Università degli studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in Giurisprudenza

a.a. 2022/2023

Il documento informatico nel processo penale

Relatrice:

Chiar.ma Prof.ssa Silvia Signorato

Laurenda:

Matilde Bellon

Matricola 1150007

A nonna Maria, senza di te non sarei mai arrivata fino a qui.

Ci auguro che questo sia il primo di tanti traguardi che raggiungeremo insieme.

INDICE

INTRODUZIONE

L'informatica, intesa come disciplina scientifico-tecnologica, ha acquisito nella società odierna un ruolo del tutto centrale in ogni ambito, anche in quello giuridico. È impensabile escludere dalla normativa, in ogni branca del diritto, delle disposizioni che tengano conto di tutti gli strumenti che le nuove tecnologie ci offrono.

Nel testo che segue verranno esaminate, nello specifico, la disciplina del documento informatico e il suo ruolo di prova documentale nel processo penale. La mente del legislatore, precedentemente agli anni Novanta dello scorso secolo, si è sempre concentrata sul concetto di materialità del documento immaginandolo solo cartaceo e tangibile.

Dai primi anni Novanta del Novecento, il legislatore italiano ha timidamente iniziato a considerare non solo il documento stampato su carta, ma anche quello informatico, il quale ha pian piano acquisito completa autonomia. La svolta, per quanto riguarda la sua definizione, può essere individuata nel CAD (Codice dell'amministrazione digitale) il quale ha ufficialmente introdotto nel nostro ordinamento il nuovo istituto.

All'interno del codice di procedura penale, in seguito alla legge 18 marzo 2008, n. 48, che ratifica la Convenzione di Budapest del 2001 sul *cybercrime,* il legislatore ha cercato di fornire una disciplina il più chiara e uniforme possibile per contrastare la criminalità informatica e disciplinare al meglio l'utilizzo degli strumenti tecnologici utilizzati dalla società moderna.

Tuttavia, non è risultato agevole effettuare un intervento normativo in tema di documenti informatici poiché il progresso tecnologico è talmente tanto repentino che sarebbe quasi impossibile normare ogni strumento disponibile.

Nell'elaborato che segue verranno evidenziate le criticità legate alla disciplina del documento informatico comparandole a ciò che è stabilito per il documento cartaceo.

Nel terzo e ultimo capitolo, verrà esaminato nel particolare un mezzo di ricerca della prova; ossia il sequestro probatorio di un documento informatico. Al di là della disciplina codicistica, è interessante notare la profonda differenza operativa tra il sequestro probatorio di un documento cartaceo e di uno informatico. Di norma, durante le indagini tradizionali avviene prima la perquisizione e successivamente il sequestro; invece, nel caso del sequestro probatorio di solito avviene esattamente il contrario: prima gli inquirenti operano il sequestro e successivamente procedono con la perquisizione. L'autorità giudiziaria è tenuta a rispettare nel modo più ligio possibile i diritti costituzionalmente garantiti degli individui quando procede con il sequestro. Invero, ad esempio,

sequestrando un *computer* senza fornire un'adeguata motivazione nel decreto di sequestro, gli inquirenti potrebbero determinare una indebita ingerenza nei diritti fondamentali del soggetto che subisce l'attività investigativa senza che vi sia uno stretto nesso tra il dato trovato e conseguentemente letto e il reato che si vuole perseguire.

L'analisi non ha mancato di considerare anche taluni casi significativi che inducono a riflettere su quanto dottrina e giurisprudenza stiano, sempre di più, elaborando nuove teorie per una tutela maggiore dell'individuo senza però trascurare la possibilità di utilizzo dei nuovi strumenti tecnologici da parte degli inquirenti.

Capitolo I-Evoluzione normativa e disciplina nel CAD del documento informatico

I.1 Panoramica sulle fonti

La disciplina del documento informatico ha subito un'ampia evoluzione nel tempo. Iniziando dall'analisi dell'art. 22, comma 1, lettera D, l. 241/1990 per documento amministrativo si intende "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del* contenuto *di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale"*[1]. Non siamo in presenza di una vera e propria definizione del documento informatico, ma è un timido avvicinamento del legislatore alle nuove tecnologie; infatti, si inseriscono all'interno dell'ampia categoria del documento amministrativo rappresentazioni sia grafiche che fotocinematografiche, elettromagnetiche o di qualsiasi altra specie.

Dal canto suo, l'art. 3, comma 2, d.lgs. del 12 febbraio 1993 n. 39[2] prevede che "*Nell'ambito delle pubbliche amministrazioni l'immissione, la riproduzione su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante sistemi informatici o telematici, nonché l'emanazione di atti amministrativi attraverso i medesimi sistemi, devono essere accompagnate dall'indicazione della fonte e del responsabile dell'immissione, riproduzione, trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile*"[3]. Anche in questo caso, come nell'articolo 22 della Legge 241/1990, non troviamo una puntuale disciplina del documento informatico, ma un riferimento alla riproduzione di documenti mediante sistemi informatici e telematici. È importante sottolineare come le norme, lentamente e non in modo omogeneo, sin dai primi anni Novanta del secolo scorso abbiano cercato di avvicinarsi al sempre più emergente mondo dell'informatica, in quanto i nuovi strumenti tecnologici hanno radicalmente sconvolto anche il diritto in ogni sua branca.

Un'importante svolta nella determinazione del concetto di documento informatico è inserita nella Legge del 23 dicembre 1993, n.547, rubricata: "*Modificazioni ed integrazioni alle norme del Codice*

[1] Art. 22 comma 1 lettera D, L. 241/1990.
[2] D.lgs. 12 febbraio 1993, n.39. Norme in materia di sistemi informativi automatizzati delle pubbliche amministrazioni a norma dell'articolo 2, comma 1, lettera mm), della Legge 23 ottobre 1992, n. 421.
[3] Art. 3 comma 2 D.lgs. 39/1993.

penale e del codice di procedura penale in tema di criminalità informatica"[4]. Questa legge introduce l'articolo 491 *bis* nel Codice penale definendo nel seguente modo il documento informatico: "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*"[5]. Questa è la prima definizione del documento informatico che troviamo nel panorama della legislazione italiana, che sarà successivamente rimodellata e adattata alla realtà giuridico sociale alla quale deve far fronte. La legge 547/1993 è stata in seguito abrogata dalla legge 18 marzo 2008, n. 48 "*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*"[6] la quale*: «* all'articolo 3 comma 1 dispone che: "*All'articolo 491-bis del codice penale sono apportate le seguenti modifiche: al primo periodo, dopo la parola privato» sono inserite le seguenti: «avente efficacia probatoria»; b) il secondo periodo è soppresso"*[7].

Un'accelerazione particolarmente decisiva per l'introduzione del documento informatico nel nostro ordinamento è stata apportata dalla legge 15 marzo 1997, n. 59, "*Delega al governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa*"[8]. Questa legge si inserisce all'interno di un più ampio complesso legislativo chiamato Leggi Bassanini costituito da: legge 59/1997, 127/1997, 191/1997 e 50/1999. Queste norme costituiscono un momento decisivo per il riordino della Pubblica Amministrazione e il suo rapporto con i cittadini.

In particolare, l'art. 15, comma 2, della legge 59/1997 afferma che: "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*"[9]. Conseguentemente si può affermare che con la legge Bassanini gli atti della P.A. e i negozi privati, emanati e stipulati mediante l'utilizzo di sistemi informatici e telematici, divengono dunque validi e rilevanti a prescindere dalla loro trasposizione sulla carta. Questo ha portato a uno sdoppiamento sempre più evidente del regime giuridico dei

[4] Legge del 23 dicembre 1993, n.547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
[5] Art 3 legge 547/1993.
[6] Legge 18 marzo 2008, n. 48 "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".
[7] Art. 3 Legge 48/2008.
[8] Legge 15 marzo 1997, n. 59, "Delega al governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa".
[9] Art. 15 comma 2 legge 59/1997.

documenti: da un lato quelli cartacei e dall'altro quelli informatici che hanno acquisito una piena autonomia.

Venendo al decreto del Presidente della Repubblica del 10 novembre 1997, n. 513 rubricato "*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59"*[10] era una disposizione attuativa della Legge 59/1997 e conteneva una sistemazione organica ed esaustiva, per il suo tempo, della materia che si sta affrontando. Questo regolamento si caratterizzava per due principali aspetti. Anzitutto, era "tecnologicamente orientato" poiché conteneva una particolare modalità d'identificazione dell'autore del contenuto di un documento informatico ovvero la firma digitale basata sul sistema della crittografia a doppia chiave asimmetrica. In secondo luogo, limitava l'accesso al mercato dei servizi di certificazione riservandolo a dei soggetti che, se privati, avrebbero dovuto soddisfare requisiti uguali a quelli richiesti per l'esercizio dell'attività bancaria[11].

In seguito, il d.P.R. 513/1997 è stato espressamente abrogato e la disciplina ivi contenuta è transitata all'interno del d.P.R. 28 dicembre 2000, n.445, recante il "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*"[12].

Quanto al D.P.C.M. del 13/01/2004 esso ha ultimato il recepimento della Direttiva europea 1999/93/CE introducendo le "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*"[13]. Questo testo normativo ha disciplinato le modalità di formazione dei documenti amministrativi attraverso i supporti informatici, riservando una particolare attenzione alle attività di generazione, apposizione e verifica delle firme digitali.

[10] D.P.R. 10 novembre 1997, n.513, Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

[11] G. Navone, *Instrumentum digitale: teoria e disciplina del documento informatico*, Giuffrè editore, 2012, p. 86 e ss.

[12] D.P.R. 28 dicembre 200, n.445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

[13] D.P.C.M. 13 gennaio 2004 Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

I.2 La disciplina prevista dal codice dell'amministrazione digitale (CAD)

Il Decreto Legislativo 7 marzo 2005, n.82[14], meglio conosciuto come Codice dell'amministrazione digitale, è tutt'oggi il testo normativo di riferimento per la regolamentazione giuridica del documento informatico. Il CAD ha finalmente riconosciuto l'importanza fondamentale del documento informatico, dal momento che non può esistere una Pubblica amministrazione digitale senza quelle imprescindibili attività di formazione, trasmissione e conservazione di documenti amministrativi realizzati interamente in formato elettronico. Nel tempo ha subito varie modifiche, le ultime due particolarmente significative sono: D. Lgs. 22 agosto 2016 n.179 e D. Lgs. 13 dicembre 2017 n.217.

Le linee portanti del D. Lgs. 22 agosto 2016[15], n.179 possono essere individuate nelle seguenti. Anzitutto, la prosecuzione della razionalizzazione delle disposizioni contenute nel CAD e semplificazione, anche del linguaggio, sostituendo le regole tecniche con delle linee guida adottate dell'Agenzia per l'Italia digitale per mantenere le disposizioni legislative al passo con l'evoluzione tecnologica e scongiurare il rischio che i cittadini e la P.A. possano avere a disposizione soluzioni e servizi meno moderni di quelli utilizzabili sul mercato. In secondo luogo, il sottolineare maggiormente la natura di carta di cittadinanza digitale. Inoltre, il promuovere l'interazione tra i vari servizi pubblici. Ancora, il garantire maggiore certezza giuridica in ambito della formazione, gestione e conservazione dei documenti digitali, prevedendo che tutti i documenti firmati digitalmente, ricorrendo i criteri specifici delineati dell'AgID, possano produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza che debba essere un giudice, per ogni documento, a verificarne l'efficacia. L'obiettivo è quello di promuovere un utilizzo sempre più frequente delle nuove tecnologie senza rinunciare al rispetto della disciplina legislativa. In aggiunta, il potenziare l'applicabilità dei diritti di cittadinanza digitale istituendo presso l'AgID un ufficio del difensore civico e ampliando le sanzioni in caso di violazione dei diritti di cittadini e imprese. Infine, il promuovere la valorizzazione del patrimonio informatico garantendo l'utilizzo più efficace dei dati pubblici attraverso soluzioni di *data analysis* rispettando sempre la protezione della *privacy* e la tutela dei dati personali[16].

[14] D. Lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale.
[15] D. Lgs. 22 agosto 2016, n. 179.
[16] Cfr. Relazione illustrativa del D. Lgs. 22 agosto 2016, n.179, sito web https://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0452_F001.pdf&leg=XVII.

Per ciò che concerne, invece, il D. Lgs. 13 dicembre 2017, n.217,[17] la relazione illustrativa del decreto indica come fine l'adeguamento del nostro ordinamento alle disposizioni del regolamento UE 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 e alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE[18].

È necessaria un'analisi più approfondita della norma ai fini di individuare le caratteristiche principali del documento informatico nel mondo giuridico odierno. La definizione del documento informatico nel CAD si trova all'articolo 1 lettera p che lo definisce come "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*[19]". L'introduzione della dicitura "documento elettronico" è in linea con il Regolamento eIDAS[20] che ha disciplinato questo concetto all'articolo 1 comma 35 definendolo come "*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"*[21].

È evidente che il linguaggio del legislatore europeo con riferimento al documento elettronico sia molto più neutro rispetto a quello italiano per ciò che concerne la definizione del documento informatico. In primo luogo, perché notoriamente la disciplina europea contiene definizioni più fluide rispetto a quelle degli Stati membri; in secondo luogo, perché i due concetti nascono in contesti totalmente differenti.

Il documento informatico ha origine nell'ambito della digitalizzazione della Pubblica Amministrazione che ha come scopo la progressiva dematerializzazione dell'attività amministrativa passando prima per l'equiparazione dell'attività amministrativa elettronica a quella cartacea e poi addirittura facendo prevalere la seconda sulla prima. Il documento elettronico, invece, è nato in seguito all'obiettivo principale dell'eIDAS cioè quello di rafforzare la fiducia nelle transazioni economiche nel mercato interno fornendone una base legislativa europea[22].

Per ciò che concerne, invece, l'efficacia probatoria del documento informatico si deve far riferimento agli articoli 20 e 21 del CAD. In particolare, l'articolo 20 stabilisce che il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile,

[17] D. Lgs. 13 dicembre 2017, n.217.

[18] Cfr. Relazione illustrativa del D. Lgs. 13 dicembre 2017, n.217, sito web https://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII.

[19] Art. 1 lettera p del D. Lgs. 12 marzo 2005, n.82.

[20] Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta Ufficiale dell'Unione Europea L. 257/73 del 28 agosto 2014. eIDAS è l'acronimo di electronic IDentification, Authentication and trust Services.

[21] Art. 1 comma 35 eIDAS.

[22] P. Giacalone, *Il ciclo di vita del documento informatico, gestione e aspetti normativi, Franco Angeli/Informatica*, 2021, pag. 13 e ss.

ovvero quella della scrittura privata che fa piena prova fino a querela di falso[23], quando vi è la firma digitale o altra firma elettronica qualificata o avanzata; oppure è formato tramite il processo disciplinato dall'articolo 71 CAD che segue le linee guida AgID purché sia antecedentemente verificata l'identità informatica del suo autore. In tutti gli altri casi sarà il giudice a valutare, caso per caso, l'efficacia probatoria del documento informatico valutandone sicurezza, integrità e immodificabilità[24]. L'articolo 21 impone la sottoscrizione, a pena di nullità, delle scritture private, *ex* articolo 1350[25] del Codice civile, con firma elettronica qualificata o firma digitale che sono fatte sotto forma di documento informatico[26]. La differenza tra l'articolo 20 e il 21 sta nei riferimenti al Codice civile. Infatti, nell'articolo 20 la norma si riferisce all'efficacia probatoria della scrittura privata, mentre nell'articolo 21 la disciplina è delineata per gli atti che si fanno per iscritto ex articolo 1350.

Per l'analisi dell'efficacia probatoria delle copie di documenti si deve far riferimento agli articoli 22, 23 e 23 bis del CAD. L'articolo 22 del CAD[27], rubricato "*copie informatiche di documenti analogici*", illustra le caratteristiche delle copie informatiche dei documenti analogici. Vengono identificati tre livelli graduali di parametri nei quali una copia informatica può avere l'efficacia probatoria della forma scritta: in primo luogo, le copie informatiche assumono efficacia probatoria se sono formate ai sensi dell'art. 20; in secondo luogo, le copie informatiche assumono efficacia probatoria se la conformità della copia informatica al suo originale analogico è certificata da un notaio o altro Pubblico Ufficiale a ciò autorizzato secondo le regole tecniche dell'art. 71; il parametro residuale afferma che le copie informatiche hanno la stessa valenza probatoria dell'originale analogico se non sono disconosciute[28].

L'articolo 23, *"copie analogiche di documenti informatici"*[29], affronta il problema della copia analogica del documento informatico e della sua autenticità. Il legislatore attribuisce il potere di attestazione della conformità della copia all'originale ad un pubblico ufficiale; in tal caso la copia, che può essere stata siglata precedentemente tramite firma elettronica avanzata, qualificata o digitale, ha la stessa efficacia probatoria dell'originale. Quando non sussiste la certificazione di un pubblico ufficiale, la copia assume la medesima efficacia probatoria quando la sua conformità non viene espressamente disconosciuta. Nell'articolo 23, inoltre, è disciplinato il contrassegno elettronico che

[23] Art. 2702 cc.
[24] Art. 20 CAD
[25] Art. 1350 c.c.
[26] Art. 21 CAD.
[27] Art. 22 CAD.
[28] D. E. Caccavella-S. Pellegrini, *CAD, bugie e dibattimento: il documento informatico in una prospettazione penalistica*, in *Ciberspazio e diritto*, vol. 23, n. 72 (3 - 2022), pp. 411-425.
[29] Art. 23 CAD.

si può apporre sulla copia cartacea per garantire la corrispondenza tra copia e originale. Esso sostituisce completamente la sottoscrizione autografa del pubblico ufficiale.

L'articolo 23 *bis*[30] affronta il tema dei duplicati e delle copie informatiche dei documenti informatici. In relazione ai duplicati, il primo comma stabilisce che questi hanno identico valore giuridico rispetto ai documenti informatici da cui sono tratti solo se sono riprodotti seguendo il contenuto dell'articolo 71 del CAD e delle nuove linee guida sulla formazione, gestione e conservazione del documento informatico del 10 settembre 2020. Queste nello specifico sul tema prevedono che: "*ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da PC ad una pen-drive di un documento nel medesimo formato*[31]." Per quanto riguarda, invece, le copie e gli estratti informatici del documento informatico si deve fare riferimento al secondo comma dell'articolo 23 bis. Le copie e gli estratti hanno la stessa valenza probatoria dell'originale se la conformità è attestata da un pubblico ufficiale autorizzato o se la conformità non è disconosciuta. Rimane l'obbligo di conservazione dell'originale informatico solo se è così previsto. Le linee guida, nel merito, definiscono la copia come "*documento il cui contenuto è medesimo all'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratta*", mentre l'estratto come: "*una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto*"[32]. Infine, è stabilito che la validità del documento informatico per le copie e/o gli estratti di documenti informatici è consentita anche tramite il confronto dei documenti e la certificazione di processo, normata dall'allegato 3 delle nuove linee guida intitolato "Certificazione di processo". Dunque, tutti questi metodi consentono di assicurare, in egual modo, la conformità della copia o dell'estratto all'originale[33].

Per una disamina completa del documento informatico nel CAD è necessario approfondire anche l'articolo 71 e le linee guida AgID che ne definiscono i requisiti tecnici. L'articolo 71 è stato novellato in seguito al decreto legislativo 13 dicembre 2017 numero 217 nel quale sono inserite le regole tecniche. A questo, per una completa definizione dell'argomento, vanno affiancate le linee guida adottate dall'Agenzia per l'Italia Digitale. Nella gerarchia delle fonti italiane le linee guida sono state inquadrate dal parere del Consiglio di Stato n.2122/2017 del 10 ottobre 2017[34] dove si afferma che: "*le linee guida adottate da AgID, ai sensi dell'articolo 71 del CAD, hanno carattere vincolante e*

[30] Art. 23bis del CAD.
[31] Linee guida sulla formazione, gestione e conservazione del documento informatico del 10 settembre 2020.
[32] Ibidem.
[33] P. Giacalone*, Il ciclo di vita del documento informatico, gestione e aspetti normativi, Franco Angeli/Informatica*, 2021, pag. 192 e ss.
[34] Parere del Consiglio di Stato n. 2122/2017 del 10 ottobre 2017.

assumono valenza erga omnes. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'articolo 2 comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'articolo 17 del CAD." Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici sono state pubblicate in Gazzetta Ufficiale il 19 ottobre 2020 e poi riformate il 17 maggio 2021. Queste sono una vera e propria svolta nel campo della disciplina della formazione del documento informatico in quanto danno dei riferimenti generali e sono una guida, evitando così di essere modificate nel tempo velocemente data la repentina evoluzione dell'informatica con la quale il legislatore molto spesso non è completamente allineato[35]. Secondo le Linee guida le modalità di formazione del documento informatico sono quattro: redazione, acquisizione, registrazione informatica di informazioni o dati e generazione o raggruppamento di un insieme di dati o registrazioni. La redazione avviene tramite l'utilizzo di strumenti software, successivamente il documento viene memorizzato nel suo formato originale di produzione. Questo potrà essere consolidato in una o più versioni fino a giungere a quella definitiva che non subirà più nessuna modifica da parte del suo autore, questa fase è molto importante perché solo così il documento assumerà il suo formato definitivo che renderà immodificabile il contenuto e predisposto alla sottoscrizione digitale. L'immodificabilità e l'integrità sono due caratteristiche essenziali del documento informatico. La seconda modalità di formazione del documento informatico è l'acquisizione. Le linee guida stabiliscono che il documento è formato tramite l'acquisizione: di un documento informatico per via telematica o su supporto informatico, della copia per immagine su supporto informatico di un documento analogico, della copia informatica di un documento analogico

Al termine della sua formazione il documento dovrà possedere cinque caratteristiche ovvero: staticità, integrità, immodificabilità, leggibilità e autenticità. L'articolo 3 comma 9 del DPCM 13 novembre 2014 stabilisce che: "*al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione*[36]". I metadati sono un insieme di dati associati a un documento informatico che servono a identificarlo, descriverne contesto, contenuto, struttura e permetterne la conservazione. Le Linee guida vigenti stabiliscono anche che un documento informatico creato tramite l'utilizzo di software o cloud qualificati sia immodificabile anche quando è trasferito a soggetti terzi a mezzo di servizio di posta elettronica certificata e anche a mezzo di servizio elettronico di recapito certificato qualificato, definito così dal Regolamento eIDAS. Le linee

[35] P. Giacalone, *Il ciclo di vita del documento informatico, gestione e aspetti normativi, Franco Angeli/Informatica*, 2021, pag. 16 e ss.
[36] Articolo 3 comma 9 del DPCM 13 novembre 2014.

guida AgID, emanate dal 2014 in poi, hanno quindi ampliato le modalità con le quali un documento può essere definito informatico e infatti lo possiamo definire come qualsiasi atto scritto idoneo a rappresentare o raffigurare un fatto per trasmettere la conoscenza a chi la osserva ed è la rappresentazione di fatti giuridicamente rilevanti. Pertanto un file registrato su un supporto informatico può essere considerato un documento informatico ai sensi del CAD se garantisce sicurezza, integrità e immodificabilità[37].

Pare opportuno soffermarsi ora su un ulteriore aspetto relativo al documento informatico nel CAD è la sua conservazione. La disciplina si trova nella sezione II rubricata "*gestione e conservazione dei documenti*" e l'articolo di riferimento è il 42[38] che autorizza le pubbliche amministrazioni alla dematerializzazione dei documenti. Anche il comma 1*bis* dell'articolo 34 del CAD ha ad oggetto la conservazione dei documenti delle pubbliche amministrazioni e stabilisce che possono procedere alla conservazione nella propria struttura organizzativa o rivolgersi ad altri soggetti pubblici o privati[39].

Sono dedicati alla conservazione anche gli articoli 43 e 44 del CAD.

L'articolo 43, al primo comma, fa riferimento sia alla conservazione che all'esibizione dei documenti e al primo comma stabilisce che: "*gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida*"[40]. L'obiettivo di questo comma è quindi quello di preservare la piena corrispondenza del documento informatico all'originale.

Il comma successivo, 1*bis*, dell'articolo 43 è molto innovativo poiché dispone il venir meno dell'obbligo per i cittadini e le imprese di conservazione dei documenti informatici previsti a loro carico nel caso in cui questi siano conservati dalle pubbliche amministrazioni. Data questa disposizione, le pubbliche amministrazioni si devono impegnare a rendere disponibili a imprese e cittadini i documenti con servizi online accessibili con identificazione tramite SPID. I documenti devono essere integrati con il Sistema pubblico di ricerca documentale e con tutti i servizi online disponibili[41].

[37] D. E. Caccavella-S. Pellegrini, *CAD, bugie e dibattimento: il documento informatico in una prospettazione penalistica, in Ciberspazio e diritto*, vol. 23, n. 72 (3 - 2022), pp. 411-425.
[38] Articolo 42 CAD.
[39] Articolo 34 CAD.
[40] Articolo 43.1 CAD.
[41] Articolo 43.1*bis* CAD.

Il secondo comma dell'articolo 43 si occupa dei documenti conservati precedentemente su qualsiasi supporto in grado di garantire la conformità dei documenti agli originali. Si fa riferimento a varie tipologie di supporto come fotografico o ottico, tutti sempre in grado di preservare l'originale[42].

Il terzo comma[43] norma l'archiviazione dei documenti informatici tenendo presente la Deliberazione CNIPA 11/2004 sulla conservazione e archiviazione dei documenti informatici che stabilisce che i documenti informatici per i quali è prevista la conservazione dalla legge o da regolamento possono essere archiviati per esigenze correnti anche su carta ma devono obbligatoriamente essere conservati in modo permanente con modalità digitali[44].

L'articolo 44, invece, disciplina i requisiti per la conservazione dei documenti informatici delineando un sistema che prevede la partecipazione di vari soggetti chiamati a gestire parte dell'intero progetto[45].

Il responsabile della gestione documentale deve collaborare con il responsabile per la transizione digitale, che ai sensi dell'articolo 17 del CAD deve garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione della pubblica amministrazione, con il Responsabile della Protezione dei Dati[46] e con il responsabile della conservazione dei documenti informatici per lavorare sulla definizione e gestione delle attività delle quali sono rispettivamente competenti. Almeno una volta all'anno devono essere resi noti dal responsabile della gestione dei documenti informatici al sistema di conservazione i fascicoli e le serie documentarie relative a tutti procedimenti, anche a quelli non ancora terminati. È d'obbligo sottolineare che tutti i documenti all'interno del sistema di conservazione devono essere gestiti mantenendo le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità richieste come elementi necessari dalle Linee guida.

Il processo di conservazione si sviluppa in varie fasi tra loro concatenate. Il primo passaggio è quello dell'acquisizione del pacchetto di versamento che è, ai sensi dell'Allegato 1 delle Nuove Linee guida sulla formazione dei documenti informatici, un "*pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione*"[47]. Successivamente si deve verificare che il pacchetto di versamento e ciò in esso contenuto rispettino

[42] Articolo 43.2 CAD.
[43] Articolo 43.3 CAD.
[44] Deliberazione CNIPA n. 11 del 19 febbraio 2004, Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
[45] Art. 44 CAD.
[46] Figura introdotta dal Regolamento UE n. 2016/679 del Parlamento Europeo e del Consiglio riguardante la protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla loro libera circolazione, meglio noto come GDPR.
[47] Allegato 1 delle nuove Linee guida sulla formazione dei documenti informatici.

la disciplina del manuale di conservazione e dell'allegato 2[48] delle nuove Linee guida sulla formazione dei documenti informatici intitolato "Formati di file e riversamento". Se ci sono dei difetti il pacchetto di versamento è rifiutato. Il sistema di conservazione è formato sia da procedure e regole che da un software che gestisce automaticamente varie operazioni, tra le quali troviamo la generazione del rapporto di versamento che riguarda i vari pacchetti di versamento identificati in modo univoco nel sistema di conservazione. Il rapporto di versamento contiene: data e ora e impronte crittografiche. Può essere richiesta anche la sottoscrizione che deve avvenire con firma digitale, elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione oppure con apposizione del sigillo elettronico, qualificato o avanzato del conservatore esterno. Il processo di conservazione deve anche possedere copie informatiche o duplicati che siano conformi alle linee guida[49].

I.3 Impostazioni dottrinali in tema di documento informatico.

Dopo avere definito il concetto di documento informatico, è necessario esaminare i principali problemi che esso ha creato all'interno della legislazione italiana. In dottrina, Paolo Tonini ha cercato di esaminarne le varie criticità durante tutto il percorso di evoluzione legislativa. Tonini sottolinea la differenza lessicale utilizzata dal legislatore del 1993 con quella del 2005; infatti nel 1993 il documento informatico sembra essere un "supporto che contiene dei dati", mentre nel 2005 il CAD lo definisce come "rappresentazione informatica di un fatto". Queste due discipline antinomiche sono rimaste entrambe in vigore fino al 2008, quando la legge n.48 del 2008[50] ha ratificato la Convenzione di Budapest eliminando la prima definizione, ovvero quella del 1993.

Stando alla definizione del CAD, Tonini riflette sul concetto di "rappresentazione informatica", più in particolare sul termine "informatica" come modo di rappresentazione di un fatto.

La tesi tradizionale e più risalente di Francesco Carnelutti[51] individua la scrittura come una modalità di "rappresentazione" di un fatto. È proprio questa interpretazione che ha ispirato il legislatore del 2005 che definisce quella informatica come modalità di "rappresentazione" al pari della scrittura. Una tesi più moderna, però, si è affermata tra i penalisti sostanziali, i quali si sono interrogati

[48] Allegato 2 delle nuove Linee guida sulla formazione dei documenti informatici, Formati di file e riversamento.
[49] P. Giacalone, *Il ciclo di vita del documento informatico, gestione e aspetti normativi, Franco Angeli/Informatica*, 2021, pag. 186 e ss.
[50] Legge n.48 del 2008, 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.
[51] F. Carnelutti, *La prova civile*, 1947, ristampa 1992, Milano, n. 35, 140 e 143.

sull'argomento in relazione ai reati in materia di falso. In particolare, nel volume "Teoria del falso documentale" del 1958[52] l'autore Alessandro Malinverni ha aggiunto al documento il requisito dell'incorporamento su una base materiale oltre a quello della rappresentazione. Questo testo è stata la base di questa seconda tesi in quanto gli studiosi asseriscono che la scrittura, la fonografia e la fotografia sono forme di "incorporamento" di un fatto e non più di "rappresentazione". Tonini aderisce a questo secondo filone e cerca di spiegarne le motivazioni. L'incorporamento può avvenire sia con modalità analogiche che digitali[53]. Nel caso di modalità analogiche l'incorporamento avviene utilizzando grandezze fisiche variabili proporzionali all'intensità del fenomeno da riprodurre, questo tipo di incorporamento è materiale perché la rappresentazione esiste solo quando è incorporata su una base materiale. Non si può quindi spostare la rappresentazione prescindendo dal suo supporto, altrimenti si dovrebbe farne una fotocopia che si distinguerebbe dall'originale perché sarebbe incorporata su una differente base materiale. L'eventuale falsità dell'originale o della sua copia si accerta con una perizia perché ne resta traccia sul supporto. Ciò avviene per il documento tradizionale di tipo analogico. Quando, invece, la modalità di incorporamento è digitale la rappresentazione è possibile soltanto tramite uno strumento digitale. La peculiarità di questa modalità è che la rappresentazione è trasferibile identica da un supporto all'altro, questo grazie al documento informatico. Da questa spiegazione Tonini ricava una nuova definizione di documento informatico: "*rappresentazione di un fatto che è incorporata con modalità digitali su una base materiale*".

I giuristi che aderiscono al filone più tradizionalista prima descritto non concordano con questa definizione di documento informatico perché affermano che il documento digitale sia immateriale[54]. Per confutare la tesi dell'immaterialità ci si può avvalere di varie dimostrazioni. Francesco Alcaro nel 2006 ha affermato che il concetto di immaterialità è dotato di speciale significato per i civilisti, un bene immateriale è il contenuto di un'idea o un'opera dell'ingegno che può essere brevettabile[55]. Francesco Ricci[56] ha sostenuto, nei primi anni 2000, che il documento informatico è dotato di materialità perché nella base materiale può esserci o meno un segnale elettrico o luminoso o magnetico. Per tali ragioni non si può definire il documento informatico immateriale e conseguentemente non si può far derivare dal concetto di immaterialità la differenza tra il documento

[52] A. Malinverni, *Teoria del falso documentale*, Milano, 1958; Id., voce Fede pubblica (delitti contro la), a) Diritto penale, in Enc. dir., vol. XVII, Milano, 1968, 69.

[53] P. Tonini, *Manuale di procedura penale*, XII ed., Milano, 2011, 353.

[54] La dottrina insiste sul concetto di "immaterialità" del documento informatico per dare contezza della sua fragilità. A. Masucci*, Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in Riv. dir. civ., 2004, I, 755. M. Cammarata - E. Maccarone, La firma digitale sicura, Milano, 2003, 68.

[55] F. Alcaro*, Riflessioni 'vecchie' e 'nuove' in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in Rass. dir. civ., 2006, 951.

[56] L'incorporamento digitale consiste nella presenza o nell'assenza di un segnale (es. elettrico) su di un supporto fisico; in tal senso, F. Ricci, voce Documento informatico, in Il diritto, Enc. De Il Sole-24 Ore, Milano, 2007, IV, 548.

informatico e quello cartaceo. A fronte di questa situazione di stallo, Francesco Alcaro ha definito il documento informatico come dematerializzato[57]. L'aggettivo centra completamente le caratteristiche peculiari del documento informatico perché l'incorporamento digitale forma un documento che esiste indifferentemente dal suo supporto fisico sul quale è incorporato, però per esistere deve necessariamente sussistere una base materiale come un hard disk o un CD o *pen drive*. Il documento informatico è, quindi, veicolato su un file ed è quest'ultimo a essere incorporato su una base materiale. Data la sua struttura, il documento informatico è facilmente modificabile sia dall'autore dell'incorporamento che da altre persone, perciò, è necessaria particolare attenzione del legislatore alla veridicità del documento originale. Dopo queste considerazioni è più chiaro il motivo dell'intervento della legge n. 48 del 2008 che accoglie pienamente la teoria moderna sul documento informatico[58]. La legge n. 48 del 2008 ha infatti introdotto cinque garanzie fondamentali nei mezzi di ricerca della prova[59].

Il dovere di conservare inalterato il dato originale nella sua genuinità. Questa garanzia appare nelle ispezioni disposte dall'autorità giudiziaria (art 244.2), nelle perquisizioni disposte dall'autorità giudiziaria (art. 247.1*bis*), nelle perquisizioni su iniziativa della polizia giudiziaria (art. 352.1*bis*), nel sopralluogo di polizia giudiziaria (art. 354.2). Ancora, il dovere di impedire l'alterazione dell'originale. Detta garanzia è prevista nelle ispezioni disposte dall'autorità giudiziaria (art. 244.2), nelle perquisizioni disposte dall'autorità giudiziaria (art. 247.1*bis*), nelle perquisizioni su iniziativa della polizia giudiziaria (art. 352.2-*bis*) e nel sopralluogo (art. 354.2). Anche il dovere di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale. La garanzia appare nel sopralluogo su iniziativa della polizia giudiziaria (art. 354.2) e nel sequestro disposto dall'autorità giudiziaria, ma soltanto in relazione ai dati informatici presso i fornitori di servizi (art. 254*bis*), e non in generale per tutti i tipi di sequestro. In questi due casi la copia deve essere fatta su un supporto adeguato. Per le altre tipologie di sequestro non è previsto né l'obbligo di copia, né viene definito adeguato il supporto richiesto. Inoltre, il dovere di assicurare la non modificabilità dei dati così acquisiti. Si deve far riferimento al sequestro disposto dall'autorità giudiziaria, però solo per ciò che riguarda i dati informatici presso i fornitori di servizi (art. 254*bis*) e non in generale per tutti i tipi di sequestro. Infine, la garanzia della installazione di sigilli informatici sulle cose sequestrate. L'articolo 260 la definisce facoltativa[60].

[57] F. Alcaro*, Riflessioni 'vecchie' e 'nuove' in tema di beni immateriali.*

[58] Legge n. 48 del 2008, 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.

[59] L'incorporamento digitale consiste nella presenza o nell'assenza di un segnale (es. elettrico) su di un supporto fisico; in tal senso, F. Ricci, voce Documento informatico, in Il diritto, Enc. De Il Sole-24 Ore, Milano, 2007, IV, 548.

[60] P. Tonini*, Il documento informatico: problematiche civilistiche e penalistiche a confronto*, Il corriere giuridico 3/2012, da pag. 432 a 439.

Capitolo II - Il documento informatico: disciplina nel Codice di Procedura Penale

II.1 Articoli 234 e 234*bis* del Codice di Procedura Penale

Dopo aver descritto l'evoluzione legislativa del documento informatico, in questo capitolo, verrà approfondito l'istituto considerando la disciplina del Codice di procedura penale[61] relativa ai documenti e ne verranno evidenziate le criticità e la casistica giurisprudenziale più significativa.

L'art. 234 c.p.p. rubricato "Prova documentale" prevede che: "*è consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia. È vietata l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti*"[62].

La definizione di documento che delinea il legislatore nel codice è piuttosto eterogenea e sembra idonea a ricomprendere in essa anche il documento informatico. Secondo Tonini il documento informatico è la rappresentazione di un fatto incorporata in una base materiale mediante il metodo digitale, quindi, sembra perfettamente assimilabile alla norma codicistica, nonostante non vi si faccia letterale menzione.

Bisogna soffermarsi, però, sulla differenza tra documento cartaceo ed informatico che consiste, non tanto, nella modalità di rappresentazione, ma nella modalità di incorporamento. Infatti, una fotografia o uno scritto possono essere analogici o digitali senza differire in alcun modo con riferimento alla loro attitudine rappresentativa. Le caratteristiche dell'incorporazione impongono particolare accortezza per ciò che riguarda l'acquisizione, l'ammissione e la valutazione della prova per evitare qualsiasi alterazione del documento. L'incorporamento è caratterizzato da un rapporto molto instabile tra il supporto materiale e ciò che sta al suo interno. Mentre nel documento tradizionale il suo contenuto rappresentativo è fissato in maniera definitiva sullo stesso documento, nei documenti informatici l'oggetto può essere facilmente copiato su un altro dispositivo.

Il principale problema è, infatti, quello di garantire la genuinità del documento; in quello cartaceo una eventuale manomissione è facilmente individuabile, poiché sarà una manomissione fisica del

[61] C.p.p., DPR 22 settembre 1988, n. 447.
[62] Art. 234 c.p.p.

documento stesso. Per quanto riguarda, invece, quello informatico è più complicato, data la facilità con la quale si può manomettere. Il legislatore, a fronte di questa problematica, adotta soluzioni differenti per il procedimento di copia delle due tipologie di documenti.

Da un lato, il legislatore, per ciò che concerne il documento tradizionale, ammette all'art. 234, comma 2, c.p.p.[63], la possibilità di acquisirne una copia quando l'originale sia distrutto e all'art. 258 c.p.p.[64] permette all'autorità che sequestra il documento di eseguirne una copia e restituire l'originale a chi ha subito il sequestro. È evidente che gli inquirenti abbiano ampie possibilità di maneggiare le copie dei documenti cartacei in quanto è facilmente verificabile un'eventuale manomissione dell'originale. È necessaria, invece, un'attenzione particolare alla copia di un documento informatico. All'autorità giudiziaria è imposto di individuare metodi di copiatura adatti a garantire conformità tra copia e originale e idonei a mantenere integri i dati che sussistono all'interno.

Nel file sono contenute anche informazioni che non attengono alla sua rappresentazione, ma che hanno comunque attitudine rappresentativa. Si tratta di dati che non possono essere qualificabili come tracce informatiche perché sono frutto della volontà del programma, quindi della macchina, e non dell'utilizzatore del *file.*

Proprio per questo motivo la legge 18 marzo 2008, n. 48[65] impone particolare attenzione agli atti d'indagine aventi ad oggetto materiale informatico[66]; così si possono evitare di confondere queste informazioni frutto del mero lavoro della macchina con quelle rilevanti ai fini probatori.

Questa legge ratifica la Convenzione del Consiglio d'Europa sui *Cybercrime* siglata a Budapest il 23 novembre del 2001 e mira a uniformare l'ordinamento processuale penale italiano agli *standard* europei per il contrasto ai crimini informatici[67]. È importante perché grazie ad essa sono state introdotte nel codice disposizioni garantiste sulla conservazione e integrità dei dati originali e la conformità delle copie dei dati utilizzati con fini giudiziari[68]. Le garanzie inserite sono il frutto dello studio giuridico informatico compiuto sui mezzi tecnici necessari all'acquisizione delle prove dei reati informatici e sono state effettuate in quel momento per la prima volta in Italia[69].

---

[63] Art. 234.2 c.p.p.

[64] Art. 258 c.p.p.

[65] Legge 18 marzo 2008, n.48, 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.

[66] Cfr. https://onelegale.wolterskluwer.it/document/art-234-c-p-p-prova-documentale-prova-documentale/C5CI0000003644?searchId=2067963356&pathId=7ec4d8a263492#comment-id-3.

[67] Convenzione del Consiglio d'Europa sui *Cybercrime,* firmata a Budapest il 23 novembre 2001.

[68] L. Luparia, *Sistema penale e criminalità informatica*, Giuffrè, Milano 2009, p. 1

[69] G. Costabile, *Scena criminis, documento informatico e formazione della prova penale*, in Riv. Inf e informatica, 2005, pp. 531 e ss.

Il fulcro di questa legge è proprio l'integrità dei dati informatici che è anche il pilastro di tutte le indagini informatiche; infatti, sono state inserite nel codice delle previsioni, nella parte dedicata alle indagini, volte a preservare i dati informatici.

In particolare, a questo fine vi è la formula inserita tra la disciplina delle perquisizioni, *ex* art. 244 c.p.p.[70], e della perquisizione, *ex* artt. 247[71] e 352 c.p.p.[72], la quale prevede che l'attività di investigazione deve essere fatta: "*adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*". Questa proposizione non deve essere interpretata in modo erroneo poiché il vocabolo "conservazione" non riguarda solo i momenti successivi all'attività acquisitiva, ma anche la necessità di dover preservare i dati nella fase acquisitiva.

Inoltre, all'art. 254*bis* c.p.p.[73], con riferimento al sequestro di dati informatici situati presso fornitori di servizi informatici, telematici e di telecomunicazioni, viene sottolineato che, quando l'acquisizione dei dati avviene tramite copia, questa deve trovarsi su un supporto idoneo che "assicuri la conformità dei dati acquisiti a quelli originali e alla loro immodificabilità" e il fornitore di servizi deve "conservare e proteggere adeguatamente i dati originali".

È necessario considerare anche la previsione dell'art. 259 c.p.p.[74], che disciplina la custodia di cose sequestrate, dove viene specificato che, quando il sequestro ha ad oggetto dati, informazioni o programmi informatici, colui che li custodisce ha il dovere di "*impedirne l'alterazione o l'accesso da parte di terzi*".

Ancora, l'art. 260 c.p.p.[75], che si occupa di apposizione dei sigilli alle cose sequestrate, in riferimento alla copia delle cose sequestrate che sono suscettibili di alterazione, prevede che nel caso di dati, informazioni o programmi informatici la copia debba essere fatta su "*supporti adeguati, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*".

Infine, nel caso di accertamenti urgenti sui luoghi, sulle cose o sulle persone*, ex* art. 354 c.p.p.[76], viene sottolineato che quando gli accertamenti hanno ad oggetto dati, informazioni, programmi informatici o sistemi informatici, la polizia giudiziaria deve adottare le "*misure tecniche*" o ordinare "*le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e*

[70] Art. 244 c.p.p.
[71] Art. 247 c.p.p.
[72] Art. 352 c.p.p.
[73] Art. 254*bis* c.p.p.
[74] Art. 259 c.p.p.
[75] Art. 260 c.p.p.
[76] Art. 354 c.p.p.

provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità".

È evidente, leggendo le disposizioni sopra citate, che la volontà del legislatore sia quella di garantire l'integrità dei dati in ogni fase delle indagini informatiche[77].

L'articolo 234*bis* rubricato "Acquisizione di documenti e dati informatici" dispone: "*è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare*[78]". È stato introdotto dalla l. 17 aprile 2015, n. 43[79], la quale ha convertito in legge il d.-l. 18 febbraio 2015, n.7[80] che disponeva misure urgenti per il contrasto al terrorismo, anche di matrice internazionale, nonché 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. La *ratio* di questa norma sta nel facilitare l'acquisizione di dati e documenti informatici conservati all'estero e, nonostante la previsione sia nata per il contrasto al terrorismo, si ritiene certa la sua portata generale.

La dottrina si è interrogata sulla posizione nella quale è stata collocata questa norma all'interno del codice. Secondo un primo orientamento dottrinale, dato che è stata inserita nel titolo II del libro III dedicato ai mezzi di prova il termine "acquisizione" deve essere inteso come sinonimo di "produzione" del documento informatico a fini istruttori[81]. Una diversa corrente, invece, ritiene che sia una collocazione sistematica errata poiché l'articolo 234*bis* non dovrebbe trovarsi tra i mezzi di prova, ma tra i mezzi di ricerca della prova. La posizione in cui è stata inserita questa norma appare, secondo gli studiosi che sostengono questa seconda tesi, eccedente rispetto alla ratio della legge antiterrorismo mediante la quale è stata inserita. Inoltre, è stato fatto notare che la necessità di acquisizione di dati digitali è predominante in fase di indagini preliminari[82]. È anche stato espresso il timore che la norma abbia "*fatto perdere di vista al legislatore qualche passaggio procedurale; a meno che l'art. 234bis non debba intendersi come strumento volto a ricordare che nessun ostacolo*

[77] S. Signorato, *Le indagini digitali, profili strutturali di una metamorfosi investigativa*, Giappichelli, pag. 126 ss.
[78] Art. 234*bis* c.p.p.
[79] Legge 17 aprile 2015, n. 43, 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, nonché 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.
[80] Decreto-legge 18 febbraio 2015, n.7, Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché 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.
[81] A. Conz, *Acquisizione di documenti e dati informatici conservati all'estero*, in Conz-Levita*, Antiterrorismo*, 126.
[82] A. Natalini, *Rivista di diritto agroalimentare* 17, 386.

all'attività di prevenzione, indagine e accertamento del fatto possa derivare dalla localizzazione all'estero dei dati utili ai fini di un'efficace intelligence. Sotto questo profilo desta ulteriori perplessità la collocazione sistematica della norma inserita tra i mezzi di prova."[83]

È, inoltre, mancante la definizione di "legittimo titolare" nonostante sarebbe stata essenziale dato che il legittimo titolare è l'unico soggetto legittimato a esprimere il consenso sull'acquisizione dei dati. Il "legittimo titolare", citato nell'art. 234*bis,* non coincide né con il concetto di "titolare del trattamento" descritto dall'art. 4 n. 7 Regolamento 2016/679/UE[84], né con quello descritto dall'art. 3 n.8 Direttiva 2016/680/UE[85]. Mancando un riferimento normativo per il concetto di "legittimo titolare", la dottrina lo ha definito come la persona fisica o giuridica che può, in modo legittimo, disporre dei documenti e dei dati informatici[86]. Questa definizione è assai generica, quasi vuota, quindi la soluzione più agevole per evitare di incorrere in errori nella sua individuazione sarà quella di valutare caso per caso.

La norma riguarda l'acquisizione all'estero di documenti e dati informatici. In questo caso, "estero" deve essere inteso come qualsiasi stato differente dall'Italia senza distinzioni tra paesi membri dell'Unione Europea e quelli extra europei[87].

L'articolo prescrive che è "sempre" consentita l'acquisizione dei dati e documenti informatici qualora questi siano disponibili al pubblico. L'avverbio "sempre" implica che in questo caso non sarà necessario ricorrere agli strumenti di cooperazione tra Stati, come l'ordine europeo di indagine penale[88], quando si tratta di stati europei, o la rogatoria[89] nel caso di stati extra europei. Trattandosi di dati e documenti informatici è facile che siano disponibili al pubblico, basti pensare a tutti i dati rinvenibili sul *web* o sui numerosi *social network*. Qualora, invece, vi sia il consenso del "legittimo

[83] F. Vergine, F. Giunchedi, C. Santoriello, v. sub art. 234bis, in Leggi d'Italia.
[84] Art. 4, n.7, Regolamento 2016/679/UE, 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
[85] Art. 3, n.8, Direttiva 2016/680/UE, 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.
[86] Illuminati-Giuliani, *Commentario breve al codice di procedura penale*, Cedam.
[87] Ibidem.
[88] L'ordine europeo di indagine penale (O.e.i.) è stato introdotto dalla Direttiva 2014/41/UE e recepito dall'Italia con il d.lgs. n.108 del 2017. Può essere*, ex* art. 3 della direttiva, impiegato per ricercare e formare qualsiasi tipo di prova, con l'eccezione delle attività istruttorie svolte dalle squadre investigative comuni. Si applica a tutti i membri dell'Unione Europea esclusi Danimarca e Irlanda, che non hanno ratificato la direttiva.
[89] La rogatoria è lo strumento impiegato tradizionalmente dagli stati per la ricerca e formazione transnazionale delle prove. Si fonda sul principio della mutua assistenza e consiste nella richiesta di acquisizione probatoria rivolta da uno stato a un altro sottoposta a vari controlli. Dopo la nascita di o.e.i. il suo utilizzo è confinato ai rapporti extra europei. La rogatoria è prevista in varie convenzioni bilaterali e multilaterali di assistenza giudiziaria alle quali si rifanno molte regole interne degli stati.

titolare" comunque sarà un procedimento agevolato, perché gli elementi in questione sono reperibili nelle reti informatiche e possono essere raccolti a distanza senza l'assistenza tecnica dell'autorità giudiziaria straniera[90].

II.2 Un nuovo approccio al concetto di documento informatico: la sentenza della Corte costituzionale del 23 luglio 2023, n.170.

Con la sentenza della Corte costituzionale del 23 luglio 2023, n. 170[91], la Corte risolve il conflitto di attribuzione tra poteri dello Stato[92] sollevato dal Senato della Repubblica, con ricorso dell'11 maggio 2022, nei confronti della Procura della Repubblica presso il Tribunale ordinario di Firenze.

Il Senato sosteneva che la Procura della Repubblica di Firenze avesse acquisito agli atti del procedimento penale pendente nei confronti del senatore Matteo Renzi e di altri soggetti la corrispondenza scritta dal senatore stesso, senza previa autorizzazione del Senato (al quale non era neanche mai stata richiesta tale autorizzazione), violando quindi l'art. 68, comma 3, della Costituzione[93]. Matteo Renzi era senatore dal 9 marzo 2018[94] quindi godeva della prerogativa offerta dall'art. 68.3 della Costituzione. Durante le attività investigative relative al procedimento penale in questione, la Procura della Repubblica presso il Tribunale di Firenze ha ottenuto, tramite il sequestro di dispositivi mobili di comunicazione appartenenti a terzi, messaggi WhatsApp tra il senatore Matteo Renzi e V. U. M. nel periodo ricompreso tra il giorno 3 e 4 giugno 2018, e tra il senatore Matteo Renzi e M. C. nel periodo tra il 12 agosto 2018 e il 15 ottobre 2019; inoltre sussisteva anche lo scambio di *e-mail* fra questi ultimi nell'arco temporale che va dal giorno 1 al 10 agosto 2018. Tramite il decreto di acquisizione, la Procura ha inoltre acquisito l'estratto del conto corrente bancario personale del senatore Renzi nel periodo dal 14 giugno 2018 al 13 marzo 2020. Quanto detto si ricava dai documenti che sono stati allegati alla relazione[95] della Giunta delle elezioni e delle immunità parlamentari del 14 dicembre 2021. Il conflitto di attribuzione è stato dichiarato ammissibile dalla

[90] R. E. Kostoris, *Manuale di procedura penale europea*, Quarta edizione, Giuffrè Francis Lefebvre, pag. 476.
[91] Corte Cost., 23 luglio 2023, n. 170.
[92] L'art. 134 della Costituzione disciplina le questioni sulle quali la Corte è chiamata a giudicare e stabilisce che: "*La Corte costituzionale giudica: sulle controversie relative alla legittimità costituzionale delle leggi e degli atti, aventi forza di legge (cfr. artt. 76 e 77), dello Stato e delle Regioni (cfr. art. 127); sui conflitti di attribuzione tra i poteri dello Stato e su quelli tra lo Stato e le Regioni, e tra le Regioni; sulle accuse promosse contro il Presidente della Repubblica, a norma della Costituzione (cfr. art. 90)*".
[93] L' art. 68.3 Cost. disciplina: "*Analoga autorizzazione è richiesta per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza*".
[94] Il 9 marzo 2018 è la data della proclamazione.
[95] doc. XVI, n. 9, approvata dall'Assemblea il 22 febbraio 2022.

Consulta con ordinanza n. 261 del 2022[96], sussistendo entrambi i requisiti richiesti, sia soggettivi che oggettivi, di ammissibilità del conflitto[97].

Venendo al merito delle questioni che rilevano dalla pronuncia della Consulta, in primo luogo, la Corte analizza il concetto di "corrispondenza" verificando se per corrispondenza debba intendersi solamente quella cartacea o se il termine si possa riferire anche a quella elettronica e telematica. In secondo luogo, si denota un problema di confine molto labile tra due diversi mezzi di ricerca della prova rappresentati rispettivamente dal "sequestro di corrispondenza" e dall'"intercettazione di comunicazioni o conversazioni". La sentenza del giudice delle leggi opera qui una vera e propria rivoluzione poiché scardina una giurisprudenza di legittimità ormai da molto tempo consolidata: la Corte, per la prima volta, afferma che anche la "corrispondenza telematica" deve godere delle medesime garanzie della corrispondenza cartacea in quanto possono essere considerate tra loro equiparabili. È lampante che il progresso tecnologico imponga di adeguare concetti e garanzie elaborate in un'epoca precedente in cui gli strumenti, che ora sono quotidianamente utilizzati, erano quasi impossibili da immaginare, anche perché gli strumenti investigativi a disposizione degli inquirenti sono in costante e rapida evoluzione[98].

Il primo interrogativo sul quale si è espressa la Corte costituzionale è se l'acquisizione, da parte della Procura della Repubblica presso il Tribunale di Firenze, di messaggi scambiati su *Whatsapp* tra il

[96] Corte Cost., Ord. 24 novembre 2022, n.261. La Corte ha dichiarato ammissibile il ricorso del Senato della repubblica asserendo che: "*LA CORTE COSTITUZIONALE:1) dichiara ammissibile, ai sensi dell'art. 37 della legge 11 marzo 1953, n. 87 (Norme sulla costituzione e sul funzionamento della Corte costituzionale), il conflitto di attribuzione tra poteri dello Stato indicato in epigrafe, promosso dal Senato della Repubblica nei confronti della Procura della Repubblica presso il Tribunale ordinario di Firenze; 2) dispone: a) che la cancelleria di questa Corte dia immediata comunicazione della presente ordinanza al Senato della Repubblica; b) che il ricorso e la presente ordinanza siano notificati, a cura del ricorrente, al Procuratore della Repubblica presso il Tribunale ordinario di Firenze, entro il termine di sessanta giorni dalla comunicazione di cui al punto a), per essere successivamente depositati, con la prova dell'avvenuta notifica, nella cancelleria di questa Corte entro il termine di trenta giorni previsto dall'art. 26, comma 3, delle Norme integrative per i giudizi davanti alla Corte costituzionale.*
Così deciso in Roma, nella sede della Corte costituzionale, Palazzo della Consulta, il 24 novembre 2022.

[97] Il Senato della Repubblica è legittimato a proporre il ricorso per far valere il conflitto di attribuzione tra poteri dello stato, essendo organo competente in relazione all'applicabilità della prerogativa di cui all'art. 68, terzo comma, Cost. Allo stesso modo, sussiste la legittimazione passiva della Procura della Repubblica poiché, secondo Giurisprudenza consolidata della Corte costituzionale, il pubblico Ministero e, in particolare, il procuratore della Repubblica sono potere dello Stato in ragione dell'attribuzione, garantita dalla costituzione, inerente all'esercizio obbligatorio dell'azione penale (art. 112 Cost.), con titolarità diretta ed esclusiva delle indagini ad esso finalizzate. Dunque, il pubblico ministero, organo non giurisdizionale, deve ritenersi competente a dichiarare definitivamente, in posizione di piena indipendenza, la volontà del potere giudiziario cui appartiene.
Sotto il profilo oggettivo, la Consulta ha evidenziato che il ricorrente ha lamentato la lesione dell'attribuzione prevista dall'art. 68, terzo comma, Cost., con riferimento alla mancata richiesta di autorizzazione della Camera di appartenenza per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza. Dato che la disposizione dell'articolo mira alla protezione dell'indipendenza delle Camere dall'interferenza degli altri poteri dello stato, non c'è alcun dubbio sul fatto che il requisito oggettivo del conflitto sia fondato.

[98] C. Fontani*, La svolta della Consulta: la corrispondenza telematica è pur sempre corrispondenza,* giurisprudenza processo penale, *Diritto penale e processo* 10/2023.

senatore Renzi e due stretti collaboratori, nonché la corrispondenza a mezzo di *e-mail* tra questi ultimi siano definibili "sequestro di corrispondenza", ai fini dell'operatività della prerogativa parlamentare di cui all'art. 68, comma 3, Cost[99]. La soluzione a questa prima questione non può prescindere dalla nozione giuridica di "corrispondenza", ossia se la stessa si riferisca soltanto a quella cartacea oppure si possa parlare anche di "corrispondenza telematica"; inoltre è necessario individuare una linea di confine molto netta tra due diversi mezzi di ricerca della prova: il "sequestro di corrispondenza" e le "intercettazioni di comunicazioni o conversazioni".

L'acquisizione di *e-mail* e messaggi *WhatsAp*p del senatore non può essere definibile come intercettazione. Non si tratta di intercettazioni non perché queste abbiano ad oggetto comunicazioni orali, mentre i sequestri di corrispondenza riguardano comunicazioni scritte, cartacee o telematiche che siano. Infatti, l'art. 266*bis* c.p.p.[100] prevede espressamente che le intercettazioni possano avere ad oggetto anche flussi di comunicazioni informatiche o telematiche (dunque, non orali); inoltre, tramite l'applicazione *WhatsApp* possono essere inviati anche messaggi vocali, così come possono essere trasmessi mediante posta elettronica file audio contenenti comunicazioni orali. Si può asserire che non si tratta nel caso di specie di intercettazione perché tale deve intendersi come "*l'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio*"[101].

Perché si possa parlare di intercettazione devono necessariamente sussistere due presupposti. Il primo attiene alla questione temporale poiché la comunicazione deve essere in corso nel momento della sua captazione da parte di terza persona; infatti, questa deve cogliere la comunicazione nel suo momento dinamico e non in quello statico, cioè quello dell'acquisizione del supporto fisico che reca memoria di una comunicazione già avvenuta. Il secondo presupposto attiene alle modalità di esecuzione: l'apprensione del messaggio comunicativo da parte del terzo deve avvenire in modo occulto, ossia all'insaputa dei soggetti che stanno comunicando tra loro. Nel caso di specie, come confermato dalla Corte, non sussiste nessuno dei due presupposti.

Essendo stata esclusa la possibilità che si tratti di intercettazione, è utile analizzare se sussistano gli elementi per asserire che si tratti di sequestro di corrispondenza.

La Procura della Repubblica è favorevole alla tesi, consolidata ormai da tempo nella giurisprudenza di legittimità, secondo la quale i dati informatici conservati nella memoria di cellulare, siano essi

[99] Art. 68.3 Cost.
[100] Art. 266*bis* c.p.p.
[101] Cass. Pen., Sez. Unite, 24 settembre 2003, n. 36747. In dottrina cfr. P. Tonini-C. Conti*, Manuale di procedura penale*, Milano, 2023.

SMS, messaggi *WhatsApp* o *e-mail*, sono documenti *ex* art. 234 c.p.p.[102]. Quindi, la loro acquisizione non è né un'intercettazione né un sequestro di corrispondenza. Ai messaggi in questione non sarebbe, secondo questa tesi, applicabile né la disciplina dell'art. 266*bis* c.p.p.[103] né quella di cui all'art. 254 c.p.p.[104] che concerne il sequestro di corrispondenza poiché questo dispone che: *" Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati".*

Per comprendere in modo chiaro quale sia il confine tra questi due mezzi di ricerca della prova, la giurisprudenza di legittimità[105] utilizza il "criterio dell'inoltro", in base al quale lo spartiacque è rappresentato dall'avvenuto invio, o meno, del messaggio dal mittente al destinatario: da ciò, dipende l'esistenza di un flusso informatico-comunicativo, circostanza da cui dipende la necessità di ricorrere alle norme sulle intercettazioni telematiche[106].

Questo approccio è in linea con la tesi della dottrina, secondo la quale il messaggio comunicativo, una volta che il destinatario ne abbia preso conoscenza, smette di essere "corrispondenza" e quindi la relativa segretezza non è più garantita dall'art. 15 della Costituzione[107], ma da altre disposizioni costituzionali, ad esempio, quelle che garantiscono la libertà personale[108], la libertà domiciliare[109], la libertà di manifestazione del pensiero[110], il diritto di proprietà[111], ecc.

---

[102] Art. 234 c.p.p.
[103] Art. 266*bis* c.p.p.
[104] Art. 254 c.p.p.
[105] Cfr. la sentenza Cass. Pen., Sez. IV, 28 giugno 2016, n. 40903, Grassi, in CED, Rv. 268228: "*indipendentemente dal sistema di intrusione utilizzato (quello dell'accesso diretto al computer ovvero occulto attraverso un programma spia), quando si vanno a recuperare e-mail ormai spedite e ricevute, o conversazioni in chat già avvenute, siamo di fronte ad un'attività intercettativa".*
[106] M. Torre, *WhatsApp e l'acquisizione processuale della messaggistica istantanea*, Diritto penale e processo, 9, 2020, 1281.
[107] L'art. 15 della Costituzione garantisce la segretezza della corrispondenza stabilendo che:
"La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria [cfr. art. 111.1] con le garanzie stabilite dalla legge".
[108] Art. 13 Cost.
[109] Art. 14 Cost.
[110] Art. 21 Cost.
[111] Art. 42 Cost.

Diversamente da ciò che ha sostenuto la Procura presso il Tribunale ordinario di Firenze, il Senato della Repubblica sostiene che la protezione costituzionale non si esaurisca con la ricezione del messaggio, ma si protragga nel tempo fino a quando mittente e destinatario lo considerano attuale.

La nozione giuridica di corrispondenza, menzionata dall'art. 68, comma 3, Cost.[112] e dall'art. 4, l. n. 140/2003[113], coinvolge anche quella di natura elettronica e/o telematica, che oggi è diventata la modalità più utilizzata, garantendo le medesime prerogative di segretezza e inviolabilità di quella cartacea. La compatibilità normativa tra questi due diversi strumenti è rinvenibile già dalla previsione dell'art. 8 CEDU[114] e sul piano del diritto interno dall'entrata in vigore della L. 23 dicembre 1993, n. 547[115], "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*". La Corte Europea dei Diritti dell'Uomo ha sempre affermato la possibilità di accostare, perché compatibili, alla nozione di corrispondenza, di cui all'art. 8 cit., la posta elettronica e la messaggistica scambiata via internet, i dati memorizzati nei *server* informatici, negli *hard disk* e nei *floppy disk* o dispositivi di memorizzazione di dati.

Tali modifiche sono tutte volte ad affermare il principio per il quale l'evoluzione rapida e costante delle nuove tecnologie ha determinato una sostanziale dematerializzazione di molti oggetti di tutela giuridica, peraltro già tutti considerati dal codice, estendendone la portata anche oltre le caratteristiche fisiche dell'oggetto di esse.

Nel contesto che si sta esaminando si può inserire anche il comma 4 dell'art. 616 c.p.[116] che fornisce la nuova nozione giuridica di "corrispondenza", prescritta dalla legge come unitaria perché è intesa come tale sia nella sua forma cartacea, sia in quella informatica e telematica: essa comprende ogni forma di comunicazione scritta, diretta nei confronti di un determinato soggetto e quindi limitata nella sua diffusione, "*purché sia chiaramente destinata allo scambio di messaggi (testuali o grafici o fotografici) tra più soggetti collegati*"[117]. La *ratio* a fondamento dell'equiparazione normativa tra la corrispondenza cartacea e quella elettronica/telematica nasce dalla necessità di non sottrarre, dal sistema di tutela della legge ordinaria, le esigenze di difesa dei diritti fondamentali, tutelati in primo luogo dalla Carta costituzionale *ex* art. 15. Nel ricorso per conflitto di attribuzione tra poteri dello stato depositato il 10 gennaio 2023 è scritto che: "*Sia la posta elettronica che la messaggistica di*

[112] Art. 68.3 Cost.
[113] L. 22 giugno 2003, n. 140, Disposizioni per l'attuazione dell'articolo 68 della Costituzione nonchè in materia di processi penali nei confronti delle alte cariche dello Stato.
[114] Art. 8 CEDU.
[115] L. 23 dicembre 1993, n. 547, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.*
[116] Art. 616.4 c.p., *"Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".*
[117] S. Resta, *Informatica, telematica e computer crimes*, in Informatica e diritto, VI, 1997, 1, 168-169.

testo attraverso piattaforma cd. chat sono forme ordinarie di corrispondenza e la loro tutela legislativa risponde pieno iure alle esigenze di protezione costituzionale stabilite dalla Costituzione che tra l'altro, impiega sia nell'art. 15 che nell'art. 68, comma terzo, il termine corrispondenza tout court, in tal maniera aprendo ad ogni forma di corrispondenza quale praticabile secondo la evoluzione tecnologica. Non ha alcun rilievo il fatto che la corrispondenza elettronica e/o telematica sia oggetto di spedizione attraverso sistemi informatici, in luogo che di trasferimento fisico[118]".

Devono anche essere prese in considerazione le *chat WhatsApp* e gli *sms* che si utilizzano per lo scambio di messaggistica istantanea di testo, si tratta di strumenti telematici di comunicazione per iscritto, con i quali il mittente trasmette un messaggio di testo al destinatario e, quando viene spedito, come nel caso della posta elettronica, rimane memorizzato nel dispositivo fisico nel quale è installata l'applicazione che solitamente è uno *smartphone*. Sul tema una sentenza della Cassazione Civile ha decretato che "*I messaggi che circolano attraverso le nuove 'forme di comunicazione', ove inoltrati non ad una moltitudine indistinta di persone ma unicamente agli iscritti ad un determinato gruppo, come appunto nelle chat private o chiuse, devono essere considerati alla stregua della corrispondenza privata, chiusa e inviolabile*"[119].

Il Senato della Repubblica si impegna inoltre a tracciare una netta linea di confine tra il concetto di corrispondenza e intercettazione. L'art. 616 c.p.[120] sanziona l'acquisizione illecita del contenuto della corrispondenza, anche informatico/telematica, mentre l'art. 617*quater* c.p.[121] punisce l'intercettazione della comunicazione informatico/telematica. Come ripetutamente asserito dai giudici di legittimità, la linea di confine tra le due fattispecie è molto chiara, infatti è stato da loro detto che: "*mentre nell'ambito dell'art. 617quater c.p. il termine corrispondenza non comprende ogni forma di comunicazione, ma assume un significato più ristretto, riferibile alla comunicazione nel suo momento 'dinamico' ossia in fase di trasmissione - come si ricava anche dai termini impiegati per definire le condotte alternative a quella di intercettazione, ossia 'impedisce' e 'interrompe' nell'art. 616 c.p. il termine 'corrispondenza' risulta invece funzionale ad individuare la comunicazione umana nel suo profilo 'statico' e cioè il pensiero già comunicato o da comunicare fissato su supporto fisico o altrimenti rappresentato in forma materiale, come si ricava anche in questo caso dai termini*

[118] Ricorso per conflitto di attribuzione tra poteri dello Stato depositato in cancelleria il 10 gennaio 2023 del Senato della Repubblica, n. 10, consultabile su www.gazzettaufficiale.it, 23.
[119] Sentenza Cass. Civ., Sez. lav., 10 settembre 2018, n. 21965.
[120] Art. 616 c.p.
[121] Art. 617*quater* c.p.

impiegati per descrivere le altre condotte tipizzate alternativamente a quella di illecita cognizione (sottrarre, distrarre, sopprimere e distruggere)"[122].

Per concludere, nella società odierna il concetto di corrispondenza comprende anche le comunicazioni, per messaggi o tramite le applicazioni più comuni come *WhatsApp* e *Telegram.* Per comprendere meglio la nozione di corrispondenza, in tale frangente, si esamineranno di seguito alcune considerazioni della dottrina[123] e della giurisprudenza. Il primo criterio per identificare la nozione di corrispondenza è quello della sua segretezza garantita diversamente nel caso di corrispondenza cartacea o elettronica. Nel caso della prima consiste nella chiusura del testo scritto in una busta, mentre, per la seconda tipologia si ha segretezza perché la visibilità del messaggio è riservata esclusivamente ai soggetti legittimati ad avere accesso al sistema informatico[124]. Con specifico riferimento alla posta elettronica la Corte di cassazione ha stabilito che "*tale corrispondenza può essere qualificata come 'chiusa' solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di avvio o di ricezione dei singoli messaggi. Infatti, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite*"[125]. Esiste, infatti, un legame molto forte tra libertà della corrispondenza e la sua segretezza: "*la corrispondenza è libera in quanto segreta ed è al contempo segreta per poter essere libera*"[126].

---

[122] Cfr. Sez. 5, n. 12603 del 2 febbraio 2017, Segagni, Rv. 26951701 che pone a raffronto l'art. 616 cp. e l'art. 617 c.p. Inoltre, Così la sentenza Cass. Pen., Sez. V, 29 settembre 2020, n.30735. La Corte di legittimità ha ribadito la natura giuridica di corrispondenza di quella elettronica anche quando è stata chiamata a tracciare la linea di confine tra gli artt. 616 e 617 c.p.: "orbene, non è dubitabile che sul piano concettuale la 'corrispondenza' costituisca null'altro che una specie del genus comunicazione, ma è altrettanto indubbio che nell'ambito dell'art. 617 c.p. quest'ultimo termine non identifichi il genus nella sua astratta omnicomprensività, ma assuma un significato maggiormente
specializzato, riferibile al profilo 'dinamico' della comunicazione umana e cioè alla trasmissione in atto del pensiero, come suggeriscono anche l'ulteriore termine dispiegato per definire l'oggetto materiale del reato ('conversazione') ... Allo stesso modo, nell'art. 616 c.p., l'evocazione del concetto 'corrispondenza' risulta invece funzionale ad individuare la comunicazione umana nel suo profilo 'statico' e cioè in pensiero dà comunicato o da comunicare fissato su un Supporto fisico o altrimenti rappresentato in forma materiale" (così la sentenza Cass. Pen., Sez. V, 2 febbraio 2017, n.
12603).

[123] Cfr. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 163 ss.; P. Barile - E. Cheli, *Corrispondenza (libertà di*), in Enc. dir., X, Milano, 1962, 743 ss. ;P. Caretti, I diritti fondamentali, Torino, 2005, 275 ss. ;P. Caretti, *Diritto dell'informazione e della comunicazione: stampa, radiotelevisione, telecomunicazioni, teatro e cinema*, Bologna, 2005, 1-313; F. Donati ,Art. 15, in R. Bufalco - A. Celotto -M. Olivetti (a cura di), *Commentario alla Costituzione*, 1, Torino, 2006, 362 ss.; M. Di Majo, *Corrispondenza* (dir. priv.), in Enc. dir., XI, Milano, 1962, 741 ss.; A. Pace, *Contenuto e oggetto della libertà di corrispondenza e di comunicazione*, in Scritti in onore di C. Mortati, I, Milano, 1977, 813 ss.
G.M. Salerno, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. Nania - P. Ridola (a cura di), I diritti costituzionali, Torino, I, 2001; A. Valastro*, Libertà di comunicazione e nuove tecnologie*, Milano, 2001, XI-396.

[124] 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", consultabile su www.federalismi.it., 7, 2023, 234 ss.

[125] Cass. Pen., Sez. V, 19 dicembre 2007, n. 47096.

[126] P. Barile, *Diritti dell'uomo*, cit., 163. Sul punto, cfr. sentenza Corte cost. n. 20 del 2017, Considerato in Diritto 3.1. che, nel riprendere la pronuncia della Corte Cost. n. 366 del 1997, afferma: *"La 'libertà' e la 'segretezza' della 'corrispondenza*

Secondo una tesi della dottrina minoritaria[127], la segretezza non sarebbe una modalità per garantire la libertà della comunicazione, ma una vera e propria caratteristica delle comunicazioni ai sensi dell'art 15[128] della Costituzione.

Secondo dottrina maggioritaria[129], invece, nonostante "libertà" e "segretezza" rimangano sempre connesse, sono due distinte situazioni soggettive, tutelate dalla norma di rango costituzionale. La distinzione tra le due situazioni renderebbe possibile ai titolari di rinunciare spontaneamente alla segretezza della comunicazione, utilizzando mezzi di trasmissione che non la garantiscono, oppure dando l'autorizzazione al destinatario a rendere pubblico il messaggio, senza che ciò comporti il venir meno delle garanzie costituzionali di cui all'art. 15 Cost[130].

Altre due caratteristiche peculiari che contraddistinguono la comunicazione sono: l'inter-subiettività o personalità e l'attualità. L'inter-subiettività è definibile come "*indice della volontà del soggetto di selezionare e delimitare la cerchia dei propri destinatari e, dunque, di comunicare con essi in modo esclusivo*"[131]. Per quanto riguarda l'attualità, la comunicazione smette di essere tale quando, per il decorrere del tempo, viene meno il carattere privato e personale ed il suo oggetto acquista: "*un mero valore retrospettivo, affettivo, collezionistico, storico, artistico, scientifico o probatorio"*[132]. Secondo questa interpretazione, in sintesi, una comunicazione acquista il carattere della inter-subiettività in ragione dell'animus del mittente, cioè la volontà del mittente di far pervenire il messaggio a soggetti da lui determinati e non a destinatari illimitati.

Secondo l'opinione del Senato della Repubblica la corrispondenza cartacea già recapitata può essere oggetto di sequestro documentale *ex* art. 253 c.p.p.[133]; tesi avvalorata dall'art. 254 c.p.p.[134], norma speciale, applicabile al sequestro di corrispondenza "*in corso di spedizione*".

Il Senato sottolinea come, secondo la tesi fatta propria dalla Procura della Repubblica, la Cassazione considera corrispondenza "tutelabile" quella recapitata. Questo esplica il motivo per cui secondo i

---

e di ogni altra forma di comunicazione' sono oggetto del diritto 'inviolabile' tutelato dall'art. 15 Cost., che garantisce 'quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana'".

[127] A. Pace, Art. 15, in Comm. Cost. Branca, Bologna-Roma, 1977, 85.

[128] Art. 15 Cost.

[129] Cfr. P. Barile, *Diritti dell'uomo*, cit., 164; M. .Petrone, *voce Segreti (delitti contro l'inviolabilità dei*), in Noviss. Dig. it., XVI, Torino, 1969, 972.

[130] Art. 15 Cost.

[131] A. Valastro, *Libertà di comunicazione e nuove tecnologie.*

[132] Questa è la tesi sostenuta da P. Barile - E. Cheli, *Corrispondenza (libertà di*), cit., 744-745;
Cfr. anche F. Antolisei, *Manuale di diritto penale*, Milano, 2003, 253, secondo cui la corrispondenza perde, caso per caso, il suo carattere di attualità- divenendo un semplice documento - "*quando, per decorso del tempo od altra causa, non le si può assegnare che un valore meramente retrospettivo, affettivo, collezionistico, storico, scientifico, artistico o probatorio*".

[133] Art. 253 c.p.p.

[134] Art. 245 c.p.p.

giudici di legittimità la posta elettronica e gli sms non sono definibili corrispondenza, ma documenti e quindi l'art. 254 c.p.p.[135] non sarebbe applicabile alla posta elettronica, suscettibile di intercettazione in fase di transito. Il Senato sottolinea che posta elettronica e *sms* restano classificabili, comunque, come corrispondenza sotto il profilo della natura giuridica quando sono recapitati al destinatario e come la corrispondenza cartacea sono suscettibili di sequestro documentale, con l'osservanza però di tutte le garanzie di legge previste per i parlamentari. Proprio la *ratio* della garanzia di cui all'art. 68 Cost. non possono che arrivare alla conclusione secondo la quale tale previsione costituzionale coinvolge necessariamente la corrispondenza di natura elettronica e telematica. Di conseguenza, l'interpretazione che vuole sottrarre alla protezione della garanzia costituzionale le forme di corrispondenza elettronica, al giorno d'oggi utilizzata giornalmente, porterebbe sia allo svuotamento completo del contenuto applicativo della prerogativa parlamentare e all'esito di subordinare l'attivazione di quest'ultima alla casualità dello strumento di corrispondenza, sia essa cartacea o elettronica, prescelta dal singolo parlamentare.

La Consulta nella sentenza n. 38 del 2019 ha chiarito che "*quel che ai fini della presente decisione conta, in ogni caso, è che sono le norme legislative a dover essere osservate alla luce della Costituzione, e non già quest'ultima alla stregua di ciò che stabilisce la disciplina legislativa (nella specie, quella processuale)*". *Per questa essenziale ragione non è consentito trarre, ma partire dalle norme processuali in materia di intercettazioni e acquisizione di tabulati, alcuna definitiva conclusione quanto alla specifica disciplina costituzionalmente sancita, nella stessa materia, per i parlamentari, anche perché la disciplina del codice potrebbe mutare in futuro, proprio sugli aspetti qui rilevanti, e anche in direzione di un più omogeneo trattamento di intercettazioni e acquisizione di tabulati*"[136]. Questa sentenza è molto importante poiché ha stabilito con fermezza che l'obbligo di previa autorizzazione riguarda anche l'acquisizione dei tabulati telefonici, confermando l'opinione dottrinale secondo la quale l'acquisizione dei tabulati è da equiparare al sequestro della corrispondenza[137].

Esposte le tesi contrapposte della Procura e del Senato, veniamo adesso alla posizione della Corte costituzionale. La Corte, come impostazione generale, afferma che lo scambio di *e-mail*, *SMS*, messaggi *WhatsApp* o applicazioni di messaggistica simili sia, a tutti gli effetti e senza alcun dubbio, una forma di corrispondenza ai sensi degli artt. 15[138] e 68, comma 3[139], Cost. Il concetto di

[135] Art. 254 c.p.p.
[136] Corte Cost. 23 gennaio-6 marzo 2019, n. 38.
[137] D. Negri, *voce Immunità parlamentare* (dir. proc. pen), in *Enc. dir.*, Agg., II-2, Milano, 2008, 694 e nt. 117, il quale osserva che *"il riferimento contenuto nell'art. 68, comma 3 cost. non può intendersi circoscritto all'istituto ex art. 254 c.p.p., ma va esteso ad ogni provvedimento acquisitivo con esso fungibile".*
[138] Art. 15 Cost.
[139] Art. 68.3 Cost.

corrispondenza è decisamente molto ampio e quindi idoneo a ricomprendere ogni comunicazione di pensiero umano, siano questi idee, propositi, sentimenti, dati, notizie, tra due o più persone determinate, attuata in modo diverso dalla comunicazione in presenza, la Corte ha affermato in varie pronunce che la tutela accordata dall'art. 15 Cost. prescinde dalle caratteristiche del mezzo tecnico utilizzato ai fini della trasmissione del pensiero, "*aprendo così il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata*"[140]. La garanzia si estende ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti e nemmeno immaginabili nel momento della stesura della Carta costituzionale[141] quindi la posta elettronica e i messaggi inviati tramite *WhatsApp* sono pienamente coperti dall'art. 15 Cost., poiché sono completamente compatibili a lettere o biglietti chiusi.

La Consulta nel merito afferma che "*la riservatezza della comunicazione, che nella tradizionale corrispondenza epistolare è garantita dall'inserimento del plico cartaceo o del biglietto in una busta chiusa, è qui assicurata dal fatto che la posta elettronica viene inviata a una specifica casella di posta, accessibile solo al destinatario tramite procedure che prevedono l'utilizzo di codici personali; mentre il messaggio WhatsApp, spedito tramite tecniche che assicurano la riservatezza, è accessibile solo al soggetto che abbia la disponibilità del dispositivo elettronico di destinazione, normalmente protetto anch'esso da codici di accesso o altri meccanismi di identificazione*".

La conclusione rimane ferma prendendo in considerazione la prerogativa parlamentare di cui all'art. 68 comma 3, Cost[142]; infatti "*é ben vero che tale disposizione fa riferimento esclusivamente alla 'corrispondenza', e non pure, come l'art. 15 Cost., alle 'altre forme di comunicazione', e che tra i due concetti - 'corrispondenza' e 'comunicazione' - intercorre, per corrente affermazione, un rapporto di species ad genus*". Però è necessario aggiungere che la nozione di "corrispondenza", utilizzata anche nell'art. 68, comma 3, Cost., appare comunque abbastanza ampia da comprendere le forme di scambio di pensiero a distanza che qui vengono in rilievo. "*Sostenere il contrario, in un momento storico nel quale la corrispondenza cartacea, trasmessa tramite il servizio postale e telegrafico, è ormai relegata, nel complesso, a un ruolo di secondo piano, significherebbe d'altronde deprimere radicalmente la valenza della prerogativa parlamentare in questione*"[143]

---

[140] Corte Cost., sentenza n.2 del 2023.

[141] Corte cost., sentenza n. 20 del 2017; già in precedenza, con riguardo agli apparecchi ricetrasmittenti di debole potenza.
Corte cost. sentenza n. 1030 del 1988; sulla libertà del titolare del diritto di scegliere liberamente il mezzo con cui corrispondere.
Corte cost. sentenza n. 81 del 1993.

[142] Art. 68.3 Cost.

[143] "*Soccorre, peraltro, nella direzione considerata anche la giurisprudenza della Corte europea dei diritti dell'uomo, la quale non ha avuto incertezze nel ricondurre sotto il cono di protezione dell'art. 8 CEDU - ove pure si fa riferimento alla 'corrispondenza' tout court - i messaggi di posta elettronica (Corte EDU, grande camera, sentenza 5 settembre 2017,*

Problema strettamente correlato al precedente, e nucleo della questione, sulla quale dibattono le contrapposte opinioni del Senato della Repubblica e della Procura, è stabilire se possano essere considerati corrispondenza, non soltanto i messaggi *in itinere*, ma anche i messaggi di posta elettronica e *WhatsApp* già recapitati e visualizzati dal destinatario e soprattutto conservati nella memoria dei dispositivi elettronici, con i quali sono stati inviati, del destinatario o del mittente. La questione riporta la diatriba ai limiti temporali finali della tutela accordata dall'art. 15 Cost[144].

In base ad un primo indirizzo, al quale aderisce il Senato della Repubblica, la tutela non termina con la ricezione del messaggio da parte del destinatario, ma permane finché la comunicazione continua ad avere carattere di attualità e interesse per le persone che stanno tra loro comunicando. La garanzia termina solo quando, per effetto del passare del tempo o per altra motivazione, il documento diventa storico, assumendo dunque un valore retrospettivo artistico, collezionistico.

Secondo la Procura di Firenze, al contrario, la corrispondenza già ricevuta e letta dal destinatario non è più un mezzo di comunicazione, ma un documento; dunque, tale corrispondenza non sarebbe più tutelata dall'art. 15 Cost., ma da altre disposizioni costituzionali. A supporto della propria tesi, la Procura invoca quella giurisprudenza di legittimità ormai consolidata, come descritto precedentemente, secondo la quale i messaggi di posta elettronica, *SMS* e *WhatsApp*, ricevuti e memorizzati nei dispositivi elettronici come *computer* o *smartphone* del mittente o del destinatario, hanno natura documentale ai sensi dell'art. 234 c.p.p.[145], l'acquisizione dei quali non sarà soggetta né alla disciplina delle intercettazioni di comunicazioni informatiche o telematiche, *ex* art. 266*bis* c.p.p.[146], né a quella del sequestro di corrispondenza di cui all'art. 254 c.p.p.[147]

La Corte costituzionale aderisce alla tesi del Senato della Repubblica poiché classificando la comunicazione come documento, quando non più *in itinere*, si potrebbe arrivare ad azzerare la tutela costituzionale di cui all'art. 15 Cost.[148] rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea. Inoltre, l'art. 68, comma 3, Cost.[149] non preserva un

---

Barbulescu contro Romania, paragrafo 72; Corte EDU, sezione quarta, sentenza 3 aprile 2007, Copland contro Regno Unito, paragrafo 41), gli SMS (Corte EDU, sezioni quinta, sentenza 17 dicembre 2020, Saber contro Norvegia, paragrafo 48) e la messaggistica istantanea inviata e ricevuta tramite internet (Corte EDU, Grande Camera, sentenza Barbulescu, paragrafo 74).Come ricorda il ricorrente, d'altro canto, a livello di legislazione ordinaria interna, il quarto comma dell'art. 616 cod. pen., come sostituito dall'art. 5 della legge n. 547 del 1993, già da tempo include espressamente nella nozione di 'corrispondenza' - agli effetti delle disposizioni che contemplano i delitti contro l'inviolabilità dei segreti - oltre a quella epistolare, telegrafica e telefonica, anche quella 'informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza". In questo senso sentenza Corte Cost. n 170, 2023.

[144] Art. 15 Cost.

[145] Art. 234 c.p.p.

[146] Art. 266bis c.p.p.

[147] Art. 254 c.p.p.

[148] Art. 15 Cost.

[149] Art. 68.3 Cost.

privilegio del singolo parlamentare, ma una prerogativa "*strumentale [...] alla salvaguardia delle funzioni parlamentari", in quanto si vuole impedire che intercettazioni e sequestri di corrispondenza possano essere "indebitamente finalizzati ad incidere sullo svolgimento del mandato elettivo, divenendo fonte di condizionamenti e pressioni sulla libera esplicazione dell'attività"*[150].

Sul punto la Corte asserisce: "*Come nota anche la difesa del Senato, nella prospettiva avversata, sarebbe agevole per gli organi inquirenti eludere l'obbligo costituzionale di autorizzazione preventiva per acquisire la corrispondenza del parlamentare: anziché captare le comunicazioni nel momento in cui si svolgono, basterebbe attenderne la conclusione (che nel caso dei messaggi elettronici è peraltro pressoché coeva), per poi sequestrare il dispositivo in cui vi è traccia del loro contenuto*[151]".

Il sequestro di messaggi elettronici, anche se già ricevuti dal destinatario, non può non avere le prerogative di cui agli artt. 15 e 68, comma 3, Cost.; anche perché tale operazione consente agli inquirenti di conoscere non solo i dati identificativi estrinseci delle comunicazioni, ma anche il loro contenuto e quindi sussiste un'intrusione importante nella sfera personale di chi è mittente o destinatario di tali comunicazioni.

Il diverso indirizzo dei giudici di legittimità, sul quale fa leva la Procura, risulta concentrato sulla specificità della disciplina di cui all'art. 254 c.p.p.,[152] che si sofferma soltanto sulla disciplina del sequestro di corrispondenza operato presso i gestori di servizi postali, telegrafici, telematici o di telecomunicazioni: dunque, il sequestro di corrispondenza *in itinere*, che interrompe il flusso comunicativo. Dunque, l'art. 15 Cost.[153] tutela la corrispondenza di tutti i cittadini e a maggior ragione quella dei membri del Parlamento anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, trasformandosi in un mero documento "storico". L'attualità si presume, fino a prova contraria, quando si tratta di messaggi che sono stati scambiati a breve distanza di tempo rispetto al momento in cui dovrebbero

[150] Cfr. la sentenza Corte cost. n. 390 del 2007; in senso analogo anche: Corte cost. n. 38 del 2019, Corte cost. n. 74 del 2013 e ord. Corte cost. n. 129 del 2020.

[151] Afferma sul punto la Corte cost. nella sentenza in commento: "*Questa Corte, d'altronde, ha già da tempo affermato che la garanzia apprestata dall'art. 15 Cost. si estende anche ai dati esteriori delle comunicazioni (quelli, cioè, che consentono di accertare il fatto storico che una comunicazione vi è stata e di identificarne autore, tempo e luogo): problema postosi particolarmente in rapporto ai tabulati telefonici, contenenti l'elenco delle chiamate in partenza o in arrivo da una determinata utenza (sentenza n. 81 del 1993; in senso conforme, sentenze n. 372 del 2006 e n. 281 del 1998). In proposito, si è rilevato che 'la stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità- attinenza che induce a qualificare il corrispondente diritto 'come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana' (v. sent. n. 366 del 1991) - comporta un particolare vincolo interpretativo, diretto a conferire a quella libertà, per quanto possibile, un significato espansivo' (sentenza n. 81 del 1993)".*

[152] Art. 254 c.p.p.

[153] Art. 15 Cost.

essere acquisiti e nel corso dello svolgimento del mandato parlamentare in cui tale momento si colloca, e peraltro ancora custoditi in dispositivi protetti da codici di accesso. La Corte ha concluso statuendo che ci si trova al cospetto di sequestri di corrispondenza rientranti nell'ambito della guarentigia di cui all'art. 68, comma 3,[154] Cost.

La sentenza della Corte mira, come ogni altra pronuncia della Consulta, a tutelare il quadro democratico costituzionale del nostro stato di diritto; si pone, nel caso di specie, in linea con l'art. 12 delle c.d. Preleggi[155] che, con l'espressione "*significato proprio delle parole secondo la connessione di esse*", delimita l'opera del giurista all'interpretazione letterale[156] della norma. Infatti, "'corrispondenza telematica' è un sintagma molto chiaro; non solo, la corrispondenza telematica è una modalità concreta della corrispondenza epistolare, che solo per convenzione consolidata è ritenuta cartacea"[157]

Analogo discorso deve essere fatto per l'art. 68, comma 3, Cost. perché chiaramente i Padri Costituenti durante la formazione della Carta Costituzionale non potevano legiferare pensando all'utilizzo dei messaggi *Whatsapp* tramite *smartphone*, ma hanno cercato di tutelare nella maniera più ampia possibile il flusso di comunicazioni tra i cittadini ed alla tutela della figura del parlamentare, imponendo la necessità dell'autorizzazione della camera di appartenenza da dare agli inquirenti per poter procedere con il sequestro della corrispondenza.

Questa sentenza della Corte Costituzionale[158] rappresenta una svolta epocale, che scardina del tutto una giurisprudenza di legittimità ormai consolidata da tempo sul concetto del "criterio dell'inoltro", in base al quale il *discrimen* tra sequestro di corrispondenza e intercettazioni di comunicazioni e conversazioni è dato dall'invio effettuato, o meno, del messaggio dal mittente al destinatario: da ciò, infatti, viene fatta dipendere l'esistenza di un flusso informatico di comunicazioni e dunque la necessità di ricorrere alle norme sulle intercettazioni telematiche.

Secondo Carolina Fontani nell'articolo "*La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*"[159], la pronuncia in esame rappresenta un grosso passo in avanti in termini di progressi del diritto e modernità giuridica. Il velocissimo progresso tecnologico impone di adeguare concetti e garanzie, che sono state stabilite in un'epoca in cui determinati strumenti non

[154] Art. 68.3 Cost.
[155] Art. 12 Preleggi.
[156] L'interpretazione cosiddetta letterale è *volta ad attribuire alla norma il significato che si evince immediatamente dalle parole utilizzate.*
[157] M. Borgobello, *Il concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale*, agosto 2023, in www.giurisprudenzapenale.it.
[158] Corte Cost., 170/2023.
[159] C. Fontani, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, *Diritto penale e processo 10/2023.*

esistevano ancora, ad un contesto storico-culturale in cui le modalità di comunicazione, da un lato, e gli strumenti investigativi in mano agli inquirenti, dall'altro, sono in costante e rapida evoluzione. Un'opinione diversa potrebbe svuotare del tutto il significato delle garanzie dettate dalla Costituzione e tentare di aggirarle[160].

Non si può non asserire che la tesi della Procura presso il Tribunale di Firenze sovrappone in modo del tutto erroneo dei concetti di teoria generale del diritto che sono molto differenti tra loro; infatti come definizione generale di documento si può dire che "*in un significato generico, il documento è quella rappresentazione di un fatto che è incorporata su un base materiale con un metodo analogico o digitale"*[161].

Bisogna distinguere il fatto rappresentato, dal metodo di incorporamento dello stesso. Nella concezione di fatto rappresentato sono ricompresi sia i "*fatti, persone o cose*" ai quali fa riferimento l'art. 234 c.p.p.[162], sia i contenuti di pensiero espressi nelle dichiarazioni di scienza e volontà. Per incorporamento si intende, invece, l'operazione mediante la quale la rappresentazione è fissata su una base materiale. Il codice prevede varie modalità di incorporamento quali: l'art. 234 c.p.p.[163] prevede la scrittura accanto alla fotografia, alla fonografia e alla cinematografia, lascia anche la possibilità che l'incorporamento avvenga tramite qualsiasi altro mezzo. In base ai numerosi progressi tecnologici i metodi di incorporamento attualmente sono due: quello analogico e quello digitale. Dunque, accanto al documento tradizionale, che possiamo definire come quella rappresentazione di un fatto che è incorporata su una base materiale con un metodo analogico, abbiamo il documento informatico, rappresentazione incorporata, invece, su una base materiale con metodo digitale, per citare alcuni esempi possiamo individuare un *file word*, *MP3* oppure un messaggio *Whatsapp* o *Telegram*.

Tornando alla pronuncia della Corte, per una visione completa di quanto stabilito di seguito brevemente verrà descritto cosa è stato statuito in merito al conto bancario personale del Senatore Matteo Renzi. Questa parte della pronuncia lascia dei dubbi poiché in merito all'estratto di conto

---

[160]*Non si è potuto negare in dottrina come la tesi fatta propria dalla Procura della Repubblica presso il Tribunale ordinario di Firenze sembri adottare una interpretazione "creativa" del dettato normativo. In termini critici si esprime M. Borgobello, Il concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale, cit.:"La tesi che ha individuato nella corrispondenza non più in itinere ma giunta a destinazione un documento - e non corrispondenza -, peraltro, appare più frutto di un abuso logico giuridico che di un ragionamento basato sul dato testuale delle disposizioni e sulle norme che da esso scaturiscono. Anche in questo caso il dato letterale è chiarissimo: nessun appiglio testuale consente di relegare la corrispondenza tra persone al solo contesto del trasferimento tra le stesse". Ed ancora, "In conclusione, l'attività interpretativa giudiziale che prescinde dal dato testuale, per forzarlo, tendenzialmente contra reum o per 'salvare' attività di indagine non sempre effettuate con tutti i crismi, portano a precedenti stratificati che devono essere demoliti dalle giurisdizioni di livello costituzionale, le uniche che possono garantire i cittadini dagli abusi commessi dalle giurisdizioni ordinarie*".

[161]P. Tonini - C. Conti, *Manuale di procedura penale*, Milano, 2023, 352 ss.

[162] Art. 234 c.p.p.

[163] Ibidem.

corrente bancario, la Consulta ha stabilito che se oggetto di apprensione da parte degli organi inquirenti fosse stato l'estratto conto spedito dalla banca al correntista, allora le garanzie previste dagli artt. 15[164] e 68, comma 3, Cost.[165] sarebbero state operative. L'unico motivo per cui tali garanzie non trovano applicazione, secondo il giudice delle leggi, in questa fattispecie, risiede nelle modalità attraverso le quali l'estratto del conto corrente bancario del senatore Renzi è entrato a far parte degli atti di indagine: tramite un decreto di acquisizione di segnalazioni di operazioni bancarie sospette effettuate in base alla normativa antiriciclaggio. Le modalità di acquisizione non mutano la natura giuridica della *res* che è entrata nella disponibilità degli inquirenti: la corrispondenza bancaria è un fatto comunicativo personalissimo, che riporta tutte le operazioni di dare e avere in un determinato periodo con l'indicazione dei destinatari e delle causali: dunque, qualificabile come corrispondenza. In conclusione, è necessario segnalare che l'occasione si fa propizia per un disegno legislativo volto ad un complessivo ripensamento del sistema delle garanzie poste a tutela della corrispondenza, ed anche per intervenire in modo più pregnante nel senso di un irrobustimento delle garanzie a presidio della segretezza delle conversazioni private[166].

II.3 La messaggistica Sky Ecc effettuata tramite cripto telefonini

Pare ora opportuno soffermarsi sulla giurisprudenza in merito alla disciplina dell'art. 234*bis* c.p.p.[167], con particolare riferimento alla messaggistica di *Sky Ecc* effettuata tramite cripto telefonini.

Per iniziare l'analisi della questione, è interessante notare che la messaggistica di *Sky Ecc,* che avviene tramite cripto telefonini, *smartphone* e *tablet*, non è l'esito di captazione di conversazioni durante il flusso dinamico delle stesse, ma si tratta acquisizione di dati informatici direttamente utilizzabili, a fini di prova *ex* art. 234*bis* c.p.p.[168], dall'autorità giudiziaria di uno Stato dell'Unione Europea, in attuazione della Direttiva 2014/41/UE[169].

Vige il principio generale di presunzione di legittimità delle prove acquisite dall'autorità giudiziaria di un altro Stato membro dell'Unione Europea: l'utilizzazione degli atti trasmessi, infatti, non è condizionata ad un accertamento da parte del giudice italiano concernente la regolarità delle modalità di acquisizione esperite dall'autorità straniera, in quanto vige la presunzione di legittimità dell'attività

[164] Art. 15 Cost.
[165] Art. 68.3 Cost.
[166] Cfr. C. Fontani, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, Diritto penale e processo 10/2023.
[167] Art. 234*bis* c.p.p.
[168] Ibidem.
[169] Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014.

svolta e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari.

In base a quanto appena descritto, la sentenza n. 19623 della Cass. pen., Sez. IV, data ud. 28/03/2023, deposito motivazione 10/05/2023[170] ha rigettato il ricorso dei difensori.

Di seguito verranno riportate le principali tappe della vicenda processuale in questione.

Con ordinanza pronunciata a norma dell'art. 309 c.p.p.[171], il Tribunale di Reggio Calabria ha confermato l'ordinanza con la quale il giudice per le indagini preliminari di Reggio Calabria aveva applicato nei confronti di A.A. la misura della custodia cautelare in carcere in ordine ai reati di cui agli artt. 61*bis*[172], 416*bis*.1 c.p.,[173] D.P.R. 9 ottobre 1990, n. 309, art. 74, commi 1, 2, 3, 4[174] in relazione alla partecipazione ad associazione dedita al narcotraffico posto in essere; D.P.R. n. 309 del 1990, artt. 73 e 80[175] in relazione al concorso nella importazione di ingenti quantitativi di sostanza stupefacente quale la cocaina.

Il Tribunale distrettuale ha desunto la sussistenza dei gravi indizi di colpevolezza dalle risultanze di una complessa attività di indagine, che aveva portato alla luce l'esistenza nel territorio interessato di un gruppo criminale articolato su più livelli e dotato di elevatissime disponibilità finanziarie, dedito alla commissione di più delitti fra quelli di cui al D.P.R. n. 309 del 1990, art. 73 e in particolare al reperimento e all'acquisto all'estero, alla importazione e al trasporto in Italia, attraverso container riposti su navi cargo in arrivo al porto di (Omissis) con la complicità di portuali infedeli, nonchè alla commercializzazione di ingenti quantitativi di sostanza stupefacente del tipo cocaina.

Il materiale investigativo su cui si è fondata la misura cautelare è costituito: dalle intercettazioni, dai risultati dei tabulati telefonici e della geolocalizzazione, dalle riprese video e dall'attività di riscontro della polizia giudiziaria, per gran parte da comunicazioni intercorse tra gli indagati attraverso il sistema *Sky Ecc* acquisite dalla Procura di Reggio Calabria tramite l'emissione di specifici Ordini di Indagine Europei[176] versarti in atti, il primo dei quali è datato 13 aprile 2021, con cui è stata chiesta all'autorità giudiziaria di Parigi la trasmissione dei messaggi decifrati riferibili alle comunicazioni di

[170] Cass. Pen., Sez. IV, 10/05/2023, n. 19623.
[171] Art. 309 c.p.p.
[172] Art. 61*bis* c.p.
[173] Art. 416bis.1 c.p.
[174] D.P.R. 9 ottobre 1990, n. 309, art. 74 commi 1,2,3,4. Titolato: Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.
[175] D.P.R. 9 ottobre 1990, n. 309, artt. 73 e 80.
[176] L'ordine europeo di indagine penale (O.e.i.) è stato introdotto dalla Direttiva 2014/41/UE e recepito dall'Italia con il d.lgs. n.108 del 2017. Può essere*, ex* art. 3 della direttiva, impiegato per ricercare e formare qualsiasi tipo di prova, con l'eccezione delle attività istruttorie svolte dalle squadre investigative comuni.

interesse già avvenute e conservate nel relativo *server* e ritenute pienamente utilizzabili dal Tribunale del riesame.

Contro l'ordinanza, ha proposto ricorso l'indagato tramite il suo difensore formulando quattro motivi. Con il primo motivo ha sostenuto che ci sia stata la violazione di legge in relazione alla utilizzabilità della chat scambiate tramite il sistema di *Sky Ecc*. Il difensore rileva che le modalità di acquisizione e decriptazione di tali messaggi non sarebbero note e verificabili: i messaggi decriptati erano stati ottenuti tramite attività compiuta da organi inquirenti esteri secondo procedure di acquisizione, estrazione e decriptazione ignote, non verificabili e non censurabili dall'indagato. L'affermazione contenuta nell'ordinanza impugnata, per cui tali atti di indagine troverebbero automatico ingresso nel processo italiano in forza di un OEI ed in ragione della presunzione di legittimità degli atti esteri, sarebbe contraddetta dalla sentenza n. 32915 del 15 luglio 2022[177] con la quale la Suprema Corte ha correttamente riconosciuto che "*rimane ferma la necessità di valutare, nell'ambito sia del procedimento principale che del procedimento incidentale de libertate, che le modalità di acquisizione di tale messaggistica non siano in contrasto con norme inderogabili e principio fondamentali del nostro ordinamento*". Questo principio deve valere nel medesimo modo sia se la importazione delle chat nel procedimento penale è avvenuta tramite organo di polizia giudiziaria (Europol)[178], sia se i dati provengono direttamente dall'autorità giudiziaria francese (Tribunale di Parigi). Disposizione non colta dal Tribunale del riesame poiché opera una netta distinzione tra acquisizione mediante organo di polizia giudiziaria ed acquisizione diretta dall'autorità giudiziaria

[177] Cass. Pen., Sez. IV, 15 luglio 2022, n. 32915. In questa pronuncia è decretato che: "*In relazione all'utilizzabilità processuale, anche in sede cautelare, della messaggistica crittografata acquisita con ordine europeo di indagine mediante l'accesso al server di una società estera, l'acquisizione dei dati informatici originari criptati e la loro trasformazione in messaggi di testo, messaggi vocali o immagini, è necessario garantire alla difesa, a pena di inutilizzabilità ex art. 191 cpp, il contraddittorio sulle modalità di acquisizione e trasformazione in forma intellegibile dei dati informatici criptati, al fine di consentire la verifica dell'attività concretamente svolta, della corrispondenza tra il dato informatico conservato nel server e il messaggio decodificato e della coincidenza delle utenze dei soggetti individuati come mittenti e destinatari".*

[178] Europol è un organismo dell'Unione Europea, istituito con regolamento 2016/794/UE del Parlamento europeo e del Consiglio l'11 maggio 2016. Opera nell'ambito della cooperazione di polizia e il suo principale compito è quello di raccogliere, conservare, analizzare e scambiare informazioni, compresi i dati di *intelligence* criminale, per sostenere e potenziare le azioni delle autorità competenti degli Stati membri e la loro cooperazione con fine di prevenzione e lotta contro la criminalità più grave che interessa due o più stati membri, il terrorismo e le forma di criminalità che ledono un interesse comune oggetto della politica dell'Unione europea*, ex* art 3.1. reg. Europol si trova all'Aia.
L'ambito di competenza di Europol è molto vasto, si occupa dei reati elencanti espressamente nell'allegato I al regolamento; per citarne alcuni: traffico illecito di stupefacenti, attività illecite di riciclaggio di denaro, criminalità nel settore delle materie nucleari e radioattive, organizzazione clandestina di immigrazione e tratta di esseri umani. Ai reati indicati tassativamente dal Regolamento si devono aggiungere i reati ad essi connessi, secondo le puntuali indicazioni dell'art. 3.2 reg 2016/794. Inoltre, Europol è designato come ufficio centrale competente per la lotta contro la falsificazione della moneta unica europea e promuove il coordinamento delle misure da applicare a riguardo delle autorità competenti degli Stati membri, anche nel quadro delle attività svolte dalle squadre investigative comuni.
Cfr. R.E. Kostoris, Manuale di procedura penale europea, Quarta edizione, Giuffrè Francis Levebvre, pag. 246 e ss.

estera: le garanzie costituzionali non cambiano e il diritto di difesa non si deve intendere diversamente in base alla modalità con la quale le *chat* sono riportate nel nostro ordinamento.

Il Tribunale, inoltre, avrebbe anche rilevato che il legale difensore non aveva formulato alla Procura nessuna richiesta di messa a disposizione di documentazione relativa alla acquisizione del materiale ulteriore rispetto a quella già versata in atti e costituita dagli OEI, dai verbali di esecuzione e dai file di conversazioni, quindi non sarebbe predicabile in astratto alcuna violazione del diritto del contraddittorio[179]: la difesa invero non aveva formulato alcuna richiesta, in quanto il PM, presente all'udienza del 25 ottobre 2022, aveva riconosciuto che non vi era alcuna documentazione riguardante lo scambio informativo fra forze di polizia di paesi diversi oggetto di una eventuale richiesta della difesa, dato che i messaggi della *chat* erano stati forniti direttamente dall'autorità giudiziaria francese.

Illegittima, inoltre, sarebbe l'ordinanza che ha ritenuto utilizzabili le chat *Sky Ecc* in forza dell'art. 234*bis* c.p.p.[180]. In primo luogo, perché l'acquisizione per esser consentita deve riguardare dati acquisiti, estratti e decrittati nel rispetto delle norme inderogabili e dei principi fondamentali dell'ordinamento. In secondo luogo, perché il consenso del titolare, cui fa riferimento la norma, non potrebbe essere, come sostenuto dal Tribunale, il consenso del possessore del dato ovvero gestore del server e autorità francese: nel caso di specie, peraltro, saremmo in presenza del solo consenso dell'autorità giudiziaria francese e non anche del gestore del *server*.

Con il secondo motivo ha dedotto il vizio di motivazione in ordine alla ritenuta esistenza della circostanza aggravante di cui all'art. 416bis.1 c.p.[181] in relazione al reato associativo.

Il Tribunale aveva sostenuto che A.A., nonostante non avesse agito personalmente, sarebbe stato comunque complice nel perfezionare la fattispecie di reato. In tal modo il Tribunale non avrebbe chiarito chi sarebbe il partecipe dell'associazione che avrebbe agito con il dolo intenzionale di agevolare le cosche di 'ndrangheta e da quali elementi in ogni caso dovesse trarsi detto dolo intenzionale. Inoltre, non potrebbero ritenersi rilevanti la conversazione fra B.B. e C.C., citata dal Tribunale, poiché A.A. non aveva partecipato a quel dialogo, nel quale non era contenuto alcun riferimento alla sua persona, ovvero la pregressa condanna di A.A. per reati di criminalità organizzata, ovvero ancora i dialoghi capatati nella riunione del 13 dicembre 2020 e la discussione intercorsa con

[179] Il diritto al contraddittorio è una delle colonne portanti del processo penale. Il riferimento normativo costituzionale è dato dall'art. 111. L'art. 111.4 statuisce che: "*Il processo penale è regolato dal principio del contraddittorio nella formazione della prova. La colpevolezza dell'imputato non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre volontariamente sottratto all'interrogatorio da parte dell'imputato o del suo difensore*". La dicitura "*nella formazione della prova*" sta a significare che il contraddittorio serve a formare la prova; se fosse stato scritto "contraddittorio sulla prova" si sarebbe trattato un contraddittorio diverso, cioè la prova sarebbe già stata formata.

[180] Art. 234*bis* c.p.p.

[181] Art. *416bis.*1 c.p.

D.D., posto che da nessuno di tali elementi era emerso il dolo intenzionale in capo ad alcuno dei sodali.

Infine, è molto particolare la motivazione dell'ordinanza nella parte in cui afferma l'assenza dell'interesse del ricorrente a sterilizzare l'efficacia della contestazione della aggravante, in quanto il ricorrente avrebbe pur sempre interesse a vedere ridimensionata la gravità del fatto e conseguentemente alla attenuazione delle esigenze cautelari.

Con il terzo motivo ha dedotto la violazione di legge perché riteneva sussistente la circostanza aggravante di cui all'art. 61*bis* c.p.[182]. Il difensore lamenta che a fronte della specifica censura posta all'udienza camerale del 25 ottobre 2022, il Tribunale avrebbe omesso qualsiasi motivazione.

Con il quarto motivo ha dedotto la violazione di legge e il vizio di motivazione in ordine alla ritenuta adeguatezza della sola misura della custodia cautelare in carcere.

Il tribunale aveva fatto riferimento a due elementi. Il primo consiste nel pericolo di inquinamento probatorio, che si sarebbe potuto concretizzare se il soggetto fosse stato lasciato libero; tale giustificazione appare illogica al difensore poiché con la misura degli arresti domiciliari l'indagato non sarebbe libero. Il tribunale aveva ritenuto inidonea la misura degli arresti domiciliari poiché temeva che l'indagato potesse avere contatti con altre persone coinvolte nella vicenda. Non tenendo conto della possibilità, dettata nel codice all'art. 284 c.p.p.[183] proprio per scongiurare una simile situazione, di imporre il divieto all'indagato agli arresti domiciliari di comunicare con terze persone esclusi coloro che lo assistono e vi coabitano.

Il secondo elemento consiste nel pericolo di reiterazione, tratto da elementi congetturali e privi del requisito della concretezza e attualità, tanto che sarebbero stati valorizzati i precedenti penali del ricorrente che erano risalenti addirittura agli anni 90.

Il ricorso è stato rigettato. Il primo motivo, relativo alla dedotta inutilizzabilità della messaggistica scambiata su una piattaforma denominata *SKY ECC*, è infondato. Il Tribunale ha chiarito che tale piattaforma è un sistema che consente lo scambio di comunicazioni mediante uso di cripto-telefonini o *smartphone*, modificati in modo da garantirne la inviolabilità poiché consentono di disattivarne la geolocalizzazione, i servizi *Google*, il Bluetooth, la fotocamera e tutto ciò che rischia di renderne possibile la captazione. La violazione della piattaforma criptata era avvenuta da parte di *law*

[182] Art. 61*bis* c.p. rubricato "*Circostanza aggravante del reato transnazionale*" che stabilisce : "*Per i reati puniti con la pena della reclusione non inferiore nel massimo a quattro anni nella commissione dei quali abbia dato il suo contributo un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato la pena è aumentata da un terzo alla metà. Si applica altresì il secondo comma dell'articolo 416bis.1*".
[183] Art. 284 c.p.p.

enforcement agencies[184] e il suo utilizzo si era arrestato nel marzo del 2021, nel momento in cui si era diffusa la notizia dell'avvenuta violazione. Gli esiti dell'indagine presupposta, cioè condotta dalle squadre investigative appena menzionate sulla piattaforma utilizzata dai dispositivi controllati, avevano consentito l'acquisizione e l'analisi di milioni di messaggi scambiati tra membri di organizzazioni criminali operanti in vari Paesi UE ed è in questo contesto si era inserita l'indagine condotta dalla Procura della Repubblica di Reggio Calabria. La polizia giudiziaria, infatti, analizzando il traffico telefonico storico delle celle abitualmente abbinate alle utenze "ufficiali" in uso agli indagati, aveva individuato alcuni *PIN* collegati alla piattaforma criptata. Conseguentemente il Pubblico Ministero procedente, a partire dal 13 aprile, aveva, tramite vari ordini europei di indagine penale rivolti all'Autorità Giudiziaria francese, richiesto la trasmissione dei messaggi già decifrati riferibili alle comunicazioni che avevano riguardato i *PIN* d'interesse, conservate in un *server.*

Il Tribunale, in replica ad analoga censura fatta valere in sede di riesame ha, dunque, dedotto vari concetti.

In primo luogo, la Procura di Reggio Calabria, attraverso l'emissione di specifici O.E.I., tutti versati in atti, ha richiesto all'autorità giudiziaria francese la trasmissione dei messaggi decifrati riferibili alle comunicazioni già avvenute e conservate nel *server* e, a seguito di tale richiesta, l'autorità francese ha trasmesso su *CD* i file integrali, estratti dal *server* e decriptati, delle comunicazioni riferibili allo specifico pin oggetto di richiesta: in atti risulta versata la copia dei predetti file.

Inoltre, la messaggistica non è stata acquisita attraverso operazioni di intercettazione di comunicazioni telematiche, ma attraverso la richiesta ad uno stato estero, la Francia, con O.E.I., di trasmettere, previa decriptazione, messaggi di comunicazioni già avvenute e conservati presso il server della società che gestisce il servizio di messaggistica, acquisiti nell'osservanza dell'ordinamento francese.

Ancora, il mezzo di prova in argomento deve essere ricondotto nell'ambito di applicazione dell'art. 234*bis* c.p.p.[185], secondo cui *è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero anche diversi da quelli disponibili al pubblico, previo consenso in tale ultimo caso, del legittimo titolare*. Il consenso nel caso in esame esisteva, come legittimo titolare è stato inteso colui che abbia il possesso del dato, tale da garantirgli un livello di autonomia che consenta di accedere in modo autonomo ad esso anche al di fuori della diretta vigilanza della persona che abbia sul dato un potere maggiore ovvero il gestore del *server*: legittimo titolare nel caso di specie, è dunque

[184] Sono squadre dalle polizie francese, belga e olandese.
[185] Art. 234*bis* c.p.p.

l'autorità giudiziaria francese che di quei dati poteva giuridicamente disporre in quanto aveva sottoposto a sequestro il *server* in cui i dati erano archiviati.

Inoltre, devono trovare applicazione, per il principio *locus regit actum* e in conformità con i canoni del diritto internazionale della prevalenza della *lex loci* sulla *lex fori*[186].

Ancora, vi è un richiamo alla sentenza della Cassazione del 7 settembre 2022 n. 32915[187], Lori è inconferente poiché in quel caso, sicuramente inerente perché trattava la messaggistica scambiata sulla piattaforma *SKY ECC*, era stato censurato il provvedimento del PM di rigetto dell'ostensione alla difesa della documentazione riferibile alle comunicazioni criptate, consegnate tramite Europol e non direttamente dall'autorità giudiziaria dello Stato estero, come nella specie, in cui il materiale informatico era stato trasmesso dal Tribunale di Parigi. Il Tribunale ha rilevato che negli atti erano stati versati tutti i documenti inviati dall'autorità francese in risposta ai singoli O.E.I. e depositati i provvedimenti genetici con i quali l'autorità giudiziaria francese aveva disposto l'acquisizione della messaggistica; ha osservato che nel caso di specie la difesa non aveva formulato alla Procura alcuna richiesta di messa a disposizione di documentazione relativa all'acquisizione del materiale probatorio, ulteriore rispetto a quella già versata in atti, in seguito a ciò non poteva essere ravvista alcuna violazione del principio del contraddittorio[188].

In aggiunta, si tratta di percorso argomentativo che ha completamente rispettato i principi di diritto che governano la materia della cooperazione internazionale. Si deve, innanzitutto, premettere che il PM ha agito nell'ambito dei poteri previsti nel Capo 1 del Titolo 3 del D.lgs. 21 giugno 2017, n. 108[189], contenente le norme di attuazione della direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014[190], relativa all'ordine Europeo d'indagine penale. È uno strumento inteso che ha lo scopo di implementare le già esistenti forme di cooperazione penale nell'ambito dell'Unione

---

[186] Secondo le regole del diritto internazionale in base al principio del locus *regit actum* devono prevalere le norme dello Stato in cui l'atto viene compiuto e non quelle del codice di rito del paese richiedente che disciplinano il processo

[187] Cass. Pen., Sez. IV, 7 settembre 2022, n. 32915.

[188] Disciplinato dall'art. 111 Cost.

[189] D. lgs. 21 giugno 2017, n. 108. Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

[190] Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014.

La presente direttiva ha lo scopo di semplificare e accelerare le indagini penali transfrontaliere nell'Unione europea. Essa introduce l'ordine europeo di indagine, che consente alle autorità giudiziarie in un paese dell'UE («Stato di emissione») di chiedere che siano raccolte e trasferite le prove da un altro paese dell'UE («Stato di esecuzione»).

Poiché l'OEI si basa sul principio del reciproco riconoscimento, ogni paese dell'UE è tenuto in linea di principio a riconoscere ed eseguire una tale richiesta. Essa deve inoltre essere eseguita in tempi brevi e senza ulteriori formalità.

L'OEI rende più facile far fronte ai reati, tra cui i reati come la corruzione, il traffico di droga e la criminalità organizzata. Ad esempio, la polizia greca potrebbe chiedere ai suoi omologhi nel Regno Unito di effettuare perquisizioni o interrogare testimoni per suo conto.

L'OEI migliora le leggi UE esistenti che disciplinano questo settore fissando scadenze rigorose per raccogliere le prove richieste e limitando i motivi per rifiutare tali richieste. Riduce anche il lavoro di ufficio con l'introduzione di un unico modulo standard per le autorità che richiedono aiuto nella raccolta delle prove.

Europea di cui all'art. 82, paragrafo 1, TFUE[191], che si fonda sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie. Tale principio è a sua volta fondato sulla fiducia reciproca, sulla presunzione del rispetto degli altri Stati membri del diritto dell'Unione e, in particolare, i diritti fondamentali[192]. In tale cornice, si inseriscono l'art. 2 della direttiva[193], il quale dispone che "*Gli Stati membri eseguono un OEI in base al principio del riconoscimento reciproco e conformemente alla presente direttiva*" e l'art. 9[194], secondo cui "*L'autorità di esecuzione riconosce un OEI, trasmesso conformemente alle disposizioni della presente direttiva, senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione, a meno che non decida di addurre uno dei motivi di non riconoscimento o di non esecuzione ovvero uno dei motivi di rinvio previsti dalla presente direttiva*". Perciò, viste le disposizioni appena citate, l'ordine Europeo di indagine penale deve aver ad oggetto una prova acquisibile nello Stato di emissione e deve essere eseguito in conformità di quanto previsto nello Stato di esecuzione per il compimento di un analogo

[191] Art. 82, paragrafo 1, TFUE. Impone: "1. La cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri nei settori di cui al paragrafo 2 e all'articolo 83.
Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, adottano le misure intese a: a) definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria; b) prevenire e risolvere i conflitti di giurisdizione tra gli Stati membri; c) sostenere la formazione dei magistrati e degli operatori giudiziari; d) facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni.
2. Laddove necessario per facilitare il riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e la cooperazione di polizia e giudiziaria nelle materie penali aventi dimensione transnazionale, il Parlamento europeo e il Consiglio possono stabilire norme minime deliberando mediante direttive secondo la procedura legislativa ordinaria. Queste tengono conto delle differenze tra le tradizioni giuridiche e gli ordinamenti giuridici degli Stati membri.
Esse riguardano: a) l'ammissibilità reciproca delle prove tra gli Stati membri; b) i diritti della persona nella procedura penale; c) i diritti delle vittime della criminalità; d) altri elementi specifici della procedura penale, individuati dal Consiglio in via preliminare mediante una decisione; per adottare tale decisione il Consiglio delibera all'unanimità previa approvazione del Parlamento europeo. L'adozione delle norme minime di cui al presente paragrafo non impedisce agli Stati membri di mantenere o introdurre un livello più elevato di tutela delle persone.
3. Qualora un membro del Consiglio ritenga che un progetto di direttiva di cui al paragrafo 2 incida su aspetti fondamentali del proprio ordinamento giuridico penale, può chiedere che il Consiglio europeo sia investito della questione. In tal caso la procedura legislativa ordinaria è sospesa. Previa discussione e in caso di consenso, il Consiglio europeo, entro quattro mesi da tale sospensione, rinvia il progetto al Consiglio, ponendo fine alla sospensione della procedura legislativa ordinaria. Entro il medesimo termine, in caso di disaccordo, e se almeno nove Stati membri desiderano instaurare una cooperazione rafforzata sulla base del progetto di direttiva in questione, essi ne informano il Parlamento europeo, il Consiglio e la Commissione. In tal caso l'autorizzazione a procedere alla cooperazione rafforzata di cui all'articolo 20, paragrafo 2 del trattato sull'Unione europea e all'articolo 329, paragrafo 1 del presente trattato si considera concessa e si applicano le disposizioni sulla cooperazione rafforzata.

[192] Come rifermenti giurisprudenziali si consultino: Sentenza del 21 novembre 2021 della Corte di Giustizia Europea e la sentenza dell'8 dicembre 2020 della Corte di giustizia Europea.
La prima è contestualizzata nel corso del procedimento penale nei confronti di Ivan Gavanozov durante il quale è stata proposta domanda di pronuncia pregiudiziale dallo Spetsializiran nakazatelen sad. La seconda, invece, tratta la causa C-584/19, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Landesgericht für Strafsachen Wien (Tribunale del Land in materia penale di Vienna, Austria), con decisione del 1° agosto 2019, pervenuta in cancelleria il 2 agosto 2019, nel procedimento penale a carico di A. e a., con l'intervento di Staatsanwaltschaft Wien.

[193] Art. 2 Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014.

[194] Art. 9 Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014.

atto di acquisizione probatoria, potendosi peraltro presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo che non sussista un'evidente violazione. Il pubblico ministero, con gli O.E.I in esame, ha chiesto la trasmissione di documentazione già acquisita dall'autorità estera nel corso di un diverso procedimento pendente in quel Paese.

L'ordine europeo di indagine doveva solo dar conto dello specifico oggetto della prova, essendo rimessa allo Stato di esecuzione, con le modalità previste in quell'ordinamento, la concreta acquisizione della prova, da trasferire poi allo Stato di emissione: nella specie, come detto, la richiesta ha riguardato le chat del sistema *Sky ECC*, già acquisite dal Tribunale di Parigi autonomamente e non su richiesta della Procura procedente nel nostro Paese. L'Autorità francese, dunque, si è resa garante, in assenza di specifiche deduzioni di segno diverso, del rispetto delle procedure dello Stato di esecuzione, ovvero la Francia, avendo il Tribunale del riesame dato atto che dalla documentazione trasmessa era dato verificare la modalità di acquisizione e conservazione dei dati da parte dell'Autorità giudiziaria francese. La messaggistica esaminata dal Tribunale di Reggio Calabria non costituisce esito di captazione di conversazioni durante il flusso dinamico delle stesse, bensì acquisizione di dati informatici direttamente utilizzabili a fini di prova. In una precedente pronuncia della Cassazione, la sentenza n. 34059 del 2022[195], era stato ritenuto applicabile l'art. 234 bis c.p.p.[196] il quale consente "*l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare*". A sostegno di tale interpretazione della Cassazione si è giustamente sottolineato che, ai fini dell'applicazione dell'art. 234 bis c.p.p.[197], è documento ogni "rappresentazione comunicativa incorporata in una base materiale con un metodo digitale" ed è "legittimo titolare" la persona giuridica che può legittimamente disporre del documento. Ne consegue che, se l'autorità giudiziaria di uno Stato dell'Unione Europea, in attuazione della Direttiva 2014/41/UE, dà esecuzione a un ordine di indagine Europeo emesso dall'autorità giudiziaria di altro Stato membro trasmettendo dati che ha ottenuto in conformità alla propria legislazione interna e ha incorporato in una base comunicativa con metodo digitale, vi è consenso da parte del "legittimo titolare", quindi di "colui che legittimamente conserva i dati", all'acquisizione di quei dati da parte dell'autorità giudiziaria richiedente. Nel caso di specie, i dati non sono stati richiesti a un detentore privato, ma ad un'autorità giudiziaria che, nell'ambito di un diverso e autonomo procedimento, li aveva acquisiti dal *server* dove i dati stessi erano stati immagazzinati nell'ambito di altra indagine, avente ad oggetto proprio la violazione di quella piattaforma.

[195] Cass. Pen., Sez. I, 1° settembre 2022, n. 34059.
[196] Art. 234*bis* c.p.p.
[197] Ibidem.

Infine, il richiamo alla sentenza n. 32915 del 15/07/2022[198], invocata a sostegno della eccezione di inutilizzabilità del materiale acquisito tramite l'autorità giudiziaria francese, è inconferente, in quanto il caso ivi trattato è diverso da quello in esame. In quel caso, il pubblico ministero aveva respinto la richiesta di mettere a disposizione della difesa "*la documentazione consegnata da Europol a seguito dell'accesso ai server di Sky-Ecc con indicazione delle modalità di acquisizione da parte della stessa Europol dei dati in oggetto dai server, con annessi verbali delle attività compiute*", sostenendo che si trattava di scambi informativi tra forze di polizia di paesi diversi, non utilizzabili processualmente. Una risposta siffatta è stata ritenuta lesiva del principio del contraddittorio e delle garanzie di difesa perché dalla stessa non era dato comprendere quale fosse "*il contenuto dei citati "scambi informativi tra forze di polizia di paesi diversi"" e quali fossero state le "modalità di acquisizione" del materiale utilizzato a fini cautelari; informazioni "funzionali al controllo della legittimità del procedimento acquisitivo, anche nell'ottica delineata dall'art. 191 c.p.p.*[199]".

Nel caso oggetto del presente giudizio, invece, come ampiamente illustrato nell'ordinanza impugnata, tutto il materiale ricevuto dall'autorità francese era stato versato in atti. La censura deve essere respinta anche nella parte in cui sembra dolersi della mancata conoscenza dell'algoritmo utilizzato per la decriptazione della messaggistica acquisita e, in genere, della violazione delle prerogative difensive sul controllo di correttezza delle procedure utilizzate dall'A.G francese. L'attività di acquisizione di dati in giacenza, definiti freddi, ne permette l'acquisizione, qualora il messaggio telematico sia criptato mediante l'impiego di un algoritmo o di una chiave di cifratura e trasformato in un mero dato informatico, di una stringa informatica composta da un codice binario. L'intelligibilità del messaggio è subordinata all'attività di decriptazione che presuppone la disponibilità dell'algoritmo attraverso cui si trasforma il codice binario in un contenuto dimostrativo: ogni messaggio cifrato è inscindibilmente accoppiato alla sua chiave di cifratura, quindi la sola chiave esatta produrrà una decifratura corretta, dovendosi escludere che possa decifrarne una parte corretta e una non corretta; di conseguenza non vi sono possibilità che una chiave errata possa decrittare il contenuto, anche parziale, del codice umano contenuto.

Corretto è anche il richiamo operato nell'ordinanza impugnata al principio generale di presunzione di legittimità delle prove acquisite dall'autorità giudiziaria di un altro Stato membro dell'Unione Europea: l'utilizzazione degli atti trasmessi, infatti, non è condizionata ad un accertamento da parte del giudice italiano concernente la regolarità delle modalità di acquisizione esperite dall'autorità straniera, in quanto vige la presunzione di legittimità dell'attività svolta e spetta al giudice straniero

[198] Cass. Pen. Sez. IV, 15 luglio 2022, n. 32915.
[199] Art. 191 c.p.p.

la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari.[200]

Il secondo motivo e il terzo motivo, con i quali viene contestata la ritenuta sussistenza delle circostanze aggravanti di cui agli artt. 416*bis.*1[201] e 61 *bis* c.p.[202] sono inammissibili. In proposito si deve ribadire il principio per cui è inammissibile, per carenza di interesse, il ricorso per Cassazione contro un provvedimento *de libertate* volto a contestare la configurabilità di determinate circostanze aggravanti, quando dall'esistenza o meno di tali circostanze non dipende, per l'assenza di ripercussioni sull'*an* o sul *quomodo* della cautela, la legittimità della disposta misura. Si tratta di un orientamento che discende dal principio generale, dettato dall'art. 568 c.p.p., comma 4[203], secondo il quale per proporre impugnazione è necessario avervi interesse: per evidenti ragioni di economia processuale il legislatore ha subordinato l'attivazione dello strumento di controllo all'esistenza in capo al soggetto legittimato di un concreto ed attuale interesse, inteso, nella elaborazione della giurisprudenza di legittimità, non già quale pretesa della esattezza teorica della decisione, bensì come misura della utilità pratica derivante dalla impugnazione, sussistente ogni qualvolta dal raffronto fra la decisione oggetto di gravame e quella che potrebbe essere emessa, se il gravame fosse accolto, emerge per l'impugnante una situazione di vantaggio meritevole di tutela giuridica[204].

Nel caso di specie a A.A. è contestato il delitto D.P.R. n. 309 del 1990, *ex* art. 74[205], rientrante tra quelli previsti nell'art. 51 c.p.p. comma 3*bis*[206], per i quali vige, a norma dell'art. 275 c.p.p., comma 3[207], la presunzione di esistenza delle esigenze cautelari e di adeguatezza della sola misura della custodia in carcere e rientrante, altresì, tra quelli di cui all'art. 407 c.p.p., comma 2, lett. a)[208], per i quali sono previsti i termini più elevati in assoluto della durata della custodia cautelare. Pertanto, l'eventuale accoglimento del ricorso, con l'eliminazione della circostanza aggravante, non produrrebbe alcun concreto effetto sul dispositivo dell'ordinanza impugnata.

Il quarto motivo relativo al trattamento cautelare è manifestamente infondato. In tema di misure coercitive, infatti, quando si procede per un delitto per il quale opera la doppia presunzione relativa di sussistenza delle esigenze cautelari e di adeguatezza della sola misura carceraria, ai fini della prova

[200] in tal senso, sez. 3, n. 1396 del 12/10/2021, dep. 2022, Torzi, in cui in motivazione si rinvia anche a sez. 5, n. 1405 del 16/11/2016, dep. 2017, Ruso, Rv. 269015 - 01; a sez. 2, n. 24776 del 18/5/2010, Mutari, Rv. 247750 - 01; e a sez. 1, n. 21673 del 22/1/2009, Pizzata, Rv. 243796; ma anche a sez. 5, n. 45002 del 13/7/2016, Crupi, Rv. 268457.
[201] Art. 416*bis* c.p.
[202] Art. 61*bis* c.p.
[203] Art. 568.4 c.p.p.
[204] In tal senso Cass., Sez. Unite, 27 settembre 1995, n.10372.
[205] Art. 74 D.P.R. n.309 del 1990.
[206] Art. 51.3*bis* c.p.p.
[207] Art. 275.3 c.p.p.
[208] Art. 407.2 lettera a) c.p.p.

contraria, occorrono elementi idonei ad escludere la sussistenza di ragionevoli dubbi, posto che la presunzione detta un criterio da applicarsi proprio in caso di incertezza[209].

Nel caso in esame, il Tribunale ha fornito una motivazione rafforzata, ed ha operato, pur in difetto di allegazioni difensive rilevanti, la concreta verifica della pericolosità dell'indagato. I giudici, infatti, hanno richiamato la doppia presunzione relativa di sussistenza delle esigenze cautelari e di adeguatezza della custodia in carcere ai sensi dell'art. 275 c.p.p., comma 3[210] e l'assenza di elementi atti a neutralizzare tali presunzioni, ma hanno anche sottolineato lo spessore criminale del ricorrente. Così è stato ritenuto sussistente il pericolo di inquinamento probatorio, in ragione della necessità di approfondire le indagini, al fine di identificare altri complici e individuare ulteriori attività connesse al narcotraffico, che sarebbe stata inquinata se l'indagato fosse stato lasciato libero. Sotto tale profilo il rilievo contenuto nel ricorso, secondo cui la misura degli arresti domiciliari sarebbe sufficiente a salvaguardare l'esigenza cautelare in esame, non coglie nel segno, poiché il rispetto della prescrizione di non comunicare con soggetti diversi rispetto ai coabitanti è rimesso in tal caso allo stesso indagato e nessuna forma di reale controllo può essere esercitata da parte dell'autorità rispetto a tale prescrizione. E' stato ritenuto sussistente anche il pericolo di reiterazione di reati della stessa specie desunto dalle specifiche modalità esecutive e dalla pericolosità del soggetto agente: i fatti, hanno osservato i giudici, sono indicativi di spiccata capacità a delinquere, posto che sono stati realizzati in un contesto associativo dedito al traffico su larga scala e A.A. risulta, comunque, gravato da un precedente per reato di cui all'art. 416*bis* c.p.[211] e per il favoreggiamento della latitanza del capo della Cosca E.E.. La motivazione adottata, dunque, è da un lato conforme al diritto e, dall'altro, logica ed esaustiva con riferimento alla motivazione del diniego degli arresti domiciliari.

Dal rigetto del ricorso consegue la condanna del ricorrente al pagamento delle spese processuali, oltre che la trasmissione degli atti alla cancelleria per gli adempimenti di cui all'art. 94 comma 1*ter* disp. att. c.p.p.[212].

II.4 Distinzione tra documento e documentazione

Non è secondario determinare la differenza tra documento e documentazione poiché non sempre è semplice comprendere quando si tratti del primo o della seconda. È importante sottolineare che non

[209] Cass. pen., Sez. 2, 21 settembre 2017, n. 19341.
[210] Art. 275.3 c.p.p.
[211] Art 416*bis* c.p.
[212] Art. 94.1*ter* disp. att. c.p.p.

si può sovrapporre il concetto di documentazione di un'attività d'indagine con quello di documento perché si violerebbe un principio cardine del processo penale che è quello di separazione delle fasi[213] [214]; il documento, infatti, non può formarsi nell'ambito di un'attività investigativa ma solo al di fuori di essa[215].

Come primo punto è necessario chiarire che si può parlare di documentazione solo quando un atto è stato redatto da un soggetto del procedimento e per i fini del procedimento stesso. Se, invece, non sussistono entrambi i presupposti allora si tratta di documento.

Nel caso di documento dichiarativo sussiste estraneità, rispetto al procedimento, del dichiarante e non di colui che ha incorporato la dichiarazione su base materiale. Quest'ultimo è soggetto del procedimento che redige il verbale della dichiarazione della persona offesa che viene ascoltata come *teste*; si tratta quindi di incorporazione su base materiale di una dichiarazione ad opera di un soggetto del procedimento. Per comprenderne la natura bisogna verificare se la rappresentazione in questione sia stata sin dall'origine finalizzata a quel determinato procedimento. Ne consegue che sono documenti tutti gli atti indipendentemente da chi li abbia redatti; sia che abbiano un valore certificativo o dispositivo in quanto ciò è di certo indice di una finalità estranea al processo penale. La finalità espressamente indicata dalla legge è quella di individuazione dell'atto pubblico. Per la contestazione del contenuto di esso, in tal caso, non sarà necessaria la querela di falso anche se ciascuna parte ha la facoltà di chiedere come controprova l'esame dell'ufficiale che ha redatto il documento stesso.

La Corte di cassazione è più volte intervenuta sul punto, in particolare su casi limite nei quali il confine tra documento e documentazione era molto labile.

È stata considerata un documento la confessione che è stata registrata da un agente sotto copertura al di fuori della sua attività di polizia giudiziaria nella sentenza della Corte di cassazione penale, sezione II, del 19 dicembre 2006, n. 5601[216]. La Cassazione ha stabilito che: "*Il documento fonografico contenente le dichiarazioni confessorie dell'autore di un fatto reato, rese ad un operatore di polizia giudiziaria non conosciuto come tale ed impegnato, quale agente "sotto copertura", in tutt'altre investigazioni, è utilizzabile probatoriamente, perché il divieto di testimonianza su quanto dichiarato*

[213] S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, Rivista italiana di diritto e procedura penale, Anno LV Fasc. 2-2012.
[214] Bisogna distinguere il procedimento dal processo penale. Il procedimento è la fase che precede l'esercizio dell'azione penale del Pubblico Ministero, comprende quindi tutte le indagini. Il processo, invece, inizia con l'esercizio dell'azione penale del Pubblico ministero proseguendo fino all'emanazione della sentenza di primo grado.
[215] Cfr. *Relazione al progetto preliminare del c.p.p.,* in Gazz. Uff. suppl. ord., n. 2, 24 ottobre 1998; In dottrina L. Kalb*, Il documento nel sistema probatorio*, Torino, 2000.
[216] Cass. Pen., sezione II, 19/12/2006, n. 5601.

dal sottoposto ad indagine ed il divieto di utilizzazione delle dichiarazioni rese prima dell'assunzione della qualità di indagato operano soltanto nel corso e nell'ambito del procedimento nel quale il soggetto è sottoposto ad indagine o è imputato. (Rigetta, App. Ancona, 19 dicembre 2005)[217]*"*.

In materia di procedura fallimentare la Suprema Corte ha stabilito che i verbali e gli inventari redatti dal curatore non fanno parte della categoria di *notitia criminis*, ma sono prove documentali sia quando concernono una organizzazione aziendale o contabile ma anche quando riportano dichiarazioni di soggetti terzi o dello stesso imputato che è fallito. In questi casi si tratta di documenti perché non hanno origine nel processo penale e non sono assolutamente finalizzati ad esso. Questi documenti, infatti, sono diretti al giudice delegato e non al pubblico ministero e, per questa motivazione, non sono definibili *notitia criminis* anche se possono contenere indicazioni inerenti all'esercizio dell'azione penale.

Le sentenze della Cassazione che trattano il tema appena descritto sono molteplici. Si può considerare come modello la sentenza del 15 ottobre 2001, n. 41134[218], la quale prevede che in tema di dichiarazioni autoindizianti, non è applicabile alle dichiarazioni rilasciate dal fallito al curatore la disciplina dell'art. 64 comma 2 c.p.p.[219] e tale esclusione può ritenersi in contrasto con gli articoli 3[220] e 24[221] della Costituzione[222].

Anche la sentenza del 9 giugno 2004, n. 39001[223] è intervenuta su questo tema stabilendo che in materia di prova documentale le relazioni e gli inventari redatti dal curatore fallimentare sono ammissibili come prove documentali in ogni caso e non solo quando siano ricognitivi di una organizzazione aziendale e di una realtà contabile, solo se gli accertamenti documentali e le dichiarazioni ricevute dal curatore costituiscono prove rilevanti nel processo penale, per ricostruire le vicende amministrative della società. È, quindi, secondo la Cassazione corretto l'inserimento della relazione diretta al giudice delegato nel fascicolo processuale, in quanto il principio di separazione delle fasi non si applica agli accertamenti aventi funzione probatoria, preesistenti rispetto all'inizio del procedimento o che appartengano comunque al contesto del fatto da accertare[224].

[217] Gatti, *Utilizzabilità delle dichiarazioni autoindizianti*, in Diritto penale e processo, 2007.
[218] Cass. Pen., sez. IV, 15 ottobre 2001, n. 41134.
[219] Art. 64.2 c.p.p.
[220] Art. 3 Costituzione.
[221] Art. 24 Costituzione.
[222] M. Lottini, Diritto e giustizia, 2002.
[223] Cass. Pen., Sezione V, 09/06/2004, n. 39001.
[224] Rivista penale 2005, 1017.

Infine, si può citare la sentenza della Corte Suprema del 3 febbraio 2004, n. 8857[225], la quale stabilisce che la relazione del curatore fallimentare destinata al giudice delegato non costituisce di per sé notizia di reato, ma documento utilizzabile in giudizio[226].

È più difficile capire se si tratti di documento o documentazione nel caso in cui un documento venga redatto da un soggetto tipico del procedimento. La giurisprudenza recente sembra essere favorevole all'utilizzo come documento, quindi non come documentazione, del diario della persona offesa o delle registrazioni della videosorveglianza della vittima del reato. In tema di videoriprese, più precisamente di videoriprese effettuate con telecamere installate all'interno del luogo di lavoro, la Cassazione ha accordato l'utilizzabilità dei risultati delle videoriprese eseguite con telecamere posizionate all'interno dei luoghi di lavoro a opera del datore di lavoro ai fini di beneficiare il patrimonio aziendale potenzialmente a rischio per qualche comportamento infedele dei dipendenti[227], solo nel caso in cui la persona imputata sia un lavoratore subordinato. La motivazione è che anche le norme dello statuto dei lavoratori, che preservano la riservatezza di questi ultimi, prevedono i controlli difensivi del patrimonio aziendale e quindi non avrebbe senso escludere la loro valenza probatoria.

Non sono classificate come documenti le missive inviate da persona offesa da reato o da qualunque teste che voglia descrivere i fatti posti alla base dell'imputazione perché in questo caso è un atto per il procedimento[228]. Esempio giurisprudenziale di queste considerazioni è la sentenza della Cassazione penale del 4 febbraio 2003, n. 9964[229] nella quale si stabilisce che ai fini dell'acquisizione e della lettura a dibattimento delle dichiarazioni rese da persona residente all'estero, *ex* art. 512*bis* c.p.p.[230], occorre che le dichiarazioni orali siano state rese davanti ad un ufficiale di Polizia giudiziaria, siano

[225] Cass. Pen., Sez. V, 03/02/2004, n. 8857.
[226] Rivista penale 2005, 640.
[227] Art 4 Statuto dei lavoratori: *1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.*
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.
[228] Spangher, *Trattato di procedura penale*, II, I, Torino, 2009.
[229] Cass. Pen., Sez. VI, 04/02/2003, N. 9964.
[230] Art. 512*bis* c.p.p.

state raccolte a verbale e che sia stata preventivamente esperita la procedura della rogatoria ai fini della citazione. Non possono, pertanto, considerarsi un valido equipollente a fini probatori le missive, contenenti la descrizione dei fatti posti a fondamento della contestazione all'imputato, inviate dall'estero da parte del teste-persona offesa, che non abbia in precedenza mai reso dichiarazioni e non sia stato citato a comparire a dibattimento.

Ogni atto compiuto prima del fatto di reato è un documento a pieno titolo anche nel caso in cui contenga dichiarazioni rese dall'imputato che, se sono successive a indizi di reato, sono soggette a limiti di utilizzabilità. Sul punto la Cassazione a Sezioni Unite si è espressa tramite la sentenza del 28 novembre 2001, n. 45477[231], nella quale statuisce che il divieto di testimonianza sulle dichiarazioni dell'imputato o dell'indagato e il divieto di utilizzazione si applicano alla testimonianza resa da un ispettore del lavoro su quanto a lui riferito da persona nei cui confronti siano emersi, nel corso dell'attività ispettiva, anche semplici dati indicativi di un fatto apprezzabile come reato e le cui dichiarazioni siano state assunte in violazione delle norme poste a garanzia del diritto di difesa, atteso che il significato dell'espressione "*quando emergano indizi di reato*" contenuta nell'art. 220 disp. att. cod. proc. pen.[232] e tesa a fissare il momento a partire dal quale, nell'ipotesi di svolgimento di ispezioni o di attività di vigilanza, sorge l'obbligo di osservare le disposizioni del codice di procedura penale per assicurare le fonti di prova e raccogliere quant'altro possa servire ai fini dell'applicazione della legge penale deve intendersi nel senso che presupposto dell'operatività della norma sia non l'insorgenza di una prova indiretta quale indicata dall'art.192 cod. proc. pen.[233], bensì la sussistenza della mera possibilità di attribuire comunque rilevanza penale al fatto che emerge dall'inchiesta amministrativa e nel momento in cui emerge, a prescindere dalla circostanza che esso possa essere riferito ad una persona determinata[234].

È, inoltre, essenziale analizzare la qualificazione delle attività ispettive e di vigilanza svolte in forza di previsioni di leggi o decreti. Laddove si tratti di eseguire accertamenti che potrebbero condurre ad una *notitia criminis*, il legislatore, agli artt. 220[235] e 223[236] disp. att. c.p.p., ha dettato una particolare disposizione. Nello specifico, nel caso in cui nel corso di tali attività emergano indizi di reato, occorre rispettare le disposizioni del codice di procedura penale al fine di assicurare le fonti di prova e, inoltre, se nel corso delle medesime attività si debba procedere all'analisi di campioni occorre rispettare le garanzie difensive al fine di rendere utilizzabili i risultati in dibattimento. Per tale ragione non tutti

[231] Cass. Pen., Sez. Unite, 28/11/2001, n. 45477.
[232] Art. 220 disp. att. cod. proc. pen.
[233] Art. 192 cod. proc. pen.
[234] Raineri, in *CP*, 2002, 1304.
[235] Art. 220 disp. att. c.p.p.
[236] Art. 223 disp. att. c.p.p.

gli atti compiuti nel corso di queste attività sono identificabili come documenti e, infatti, l'art. 220 disp. att. c.p.p. stabilisce che, se emergono indizi di reato gli accertamenti compiuti a partire da quel momento, saranno atti del procedimento e non documenti pur se si collocano fuori dal procedimento penale. In tutti gli altri casi, invece, si tratta di documenti. La Suprema Corte nella sentenza del 17 febbraio 2010, n. 10996[237], stabilisce che la relazione con la quale viene documentata l'attività ispettiva d'inchiesta svolta da pubblici funzionari costituisce un atto amministrativo extraprocessuale, in quanto tale acquisibile al procedimento penale *ex* art. 234 c.p.p.[238] ed utilizzabile ai fini probatori limitatamente ai dati oggettivi in essa contenuti, oltre che per ricavare elementi di giudizio dai fatti ivi rappresentati[239].

In relazione alla qualificazione dei verbali di prelevamento dei campioni ed alle successive analisi sussistono delle profonde divergenze in dottrina. Alcuni studiosi ritengono giusto considerarli atti del procedimento nonostante si tratti di un riconoscimento *ex post*[240] ; altri, invece, sostengono che sia più opportuno continuare a classificarli documenti pur se con un regime speciale relativamente alla loro utilizzabilità[241].

Dato che il documento è tutto ciò che trova formazione fuori dal procedimento penale; allora è tale anche quell'atto che trova formazione in un procedimento penale diverso da quello ricevente[242]. Ricondurre alla definizione di documento gli atti formati in altro procedimento penale significa colmare la lacuna normativa del legislatore che ha disciplinato solo ed esclusivamente l'acquisizione di verbali di prove all'art. 238 c.p.p.[243] e delle sentenze irrevocabili agli artt. 236[244] e 238*bis* c.p.p[245]. In seguito a tale interpretazione sono classificabili documenti anche i seguenti atti.

Come primo atto c'è il verbale di ricognizione dei beni pignorati scritto dall'incaricato dell'IVG perché esso riproduce la rappresentazione di un fatto preprocessuale e cioè l'accesso e il mancato rinvenimento dei beni pignorati. Con riguardo a questa tipologia di atto la Cassazione tramite la sentenza del 7 ottobre 2003, n. 43500[246], stabilisce che: "*il verbale di ricognizione dei beni pignorati redatto dall'incaricato dell'Istituto Vendite Giudiziarie, oltre ad avere natura di prova documentale a norma art. 234 c.p.p., è anche fonte di prova delle dichiarazioni eventualmente rese dal custode o dal*

[237] Cass. Pen., Sez. VI, 17/02/2010, n.10996.
[238] Art. 234 c.p.p.
[239] Vanacore, in *Mass. Uff.,* 246686.
[240] Ubertis, Documenti, pag. 318 ss.
[241] Laronga*, La prova documentale nel processo penale,* Torino, 2004.
[242] Ubertis, *Sisifo e Penelope. Il nuovo codice di procedura penale, dal progetto preliminare alla ricostruzione del sistema,* Torino, 1993.
[243] Art. 238 c.p.p.
[244] Art. 236 c.p.p.
[245] Art. 238*bis* c.p.p.
[246] Cass. Pen., Sez. VI, 07/10/2003, n. 43500.

proprietario dei beni pignorati, seppure da questi non sottoscritte. Tali dichiarazioni rese al di fuori del processo, in quanto ammettono fatti in contrasto con l'interesse del dichiarante, hanno valore di confessione extragiudiziale, dopo la testimonianza qualificata dell'incaricato che ebbe a verbalizzarle, sempre che, in caso di ricognizione dei beni con esito negativo, sussista il riscontro oggettivo del mancato rinvenimento dei beni pignorati"[247].

Anche la relazione di consulenza tecnica d'ufficio eseguita, durante il giudizio civile, non è classificabile come prova di altro procedimento, bensì documento perché il codice di procedura civile esclude la stessa dalla categoria dei mezzi di prova essendo essa un ausilio per il giudice nella soluzione di questioni che comportano specifiche conoscenze. Questa affermazione è avvalorata da varie pronunce della Cassazione. Tra le quali possiamo individuare la sentenza del 5 febbraio 2008, n. 7916[248], dove è statuito che: "*La consulenza tecnica d'ufficio, disposta in un giudizio civile non ancora definito con sentenza passata in giudicato, può essere acquisita nel processo penale ai sensi dell'art. 234 c.p.p.[249], anche in difetto del consenso delle parti, dovendo essere considerata quale documento, in quanto formata fuori del procedimento penale, ed essendo rappresentativa di situazioni e di cose*"[250].

Ancora accostabili alla categoria dei documenti sono quegli atti "presupposto" del reato come nel caso della violazione dei provvedimenti in materia di affidamento dei minori oppure della violazione dei sigilli apposti per ordine dell'autorità giudiziaria. La Suprema Corte è entrata nel merito della questione affermando che hanno natura di documenti i provvedimenti giudiziali non definitivi utilizzabili relativamente alla esistenza delle vicende processuali e della decisione. In particolare, si consulti la sentenza 12/07/2005, n. 33748[251], nella quale è stabilito che: "*Le sentenze pronunciate in procedimenti penali diversi e non ancora divenute irrevocabili sono legittimamente acquisibili al fascicolo per il dibattimento, nel contraddittorio fra le parti, al pari degli altri documenti (si veda l'art. 234, comma 1[252], e 236 c.p.p.[253].), ma, siccome non ancora assistite dall'intangibilità del giudicato, possono essere utilizzate come prova limitatamente all'esistenza della decisione e alle vicende processuali in esse rappresentate, ma non ai fini della valutazione delle prove e della ricostruzione dei fatti oggetto di accertamento in quei procedimenti; soccorrendo, semmai, a tal fine,*

[247] Volterrani, in *Mass. Uff.*, 227607.
[248] Cass. Pen., Sez. II, 05/02/2008, n. 7916.
[249] Art. 234 c.p.p.
[250] Rossi, in Mass. Uff., 239546.
[251] Cass. Pen., Sez. Unite, 12/07/2005, n. 33748.
[252] Art. 234.1c.p.p.
[253] Art.236 c.p.p.

lo specifico modulo acquisitivo dei verbali di prove di altri procedimenti predisposto dall'art. 238[254] *del codice di procedura penale*[255]".

Per un completo quadro analitico è utile evidenziare la differenza tra documenti ed intercettazioni telefoniche. I primi si sostanziano essenzialmente nella rappresentazione di fatti verificatisi nel passato ai quali lo stesso ordinamento ricollega determinati effetti suscettibili di rivestire rilevanza giuridica, mentre le seconde si sostanziano in operazioni finalizzate alla raccolta, secondo una logica di contemporaneità rispetto a ciò che si registra, del flusso di conversazioni telefoniche tra due diversi soggetti. Inoltre, i documenti sono mezzi di prova; invece, le intercettazioni sono mezzi di ricerca della prova.

In materia la Suprema Corte ha recentemente osservato che i saggi fonici costituiscono prova documentale, non dichiarativa, né sono equiparabili alle intercettazioni tra presenti perché in essi è del tutto indifferente il contenuto delle frasi pronunciate non valutabile né pro né contro chi le pronuncia, ma utilizzabile solo parametro di riferimento ai fini dell'espletamento di una perizia sicché essi sono acquisibili senza formalità come statuisce la Cassazione il 9 luglio 2010 con la sentenza n.28681[256]. Inoltre, la Cassazione ha successivamente chiarito che la registrazione di una conversazione tra presenti, contenuta in un file audio, che riproduce un avvenimento storico che rimanda al contenuto dichiarativo di soggetti individuabili, anche in assenza dell'identificazione dell'autore della registrazione stessa, non è qualificabile come documento anonimo ma costituisce una *notitia criminis* che legittima l'avvio e il compimento di indagini da parte del pubblico ministero per verificarne la portata e compiere ogni opportuno approfondimento investigativo, ivi compresi l'adozione dei mezzi di ricerca della prova quali perquisizione e sequestro[257].

Per quanto riguarda le intercettazioni ambientali, la Suprema Corte[258] ha sostenuto che non sono legittime le intercettazioni ambientali di immagini effettuate in un appartamento privato e non

[254] Art. 238 c.p.p.

[255] Mannino, in DPP, 2005.

[256] Cass. Pen., Sez. II, 09/07/2010, n.28681; è stabilito che: Il saggio fonico costituisce prova documentale, non dichiarativa, e non è equiparabile ad una intercettazione tra presenti, perché in esso è del tutto indifferente il contenuto delle frasi pronunciate, non valutabile né pro né contro chi le pronuncia, ma utilizzabile come mero parametro di riferimento ai fini dell'espletamento di una perizia, sicché esso è acquisibile senza formalità, non incidendo sulla libertà personale dell'interessato. (Dichiara inammissibile, App. Cagliari, 4 dicembre 2008).

[257] Cass. Pen., Sez. VI, 17/12/2019, n. 5782; La registrazione fonografica di colloqui tra presenti è utilizzabile, come prova documentale ai sensi dell'art. 234 cod. proc. pen., a condizione che sia certa la sua effettuazione da parte di uno dei partecipanti o comunque legittimati ad assistere all'incontro, sicché, ove difetti la prova, incombente sulla pubblica accusa, in ordine alla sussistenza di detta condizione, la registrazione va qualificata come una intercettazione inutilizzabile, in quanto lesiva dei diritti fondamentali dell'individuo costituzionalmente tutelati e realizzata in violazione del divieto previsto dall'art. 191, comma 1, cod. proc. pen. (Rigetta, TRIB. LIBERTA' MILANO, 05/09/2019).

[258]Cass. Pen., Sez. Unite, 28/03/2006, n. 26795. Le riprese video di comportamenti "non comunicativi" non possono essere eseguite all'interno del "domicilio", in quanto lesive dell'art.14 Cost.. Ne consegue che è vietata la loro acquisizione ed utilizzazione anche in sede cautelare e, in quanto prova illecita, non può trovare applicazione la disciplina dettata dall'art. 189 c.p.p.(v Corte Costituzionale n.135 del 2001). (Annulla con rinvio, Trib. lib. Perugia, 18 Marzo 2005).

possono nemmeno essere ritenute documenti poiché non siamo di fronte a riprese visive effettuate in luoghi aperti o pubblici[259], viene qui in rilievo il limite della inviolabilità del domicilio di cui all'art. 14 della Costituzione[260].

[259] Di Bitonto, *Le riprese video al vaglio delle Sezioni Unite*, in *CP*, 2006; Ruggieri, Riprese visive e inammissibilità della prova, in CP, 2006; Conti, Accertamento del fatto e inutilizzabilità nel processo penale, Padova, 2007.

[260] Art. 14 Costituzione.

Il domicilio è inviolabile.

Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale.

Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali.

Capitolo III- Sequestro probatorio di un documento informatico

III.1 Panoramica sulle varie tipologie di sequestro nel codice di procedura penale

Per introdurre questo ultimo capitolo relativo al sequestro probatorio del documento informatico e alle varie criticità che possono emergere, verranno di seguito brevemente esaminate le tipologie di sequestro disciplinate dal codice di procedura penale per evidenziarne le profonde divergenze.

Il codice di procedura penale prevede tre tipologie di sequestro: il sequestro preventivo, quello conservativo e quello probatorio. I primi due sono misure cautelari e non hanno alcuna affinità con il terzo appena citato, poiché quest'ultimo è un mezzo di ricerca della prova.

Il sequestro preventivo e conservativo sono due misure cautelari. Il legislatore individua questi due metodi come forme di apprensione forzata di una cosa per finalità cautelari. La misura cautelare deve essere disposta dal giudice sulla base di una richiesta precedentemente presentata dal Pubblico Ministero, nella maggior parte dei casi, o dalla parte civile quando si tratta di sequestro conservativo. Il sequestro conservativo serve ad assicurare l'esecuzione della sentenza per ciò che concerne i profili civili e pecuniari; presuppone però l'avvenuto esercizio dell'azione penale e quindi non è utilizzabile nella fase delle indagini preliminari[261]. Nel caso in cui ci sia fondata ragione di ritenere che manchino o possano essere disperse le garanzie per il pagamento della pena pecuniaria, delle spese del procedimento o di ogni altra somma dovuta all'erario dello Stato, il Pubblico Ministero, in ogni stato e grado del processo di merito può chiedere il sequestro conservativo di beni mobili o immobili dell'imputato o di somme o di cose da lui dovute nei limiti imposti dalla legge per il pignoramento[262]. Nel caso in cui la fattispecie di reato sia l'omicidio del coniuge, anche legalmente separato o divorziato, o di una delle due parti in caso di unione civile, anche se l'unione è cessata, o di una delle due persone legate da una convivenza stabile e da una relazione affettiva, nel caso in cui ci siano figli minorenni o maggiorenni ma non autosufficienti economicamente, il Pubblico Ministero può chiedere il sequestro conservativo come garanzia per i figli della vittima, come disciplinato dall'art. 316.1*bis* c.p.p. [263].

[261] Bisogna distinguere le varie fasi della vicenda processuale penale. Il procedimento è la fase che precede l'esercizio dell'azione penale da parte del Pubblico Ministero e coincide solitamente con la fase delle indagini. Il processo, invece, inizia con l'esercizio dell'azione penale da parte del PM. Detto ciò, non è possibile richiedere il sequestro conservativo in fase di indagine se uno dei presupposti per richiederlo è che vi sia stato l'esercizio dell'azione penale da parte del PM.
[262] Ai sensi dell'art. 316.1 c.p.p. che dispone: "Se vi è fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento delle spese di procedimento e di ogni altra somma dovuta all'erario dello Stato, il pubblico ministero, in ogni stato e grado del processo di merito, chiede il sequestro conservativo dei beni mobili o immobili dell'imputato o delle somme o cose a lui dovute, nei limiti in cui la legge ne consente il pignoramento.
[263] Art. 316.1*bis* c.p.p.

Procede nello stesso modo la parte civile[264] che voglia richiedere il sequestro conservativo: può farlo in ogni stato e grado del processo di merito, nel caso in cui vi siano i presupposti per ritenere che manchino o si disperdano le garanzie delle obbligazioni civili che derivano da un reato; nel caso in cui la richiesta sia fatta dalla parte civile il sequestro può riguardare anche dei beni del responsabile civile[265]. Anche nel caso in cui la richiesta venga effettuata dal Pubblico Ministero, questa giova anche alla parte civile come disciplinato dall'art. 316.3 c.p.p.[266].

Il provvedimento con il quale il giudice dispone il sequestro assume la forma dell'ordinanza, come previsto dall'art. 317.2 c.p.p.[267].

Alternativamente a queste due possibilità per la parte civile e il Pubblico Ministero, sia prima che dopo l'emissione dell'ordinanza del giudice di sequestro conservativo, se l'imputato o il responsabile civile propongono di depositare una cauzione come garanzia per le somme di denaro o le altre

[264] La parte civile nel processo penale non svolge il ruolo di accusatore privato, ma è un soggetto teso al soddisfacimento delle sue pretese civilistiche. L'art. 74 c.p.p. stabilisce che l'azione civile, per le restituzioni o il risarcimento dei danni patrimoniali e non patrimoniali, che siano riconducibili al reato oggetto di accertamento, può essere esercitata "*dal soggetto al quale il reato ha recato danno ovvero dai suoi successori universali, nei confronti dell'imputato e del responsabile civile*". Il generico riferimento ad un "soggetto" consente di essere parte civile anche a un ente plurisoggettivo pur se privo di personalità giuridica. La parte civile non può stare nel processo penale da sola ma deve necessariamente essere assistito da un legale difensore munito di procura speciale alle liti. Una volta che è avvenuta la costituzione in giudizio della parte civile, questa rimarrà tale in tutti i gradi del processo; quest'ultima potrà essere revocata in ogni stato e grado del processo tramite una dichiarazione compiuta personalmente dalla parte o dal suo difensore in udienza oppure con atto scritto depositato nella cancellaria del giudice e notificato alle altre parti.
Equivale ad una revoca della costituzione la mancata presentazione delle conclusioni scritte, disciplinate dall'art. 523.2 c.p.p., le quali comprendono espressa richiesta del risarcimento dei danni nel loro preciso ammontare. Si considera, inoltre, come revoca il promuovere azione davanti al giudice civile *ex* art. 82.2 c.p.p.
Per completezza dell'argomento verranno ora descritte le principali caratteristiche anche del responsabile civile e del civilmente obbligato per la pena pecuniaria.
Il responsabile civile è la persona fisica o l'ente, tenuti *ex* art. 185.2 c.p.p., a rispondere per il fatto dell'imputato sulla base delle regole sulla responsabilità aquiliana disciplinata dal codice civile. È obbligato in solido con l'imputato e può intervenire volontariamente nel processo penale o essere citato su richiesta della parte civile o del Pubblico Ministero nel caso in cui il danneggiato sia incapace per infermità di mente o minore età e l'azione civile nel suo interesse sia stata esercitata dal Pubblico Ministero nel caso di assoluta urgenza, *ex* art 83.1. La richiesta di citazione del responsabile civile deve essere formulata al più tardi "*per il dibattimento*", *ex* art. 83.1, mentre l'intervento volontario deve essere effettuato negli stessi termini previsti per la costituzione della parte civile cioè entro il compimento per la prima volta della verifica della regolare costituzione delle parti, prima della dichiarazione di apertura del dibattimento (art. 85.1 c.p.p.). La citazione del responsabile civile ordinata dal giudice presuppone una valutazione circa il *fumus boni iuris* della richiesta. La presenza del responsabile civile è legata a quella della parte civile: il suo intervento presuppone la precedente costituzione del danneggiato nel processo penale e la sua estromissione è collegata alla revoca o esclusione della parte civile, ex artt. 83.6 e 85.4 c.p.p.
Per completare la rassegna delle parti civili nel processo penale è d'obbligo fare un breve accenno al civilmente obbligato per la pena pecuniaria. È colui che, nei casi in cui la legge penale sostanziale assoggetti una persona fisica o giuridica, in via sussidiaria ed eventuale, a una obbligazione civile pecuniaria pari all'importo della multa o dell'ammenda del condannato, può essere citato in giudizio. Escluso il caso in cui l'intervento sia volontario, la citazione può essere richiesta dal Pubblico Ministero o dall'imputato (ex art. 89.1).

[265] Art. 316.2 c.p.p. che afferma: "Se vi è fondata ragione di ritenere che manchino o si disperdano le garanzie delle obbligazioni civili derivanti dal reato (185 c.p.), la parte civile può chiedere il sequestro conservativo dei beni dell'imputato o del responsabile civile, secondo quanto previsto dal comma 1."

[266] Art. 316.3 c.p.p. disciplina che: "*Il sequestro disposto a richiesta del pubblico ministero giova anche alla parte civile*".

[267] Art. 317. 1 c.p.p. prevede che: "*Il provvedimento che dispone il sequestro conservativo a richiesta del pubblico ministero o della parte civile è emesso con ordinanza del giudice che procede*".

obbligazioni correlate al reato, il giudice dispone con decreto che non si faccia luogo al sequestro conservativo se la proposta di cauzione viene compiuta prima dell'emissione dell'ordinanza, oppure revoca il sequestro, se questo è già stato disposto, solo se il valore della cauzione è proporzionato rispetto a quello dei beni sequestrati.

Il sequestro conservativo può convertirsi in pignoramento nel caso in cui la sentenza di condanna al pagamento di una somma di denaro diventi irrevocabile oppure nel caso in cui diventi esecutiva la sentenza nella quale vengono condannati l'imputato e il responsabile civile al risarcimento del danno in favore della parte civile; l'articolo di riferimento è il 320.1 c.p.p.[268].

Nel caso in cui si proceda per omicidio del coniuge[269], anche legalmente separato o divorziato, o di una delle parti dell'unione civile, anche se cessata, o di una persona che è legata o è stata legata da relazione affettiva o stabile convivenza, si può realizzare la conversione del sequestro conservativo in pignoramento prima, cioè con la pronuncia di primo grado. Nel caso di specie il giudice, rilevata la presenza di figli della vittima minorenni o maggiorenni non economicamente autosufficienti e costituiti come parte civile, provvede anche d'ufficio all'assegnazione di una provvisionale in loro favore, in misura non inferiore al cinquanta per cento del danno presumibile, da liquidare in un giudizio civile separato e, se è già stato disposto il sequestro conservativo sui beni dell'imputato, il sequestro si converte in pignoramento nei limiti della provvisionale[270].

Il sequestro preventivo, a differenza di quello conservativo, può essere adottato nel corso delle indagini preliminari. È una misura di coercizione reale per esigenze di prevenzione, è connessa allo svolgimento del procedimento penale ed è destinata ad evitare due situazioni: sia che il trascorrere del tempo necessario allo svolgimento del procedimento possa irrimediabilmente recare pregiudizio all'effettività della sanzione[271], sia che l'utilizzo di un certo bene correlato alla commissione di un reato perpetui e consolidi il pregiudizio da esso provocato. Oggetto della misura che si sta descrivendo è la cosa pertinente al reato, nell'eventualità in cui la sua libera disponibilità possa portare ad aggravare o prolungare le conseguenze del reato, o ancora agevolare la commissione di altri reati, come disciplinato dall'art. 321.1. c.p.p.[272].

Il sequestro preventivo di una *res* pertinente al reato può essere disposto anche nel caso in cui l'ipotesi criminosa sia già perfezionata, purché il pericolo della libera disponibilità della cosa stessa presenti i requisiti della concretezza e attualità e le conseguenze del reato, ulteriori rispetto alla sua

[268] Art. 320.1 c.p.p.
[269] Art. 539.2*bis* c.p.p.
[270] Cfr. Aa. Vv., Fondamenti di procedura penale, Terza edizione, Cedam, pag. 882-883.
[271] Cass, Sez. un., 29 gennaio 2013, Innocenti, in C.e.d. 223722.
[272] Art. 321.1 c.p.p.

consumazione, possano essere rimosse in modo definitivo rimosse con l'accertamento irrevocabile del reato. Tutti questi requisiti devono essere accertati dal giudice con adeguata motivazione[273].

Il sequestro preventivo viene disposto tramite un decreto motivato dal giudice competente di pronunciarsi nel merito, nel caso in cui venga disposto durante le indagini preliminari se ne occupa il giudice per le indagini preliminari[274].

Prima dell'esercizio dell'azione penale da parte del Pubblico Ministero, nel caso in cui sussista una situazione di urgenza tale da non consentire nemmeno l'attesa del provvedimento del giudice, il sequestro può essere disposto dal Pubblico Ministero stesso con un decreto motivato[275]. Prima dell'intervento del Pubblico Ministero, possono agire anche gli ufficiali di polizia giudiziaria, i quali sono tenuti a trasmettere al Pubblico Ministero il verbale relativo al sequestro che è stato eseguito nel termine tassativo di quarantotto ore, come disposto dall'art. 321.3*bis*, secondo periodo, c.p.p.[276]. Dopo che la polizia giudiziaria ha effettuato il sequestro, il Pubblico Ministero, che non ritenga di dover disporre la restituzione delle cose sequestrate, deve richiedere al giudice la convalida della misura che è già stata adottata entro quarantotto ore da quando ha ricevuto il verbale di polizia. Nel caso in cui, invece, il sequestro è stato disposto dal Pubblico Ministero, le quarantotto ore entro le quali bisogna richiedere al giudice la convalida decorrono dall'adozione del decreto[277].

Sia nel caso in cui abbia agito il Pubblico Ministero o abbia agito la Polizia giudiziaria, il mancato rispetto dei tempi previsti dal codice comporta la perdita di efficacia della misura cautelare. Lo stesso esito sussiste nel caso in cui il giudice della convalida non si pronunci, tramite un'ordinanza, entro dieci giorni dalla ricezione della richiesta[278]. L'ordinanza del giudice è immediatamente notificata*, ex* art 321.3*ter*, secondo periodo c.p.p.[279], alla persona cui sono state sequestrate le cose.

Per concludere, sarà il giudice con la sua discrezionalità a decidere per il sequestro preventivo di "*cose di cui è consentita la confisca*"[280]; è invece obbligatorio nel caso si proceda per delitti di pubblici ufficiali contro la pubblica amministrazione[281].

Le norme sul sequestro preventivo vengono applicate anche nel caso in cui vi sia apprensione coattiva di beni appartenenti alla vittima di un sequestro di persona con fine di estorsione, al coniuge, ai parenti e affini conviventi, o altre persone, nel caso in cui vi sia motivo fondato di credere le *res* in questione

[273] Cass., Sez. un., 29 gennaio 2013, in C.e.d., 223721.
[274] *Ex* art. 321.2 c.p.p.
[275] *Ex* art. 321.3*bis* primo periodo c.p.p.
[276] Art. 321.3bis secondo periodo c.p.p.
[277] *Ex* art. 321.3*bis* secondo periodo c.p.p.
[278] *Ex* art. 321.3*ter* primo periodo c.p.p.
[279] Art. 321.3*ter* secondo periodo c.p.p.
[280] Art. 321.2 c.p.p.
[281] Art. 321.2*bis* c.p.p.

siano impiegate direttamente o indirettamente, per far conseguire agli autori del reato il denaro richiesto per la liberazione della persona rapita[282].

Per giurisprudenza consolidata, si ritiene che ai fini del sequestro preventivo resti preclusa ogni valutazione dell'esistenza di indizi di colpevolezza, il giudice deve solo, in questo caso, valutare la possibilità astratta di sussumere il fatto attribuito a una persona in una determinata ipotesi di reato[283]. Questo orientamento interpretativo è stato avallato anche dalla Corte Costituzionale[284], anche se sussistono ancora delle perplessità poiché nei casi di confisca-sanzione la misura cautelare si risolve in una forma di anticipata applicazione della pena, adottata senza un vaglio costituzionale circa la probabile sussistenza della commissione del reato.

L'imputato e il suo difensore, il soggetto al quale sono state sottratte le res sequestrate e colui che avrebbe il diritto alla sostituzione, possono presentare una richiesta di riesame contro i provvedimenti di sequestro emessi dal giudice. Il giudice di questa tipologia di riesame è quello che ha sede nel capoluogo della provincia nella quale ha la sede l'ufficio che ha emesso il provvedimento[285]. Nel caso in cui la contestazione riguardi la proprietà delle cose sequestrate, il giudice del riesame deve rimettere la questione al giudice civile, mantenendo fermo il sequestro disposto.

La decisione del Tribunale deve essere pronunciata entro il termine di dieci giorni che decorrono da quando gli atti del procedimento sono depositati presso la cancelleria del Tribunale stesso, come disciplinato dagli artt. 324.7 c.p.p. e 309 commi 9 e 10 c.p.p.[286].

Contro gli altri provvedimenti in materia di misure cautelari reali, come ad esempio la mancata convalida del sequestro preventivo disposto dalla Polizia giudiziaria o dal Pubblico Ministero, o il provvedimento del giudice che non accoglie la richiesta di sequestro conservativo, è ammesso l'appello davanti al tribunale del riesame, individuato dall'art. 324.5 c.p.p.[287], proponibile dal Pubblico Ministero, dall'imputato e dal suo difensore e dalle persone interessate alle cose sequestrate[288].

Il sequestro probatorio, invece, non ha nulla a che vedere con i due sequestri appena esaminati, che sono misure cautelari, poiché è un mezzo di ricerca della prova[289] che consiste nell'apprensione coattiva di una cosa a fini istruttori. È necessario sottolineare sin da subito che il concetto di "cosa"

[282] *Ex* art. 1 d.l. 15 gennaio 1991, che è stato convertito con l. 15 marzo 1991, n.82.
[283] Cass., Sez. un., 25 marzo 1993, Gifuni, in Cass. Pen. 1993, p. 1969.
[284] Corte Cost., 17 febbraio 1994, n.48.
[285] Art. 324.5 c.p.p.
[286] Artt. 324.7 e 309 commi 9 e 10 c.p.p.
[287] Art. 324.5 c.p.p.
[288] Cfr. A.a. V.v., Fondamenti di procedura penale, Terza edizione, Cedam, pag. 883 e ss.
[289] I mezzi di ricerca della prova sono gli strumenti volti all'acquisizione dei mezzi di prova. Essi sono: sequestri, ispezioni, intercettazioni telefoniche, perquisizioni (*ex* artt. 244-271 c.p.p.).

grazie alla legge del 18 marzo 2008, n. 48,[290] si è molto allargato comprendendo anche entità immateriali, come i dati informatici[291]. Lo spossessamento può quindi essere sia reale che simbolico tramite l'apposizione di sigilli o altri segni idonei a indicare il vincolo.

Come tutti i mezzi di ricerca della prova è centrale il conflitto tra le esigenze di accertamento penale da parte dell'autorità giudiziaria e i diritti di libertà; è menzionato, infatti, nella Costituzione all'art. 14[292] relativo alla libertà di domicilio, ma può incidere su altre libertà costituzionalmente garantite.

Il sequestro probatorio è un atto a sorpresa, quindi non c'è possibilità di contraddittorio anticipato.

Possono essere oggetto di sequestro il corpo di reato e le cose ad esso pertinenti. La descrizione del concetto di corpo di reato è data dall'art. 253.2 c.p.p. e consiste nelle "*Cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo*"[293]. Non esiste, invece, una definizione delle cose appartenenti al reato che possono essere identificate come qualsiasi cosa utile ai fini della decisione.

È importante soffermarsi sull'aggettivo "necessarie" riferito alle cose sequestrabili con fini istruttori. Questa espressione indica sia che dev'essere necessaria la cosa, sia la sua apprensione nel senso che se non si sequestrasse potrebbe essere dispersa o alterata. Questo modo di interpretare l'aggettivo in questione consente che vi sia una maggiore attenzione ai diritti individuali che necessariamente saranno compressi dal sequestro.

Il riferimento alle cose pertinenti al reato consente di porre rimedio alla lacuna della legge che non affronta per nulla il problema della "consistenza" della *notitia criminis* per l'accertamento della quale viene disposto il sequestro. Nella prassi, molto spesso, ci si accontenta della configurabilità astratta del reato, ciò significa che ci si ferma solo al fatto che non si possa escludere la rilevanza penale del fatto su cui si procede. Questo *modus operandi* è decisamente troppo poco garantista, il riferimento alla pertinenza imporrebbe almeno che vi fossero elementi a sostegno della notizia di reato; non avrebbe senso, altrimenti, una disposizione di legge che seleziona le cose da sequestrare con una relazione di pertinenza rispetto ad un termine di riferimento del tutto ipotetico.

Il sequestro è disposto dall'autorità giudiziaria tramite un decreto motivato che viene consegnato all'interessato solo se presente quando esso viene eseguito. In teoria il provvedimento dovrebbe

[290] L. 18 marzo 2008, n. 48
[291] *Ex* artt. 248.2, 254*bis* e 256 c.p.p.
[292] Art. 14 Costituzione, dispone che: "*Il domicilio è inviolabile.*
Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale.
Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali."
[293] Art. 253.2 c.p.p.

contenere: l'individuazione delle cose, la loro qualifica, la fattispecie astratta, i fatti concreti che la integrano e gli elementi di prova che li suffragano, il bisogno istruttorio. La giurisprudenza è molto spesso poco severa in riferimento a tutti questi elementi richiesti per il procedimento.

La polizia può disporre il sequestro solo nei casi di estrema urgenza disciplinati dall'art. 354 c.p.p.[294]. L'iniziativa della polizia deve essere comunicata entro quarantotto ore al Pubblico Ministero il quale, nelle quarantotto ore successive, deve decidere se convalidarla o meno[295].

Per quanto concerne, invece, le eventuali esigenze probatorie dei privati, bisogna fare riferimento agli artt. 368 e 391*quater*.3: chi è interessato deve prima chiedere il sequestro al Pubblico Ministero, se questo nega il consenso allora il privato potrà rivolgersi al giudice.

Dato che si sta trattando uno strumento finalizzato a fornire elementi di convincimento, il sequestro può essere sindacato dal giudice della cognizione[296], ma sono previsti due controlli.

Il primo concerne nella possibilità di richiedere il riesame avverso il decreto che ha disposto o convalidato il sequestro, da parte dell'imputato, della persona alla quale le cose sono state sequestrate e da quella che avrebbe diritto alla restituzione, ex art. 257 c.p.p.[297].

Il secondo controllo, invece, consiste nel procedimento di restituzione delle cose sequestrate[298]; infatti quando il bisogno istruttorio cessa, o sono esperibili modi meno afflittivi, la res deve essere restituita a chi ne ha diritto. Durante il processo la restituzione è disposta dal giudice. Nel caso in cui sia chiara la titolarità del soggetto che ha diritto alla restituzione si procede senza alcuna difficoltà; se, al contrario, sorgono dei dubbi viene instaurato un contraddittorio camerale disposto dall'art. 127 c.p.p.[299].

---

[294] Art. 354 c.p.p. contenente la disciplina dei casi in cui la polizia giudiziaria può disporre il sequestro.
"1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. 2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti. 3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale".
[295] Art. 355 c.p.p.
[296] Art. 191 c.p.p.
[297] Art. 357 c.p.p.
[298] Artt. 262 e 263 c.p.p.
[299] Art. 127 c.p.p.

Fra il riesame e la procedura di restituzione ci sono varie differenze. In primo luogo, i soggetti che possono richiederli sono diversi. In secondo luogo, il riesame verifica il provvedimento originario sotto i profili di legittimità e di merito; il procedimento di restituzione controlla la protrazione nel tempo del vincolo, le questioni sopravvenute e quelle che riguardano l'esecuzione dell'atto[300].

III.2 Il sequestro probatorio di un documento informatico

La disciplina del sequestro probatorio per quanto riguarda la sua disposizione su elementi informatici ha subito profonde integrazioni dalla legge 18 marzo 2008, n. 48[301]. Dall'analisi del codice di procedura penale si evince che nel caso di sequestro probatorio informatico "*per corpi di reato e cose pertinenti al reato*" si debbano intendere i dati, le informazioni o i programmi informatici; questo anche perché dal provvedimento di sequestro deve derivare minore pregiudizio possibile e deve rispettare il principio di proporzionalità[302]. L'applicazione di questo importante principio è essenziale poiché il sequestro probatorio informatico è ancora più invasivo nei confronti del soggetto che lo subisce e quindi è necessaria una peculiare attenzione. Il legislatore del 2008, attuando la Convenzione di Budapest sul cybercrime, è stato particolarmente attento alla questione legiferando puntualmente per preservare il rispetto di tale principio[303]. Il sequestro, infatti, è stato legittimato solo come "attività mirata" all'apprensione di singoli dati, informazioni e programmi in modo tale da evitare un'acquisizione generalizzata[304]; deve essere effettuato quindi solo nel caso sia effettivamente utile all'indagine in corso[305].

Questa ricostruzione sul principio di proporzionalità è l'unica affine alla normativa sovranazionale e alla giurisprudenza della Corte Europea dei Diritti dell'Uomo. Per quanto concerne la normativa sovranazionale, la Convenzione di Budapest all'art. 15[306] subordinava all'attuazione del principio di proporzionalità l'adozione, da parte degli Stati firmatari, di una normativa diretta a dotare gli investigatori di nuovi strumenti di ricerca della prova in campo informatico. Nel rapporto esplicativo

[300] Cfr. Aa. Vv., *Fondamenti di procedura penale, Terza edizione*, Cedam, pag. 371 e ss.
[301] L. 18 marzo 2008, n. 48.
[302] S. Signorato, *Le indagini digitali profili strutturali di una metamorfosi investigativa*, Giappichelli editore- Torino, 2018, p. 219.
[303] C. Costanzi, *Perquisizione e sequestro informatico. L' interesse al riesame nel caso di estrazione di copie restituzione dell'originale*, in Cass. Pen., 2016., 278.
[304] C. Costanzi, *Perquisizione e sequestro informatico*, cit., 278, il quale richiama la formulazione del nuovo art. 247, comma 1*bis*, c.p.p.
[305] A. Testaguzza*, Il sequestro di dati e sistemi*, in AA.VV., *Cybercrime,* a cura di A. Cadoppi – S. Canestrieri – A. Manna, Torino, 2019, 1459.
[306] Art. 15 Convenzione di Budapest sul *Cybercrime.*

della Convenzione, nello specifico nei paragrafi 145 e 146[307], viene specificato che nelle procedure adottate dagli Stati per l'implementazione della Convenzione in ambito del principio di proporzionalità, questi avrebbero dovuto incorporare il principio in parola, con la precisazione che quanto ai contraenti dell'area europea, tale obbligo deriva anche dagli stessi principi contenuti nella Convenzione Europea dei Diritti dell'Uomo[308]. Proprio a questo proposito e sul secondo versante, la Corte di Strasburgo ravvisa una violazione dell'art. 8 della Convenzione, che tutela il rispetto della vita privata e familiare, in caso di sequestro di dati informatici effettuato senza considerare il principio di proporzionalità. L'affermazione del principio di proporzionalità nel campo dei sequestri penali, da un lato, la presenza di referenti normativi del principio stesso nello specifico contesto dei mezzi informatici di ricerca della prova, dall'altro, hanno indotto la giurisprudenza di legittimità a riconoscere, almeno in linea di principio, come pacifica l'applicazione del principio al sequestro di materiale informatico. Questo, anzi, dovrebbe essere applicato con maggior severità per limitare le mere attività esplorative ed evitare il pregiudizio di alcune garanzie costituzionali[309].

L'art. 254 c.p.p., come oggetto del sequestro, individua "*oggetti di corrispondenza, anche se inviati in modo telematico*"[310]. Questo articolo uniforma perfettamente la corrispondenza telematica a quella cartacea, rendendo così applicabili le garanzie sulla segretezza e libertà della corrispondenza definite nella Costituzione nell'art. 15[311]. Fornisce, inoltre, la costruzione della relazione tra la corrispondenza e il reato oggetto di indagine; il mezzo di ricerca della prova in questione ha ad oggetto reati tradizionali che vengono compiuti con le tecnologie informatiche. L'art. 254*bis* c.p.p. disciplina "*il sequestro dei dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni*"[312] e consente l'acquisizione di un particolare tipo di *file* ossia il *file* di *log*. Quindi, oggetto di questa disciplina codicistica sono i *log* detenuti dai *provider* e relativi al traffico telematico e all'identificazione del luogo di accesso alla rete usata dall'utente[313]. La disciplina di acquisizione

[307] Paragrafi 145 e 146 Convenzione di Budapest sul *Cybercrime.*

[308] Convenzione Europea dei Diritti dell'Uomo è stata firmata nel 1950 dal Consiglio d'Europa. La convenzione è un trattato internazionale volto a tutelare i diritti umani e le libertà fondamentali in Europa. Tutti i 47 paesi che formano il Consiglio d'Europa sono parte della convenzione, 27 dei quali sono membri dell'Unione europea (UE).
La convenzione ha istituito la Corte europea dei diritti dell'uomo, volta a tutelare le persone dalle violazioni dei diritti umani. Ogni persona i cui diritti sono stati violati nel quadro della convenzione da uno Stato parte può adire alla Corte. Si tratta di una novità, in quanto ha conferito diritti alle persone in un contesto internazionale. Le sentenze che hanno riscontrato violazioni sono vincolanti per i paesi interessati. Il comitato dei ministri del Consiglio d'Europa vigila sull'esecuzione delle sentenze. La convenzione ha diversi protocolli, che modificano il suo quadro.
Il trattato di Lisbona, in vigore dal 1° dicembre 2009, consente all'UE di accedere alla CEDU e un progetto di accordo di adesione è stato predisposto nel 2013.

[309]Si ritiene che il principio di proporzionalità, già operante in caso di sequestro penale "classico", debba viepiù operare applicarsi in caso di sequestro informatico, M. Torre, *Indagini informatiche*.

[310] Art. 254 c.p.p.

[311] Art. 15 Costituzione.

[312] Art. 254*bis* c.p.p.

[313] Due esempi esplicativi di questo concetto potrebbero essere i *log* dei *server* di posta o i log di connessione telefonica per telefonia mobile.

dei file di log è espressamente indicata dall'art. 132 del d.lgs. 30 giugno 2003, n. 196[314] che ha istituito il Codice della Privacy[315].

Gli articoli 259 e 260 c.p.p.[316], riguardanti rispettivamente la custodia e l'apposizione dei sigilli a cose sequestrate, consentono di armonizzare le disposizioni sul sequestro probatorio informatico disciplinando una chiara concatenazione tra la custodia e la gestione degli oggetti informatici sequestrati. Il problema centrale, in questo ambito, è che in seguito della copia forense dei dati c'è la

[314] Art. 132 del d. lgs. 30 giugno 2003, n. 196. Per una maggiore chiarezza viene di seguito riportato l'articolo:
"*1-Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione; 1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni; 2. COMMA ABROGATO; 3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 c.p.p., e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, 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; 3-bis. Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato; 3-ter. Rispetto ai dati conservati per le finalità indicate al comma 1 i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalità di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo; 3-quater. I dati acquisiti in violazione delle disposizioni dei commi 3 e 3-bis non possono essere utilizzati; 4. COMMA ABROGATO; 4-bis. COMMA ABROGATO; 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del c.p.p., di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi; 4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'art. 326 c.p.; 4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia; 5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante ((con provvedimento di carattere generale)) , volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché ad indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1; 5-bis. È fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167*.".

[315] Il codice della Privacy è stato istituito con d. lgs. 30 giugno 2003, n.196 ed è stato modificato nel tempo. Le ultime due modifiche sono state apportate dalla l. 3 dicembre 2021, n. 205 e dal d.lgs. 10 marzo 2023, n. 24, con effetto a decorrere dal 15 luglio 2023.

[316] Artt. 259 e 260 c.p.p.

privazione del supporto informatico e questa diviene superflua e soprattutto lesiva per l'indagato, il quale potrebbe anche utilizzare il dispositivo per motivi leciti[317]. Dall'altro lato, però, è essenziale che l'indagato non possa utilizzare i dati oggetto del sequestro per evitare la reiterazione del reato. Per armonizzare le due questioni si veda l'art. 260 c.p.p.[318] il quale prevede: al primo comma che vi sia apposizione dei sigilli giudiziali anche di carattere elettronico o informatico ai dati acquisiti in modo da renderli inaccessibili all'indagato e ai terzi; al secondo comma, invece, prevede la possibilità di custodia degli originali sigillati anche in luoghi differenti dalla segreteria del Pubblico Ministero o della cancelleria del tribunale, offrendo la possibilità di dare in custodia all'indagato i dati sottoposti a vincolo nel supporto dandogli la possibilità di usufruire liberamente delle parti non digitalmente vincolate. L'elemento cardine per effettuare una corretta catena di custodia digitale dei dati è il sigillo digitale, che è completamente differente da quello giudiziale tradizionale per la sua immaterialità e affidabilità. Il sigillo digitale è una crittazione dei dati originali acquisiti in copia, illeggibili e immodificabili senza la chiave di decrittazione, che consente di affidare tali dati in custodia senza il rischio di inquinamento delle prove. Le caratteristiche del sigillo digitale implicano per il custode l'impossibilità di accesso o alterazione dei dati ai terzi[319]. Nel caso in cui venisse distrutto il supporto di memorizzazione, costituirebbe di certo reato *ex* art. 388.3 c.p.[320], ma non influirebbe sulle indagini poiché gli inquirenti sarebbero già in possesso di una copia forense dei dati del supporto[321].

A livello operativo il sequestro sembra poter essere effettuato in due modalità: con il cd. "blocco dei dati" oppure tramite il sequestro dell'intero dispositivo informatico.

La prima modalità consiste in una tecnica volta a "congelare" i dati di un dispositivo informatico, i quali successivamente vengono sigillati elettronicamente in modo da renderli immodificabili e intangibili. Per quanto riguarda, invece, il sequestro dell'intero dispositivo informatico è necessario sottolineare che esso è volto all'apprensione dei dati contenuti nel dispositivo in questione[322]. È un provvedimento ablativo che deve necessariamente essere proporzionato[323] alle esigenze di accertamento dei fatti che sono oggetto delle indagini. Insieme alla valutazione di proporzionalità, verrà anche verificato che il sequestro non sia solo un modo per aggirare le garanzie che devono essere rispettate.

---

[317] Cfr. C. Manchia, *Sequestro di computers: un provvedimento superato dalla tecnologia*?, in Cass. Pen., 2005, pag. 1634 e ss.
[318] Art. 260 c.p.p.
[319] *Ex* art. 259.2 c.p.p.
[320] Art. 388.3 c.p.
[321] Cfr. F. Novario, *Prove penali informatiche*, edizioni libreria cortina Torino, 2011.
[322] G. Illuminati, *Le direttive del d.l.l. n. 4368*, in *Jusonline,* 3/2017, p. 329.
[323] Come riferimento per la comprensione di questo principio si vedano a titolo esplicativo: Cass, Sez. III, 16 maggio 2012, n. 21931 e Cass., Sez. III, 7 maggio 2014, n. 21271.

È opportuno in questa sede evidenziare che solitamente nelle indagini tradizionali la perquisizione di norma precede il sequestro, invece, in quelle informatiche succede esattamente il contrario, cioè prima avviene il sequestro di un dispositivo informatico e poi lo si perquisisce.

Questa inversione di procedimento può portare conseguenze sistematiche in rapporto alle indagini tradizionali. L'impostazione più radicata delle indagini tradizionali connette la perquisizione e il sequestro con la logica della consequenzialità; dall'illegittimità della perquisizione deriva conseguentemente quella del sequestro[324]. Questa severa impostazione è solo lievemente mitigata dalle Sezioni Unite della Cassazione che, dopo aver ribadito che la perquisizione illegittima estende i suoi effetti invalidanti anche al sequestro, hanno stabilito che questa conseguenza non si verifica nel caso in cui si sequestrino il corpo del reato o le cose pertinenti al reato perché questo è un atto dovuto e quindi la sua omissione "*esporrebbe gli autori a specifiche responsabilità penali, quali che siano state, in concreto, le modalità propedeutiche e funzionali che hanno consentito l'esito positivo della ricerca compiuta*"[325].

Proprio il fatto che nelle indagini digitali è quasi sempre invertito il procedimento, quindi prima c'è il sequestro e poi la perquisizione, la propedeuticità della seconda rispetto al primo è un mero dato di frequenza statistica e non una necessità logico giuridica. In più, il sequestro è frequentemente funzionale a consentire la copia dei dati, sulla quale verrà poi operata la perquisizione. Da ciò possiamo desumere che sequestro e perquisizione sono due mezzi di ricerca della prova perfettamente autonomi e quindi non sembra individuabile alcun effetto "a cascata" secondo il quale l'illegittimità della perquisizione comporti illegittimità del sequestro successivo. La legittimità o meno del sequestro dovrà, dunque, essere valutata in base ai requisiti in esso contenuti e non in base alla legittimità della perquisizione[326].

---

[324] L.M. Comoglio, *Perquisizione illegittima e inutilizzabilità derivata delle prove acquisite con il susseguente sequestro,* in *Cass. Pen*., 1996, p. 1547 ss.
M. Nobili, *Divieti probatori e sanzioni*, in Giust. Pen., 1991, III, c. 641.
A. Zappulla, *Le indagini per la formazione della notitia criminis: il caso della perquisizione seguita da sequestro*, in Cass. Pen. 1996, p. 1878 ss.

[325] Cass., Sez. Un., 27 marzo 1996, S., in Cass. Pen., 1996, p. 3273.
In dottrina E. Fortuna-S. Dragone, *Le prove*, in E. Fortuna-S. Dragone-E. Fassone-R. Giustozzi, *Manuale pratico del processo penale,* Cedam, Padova, 2007, p. 400.

[326] Cfr. S. Signorato, *Le indagini digitali profili strutturali di una metamorfosi investigativa*, Giappichelli editore-Torino, 2018, pag. 220 e ss.

III.3 L'importanza della motivazione del decreto che dispone il sequestro di un documento informatico

Come già descritto, il sequestro probatorio consiste nell'assicurare una cosa mobile o immobile al procedimento per fini probatori[327], tramite lo spossessamento della *res* e creando un vincolo di indisponibilità su di essa. Questo vincolo permette di conservare immutate le caratteristiche della cosa sequestrata in modo tale da accertarne i fatti. Servono, per far ciò, due requisiti: uno naturalistico, cioè la *res*, e uno giuridico ossia deve trattarsi del corpo del reato o di una cosa pertinente al reato[328] e deve essere assolutamente necessaria per l'accertamento dei fatti.

La perquisizione di un computer costituisce un'attività che, per sua natura, si presta ad essere eseguita dopo il sequestro dello stesso. Il sequestro del dispositivo elettronico è attività che va ad incidere non soltanto sul diritto al possesso della *res*, che in questo è il *computer*, ma anche sul diritto alla riservatezza, nonché sulla privacy dei dati personali archiviati nella memoria elettronica[329]. Il numero dei diritti costituzionalmente garantiti aumenta nel caso in cui oggetto di sequestro siano documenti informatici che incorporano messaggi di posta elettronica[330]. Se ci si ferma a riflettere, la creazione di una *bitstream image*[331] dell'*hard disk*, comportando la copiatura completa della memoria del *computer*, rende potenzialmente disponibili agli inquirenti moltissimi dati, molti dei quali non pertinenti all'accertamento dei fatti oggetto di prova e dai quali si possono ricavare informazioni che vanno oltre il semplice "contenuto logico" di un documento tradizionale[332].

Il computer deve essere visto come "sfera di esplicazione della libertà della persona di cui esso ne è la proiezione spaziale"[333] e di conseguenza la motivazione contenuta nel decreto che dispone il

---

[327] P. Tonini, *Manuale di procedura penale*, Milano, 2020, 378 ss.

[328] La giurisprudenza ha chiarito "*come la nozione di 'cosa pertinente al reato' abbia una portata più ampia di quella impiegata all'art. 253 c.p.p., comprendendo non solo il corpo del reato ma anche qualunque cosa sulla quale o a mezzo della quale il reato fu commesso o che ne costituisce il prezzo, il prodotto o il profitto, o anche quelle cose legate indirettamente alla fattispecie criminosa*", così si esprime la sentenza in commento. Cfr. altresì Cass. pen., Sez. V, 28 maggio 2014, n. 26444, Denaro, Rv. 259840; Sez. II, 19 giugno 2013, n. 34986, Pini, Rv. 256100; Sez. II, 22 gennaio 2009, n. 17372, Romeo e altri, Rv. 244342.

[329] Queste le parole di F.M. Molinari, Questioni in tema di perquisizione e sequestro di materiale informatico, cit., 12 ss. Sul punto, si veda M. Bonetti, Riservatezza e processo penale, Milano, 2003; S. Carnevale, Autodeterminazione informativa e processo penale, in AA.VV., Protezione dei dati personali e accertamento penale, a cura di Negri, Roma, 2007, 3 ss.; Fiore, voce Riservatezza (diritto alla): IV) Dir. pen., in Enc. giur., XXVII, Roma, 1998, 17; A. Manna, Beni della personalità e limiti della protezione penale, Padova, 1989; M.S. Pisani, La tutela penale della "riservatezza": aspetti processuali, in Riv. it. dir. proc. pen., 1967, 785; G. Ubertis, Principi di procedura penale europea, Milano, 2009, 126.

[330] Nel caso specifico si parla di diritto alla segretezza della corrispondenza disciplinato dall'art. 15 Cost.
Cfr. A. Logli, *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in Cass. pen., 2008, 2956.

[331] È la copia bit per bit dei dati digitali presenti in un dispositivo di memorizzazione di dati digitali verso un altro dispositivo di memorizzazione di dati digitali, in modalità clone o in modalità immagine.

[332] F.M. Molinari*, Questioni in tema di perquisizione e sequestro di materiale informatico*, in Cass. pen., 2012, 708.

[333] S. Pisani, *La tutela penale della "riservatezza*", pag. 785 e ss.

sequestro deve essere molto più dettagliata e puntuale per quanto riguarda la raccolta dei dati, rispetto al provvedimento di un sequestro tradizionale. Non può più essere accettata l'adozione di provvedimenti con la finalità di generica esplorazione di tutti i dati digitali contenuti nell'hard disk e l'apertura di tutti i files per poi sostenere che verranno presi in considerazione solo quelli utili alle indagini.

La creazione di una copia-clone e la conservazione dei dati incidono sul diritto alla privacy; l'esigenza di un effettivo rimedio per l'interessato contro eventuali ingerenze arbitrarie, dettate da una motivazione del provvedimento quasi nulla, trova un riscontro in ambito europeo[334]. La disposizione normativa di riferimento è l'articolo 8 CEDU[335], il quale sancisce il diritto di ogni persona al rispetto della propria vita privata e familiare, del domicilio e della corrispondenza; tuttavia, questo non è un diritto assoluto perché al comma 2[336] sono ammesse ingerenze da parte dell'autorità giudiziaria solo se previste per legge e finalizzate ad un obiettivo lecito in una società democratica. La motivazione del provvedimento di sequestro deve necessariamente: giustificare in modo esaustivo l'ingerenza nella sfera privata dell'individuo, elencare i motivi in modo esaustivo e sufficiente, l'ingerenza deve essere proporzionale allo scopo che l'autorità vuole raggiungere[337]. La Corte europea dei diritti dell'uomo ha dato disposizioni precise affinché possa ritenersi rispettato l'art. 8 CEDU; deve essere indicato già nel provvedimento di sequestro un "protocollo di ricerca" per la successiva perquisizione, che contenga delle indicazioni specifiche rispetto all'oggetto di prova e collegate alla *res iudicanda*; la predisposizione di adeguate garanzie di custodia da parte delle autorità prima del compimento di successive attività processuali, come la perquisizione e/o perizia; la possibilità per il titolare del materiale, che sia l'indagato o un terzo, di contestare di fronte ad un organo giurisdizionale la legittimità dei provvedimenti e relative attività di sequestro e perquisizione, nonostante la restituzione dell'originale[338].

La Cassazione riconosce in generale all'autorità giudiziaria la possibilità di disporre sequestri dai contenuti molto estesi con il solo fine di esaminare un'ampia massa di dati i cui contenuti sono in astratto potenzialmente rilevanti per le indagini. Tuttavia, gli inquirenti devono provvedere, nel rispetto del principio di proporzionalità e adeguatezza, all'immediata restituzione delle cose sottoposte a vincolo una volta decorso il tempo ragionevolmente necessario per gli accertamenti. In caso di mancata tempestiva restituzione, è consentito all'interessato presentare la relativa istanza e

[334] Come caso esplicativo si veda, tra i tanti, Corte EDU, 16 febbraio 2000, Amann c. Svizzera.
[335] Art. 8 CEDU.
[336] Art. 8.2 CEDU.
[337] Si veda il caso: Corte EDU, sent., 28 gennaio 2003, Peck c. Regno Unito, par. 76.
[338] F.M. Molinari, Questioni in tema di perquisizione e sequestro di materiale informatico.

far valere le proprie ragioni attraverso i rimedi offerti dal nostro ordinamento[339]. È dunque possibile ricorrere al sequestro anche totalizzante solo nel caso in cui il Pubblico Ministero lo ritenga necessario e il giudice lo accordi verificando che vi sia la sussistenza di un vincolo di pertinenzialità tra *res*, reato per cui si procede e finalità probatoria perseguita[340].

Un principio in sintonia con quanto affermato in una recente pronuncia delle Sezioni Unite, del 19 aprile 2018, n. 36072[341], secondo la quale il decreto di sequestro probatorio, così come il decreto di convalida, anche qualora abbia ad oggetto cose costituenti corpo del reato, deve contenere una motivazione che, per quanto concisa, dia conto specificamente della finalità perseguita per l'accertamento dei fatti in questione. Le Sezioni Unite, in questo caso, sono intervenute per dirimere un contrasto di orientamenti circa la motivazione del decreto che dispone il sequestro probatorio volto all'apprensione del *corpus delicti*. Secondo un primo orientamento, il decreto di sequestro probatorio del corpo del reato deve essere provvisto, a pena di nullità, di un'idonea motivazione che renda conto della finalità perseguita, in concreto, per l'accertamento dei fatti. Il ricorso ad una formula sintetica è ammesso esclusivamente nel caso in cui la funzione probatoria del sequestro del corpo del reato sia di evidenza immediata e facilmente desumibile[342]. Il secondo orientamento, invece, sostiene che il decreto debba essere sorretto, a pena di nullità, da un'idonea motivazione in base all'esistenza della relazione di immediatezza tra la *res* sequestrata ed il reato oggetto di indagine. Non sarebbe necessaria una specifica e puntuale motivazione relativa alla funzionalità del sequestro rispetto all'accertamento dei fatti, posto che l'esigenza probatoria del corpo del reato è in *re ipsa*. In ordine a quest'ultimo specifico aspetto, il sequestro delle cose pertinenti al reato, al contrario, necessita di apposita motivazione. Le Sezioni Unite, sul punto, hanno sin da subito eliminato l'idea di differenziazione del regime del sequestro probatorio tra il corpo del reato e le cose pertinenti al reato. La funzione probatoria della cosa oggetto del reato rappresenterebbe il cuore della motivazione, atteso che, afferma la Suprema Corte "*l'aspetto di relazione di immediatezza tra bene sequestrato e reato per il quale si procede non costituirebbe altro che la descrizione, effettuata in termini differenti, del necessario requisito di finalizzazione probatoria del bene appreso*". L'obbligo di motivazione del

[339] A titolo esplicativo si vedano: Cass. Pen., Sez. V, 14 marzo 2017, n. 16622, Storari; Cass. Pen., Sez. VI, 15 dicembre 2016, n. 53168, Amores, Rv. 268489; Cass. Pen., Sez. II, 12 aprile 2013, n. 16544, Verni; Cass. Pen., Sez. III, 7 luglio 2008, n. 27508, Rv. 240254.

[340] Sul tema cfr. Cass. Pen., Sez. VI, 12 settembre 2018, n. 56733, Macis, Rv. 274781; Cass. Pen., Sez. V, 27 febbraio 2015, n. 13594, Gattuso, Rv. 262898.

[341] Cass. Pen., Sez. Unite, 19 aprile 2018, n. 36072.

[342] P. Grillo, *Ultimissime sul sequestro del corpo del reato: come va motivato*?, in D&G, fasc. 17, 2015, 53;
A. Foti, *Qual è l'esatta portata dell'onere motivazionale afferente le esigenze probatorie del provvedimento cautelare*, in D&G, fasc. 16, 2018, 2; A. Ubaldi, *Sequestro probatorio di documenti e server: vincolo illegittimo se non proporzionato ai bisogni probatori*, in D&G, fasc. 193, 2019, 12; A. Mari, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati (nota a margine di Cass. Pen., SS.UU., 20 luglio 2017, n. 40963)*, in Cass. pen., fasc. 12, 2017, 4312.

decreto di sequestro probatorio, nonché del decreto di convalida, sottolinea infine la Cassazione, troverebbe il proprio appiglio anche nelle disposizioni costituzionali e sovranazionali sul diritto di proprietà, di cui agli artt. 42 Cost.[343] e 1 Prot. addizionale CEDU[344].

La strumentalità del bene rispetto alla condotta criminosa e alla finalità probatoria del sequestro è uno dei canoni di valutazione della pertinenza e svolge una funzione selettiva. Il tema della strumentalità si pone, soprattutto, per l'indiscussa utilità delle informazioni acquisite, destinata solitamente ad aumentare in modo proporzionale all'entità dell'ingerenza dell'autorità giudiziaria nella sfera più personale dell'individuo: più l'attività di ricerca della prova si avvicina al nucleo della sfera privata, costituito da quell'intimità che la persona ritiene di non condividere, più il dato acquisito può risultare prezioso per l'accertamento del fatto. La strumentalità è astrattamente configurabile in un numero indefinito di casi e ciò impone di attribuire a tale requisito un significato conforme ai principi generali di adeguatezza e proporzionalità espressamente previsti dal nostro ordinamento. È necessario un esame particolarmente rigoroso in ordine al rapporto sussistente tra la cosa e il reato ed è altresì necessario, quando il legame prospettato sia di natura funzionale, che tale rapporto non sia meramente occasionale[345]. La verifica del nesso di funzionalità non occasionale, come precisato dalla Cassazione, tra il bene e la condotta, deve essere maggiormente rigorosa nei casi in cui il bene appartenga ad un soggetto terzo estraneo al reato.

L'attività di perquisizione e sequestro di un *personal computer* prevede una serie di operazioni tra loro concatenate che sono: perquisizione locale, sequestro del *personal computer*, perquisizione dell'*hard disk*, individuazione e sequestro dei *files* reputati rilevanti per l'accertamento penale. Ci troviamo di fronte ad un atto investigativo molto complesso, che necessita di adeguati presupposti giustificativi. Pertanto, la motivazione dovrà essere particolarmente scrupolosa nel giustificare l'intera sequenza investigativa, in particolare dovrà essere dettagliatamente motivato lo stretto collegamento tra attività di ricerca e *thema probandum*[346].

Non è sempre possibile individuare prima i files utili all'accertamento dei fatti. Tuttavia, anche laddove sia possibile l'indicazione preventiva, non è detto che la polizia giudiziaria, in fase di perquisizione o comunque nell'immediatezza dei fatti, sia in grado di localizzare tali *files* sul *server*

[343] Art. 42 Cost.
[344] Prot. Addizionale CEDU.
[345] Cfr. Cass. Pen., Sez. VI, 25 gennaio 2018, n. 33045, Mazza; Cass. Pen., Sez. V, 28 maggio 2014, n. 26444, Denaro, cit.; Cass. Pen., Sez. VI, 20 gennaio 2017, n. 5845, F., Rv. 269374; Cass. Pen., Sez. V, 16 dicembre 2009, n. 12064; dep. 2010, Marcante, Rv. 246881.
[346] A. Logli, *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in Cass. pen., fasc. 7-8, 2008, 2952; cfr. G. Costabile, *Scena criminis, documento informatico e formazione della prova penale*, in www.altalex.com, n. 1096 del 14 luglio 2005; G. Braghò, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in Riv. inf. e informatica, 2005, 217; C. Manchia, *Sequestro probatorio di computers: un provvedimento superato dalla tecnologia?*, in Cass. pen., 2005, 1634.

aziendale o sul *computer personale*. L'art. 248 c.p.p.[347], che disciplina la richiesta di consegna di cose determinate, ammette la possibilità di emanazione di provvedimenti senza previamente determinare l'oggetto, ma devono presentare solamente indentificare la caratteristica di una possibile attinenza meramente eventuale col reato che si presume essere stato commesso, ossia quei *files* che "*anche senza essere in rapporto qualificato con il fatto illecito, presentino capacità dimostrativa dello stesso*"[348].

La Suprema Corte ha previsto che il Pubblico Ministero possa delegare alla polizia giudiziaria il compito di sequestrare tutto quello che, in esito ad un'analisi di quanto rinvenuto, la stessa ritenga utile ai fini della prosecuzione delle indagini; però "*quando la polizia giudiziaria abbia individuato e sequestrato cose non indicate nel decreto o il cui ordine di sequestro non sia desumibile dalle nozioni di corpo di reato o di cose pertinenti a reato, in relazione ai fatti per i quali si procede, l'autorità giudiziaria dovrà procedere alla convalida del sequestro ovvero ordinare la restituzione delle cose non ritenute suscettibili di sequestro*"[349]. . L'eventuale illegittimità della perquisizione non ha effetti preclusivi sul sequestro; dato che il potere di sequestro "*in quanto riferito a cose obiettivamente sequestrabili, non dipende dalla modalità con cui queste siano state reperite, ma è condizionato unicamente all'acquisibilità e all'insussistenza di divieti probatori enucleabili dal sistema*"[350].

III.4 Il sequestro probatorio e la copia dei dati informatici

Per quanto concerne il problema della copia dei dati informatici sequestrati verrà di seguito riportato un caso per esplicare gli orientamenti giurisprudenziali in materia.

La sentenza della Corte di Cassazione, Quinta Sezione Penale, n. 13694 del 15 febbraio 2019[351], depositata il 28 marzo 2019, ha deciso sul ricorso proposto dall'indagato avverso l'ordinanza resa dal Tribunale di Trieste di conferma del sequestro probatorio disposto, in data 10 settembre 2018, dal Pubblico Ministero, affronta la lunga discussione giurisprudenziale relativa alla permanenza dell'interesse a ricorrere nei casi in cui sia intervenuto il dissequestro dei documenti informatici, previa ''copiatura'' dei dati in essi contenuti. Nel caso di specie, è stato disposto il sequestro

[347] Art. 248 c.p.p.
[348] C. Parodi*, Il sequestro probatorio dei dispositivi informatici: necessario contemperare esigenze investigative e principio di proporzionalità*, consultabile su ilpenalista.it, 10 dicembre 2020.
[349] Cass. Pen., Sez. Unite, 19 aprile 2018, n. 36072.
[350] Cfr. C. Fontani, Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi, Diritto penale e processo, 2/2022.
[351] Cass. Pen., V Sez., 15 febbraio 2019, n.13694.

probatorio di dati presenti in supporti documentali ed informatici relativi a false comunicazioni sociali, ex art. 2621 c.c.[352], per i quali si procedeva nei confronti dell'amministratore dell'azienda. La richiesta di riesame della misura proposta dall'indagato non è stata accolta dal Tribunale, rilevando quest'ultimo l'accertata sussistenza del nesso di pertinenza del materiale sottoposto a vincolo di sequestro rispetto al reato ipotizzato. L'ordinanza di rigetto del Tribunale è stata impugnata dall'indagato con ricorso per Cassazione, all'esito del quale è stata dichiarata l'inammissibilità del gravame per intervenuta carenza di interesse, non risultando allegato, a seguito del dissequestro, quell'"*interesse concreto ed attuale, specifico ed oggettivamente valutabile sulla base di elementi univocamente indicativi della lesione di interessi primari conseguenti alla indisponibilità delle informazioni contenute*" nei documenti informatici che soltanto avrebbe potuto giustificare la permanenza "*di una posizione giuridica tutelabile all'esito della disposta restituzione*"[353].

Con questa pronuncia la Cassazione affronta varie tematiche processuali che di seguito verranno descritte.

L'esistenza della condizione a ricorrere per Cassazione postula l'individuazione di un'utilità concreta, come effetto connesso all'eventuale accoglimento della domanda, essendo il ricorrente tenuto a dedurre la prospettazione di un vantaggio sostanziale sotteso all'attivazione dell'impugnazione[354] , come imposto dall'art. 568.4 c.p.p.[355]. La questione si pone in relazione alla verifica circa la persistenza dell'interesse ad agire dell'indagato, anche in caso di restituzione del bene preceduta dalla estrazione di copia dei dati previamente sequestrati , dovendosi in altre parole accertare, in concreto, se la stessa restituzione materiale del bene, che sia su supporto informatico o digitale, sia in grado di

[352] Art. 2621 cc. Il quale dispone che: "*Fuori dai casi previsti dall´art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione e´ imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.*
La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.".

[353] Cfr. P. Rivello, L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico, in Cass. Pen., 2018, fasc. 1 ; A. Mari, Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati (note a margine di sez. Un., 20 luglio 2017, n. 40963), in Cass. Pen., 2017, fasc. 12, 4312; G. Todaro, Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite; in Dir. Pen. Cont., 2017, fasc. 11, 157 e seg.; F. Denti, La tutela della privacy e dell'esclusività del patrimonio informativo alla prova del sequestro dei dati informatici, in Resp. Civ. e Prev., 2016, fasc. 4, 1304; F. M. Molinari, Questioni in tema di perquisizione e sequestro di materiale informatico, in Cass. Pen., 2012, fasc. 2.

[354] Cfr. Cass., Sez. I, 25 novembre 2016– 22 febbraio 2017, n. 8763, in CED 269199; Sez. V, 21 settembre 2015-15 febbraio 2016, n. 6166, in CED 266259; Sez. un., 27 ottobre 2011-17 febbraio 2012, n. 6624, in CED 251693.

[355] Art. 568.4 c.p.p.

elidere, dal punto di vista del diritto sostanziale, le conseguenze pregiudizievoli della misura ablatoria, quanto alle esigenze di privacy causate dallo spossessamento.

In materia vi è un acceso contrasto giurisprudenziale. L'individuazione di diritti idonei a giustificare il perdurante interesse alla impugnazione è del tutto connessa all'intrinseca difficoltà di procedere ad una univoca qualificazione dogmatica dei tradizionali strumenti di ricerca della prova, tanto che, in un primo tempo, la giurisprudenza riteneva che il sequestro perpetrasse i propri effetti ablatori con riferimento ai soli supporti informatici appresi, tralasciando di considerare la permanenza del vincolo di indisponibilità in caso di copiatura dei dati originali[356]; successivamente, invece, veniva data rilevanza al dato considerandolo *in toto*[357].

Si osserva che sul tema sono state abbracciate differenti conclusioni; talvolta si era ritenuto che la legittimazione dell'indagato ad impugnare il provvedimento di sequestro dovesse essere strettamente legato alla esclusiva necessità di sottrarlo dal materiale probatorio utilizzabile[358], altre volte invece si era ritenuto che, considerata la riconsegna del bene alla stregua dell'unico scopo del riesame, non potesse residuare ulteriore interesse in capo al destinatario della *res*, da ciò doveva discendere la dichiarazione di inammissibilità del gravame per sopravvenuta carenza di interesse.

Come punto centrale della discussione, però, è sempre rimasta l'esigenza di offrire adeguata tutela ai diritti primari della persona, quali la privacy, la riservatezza ed il segreto delle informazioni contenute nei supporti digitali sequestrati[359], in maniera conforme al processo di modernizzazione delle tecniche scientifiche e tecnologiche in tema di ricerca della prova che ora sono molto più invasive rispetto ai tempi passati[360].

In passato non veniva attribuita alcuna rilevanza sostanziale al fenomeno in esame: risultava del tutto ininfluente l'estrazione della copia dei dati informatici e/o analogici rispetto alla persistenza dell'interesse ad agire[361].

---

[356] Cfr. Sez. IV, 21 giugno 2006, n. 26903; Sez. VI, 20 luglio 2012, n. 29846, in CED 253251; Sez. II, 30 maggio 2014, n. 27503, in CED 259197.

[357]Cfr. Sez. un., 2008. n. 18253, Tchiml cit.; Sez. VI, 24 febbraio 2015, n. 24617, Rizzo, Rv. 264093; Sez. III, 23 giugno 2015, n. 38148, Cellino, Rv. 265181; Sez. un., 20 luglio 2017 – dep. 7 settembre, n. 40963 cit.

[358] Sez. VI, 1º luglio 2003, n. 36775, in CED 227013; Sez. IV, 1º dicembre 2005, n. 6279/2006, in CED 233402.

[359]L. Picotti, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati, in AA.VV., Il diritto penale dell'informatica nell'epoca di internet, a cura di L. Picotti, Padova 2004, 86 e seg.; C. Sarzana di S. Ippolito, Informatica, internet e diritto penale, III Ed., Milano 2010, 61 e seg.; L. Luparia, La disciplina processuale e le garanzie difensive, in L. Luparia, G. Ziccardi, Investigazione penale e tecnologia informatica, Milano 2007, 130.

[360] Sull'impatto delle nuove tecnologie sui diritti costituzionali, da notare la creazione, da parte della Corte Costituzionale tedesca, del diritto alla ''garanzia della segretezza e integrità dei sistemi informatici '', cfr. BverfG 27 febbraio 2008 (1 Bvr 370/07; 1 BvR 595/07); sulla necessaria rivisitazione delle regole probatorie nei casi di prove digitali, v. O.S. Kerr, Digital evidence and the new criminal procedure, in 105 Columbia law rev. 2005, 290 e seg. In chiave comparatistica, cfr., F. Iovene, Perquisizione e sequestro di computer: un'analisi comparatistica'', in Riv. Dir. Proc., 2012, fasc. 6, 1607.

[361]Cass., Sez. un., 20 dicembre 2007, n. 230.

Tale tesi, che è stata definita "negativa", trovava inquadramento nella parziale, se non erronea, declassificazione del concetto di dato informatico, il quale non veniva valorizzato rispetto alle peculiarità caratterizzanti e potenzialmente idonee a pregiudicare il diritto alla riservatezza delle informazioni in esso contenute. Si trattava, evidentemente, di un equivoco provocato dall'indistinto riferimento alla nozione di documenti informatici, supporti e materiale informatico, che non teneva assolutamente in considerazione la Convenzione di Budapest del 2001[362], ratificata in Italia nel 2008 con la L. n. 48[363], la quale espressamente prevedeva, all'art. 1[364], la distinzione concettuale tra il ''*dato informatico*'', inteso come ''*qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato*'', rispetto al ''*sistema informatico*'', ovverosia ''*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*''.

Questa interpretazione sosteneva che, ai sensi degli artt. 258 e 262.1 c.p.p.[365], l'efficacia del provvedimento di sequestro si interrompesse in caso di restituzione del documento originale, con la conseguenza che l'interesse a proporre impugnazione non dovesse ancorarsi alla valutazione della legittimità o meno della misura, ma esclusivamente risiedere nella necessità di rispristino della situazione di possesso o detenzione del bene sequestrato. La Cassazione non ravvisava, nell'estrazione di copia, alcuna potenziale persistenza degli effetti pregiudizievoli del sequestro nei confronti dei diritti della persona, essendo stato quest'ultimo, per l'appunto, ''revocato''; inoltre, si riteneva il trattenimento delle copie un'operazione del tutto distinta. A sostegno di questa convinzione, in caso di eventuale illegittimità del medesimo sequestro, si escludeva dall'oggetto del procedimento di riesame la dedotta copiatura, questo alla luce dell'affermata tipicità e/o tassatività dei mezzi di impugnazione. Nell'ipotesi di restituzione della *res* controversa, previa estrazione di copia dei dati contenuti, si perveniva, quindi, alla declaratoria d'inammissibilità sopravvenuta del gravame.

La teoria sino ad ora esposta, è stata completamente sconfessata dalle Sezioni Unite Tchmill, n. 18253/2008[366]; qui è emersa una prima apertura nei confronti del riconoscimento dell'interesse a ricorrere in tali casi, tuttavia al solo fine di impedire l'ingresso della copia nel patrimonio probatorio utilizzabile. In questa pronuncia è stata data rilevanza alla copia del documento informatico quanto alla sua potenzialità lesiva ai fini dell'accertamento del reato, dunque, l'invalidità dell'operazione di

[362] Convenzione di Budapest del 2001.
[363] L. 18 marzo 2008, n.48.
[364] Art. 1 l. 18 marzo 2008, n.48.
[365] Artt. 258 e 262.1 c.p.p.
[366]Cass. pen., Sez. un., 24 aprile 2008, n. 18253.

copia rappresentava una conseguenza ineludibile della rilevata ed eccepita invalidità del sequestro, attraverso una derivazione a catena, *simul stabunt simul cadent*.

Rilevata l'inadeguatezza di tali principi rispetto alle nuove esigenze di raccordo con la Convenzione di Budapest[367], nella sentenza della Sez. IV, del 24 febbraio 2015, n. 24617[368], seguendo la preliminare distinzione concettuale e sostanziale tra ''sistemi'', ''supporti'' e ''dati'' e ampliando la portata concettuale e applicativa del bene giuridico protetto tale da ricomprendere in esso l'esclusiva disponibilità delle informazioni tout court, è stato valorizzato il principio della proporzionalità, così da ritenere non congruo, e dunque illegittimo, il sequestro indiscriminato dell'intera memoria informatica, in assenza di analitica indicazione dei dati da sottoporre a vincolo nonché gli oneri motivazionali in tema pertinenzialità *ex* art. 253 c.p.p.[369] nei casi di sequestro probatorio[370].

Il principio fondante di tale pronuncia risiede nella positiva rilevanza attribuita all'operazione di copiatura dei dati informatici tanto che, anche in caso di successiva restituzione dei compendi sottoposti a vincolo, si esclude che possa configurarsi come avvenuta la restituzione del materiale informatico, in virtu` della valorizzazione della disciplina dell'art. 254*bis*[371] c.p.p.[372].

Per concludere, la sentenza della Corte di cassazione, Quinta Sezione Penale, n. 13694 del 15 febbraio 2019, depositata il 28 marzo, aderendo al principio di diritto statuito dalle Sezioni Unite del 2017, pur negando nella fattispecie sottoposta al suo giudizio l'interesse a ricorrere, precisa la necessaria allegazione dell'interesse a ricorrere, da intendersi nel senso di interesse finalizzato all'accertamento dell'invalidità del sequestro sotto il profilo della ''*lesione dalla indisponibilità esclusiva delle informazioni contenute nelle cose sottoposte a vincolo"*'', in mancanza del quale l'interesse stesso al ricorso non può ravvisarsi ''*nel mero ottenimento di una pronuncia sulla legittimità del provvedimento cautelare*''.

Il rilievo mosso dalla Corte è volto ad una apertura ''sostanzialistica'' della posizione giuridica tutelabile dell'indagato, quanto al diritto alla esclusiva disponibilità del patrimonio informatico copiato nel corso delle indagini. Tuttavia, tale maggiore flessibilità interpretativa risulta accompagnata da un rilevante temperamento processuale, consistente nella devoluzione al privato dell'onere di allegazione delle specifiche ragioni indicative della lesione di interessi primari. Solo in

[367] Convenzione di Budapest del 2001.
[368] Cass. Pen., Sez. IV, del 24 febbraio 2015, n. 24617.
[369] Art. 253 c.p.p.
[370]Nel caso di violazione del principio di proporzionalità tra l'entità dei dati sottoposti a vincolo e le contrapposte esigenze processuali di indagine, alcune pronunce della Corte di Strasburgo ravvisavano la violazione dell'art. 8 CEDU: Corte Edu, 28 gennaio 2003, Peck c. Gran Bretagna; Corte Edu, 16 ottobre 2007, Wieser e Bicos Beteillingungen GMBH c. Austria; Corte Edu, 22 agosto 2008, Ilya Stefanof c. Bulgaria.
[371] Art. 254*bis* c.p.p.
[372] Cass. Pen., Sez. III, 23 giugno 2015, n. 28148 .

caso di avveramento di tale condizione, infatti, si riconosce la sopravvivenza dell'interesse a ricorrere anche nei casi di dissequestro del bene fisico prima sottoposto a vincolo.

In definitiva, la ricostruzione interpretativa citata, stante la compresenza di elementi che valorizzano, da un lato, il dato sostanziale, quindi i diritti primari alla riservatezza, dall'altro, aspetti tecnici processuali come gli oneri di specifica allegazione delle lesioni subite. Questa potrebbe qualificarsi come tesi che sta nel mezzo tra quelle precedentemente citate. Questa tesi giurisprudenziale appena delineata è sostenuta anche dalla recente sentenza n. 15133/2019[373].

Le mobili frontiere della tematica che si sta trattando trovano ulteriore riscontro nella recente pronuncia della Suprema Corte di cassazione n. 15133/2019. Detta statuizione afferma che, quanto all'estrazione di copia dei dati contenuti in supporti informatici, "*se il ricorrente intende controvertere in merito alla loro utilizzabilità, come spiegato dal Tribunale, deve aspettare il processo, se invece intende ottenere l'immediata restituzione dei documenti privati allora nulla osta a che formuli specifica domanda ed in caso di diniego presenti impugnazione*".

Il conflitto giurisprudenziale sopra enucleato testimonia come la tematica relativa al sequestro probatorio e l'estrazione di copia dei dati informatici non abbia ancora del tutto trovato una sua definitiva composizione, non potendosi infatti ritenere del tutto sopito il dibattito sorto al riguardo[374], mentre appare come certa la rilevanza del dato informatico in sé trasfuso anche attraverso operazioni di copiatura e, dunque, non solo quando esso risulti collocato all'interno di un supporto fisico informatico.

La nuova dimensione attribuita al dato informatico riposa sull'esigenza di assicurare una tutela effettiva di diritti primari costituzionalmente garantiti, quali quelli alla riservatezza, al segreto, e di salvaguardare le altrettanto ineludibili esigenze probatorie e/o di speditezza processuale, attuate mediante un contemperamento processuale consistente nella necessaria allegazione da parte dell'indagato delle specifiche ragioni sottese alla restituzione delle informazioni informatiche, quand'anche copiate.

Nonostante le conclusioni alle quali la giurisprudenza è arrivata, sembra necessario disciplinare in una maniera più unitaria ed esaustiva tanto il procedimento estrattivo delle copie, quanto i relativi strumenti d'impugnazione, il tutto in una prospettiva sia nazionale che internazionale[375].

[373] Cass., 3 giugno 2019, n. 15133.
[374] S. Carnevale, Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare, in Dir. Pen. Proc., 2009, fasc. 4, 472 e ss.
[375] Cfr. T. Linardi, Il sequestro probatorio e la "copia" dei dati informatici, Giurisprudenza italiana, ottobre 2019.

CONCLUSIONI

La digitalizzazione di ogni ambito della vita dei cittadini ha comportato, conseguentemente, l'utilizzo di tutti gli strumenti informatici disponibili anche nell'ambito del diritto.

In particolare, il documento informatico che possiamo intendere come "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"* ai sensi della disciplina del CAD ha un ruolo importante all'interno del processo penale, anche se, inizialmente, il legislatore aveva considerato la mera forma cartacea. È stato proprio il CAD, Codice dell'amministrazione digitale, a fornire una disciplina il più omogenea possibile del ciclo di vita di un documento informatico. Inizia dalla sua formazione, come disciplinato dall'art. 40 CAD, per poi essere sottoscritto, trasmesso, registrato e conservato. Il documento informatico può anche essere copiato, tale aspetto lo troviamo disciplinato dall'art. 23 CAD che è rubricato "*copie analogiche di documenti informatici*" dove l'aspetto più rilevante è garantire la conformità della copia cartacea all'originale informatico. Questo articolo disciplina, anche, il contrassegno elettronico che può essere apposto alla copia cartacea per garantire corrispondenza tra la copia e l'originale. L'art. 23*bis CAD*, invece, ha come disciplina le copie informatiche dei documenti informatici: queste hanno la stessa valenza giuridica del documento informatico dal quale sono tratti solo nel caso in cui vengano prodotti rispettando in tema di regole tecniche l'art. 71 CAD.

Nel secondo capitolo di questo testo, è stato esaminato il documento informatico nel processo penale. Il codice non contiene una normativa completamente omogenea dell'istituto. Gli articoli di riferimento all'interno del codice di procedura penale sono l'art. 234 e 234*bis* c.p.p., i quali rappresentano la base dell'interpretazione giurisprudenziale e dottrinale in materia. Per concedere al lettore una visione più organica della tematica sono stati esplicati due casi significativi che si possono riferire all'applicazione degli articoli del codice che sono stati presi a riferimento: la sentenza della Corte Costituzionale del 23 luglio 2023, n. 170 e per quanto concerne la disciplina dell'art. 234*bis* è stato esposto un caso che ha come punto centrale la messaggistica di *Sky Ecc* effettuata tramite cripto telefonini.

Infine, all'interno dell'ultimo paragrafo del secondo capitolo, è stata fatta chiarezza sulla differenza tra documento e documentazione. Confondendo il primo con il secondo, o viceversa, verrebbe violato un principio fondante del processo penale ossia quello di separazione delle fasi: non si deve confondere la documentazione di un'attività d'indagine con il documento poiché quest'ultimo, non può formarsi nell'ambito di un'attività investigativa, ma solo al di fuori di essa.

Il terzo capitolo ha come oggetto il sequestro probatorio di un documento informatico.

Come prima analisi è stata effettuata una breve differenziazione tra le tre tipologie di sequestro disciplinate dal codice: il sequestro conservativo e quello preventivo sono due misure cautelari, mentre il sequestro probatorio è un mezzo di ricerca della prova. Di seguito, è stato sottolineato che la disciplina del sequestro probatorio di un documento informatico differisce a livello pratico-operativo con quella del sequestro di un documento tradizionale. È necessario soffermarsi sulla necessità, durante l'operazione, di applicare correttamente le garanzie costituzionalmente garantite dalla Carta Costituzionale senza però ostacolare le indagini dell'autorità giudiziaria.

Dopo l'analisi effettuata nel testo qui sopra riportato, si è ritenuto che la disciplina normativa sia ancora acerba data l'importanza dell'informatica nel processo penale e sarebbe necessario un intervento organico per garantire una piena tutela del cittadino di fronte alle indagini informatiche e una conoscenza più dettagliata per il lettore per ciò che concerne l'utilizzo e la disciplina del documento informatico.

Bibliografia

ALCARO F., *Riflessioni 'vecchie' e 'nuove' in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in Rass. dir. civ., 2006, 951.

ANTOLISEI F., *Manuale di diritto penale*, Milano, 2003, 253.

BARILE P. – Cheli E., *Corrispondenza (libertà di*), in Enc. dir., X, Milano, 1962, 743 ss.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 163 ss.

BONETTI M., Riservatezza e processo penale, Milano, 2003.

BORGOBELLO M., *Il concetto di "corrispondenza" nella sentenza 170 del 2023 della Corte costituzionale*, agosto 2023, in www.giurisprudenzapenale.it.

BRAGHÒ G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in Riv. inf. e informatica, 2005, 217.

CACCAVELLA D. E. – PELLEGRINI S., *CAD, bugie e dibattimento: il documento informatico in una prospettazione penalistica*, in *Ciberspazio e diritto*, vol. 23, n. 72 (3 - 2022), pp. 411-425.

CAMMARATA M. – MACCARONE E., La firma digitale sicura, Milano, 2003, 68.

CARETTI P., *Diritto dell'informazione e della comunicazione: stampa, radiotelevisione, telecomunicazioni, teatro e cinema*, Bologna, 2005, 1-313.

CARETTI P., *I diritti fondamentali*, Torino, 2005, 275 ss.

CARNELUTTI F., *La prova civile*, 1947, ristampa 1992, Milano, n. 35, 140 e 143.

CARNEVALE S., Autodeterminazione informativa e processo penale, in AA.VV., Protezione dei dati personali e accertamento penale, a cura di Negri, Roma, 2007, 3 ss.

COMOGLIO L. M., *Perquisizione illegittima e inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. Pen.,* 1996, p. 1547 ss.

CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007.

CONZ A., *Acquisizione di documenti e dati informatici conservati all'estero*, in Conz-Levita, *Antiterrorismo*, 126.

COSTABILE G., *Scena criminis, documento informatico e formazione della prova penale*, in Riv. Inf e informatica, 2005, pp. 531 e ss.

COSTANZI C., *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie restituzione dell'originale*, in Cass. Pen., 2016., 278

DENTI F., *La tutela della privacy e dell'esclusività del patrimonio informativo alla prova del sequestro dei dati informatic*i, in *Resp. Civ*. e *Prev.*, 2016, fasc. 4, 1304.

DI MAJO M., *Corrispondenza* (dir. priv.), in Enc. dir., XI, Milano, 1962, 741 ss.

DONATI F. ,*Art. 15*, in Bufalco R. – Celotto A. -Olivetti M. (a cura di), *Commentario alla Costituzione*, 1, Torino, 2006, 362 ss.

FIORE, voce *Riservatezza* (diritto alla): IV) Dir. pen., in Enc. giur., XXVII, Roma, 1998, 17

FONTANI C., *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi*, Diritto penale e processo, 2/2022.

FONTANI C., *la svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, Diritto penale e processo 10/2023.

FORTUNA E.- DRAGONE S., *Le prove*, in Aa. Vv., *Manuale pratico del processo penale,* Cedam, Padova, 2007, p. 400.

FOTI A., *Qual è l'esatta portata dell'onere motivazionale afferente le esigenze probatorie del provvedimento cautelare*, in D&G, fasc. 16, 2018, 2.

GIACALONE P., *Il ciclo di vita del documento informatico, gestione e aspetti normativi, Franco Angeli/Informatica*, 2021, pag. 13 e ss.

GRILLO P., *Ultimissime sul sequestro del corpo del reato: come va motivato*?, in D&G, fasc. 17, 2015, 53.

ILLUMINATI G., *Le direttive del d.l.l. n. 4368*, in *Jusonline,* 3/2017, p. 329.

ILLUMINATI-GIULIANI, *Commentario breve al codice di procedura penale*, Cedam

KOSTORIS R. E., *Manuale di procedura penale europea*, Quarta edizione, Giuffrè Francis Lefebvre, p. 476.

LINARDI T., *Il sequestro probatorio e la "copia" dei dati informatici*, in Giurisprudenza italiana, ottobre 2019

LOGLI A., *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in Cass. Pen., 2008, 2956.

LUPARIA L, *Sistema penale e criminalità informatica*, Giuffrè, Milano 2009, p. 1.

LUPARIA L., *La disciplina processuale e le garanzie difensive, in L. Luparia, G. Ziccardi, Investigazione penale e tecnologia informatica*, Milano 2007, 130.

MALINVERNI A., *Teoria del falso documentale*, Milano, 1958; Id., voce Fede pubblica (delitti contro la), a) Diritto penale, in Enc. dir., vol. XVII, Milano, 1968, 69.

MANCHIA C., *Sequestro di computers: un provvedimento superato dalla tecnologia*?, in Cass. Pen., 2005, pag. 1634 e ss.

MARI A., *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati (nota a margine di Cass. Pen., SS.UU., 20 luglio 2017, n. 40963)*, in Cass. pen., fasc. 12, 2017, 4312.

MASUCCI A.*, Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in Riv. dir. civ., 2004, I, 755.

MOLINARI F.M.*, Questioni in tema di perquisizione e sequestro di materiale informatico*, in Cass. Pen., 2012, 708.

MONTI A., *La nuova disciplina del sequestro informatico*, in L. Luparia (a cura di), *Sistema penale e criminalità informatica*, p. 199.

NATALINI A., *Rivista di diritto agroalimentare* 17, p. 386.

NAVONE G., *Instrumentum digitale: teoria e disciplina del documento informatico*, Giuffrè editore, 2012, p. 86 e ss.

NEGRI D., *voce Immunità parlamentare* (dir. proc. pen), in Enc. dir., Agg., II-2, Milano, 2008, 694 e 117.

NOBILI M*, Divieti probatori e sanzioni*, in Giust. Pen., 1991, III, c. 641.

NOVARIO F., *Prove penali informatiche*, edizioni libreria cortina Torino, 2011, p. 36.

PACE A., *Art. 15*, in Comm. Cost. Branca, Bologna-Roma, 1977, 85.

PACE A., *Contenuto e oggetto della libertà di corrispondenza e di comunicazione*, in Scritti in onore di C. Mortati, I, Milano, 1977, 813 ss.

PARODI C., *Il sequestro probatorio dei dispositivi informatici: necessario contemperare esigenze investigative e principio di proporzionalità*, consultabile su ilpenalista.it, 10 dicembre 2020.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet,* a cura di L. Picotti, Padova 2004, 86 e ss.

PISANI M. S., *La tutela penale della "riservatezza": aspetti processuali*, in Riv. it. dir. proc. pen., 1967, p. 785.

PISANI S., *La tutela penale della "riservatezza*", pag. 785 e ss.

RESTA S., *Informatica, telematica e computer crimes*, in Informatica e diritto, VI, 1997, 1, 168-169.

RIVELLO P., *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in Cass. Pen., 2018, fasc. 1.

SALERNO G. M., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. Nania R.- Ridola P.(a cura di), *I diritti costituzionali*, Torino, I, 2001.

SARZANA DI S. IPPOLITO C., Informatica, internet e diritto penale, III Ed., Milano 2010, 61 e ss.

SIGNORATO S., *La localizzazione satellitare nel sistema degli atti investigativi*, Rivista italiana di diritto e procedura penale, Anno LV Fasc. 2-2012.

SIGNORATO S., *Le indagini digitali profili strutturali di una metamorfosi investigativa*, Giappichelli editore Torino, 2018, p. 219.

TESTAGUZZA A., *Il sequestro di dati e sistemi*, in AA.VV., *Cybercrime,* a cura di Cadoppi A. – Canestrieri S. – Manna A., Torino, 2019, 1459

TODARO G., *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*; in Dir. Pen. Cont., 2017, fasc. 11, 157 e ss.

TONINI P., CONTI C., *Manuale di procedura penale*, Milano, 2023, 352 ss.

TONINI P., *Il documento informatico: problematiche civilistiche e penalistiche a confronto*, Il corriere giuridico 3/2012, da pag. 432 a 439.

TORRE M., *WhatsApp e l'acquisizione processuale della messaggistica istantanea*, Diritto penale e processo, 9, 2020, 1281.

UBALDI A., *Sequestro probatorio di documenti e server: vincolo illegittimo se non proporzionato ai bisogni probatori*, in D&G, fasc. 193, 2019, 12.

UBERTIS G., Principi di procedura penale europea, Milano, 2009, 126.

VALASTRO A.*, Libertà di comunicazione e nuove tecnologie*, Milano, 2001, XI-396.

VILLASCHI P., *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"*, consultabile su www.federalismi.it., 7, 2023, 234 ss.

ZAPPULLA A., *Le indagini per la formazione della notitia criminis: il caso della perquisizione seguita da sequestro*, in Cass. Pen. 1996, p. 1878 ss.

Ringraziamenti

È arrivato il momento di ringraziare tutte le persone che mi sono state vicine durante questo percorso lungo e faticoso. Grazie a tutti, mi ritengo molto fortunata ad avervi nella mia vita.

Ringrazio la Professoressa Signorato per la sua estrema disponibilità, pazienza e comprensione. Mi ha seguita con molta attenzione e premura e le sono molto grata.

Grazie alla mia numerosa, rumorosa e meravigliosa famiglia. Grazie perché siete sempre rimasti tutti al mio fianco senza mai smettere di credere in me. Ho pochissime certezze sul mio futuro, ma per fortuna almeno una ce l'ho: il pic nic del 15 di agosto al Lagazzon. Grazie zie e zii per i preziosi consigli, il sostegno e la comprensione.

Grazie Zia Pampa perché sei la mia spalla da quando sono nata, per le urla, per i pianti, per i pomeriggi passati a giocare con le bambole. Grazie perché mi pensi sempre e mi vuoi un bene dell'anima. Sei forte e sai affrontare le situazioni difficili cercando di non far preoccupare chi ti sta intorno perché metti sempre tutti noi al primo posto.

Grazie Zia Chicca, Zio Mauro, Pietro e Anna perché siete il mio porto sicuro in ogni situazione. Casa Padoan è e sarà per sempre il mio punto di riferimento perché siete la mia seconda famiglia.

Grazie ai miei cugini, siete preziosi e crescere con voi è meraviglioso. Grazie per le risate, i giochi e l'amore che mi avete sempre dimostrato.

Grazie nonna Gianna e nonno Luigi per avermi sempre sostenuta e aver fatto il tifo per me da quando sono nata. Anche se non sei qui fisicamente nonno, so che sei e sarai sempre al mio fianco in ogni momento della mia vita.

Grazie Tommaso e Martina per la vostra vicinanza e per il vostro amore. Vi voglio bene e sarò sempre pronta ad ascoltarvi e a sgridarvi al momento opportuno.

Grazie Alice per essere la parte razionale e ragionevole di me. Anche se sei bionda e ingegnera, ti voglio tanto bene lo stesso.

Grazie a tutti i miei amici per non avermi mai lasciata sola e per avermi sempre supportata e incoraggiata.

Grazie alle mie Beppine: Sev, Rid, Petti, Sof ed Emma. Siete il mio porto sicuro e la mia ancora di salvezza. Anche se i tempi del liceo sono purtroppo terminati e non possiamo vederci tutti i giorni, so che posso e potrò sempre contare su di voi perché siete le amiche migliori che potessi desiderare. Grazie Sof perché senza di te non so come avrei affrontato questi anni di studio matto e disperatissimo, mi hai sempre capita e consolata. Grazie Rid, per le tue parole sempre giuste e per essere un esempio di tenacia e forza di volontà. Grazie Petti perché sei il mio dolce pulcino, mi auguro che la tua vita newyorkese termini molto presto perché mi manchi tanto. Grazie Emma perché sai come goderti la vita e trovare il lato positivo di ogni situazione.

Grazie Marghe e Sofia. Siete state le compagne di tesi migliori del mondo, senza di voi e il vostro sostegno starei ancora fissando la prima pagina vuota del primo capitolo.

Grazie ai miei compagni di università, siete diventati una parte importantissima della mia vita e senza di voi non ce l'avrei mai fatta. Grazie Apo, Ale, Brando, Cami, Dario, Bala, Domi, Ema, Laura, Lisa, Gobbo, Matte, Sara, Matteo, Gio, Angela, Anna, Luca, Stefano, Francesco e Michele. Grazie Cami e Laura perché siete state la mia forza e non avete mai dubitato delle mie capacità, grazie per le chiacchierate e le lunghissime pause durante le lezioni. Grazie Sara per la tua dolcezza e pazienza, per le chiamate lunghissime, per le lezioni di skincare e per i gossip. Per fortuna ci sei tu che cerchi di darmi un minimo di equilibrio, anche se sono un caso disperato. Grazie Angela per la tua estrema bontà e per dimostrarmi il tuo affetto ogni giorno attraverso piccoli gesti. Grazie Gio, ti voglio tanto bene anche se sei il mio stress dal primo giorno in cui ci siamo conosciute. Grazie Lisa per la tua allegria, dolcezza e soprattutto per i magnifici grattini. Grazie Matte per il tuo sostegno, perché mi sopporti anche quando ti trascino in giro per negozi. Grazie perché mi capisci e ascolti tutti i miei drammi. Sappi che sarò sempre vicino a te per qualsiasi cosa vorrai. Grazie Ale per la fiducia che hai sempre riposto in me, per le lunghissime videochiamate e per tutte le interrogazioni. Grazie Ste per la tua estrema sincerità, per i caffè da Mario e per il codice di giustizia amministrativa con le glosse pronte all'uso.

Grazie Anna perché sei la sorella maggiore migliore del mondo. Sei la mia spalla da quando sono nata e la mia fonte di sicurezza. Sei sempre presente, in ogni giorno della mia vita, anche se siamo distanti fisicamente e non potrei farne a meno. Grazie per le ore e ore di chiacchiere e per essere la mia psicologa di fiducia. Ti voglio tanto bene.

Grazie Sev per essere la migliore amica che tutti dovrebbero avere. Sei l'altra metà della mia mela, noi non siamo abituate alle smancerie, ma ora te le becchi tutte. Grazie perché mi capisci al volo, anche solo con uno sguardo. Grazie perché sei estremamente sincera e capisci sempre, molto prima di me, quando sto per sbagliare completamente rotta (Nota bene: ti sto dando ragione). Sei la persona

della quale mi fido di più al mondo e l'unica che conosce veramente ogni parte di me. Grazie di essere sempre al mio fianco. Grazie per le serate solo nostre, per le bevute, per le risate, per i viaggi fatti e per tutti quelli che faremo (magari evitando di perderci nello Zen). Non te lo dico molto spesso, ma so che lo sai, ti voglio tanto bene.

Grazie mamma e papà per non avermi mai fatto mancare nulla e per avermi dato la possibilità di studiare senza avere altri pensieri. Questo traguardo è anche vostro e spero siate orgogliosi di me.

Grazie mamma per aver subito ogni mia ansia e preoccupazione, per aver sopportato pianti e urla e per aver finto interesse ascoltandomi ripetere i giorni prima di ogni esame. Grazie per avermi insegnato a trovare sempre il lato positivo in ogni situazione, come ben sai non sono incline a farlo, ma almeno ho un ottimo esempio. Grazie per avermi insegnato ad essere tenace e a lottare per raggiungere i miei obiettivi.

Grazie papà per essere il mio sostenitore numero uno da quando sono nata. Sei la persona con la quale litigo di più al mondo, ma sai perché? Purtroppo (o per fortuna) siamo uguali e quindi continueremo a urlare a cena disturbando i pasti di Rocco. Grazie per aver capito molto prima di me quale sarebbe stata la mia strada e grazie per i tuoi incoraggiamenti, dati con metodi molto discutibili, ma senza i quali non sarei la persona che sono diventata.

Grazie Rocco, ho sempre cercato di proteggerti ed essere il tuo punto di riferimento dal lontano 3 aprile 2003, ma sai qual è la verità? Sei tu la mia più grande forza, compagno di traslochi settimanali e rottura quotidiana di scatole. Grazie per la tua presenza costante nella mia vita, per i tuoi scherzi, per le tue parolacce e prese in giro. Grazie perché senza di te non ce l'avrei mai fatta, grazie per aver sopportato i miei pianti e le mie crisi e per insegnarmi ogni giorno a vivere la vita con più leggerezza e meno ansia. Grazie perché riesci a farmi sentire importante e per desiderare sempre il meglio per me. Sei il fratello migliore del mondo, sarò sempre qui per condividere insieme ogni momento della nostra vita. Ti voglio bene.

Grazie Nonna Mary. In realtà non so bene come ringraziarti perché sei la mia persona preferita nell'universo e nessun grazie basterebbe per compensare tutto ciò che hai sempre fatto e continui a fare per me. Grazie per esserti sempre presa cura di me, per l'amore incondizionato, le attenzioni, il sostegno, le sgridate e le preghiere a Santa Rita. Grazie perché so bene di essere sempre al primo posto nei tuoi pensieri, grazie per aver condiviso notti insonni prima di ogni esame e per avermi sempre protetta. Grazie perché mi fai sentire la tua bambina e perché mi vizi oltre misura, grazie per i pranzi sempre pronti, per i lunghi abbracci e per i grattini fatti sempre con amore anche se controvoglia. Questa tesi l'ho dedicata a te perché, come diciamo sempre, viviamo in simbiosi e quindi voglio che questa laurea sia anche tua. Ti voglio tanto bene, tua Matilde.