislatore, il quale, nell'ottica di un progressivo innalzamento delle garanzie procedimentali operanti in

---

[29] Sulle peculiarità dello smartphone inteso come proiezione informatica dell'individuo v. F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. Dir. proc. pen*. n. 3/2017, p. 491, nonché O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254 ter c.p.p.? brevi note a margine del d.d.l. a.s. n. 806*, in *Penale. Diritto e procedura*, 12 marzo 2024.

[30] Sul punto v. F. R. DINACCI, *L'acquisizione di tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust*., n. 2/2022, p.301 ss.; L. TAVASSI, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Arch. pen. web*, n. 1/2022, p. 1 ss

[31] Il riferimento è a Corte di Giustizia UE 2 marzo 2021, *H.K.*, C-746/18, per un commento si rinvia a G. LEO, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sist. pen*., 31 maggio 2021.

[32] Decreto legislativo 30 giugno 2003, n. 196 «*Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*» in *G.U.* n.174 del 29 luglio 2003 - Suppl. Ordinario n. 123.

[33] Così O. MURRO-W. NOCERINO, *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini,* in *Penale. Diritto e procedura*, 21 ottobre 2024.

[34] In tal senso A. CHELO, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in *Penale. Diritto e procedura*, 29 febbraio 2024.

tema di acquisizione di biglietti elettronici, si è recentemente adoperato con un nuovo disegno di legge[35].

Il tratto maggiormente innovativo della proposta legislativa in discorso è rappresentato dall'introduzione, nel codice di rito penale, di un inedito art. 254-*ter* rubricato «*Sequestri di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute*». La disposizione in esame reca un'articolata procedimentalizzazione del sequestro dei dispositivi elettronici, suddividendo le operazioni investigative in tre distinte fasi: l'apprensione del dispositivo, la copia e l'analisi dei dati e, infine, l'acquisizione dei soli dati di rilievo investigativo.

Nella fitta trama normativa dell'art. 254-*ter*, a venire in rilievo è, innanzitutto, l'introduzione di una vera e propria riserva di giurisdizione «in rima con la disciplina prevista per le intercettazioni e l'acquisizione di tabulati di traffico telefonico e telematico»[36]. Il comma 1 della disposizione in esame, infatti, prevede che «nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, dispone con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici, o di memorie digitali, necessari 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». Meritevole di rilievo è, in tal senso, l'attenzione del legislatore al principio di proporzionalità, che «assume il ruolo di limite funzionale dell'attività della pubblica accusa, a tutela dell'indagato e dei terzi interessati dall'indagine»[37], nel perdurante obiettivo di «comporre armonicamente la doverosa tutela per i diritti individuali con le esigenze legate all'efficacia dell'accertamento»[38].

Nel medesimo solco di una rinnovata attenzione per la tutela dei diritti fondamentali dell'individuo si inserisce l'ulteriore previsione di un contraddittorio tecnico nel corso della fase di acquisizione dei dati mediante copia forense. Più nel dettaglio, il pubblico ministero provvede alla duplicazione del contenuto dei dispositivi informatici, dei sistemi informatici o telematici, o delle memorie digitali in sequestro, avvisando «la persona sottoposta alle indagini, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, la persona offesa dal reato e i relativi difensori, del giorno, dell'ora e del luogo fissati per il conferimento

---

[35] Il riferimento è al d.d.l. S 806 di 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*».

[36] V. O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254-ter c.p.p.? Brevi note a margine del d.d.l. a.s. n. 806* cit.

[37] Così M. PITTIRUTI, *Principio di proporzionalità e onere di motivazione del sequestro probatorio*, in L. MARAFIOTI – G. FIORELLI – F. CENTORAME, *Procedura penale* in action. *Materiali per una critica della giurisprudenza*, Giappichelli, Torino, 2022, p. 29. In dottrina, sul principio di proporzionalità, L. TAVASSI, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, cit. L. ALGERI, *Principio di proporzionalità e sequestro probatorio di sistemi informatici*, in *Dir. pen. proc.* n. 6/2020, p. 849 ss; C. FONTANI, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi*, in *Dir. pen. proc.*, n. 2/2022, p. 237 ss.

[38] Così M. PITTIRUTI, *Principio di proporzionalità e onere di motivazione del sequestro probatorio*, cit. p. 30.

dell'incarico per la duplicazione e della facoltà di nominare consulenti tecnici». Ai sensi del comma 8 della disposizione in esame, i difensori e i consulenti tecnici eventualmente nominati hanno diritto di partecipare allo svolgimento delle operazioni di duplicazione e di formulare osservazioni e riserve. In tal modo il legislatore – optando per una disciplina che presenta tratti di innegabile contiguità con quella prevista in tema di accertamenti tecnici irripetibili – si prefigge di garantire un effettivo diritto al contraddittorio tecnico sulla prova digitale.

L'esigenza di rafforzare le garanzie minime operanti nelle fasi di acquisizione del dato digitale si concretizza, a livello normativo, nella diversificazione delle modalità operative a seconda della tipologia di elemento da acquisire: dato non comunicativo e dato comunicativo. Nella prima evenienza, il pubblico ministero 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. Nel secondo caso, il pubblico ministero deve richiedere al g.i.p. l'emissione di un nuovo decreto autorizzativo per ottenere il sequestro in presenza degli stessi presupposti che giustificherebbero lo svolgimento delle intercettazioni[39].

In tale ultima ipotesi, è evidente che il duplice vaglio giudiziale sanerebbe «le incongruenze che separano l'acquisizione dei dati comunicativi archiviati nei dispositivi elettronici dall'acquisizione dei medesimi dati attraverso le operazioni di intercettazioni»[40].

6. … e lacune procedimentali.

Le modifiche in chiave garantista appena descritte rischiano, tuttavia, di risolversi in garanzie meramente apparenti in ragione delle numerose lacune sistematiche che contraddistinguono la proposta legislativa.

Innanzitutto, il legislatore, pur avendo modellato la disciplina in tema di duplicazione del dato digitale su quella degli accertamenti tecnici irripetibili, ha nondimeno omesso qualsivoglia riferimento alla facoltà di formulare riserva di incidente probatorio.

Una simile scelta suscita perplessità in considerazione dell'ontologica fragilità che contraddistingue il dato informatico. Come segnalato da attenta dottrina, infatti, sussiste un rischio particolarmente elevato che qualsiasi operazione compiuta sul dato informatico possa inevitabilmente tradursi in una modifica irreparabile dello stesso,

---

[39] Cfr. art. 266 comma 1 e 267 comma 2 c.p.p. e nel caso di procedimenti per reati di criminalità organizzata i presupposti dell'art. 13 d.l. 13 maggio 1991, n. 152, convertito con modificazioni dalla L. 12 luglio 1991, n. 203 recante «*Conversione in legge, con modificazioni, del decreto-legge 13 maggio 1991, n. 152, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*» in *G.U.* 12 luglio 1991, n. 162.

[40] V. O. MURRO, *Sequestro dei dispositivi informatici: verso l'art. 254-ter c.p.p.? Brevi note a margine del d.d.l. a.s. n. 806* cit.

anche qualora sia utilizzino i più moderni sistemi di *digital forensics*[41]. Proprio alla luce di tali rilievi, è necessaria la previsione di un «meccanismo di riequilibrio a favore dell'indagato che non intenda abdicare alla garanzia giurisdizionale»[42].

Analogamente criticabile è la previsione di un meccanismo di duplicazione che, derogando alla procedura ordinariamente prescritta, sacrifica il diritto al contraddittorio e alla partecipazione dell'indagato. A tale riguardo, il comma 10 dell'art. 254-*ter* prevede che, nei procedimenti finalizzati all'accertamento di particolari categorie di reati[43], «nonché 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» il procedimento di duplicazione avvenga mediante non meglio specificate «modalità tecniche idonee ad assicurare la conformità del duplicato all'originale e la sua immodificabilità». Sin troppo agevole rilevare che l'estrema laconicità la quale caratterizza la deroga in esame, ben potrebbe aprire il varco ad impieghi distorsivi del meccanismo appena descritto.

Da ultimo, suscita qualche interrogativo la previsione, in tema di durata del vincolo di indisponibilità sulla copia dei dati digitali, secondo cui il duplicato informatico va conservato «fino alla sentenza o al decreto penale di condanna non più soggetti ad impugnazione».

L'operatività di un simile meccanismo procedimentale comporterebbe un significativo arretramento di garanzie rispetto a quelle elaborate dalla recente giurisprudenza di legittimità[44] secondo cui il pubblico ministero può trattenere la copia integrale dei dati informatici – significativamente denominata copia mezzo – solo per il tempo strettamente necessario a selezionare, tra la molteplicità delle informazioni in essa contenute, quelle che davvero assolvono alla funzione probatoria sottesa al sequestro.

La modalità operativa delineata dall'art. 254-*ter*, oltre a porsi in rotta di collisione con i principi di adeguatezza e proporzionalità[45] della misura, stride vistosamente con il diritto alla disponibilità esclusiva che ogni proprietario dei dati digitali esercita su di essi da cui discende «l'immediata restituzione delle copie forensi»[46]. È stato opportunamente osservato che «è proprio sui dati riservati che si estende il valore della riservatezza, poiché il loro sequestro ed analisi rappresenta una intrusione e limitazione maggiore rispetto a quella che connota il sequestro del mero dispositivo elettronico»[47].

---

[41] In tal senso M. PITTIRUTI, *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *Sist. pen.*, 14 gennaio 2021.

[42] Così P. GAETA – A. PICARDI, *sub art. 360*, in *Codice di procedura penale commentato*, II, a cura di A. GIARDA – G. SPANGHER, Wolters Kluwer, Milano, 2023, p.1883.

[43] Il riferimento è ai procedimenti di cui agli artt. 406, comma 5-*bis* e 371-*bis* comma 4-*bis* c.p.p.

[44] Cfr. Cass. sez. VI, 22 settembre 2020, n. 34265, in *C.E.D. Cass*. rv. 279949 – 01 con nota di M. PITTIRUTI, *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, cit.

[45] Sul punto M. PITTIRUTI, *Adeguatezza e proporzionalità nel sequestro di un sistema informatico*, in *Dir. internet*, 2019, p. 777 ss.

[46] In tal senso O. MURRO, *Prospettive in tema di sequestro dello* smartphone: *le novità approvate dal Senato*, in *Dir. pen. proc*., n. 12/2024, p.1626.

[47] Così O. MURRO, *Prospettive in tema di sequestro dello* smartphone: *le novità approvate dal Senato*, cit., p.1626.

In definitiva, sono evidenti le luci e le ombre che caratterizzano la proposta di legge in esame. Da un lato, è senz'altro apprezzabile l'innegabile «afflato garantista»[48] che contraddistingue il nuovo sequestro di corrispondenza e l'evidente mutamento di paradigma procedimentale rispetto al passato. Dall'altro lato, la morfologia processuale del "nuovo" sequestro di dispositivi informatici presenta ancora gravi lacune procedimentali che, se non adeguatamente colmate, potrebbero compromettere severamente diritti e prerogative dell'indagato. È auspicabile, pertanto, che i lavori parlamentari possano affinare un prodotto normativo allo stato incompiuto.

[48] V. D. ALBANESE, *La "nuova" corrispondenza nel processo penale, tra recenti sviluppi giurisprudenziali e scenari* de lege ferenda, cit. p.1530.

Editore

ASSOCIAZIONE
"PROGETTO GIUSTIZIA PENALE"