ANTONIO VELE

Aspetti critici del documento probatorio "screenshot" e acquisito mediante il captatore informatico

L'articolo tratta di alcuni profili critici relativi alla genuinità dello screenshot e del suo anomalo reperimento mediante il captatore informatico.

Critical aspects of the evidentiary document screenshot. Screenshot using the computer capturer.

The article deals whit some critical profiles relating to the authenticity of the screenshot and its anomalous retrieval through the computer capturer.

1. *Premessa.* Il documento, come fonte di prova, secondo una visione più generale, è ogni cosa atta a rappresentare, mediante segni o tracce di qualsiasi genere, un fatto[1]; altra dottrina, più incentrata sul documento come mezzo di prova nel processo penale, evidenzia la distinzione tra documento e segno, poiché al primo deve riannodarsi l'intenzione di un soggetto di rappresentare qualcosa, al secondo è, invece, estraneo il fenomeno dell'incorporamento di una rappresentazione voluta dall'individuo[2], sebbene anche il documento

[1] CARNELUTTI, *Documento e negozio giuridico*, in *Riv. dir. proc. civ.*, 1926, I, 216 ss., secondo cui il documento potrebbe identificarsi «in ogni supporto materiale idoneo a dar conto nel tempo di un fatto, di un'attività negoziale o non negoziale»; LIEBMAN, *Manuale di diritto processuale civile*, *Principi*, Milano, 1993, II, 322, il quale osserva che il documento in termini giuridici potrebbe correttamente definirsi come una cosa che rappresenta o raffigura un fatto, dotato di giuridica rilevanza, in modo tale da fornire a chi l'osserva e lo analizza una certa conoscenza di quel medesimo fatto; poi, IRTI, *Il concetto giuridico di documento*, in *Riv. trim. dir. proc. civ.*, 1969, 498 ss., secondo cui risultano inutili, giuridicamente e praticamente, tutte quelle disquisizioni tendenti vanamente a dimostrare che il documento in sé non avrebbe alcun valore o funzione, dipendendo invece essi dall'attività percettiva di chi scruta ed interpreta i segni in esso contenuti; in parte DENTI, *La verificazione delle prove documentali*, Torino, 1957, 28; sul punto, CARNELUTTI, *Documento*, *Noviss. Dig. it.*, VI, Torino, 1960, 85 ss., ove si è specificato che è ovvio che in assenza della percezione, e del percipiente, il documento non serve a nulla: ma siccome viviamo in un mondo popolato da esseri umani per natura capaci di distinguere, analizzare e comprendere i segni rappresentativi di fatti, i documenti hanno intrinsecamente valore e funzione di prova; LIEBMAN, *Manuale di diritto processuale civile*, II, cit., 108 ss.; MANDRIOLI, *Diritto processuale civile*, II, Torino, 2009, 207 ss.

[2] KALB, *Il documento nel sistema probatorio*, Torino, 2000, 110; UBERTIS, *Documenti e oralità nel nuovo processo penale*, in AA.VV., *Studi in onore di Vassalli*, II, Milano, 1991, 301 ss. Cfr., MENNA, *La prova documentale, l'acquisizione delle sentenze irrevocabili e le letture dibattimentali*, in Bargi, *Il doppio binario nell'accertamento dei fatti di mafia*, Torino, 2013, 864, il quale aggiunge che il «documento, in quanto prova rappresentativa, sollecita nel giudice un ragionamento di tipo non ricostruttivo, ma solo adesivo o meno al contenuto della rappresentazione sulla base di attendibilità della fonte di

corpo del reato sia espressione di un fatto voluto (lettera che contiene una minaccia). Può trattarsi di uno scritto, di solito contenuto in un foglio di carta o in uno strumento informatico (ad esempio un supporto digitale: file), oppure di supporti che contengono mere immagini o comunicazioni (fotografie, filmati, registrazioni ed altro)[3].

Nel documento bisogna distinguere poi il contenitore e il contenuto: il primo è lo strumento che serve a rappresentare il fatto, ad esempio la carta scritta; il secondo è il fatto rappresentato, ad esempio un'attestazione (un atto) di ricevuta della somma di denaro.

L'art. 234 c.p.p. descrive le caratteristiche dei documenti, onde farli riconoscere come tali, ai fini acquisitivi[4]. La rilevanza probatoria ne è, poi, individuata sulla base del rapporto intercorrente tra il contenuto del documento ed il fatto da provare. Il documento, come risultato probatorio, viene sottoposto all'esame valutativo del giudice (che sul medesimo esercita e forma il suo libero convincimento) non potendo il suo contenuto essere acriticamente assunto ai fini della decisione[5].

---

prova, costituita non solo dal supporto materiale, ma anche dal soggetto da cui proviene – né più o né meno come nel caso della testimonianza – l'intenzione di rappresentare». Il segno, all'inverso, in virtù della distinzione tracciata nel testo induce il giudice in un'opera di ricostruzione indiziaria, «perché [il giudice] non è spinto a leggere in prima battuta nel [...] supporto materiale il messaggio rappresentativo impressovi da un soggetto»; non si esclude, tuttavia, che il ragionamento indiziario possa svilupparsi anche rispetto al documento, ancorché la ricostruzione di un fatto ignoto non è oggetto della funzione primaria della prova documentale. Sulla scorta di tale differenza è agevole verificare la distinzione tra «cose pertinenti al reato e corpi del reato, da un lato, e documenti considerati nella loro valenza di mezzi di rappresentazione, dall'altro lato».

[3] In tema di filmati e registrazioni v. Cass., Sez. I, 2 dicembre 2020, n. 27850; Cass., Sez. V, 19 ottobre 2020, n. 32544; Cass., Sez. V, 6 ottobre 2020, n. 31831, Rv. 279776; Cass., Sez. III, 18 settembre 2020, n. 33038; Cass., Sez. II, 10 luglio 2020, n. 22500, in *Dir. prat. lav.*, 2020, 2538; Cass., Sez. V, 21 febbraio 2020, n. 21027, Rv. 279345; Cass., Sez. V, 19 novembre 2019, n. 7015, *ivi* 278803; Cass., Sez., V, 11 febbraio 2019, n. 13810, *ivi* 275237; Cass., Sez. VI, 20 dicembre 2018, n. 15838, *ivi* 275541; Cass., Sez. V, 11 giugno 2018, n. 41421, *ivi* 275111; Cass., Sez. fer., 8 agosto 2017, n. 47602, in *For. it.*, 2018, 4, 252; Cass., Sez. II, 30 novembre 2016, n. 10, Rv. 268787; Cass., Sez. II, 21 ottobre 2016, n. 3851, *ivi* 269089; Cass., Sez. II, 6 ottobre 2016, n. 50986, *ivi* 268730.

[4] Parte della dottrina evidenzia che la funzione probatoria del documento è nella rappresentazione documentale, vale a dire, nel rapporto di rappresentazione intercorrente tra il documento e il fatto documentato, al fine dell'individuazione del medesimo come eventuale strumento probatorio, NAPPI, sub. *artt. 234-243*, in *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, III, Milano, 2003, 240; cfr. SQUASSONI, sub *art. 234 c.p.p.*, in *Commentario del nuovo codice di procedura penale*, II, Torino, 1990, 646.

[5] CARNELUTTI, *Documento*, in *Nss. dig. it.*, cit., 88; in questo contesto si è evidenziato come, in riferimento al documento, non ricorrano limiti al libero convincimento del giudice, non potendosi configurare una sorta di sistema di regole legali come quelle che nel processo civile riguardano la struttura del documento, la estensione e la intensità della sua efficacia probatoria; SABATINI, *Prova*, in *Nss. D.*, XIV, Torino, 1967, 320, il quale osserva, però, come il documento, caratterizzandosi per la sua idoneità a

2. *Il rapporto tra lo screenshot e la copia forense*. L'evoluzione del sistema informatico ha determinato un significativo sviluppo del documento, come strumento contenente fatti utili alle determinazioni inerenti all'esercizio dell'azione penale, alla contestazione (e ricostruzione) del fatto in ambito cautelare, alla ricostruzione e alla rappresentazione del fatto imputazione (dall'azione penale alla fase dell'impugnazione).

Lo "*screenshot*" è un documento informatico, su cui è opportuno riflettere in particolare sulla gestione informatica dello stesso a garanzia della decisione.

Iniziamo dalla definizione di tale documento: è l'immagine di una schermata o porzione di essa visibile su di un *display* di un dispositivo elettronico (*smartphone*, *tablet*, *pc*, *monitor*, televisione, etc.) acquisita tramite copia e salvata in possibili formati digitali diversi od appositi programmi.

La Corte di cassazione ha ritenuto legittima l'acquisizione di uno *screenshot*, specificando che «non è imposto alcun adempimento specifico per il compimento di tale attività»; tale attività si concretizza «nella realizzazione di una fotografia e che si caratterizza soltanto per il suo oggetto, costituito appunto da uno schermo sul quale sia visibile un testo o un'immagine non essendovi alcuna differenza tra una tale fotografia e quella di qualsiasi altro oggetto»[6].

È necessario, invece, comprendere come lo *screenshot* non sia assimilabile ad una mera fotografia (stampata su carta fotografica), essendo un documento informatico maneggiabile, oltre che manipolabile (per certi versi l'alterazione vale anche per le foto incollate su un file di testo).

Lo *screenshot*, trattandosi di una immagine visibile ed acquisita da un dispositivo elettronico, non immediatamente stampata, potrebbe essere incollata su di una pagina di un programma di videoscrittura o di presentazione.

Talvolta, per farla risultare più leggibile, l'immagine viene modificata nelle

---

consegnare il fatto alla storia, deve necessariamente possedere i requisiti della "autenticità", della "compiutezza" e della "fedeltà"; PERCHINUNNO, voce *Prova documentale*, in *Enc. d.*, XXXVII, Milano, 1988, 725, secondo cui tali riferimenti sono utili per offrire al giudice validi parametri per la formazione della propria convinzione attraverso la logica, razionale e motivata valutazione della prova documentale.

[6] Cass., Sez. V, 5 febbraio 2021, n. 12062, Di Calogero, secondo cui è legittima l'acquisizione come documento di una pagina di un "social network" mediante la realizzazione di una fotografia istantanea dello schermo (*screenshot*) di un dispositivo elettronico sul quale la stessa è visibile; cfr., altresì, Cass., Sez., V, 15 febbraio 2022, n. 8961; Cass., Sez., III, 6 novembre 2019, n. 8332. In dottrina si è evidenziato, invece, che in mancanza del dispositivo-contenitore, la riproduzione fotografica di uno *screenshot* o di un messaggio *whatsApp* non determina la certezza dell'identità del mittente, del destinatario, né del contenuto del messaggio. Di conseguenza, senza il sequestro dell'apparecchio cellulare ed in assenza della copia forense si darebbe ingresso nel processo penale a qualunque riproduzione di fotografie o di messaggi non controllabili, sul punto v. FILIPPI, *Acquisizione di screenshot consegnato alla polizia giudiziaria: è un documento?* in *www.penaledp.it*, 2023.

proporzioni e dimensioni, utilizzando le funzioni base rese disponibili, appunto, da qualsiasi software genericamente identificato, quali quelli di *office automation.*
Vediamo come in questa operazione è stato alterato in termini tecnico informatici quello che si individua come "oggetto dell'acquisizione", non potendosi assegnare al medesimo alcuna corrispondenza alla fonte originale.
Ancora, trattandosi di una immagine o di un documento di testo, nulla esclude che anche il costituente nuovo documento "*screenshot*" sia stato ulteriormente modificato, non solo nelle dimensioni, ma anche in qualche specifico elemento del contenuto stesso.
Su questo terreno, ad esempio, come si può delimitare con certezza la data ed ora in cui è stata acquisita l'immagine, senza incorrere nel dubbio che eventuali riferimenti indicati nella stessa siano stati modificati in un momento successivo?
Le eventuali indicazioni dell'ora che generalmente appaiono nello schermo o nel *monitor* di un dispositivo elettronico sono facilmente alterabili oppure impostate al fine di sostenere un determinato fatto storico.
Si pensi ad uno *screenshot* in cui si riproduce il contenuto di una *chat* o di un *post* pubblicati ove data, ora e contenuti vengono cancellati, rimossi o modificati.
In siffatta situazione lo *screenshot* non presenterebbe connotati di garanzia da un punto di vista probatorio.
Analogamente, se il contenuto dello *screenshot* rappresentasse una sequenza di immagini di un evento più prolungato nel tempo, quale certezza si potrebbe avere nel caso fossero alterate una o più immagini?
Immaginiamo poi di considerare non una chat, ma il contenuto di una pagina di un social; all'interno di questa vi possono essere più periodi, più *chat* e magari anche più immagini collegate direttamente allo scambio testuale tra due utenti.
In questo contesto, l'acquisizione e la modalità di gestione dei dati tramite *screenshot* assume una certa indeterminatezza.
Nello *screenshot*, in cui risulta lo scambio di diversi dialoghi, se viene modificata la dimensione del riquadro di lettura, al fine di rendere gli stessi più leggibili dovrà essere necessario predisporre più pagine per permettere una visione completa dello scambio nella sua totalità.
In mancanza non parliamo ancora di alterazione o modifica del contenuto, ma di una possibile "errata consecutio temporum" dei messaggi; di conseguenza tale evenienza potrebbe già alterare il senso generale dell'intero scam-

bio e significato intrinseco dello stesso.
Una soluzione a questi interrogativi, oltre a quelli qui non riportati, può essere data dall'esecuzione di una copia forense[7]; con siffatta procedura difatti è specificatamente previsto che l'acquisizione sia svolta garantendo l'integrità del reperto originario, affinché non vi siano successive modifiche o contaminazioni.
La copia forense, quindi, è considerata dove praticabile come la forma più affidabile e precisa di generazione di un elemento di prova che per sua natura potrà essere utilizzata anche più volte, senza comprometterne la sua struttura e soprattutto assicurandone la non modificabilità del contenuto originario acquisito.
Per acquisire uno *screenshot*, di solito, si utilizzano combinazioni di tasti specifici o appositi software che consentono di estrapolare l'immagine dello schermo.
Le informazioni contenute negli *screenshot* devono essere autentiche e rappresentare la situazione reale al momento dell'operazione informatica per essere prove autentiche in sede giurisdizionale.
Rispetto agli *screenshot*, la copia forense consiste in una replica esatta di uno specifico dispositivo elettronico – come uno smartphone, un *tablet*, un computer, finanche sistemi complessi di archiviazione composti talvolta anche di più dischi e collegati ad apparati server – che viene creata mediante software forensi per preservare le prove digitali in maniera accurata e verificabile.
Il legislatore ha disciplinato "l'operatività" riconducibile a questa procedura di acquisizione dei dati con la L. 18 marzo 2008, n. 48; tale legge richiede l'adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati originali e la conformità ed immodificabilità delle copie estratte per evitare il rischio di alterazioni.
In sostanza, nel caso in cui si è reperito uno *screenshot* durante le attività d'indagine i soggetti di polizia giudiziaria, nelle situazioni disciplinate dalla l. 48/2008, dovrebbero procedere con la copia forense, in forza delle incertezze relative allo *screenshot*.
La particolarità di questa attività risiede proprio nel fatto che - da un punto di vista operativo - l'operatore utilizza applicazioni software ed apparati hardware specifici, per generare copie esatte e speculari ("immagine" del supporto di archiviazione) delle unità di memorizzazione (talvolta questa modalità di copia viene chiamata "*bit to bit*"), senza alterare in alcun modo né i dati co-

[7] La copia forense consiste in un "duplicato" bit a bit della prova digitale e, pertanto, risulta essere un clone identico.

piati né le informazioni associate a ciascun diverso tipo di file contenuto nei supporti e quindi copiato.
Per raggiungere questo risultato, che verrebbe compromesso anche solo collegando il dispositivo per eseguire la copia, la procedura da seguire è quella di utilizzare dei *tools* chiamati "*writeblocker*" in modalità *hardware* o *software*.
Tutti i dispositivi elettronici, compresi anche i dischi di archiviazione sia di tipo tradizionale sia i più recenti definiti SSD (ossia unità allo stato solido), nel momento in cui l'apparato viene acceso o "lavora" scrivono una serie di informazioni modificando alcuni *file* e/o registri principali di sistema.
Per assicurare che la copia è stata eseguita senza alterare alcun dato ed informazione presenti nel dispositivo è fondamentale procedere con questi sistemi, che ne garantiscano l'originalità e l'inalterabilità.
Anche altre forme di cautela devono essere rispettate, volte a garantire la non alterazione dei dati.
Ad esempio nel caso di uno *smartphone* – che sia oggetto di copia forense – è necessario prima di iniziare il procedimento tecnico al fine di posizionarlo in modalità "Aereo" per scollegarlo da qualsiasi possibile forma di comunicazione voce o dati; comunicazioni instaurate sia mediante la sim telefonica abbinata al contratto con il gestore, sia tramite le connessioni *wifi* o *bluetooth*, con le quali i dispositivi dialogano regolarmente connettendosi o scambiando dati ed informazioni con le "celle radio" od altri dispositivi.
Così procedendo la copia forense, ottenuta mediante l'impiego del *software* ed *hardware* specifici, garantisce in modo certo la corrispondenza del contenuto della copia con l'apparato originale.
Per quanto concerne, il rispetto di canoni tecnici nella conduzione della creazione della copia forense consente alle prove di essere genuine ai fini della valutazione giurisdizionale.
La consultazione degli archivi ottenuti dalla copia forense permette la ricostruzione precisa e puntuale di uno scambio di messaggi, della ricostruzione reale di una *chat*, la consultazione di *file* – siano essi immagini, video, audio o testi – con il presupposto di originalità, finanche quando questi possano essere stati cancellati, ma nel caso recuperati ugualmente.
Il confronto chiaramente tra uno *screenshot* ed una copia forense, nella circostanza di eventuale diversità parziale o totale dei contenuti, attribuisce alla seconda maggiore attendibilità di originalità degli stessi.
In sintesi, l'adozione e l'impiego delle copie forensi come mezzo di prova consente agli interessati di esaminare e analizzare i dati senza comprometterne l'autenticità.

A questo punto, però, è opportuno evidenziare che la disciplina vigente in tema di reperimento e/o gestione del documento informatico andrebbe migliorata sotto l'aspetto delle garanzie processuali, giacché detto strumento probatorio è suscettibile di alterazioni o danneggiamenti.
Si tratta, infatti, di individuare le modalità per acquisire i dati presenti in un supporto informatico; occorre cioè recuperare gli elementi di prova senza alterare il sistema informatico in cui essi si trovano[8].
In questa chiave, più nel dettaglio, la l. 48/2008, di ratifica e di esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, prevede alcune cautele. Il legislatore ha modificato, infatti, alcune norme del III e del IV libro del codice di procedura penale, in ordine a strumenti d'indagine sui sistemi o programmi informatici e telematici (anche se salvaguardati da misure di sicurezza), al fine di assicurare la conservazione dei dati originali, impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova, garantire la conformità della copia all'originale e l'immodificabilità della stessa (quando si procede ad una duplicazione), dotare di sigilli informatici i documenti.
Tale legge, però, non ha regolamentato nello specifico le operazioni (il metodo) di acquisizione di notizie informatiche[9], in ragione dei diversi protocolli operanti in materia e considerando che questi risultano condizionati dal continuo cambiamento tecnologico.
Analizzando le norme modificate con la l. 48/2008 (artt. 244, 247, 254, 254-*bis*, 256, 259, 260, 352, 353, 354 c.p.p.) risulta evidente come le attività di indagine degli elementi informatici rientrino nel novero dei mezzi tipici di ricerca, recependone la disciplina: di qui una serie di problemi interpretativi sul piano della tutela dei diritti fondamentali dell'individuo e della qualità del giudizio (affidabilità della prova). Problemi che derivano dalla difficoltà, come

[8] PAULESU, sub *art. 354 c.p.p.,* in *Codice di procedura penale commentato*, a cura di Giarda-Spangher, 2010, 4267 ss.; sul punto si è osservato come «"le tracce digitali" costituiscono ormai elementi cognitivi di primaria importanza nell'ambito dell'investigazione criminale. Sennonché, si sa che il dato informatico, strutturalmente "immateriale", risulta fatalmente esposto ad un elevato rischio di dispersione ed alterazione. Labilità dell'elemento cognitivo, urgenza della sua captazione, non dispersione dello stesso sono tutti fenomeni suscettibili di incoraggiare prassi investigative disinvolte. Donde l'esigenza di predisporre alcuni protocolli operativi preordinati ad assicurare la genuinità e la conservazione della *digital evidence*».

[9] Cass., Sez. VI, 20 dicembre 2018, n. 15838, secondo cui in ipotesi di perquisizione di sistema informatico o telematico, sia l'art. 247, co. 1-*bis* c.p.p. che l'art. 260, co. 2 c.p.p., si limitano a richiedere l'adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati informatici originali e la conformità ed immodificabilità delle copie estratte per evitare il rischio di alterazioni, senza imporre misure e tecniche tipizzate.

si è detto, di disciplinare per legge le procedure acquisitive dei documenti informatici.

Su questo terreno, occorre concentrare l'attenzione sulle modalità di recupero del documento informatico[10]. Una volta individuato, sul piano investigativo, il supporto digitale, è infatti necessario procedere preliminarmente all'acquisizione della *bit-stream image*[11], anche nel caso di attivazione di accertamenti urgenti e/o ispezioni, sempreché non occorrano diverse ore per effettuare tale operazione, per evitare problematiche sull'alterazione dei dati nella fase di analisi degli stessi[12].

La predetta acquisizione, ove effettuata in precedenza (ad esempio prima del sequestro), deve avvenire in modo tale da assicurare la massima corrispondenza fra l'originale e la "copia"[13].

---

[10] L'attenzione sulle modalità di recupero va rivolta anche all'acquisizione di documenti e dati informatici ai fini investigativi, disponibili al pubblico (esempio mediante la rete internet o altre modalità informatiche) conservati all'estero (art. 234-*bis* c.p.p.), in quanto anche agli stessi va garantita l'integrità dei dati acquisiti, secondo le disposizioni codicistiche introdotte dalla l. 48/2008. Per quanto riguarda le perplessità inerenti al concetto di «legittimo titolare» circa l'acquisizione di elementi informatici non disponibili al pubblico, cfr. ATERNO, sub *art. 234-bis c.p.p.*, *Codice di procedura penale commentato*, a cura di Giarda-Spangher, Milano, 2017, 2368 ss., il quale ritiene che il legislatore abbia voluto estendere il consenso a diversi soggetti titolari di diritti soggettivi, non limitandolo al mero proprietario del dato e al titolare del trattamento del dato personale (d.lgs. n. 196/2003), richiamando, infatti, gli "accordi" tra le società che forniscono servizi *on line* e i clienti per la gestione dei dati informatici, dove all'interno di tali negozi giuridici si potrebbe riscontrare il legittimo titolare. In tema v. Cass., Sez. VI, 20 aprile 2021, n. 18907, Rv. 281819; Cass., Sez. III, 26 settembre 2019, n. 47557, *ivi* 277990; Cass., Sez. III, 5 giugno 2019, n. 14725; Cass., Sez., III, 9 maggio 2019, n. 36681; Cass., Sez. IV, 8 aprile 2016, n. 16770, Rv. 266983; Cass., sez., III, 10 novembre 2015, n. 5818, *ivi* 266267.

[11] ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc.*, 2008, Dossier, *La prova scientifica nel processo penale*, 61; tale creazione viene resa non modificabile mediante determinati meccanismi ed in merito si osserva che «questa fase acquisitiva viene effettuata attraverso la *bit-stream image*, ovvero la realizzazione di una "immagine" *bit* a *bit* del contenuto del supporto posto sotto sequestro che consente di operare l'analisi forense su un *hard disk* praticamente identico all'originale: sia sotto il profilo logico sia sotto quello fisico». Tali cautele sono importanti al fine di evitare che un successivo accesso ad un *file* tramite dispositivo (tipo *personal computer*) possa essere modificato o alterato; gli aspetti problematici dell'analisi digitale si colgono prevalentemente nella fase di ricerca del documento informatico.

[12] Basti pensare che ad oggi i tempi di copia sono di circa 2 giga al minuto, per cui, ad esempio, per un *hard disk* di un *terabyte* saranno necessarie 8 ore circa per effettuare una *bitstream image*; cfr. VACIAGO, *Profili processuali delle indagini informatiche*, in *Diritto dell'internet*, a cura di Cassano-Scorza-Vaciago, Padova, 2013, 648.

[13] VACIAGO, *Profili processuali delle indagini informatiche*, cit., 651; sul punto si è osservato come «è evidente che, nel momento stesso in cui venga rispettata la procedura di acquisizione *bitstream* dell'immagine del disco e sia verificata, attraverso il calcolo dell'algoritmo di *hash*, la perfetta identità della copia, non vi sono ragioni per ritenere irripetibile tale accertamento tecnico». In tale contesto è utile ricordare che secondo un orientamento del giudice di legittimità non possono essere invocate le garanzie previste per gli accertamenti tecnici irripetibili, visto che l'attività di estrazione di copia dei file da un *computer* non determina la irriproducibilità di informazioni identiche a quelle contenute

Nella fase di acquisizione occorre redigere una "relazione tecnica", in modo da consentire alle parti e al giudice di verificare l'ammissibilità, l'utilizzabilità e l'attendibilità della prova[14]. Ecco allora che, in una prospettiva *de iure condendo,* parrebbe necessario introdurre l'obbligo di redigere un verbale, a pena di inutilizzabilità della prova documentale informatica[15]. Tale verbale dovrebbe dar conto di una serie di operazioni: recupero del supporto digitale e analisi del dato digitale, lo stato del dispositivo, l'annotazione del giorno e dell'ora di inizio e di cessazione dell'operazione, nonché i nominativi delle persone che hanno preso parte alle operazioni[16]; e sarebbe utile anche per

---

nell'originale, Cass., Sez. III, 8 luglio 2015, n. 29061; Cass., Sez. III, 24 novembre 2010, Malfanti, in *Mass. uff.,* 248767; Cass., Sez. I, 26 febbraio 2009, Ammutinato, *ivi* 243922; Cass., Sez. I, 25 febbraio 2009, Dell'Aversano, *ivi* 243495, secondo cui non dà luogo ad accertamento tecnico irripetibile la lettura dell'*hard disk* di un computer sequestrato che è attività di polizia giudiziaria volta, anche con urgenza all'assicurazione delle fonti di prova. In dottrina, SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 223 ss., per la quale il discorso è più complesso, in quanto sulla copia forense e sua ripetibilità rileva la distinzione tra «dispositivi spenti o accessi». Nel primo caso se la copia risulta effettuata seguendo le *best practices* l'attività è da qualificare come ripetibile e senza rischi di alterazione dei dati (chiavi USB, schede di memoria *flash*, *hard disk* possono essere ricopiati); nel secondo l'attività di copia con dispositivo acceso è da qualificare come irripetibile, invocando l'applicazione dell'art. 360 c.p.p. e nella situazione di urgenza (art. 354 c.p.p.) sarebbe opportuno per colmare il *deficit* di garanzie una videoripresa dell'attività di copia effettuata.

[14] Cass., Sez. V, 16 gennaio 2018, n. 8736, Rv. 272417; Cass., Sez. V, 16 novembre 2015, n. 11905, *ivi* 266477; Cass., Sez. II, 1 luglio 2015, n. 29061, *ivi* 264572; il giudice di legittimità specifica come l'estrazione di dati archiviati in un supporto informatico non costituisce accertamento tecnico irripetibile anche dopo l'entrata in vigore della l. 48/2008, che ha introdotto unicamente l'obbligo per la polizia giudiziaria di rispettare determinati protocolli di comportamento, senza prevedere alcuna sanzione processuale in caso di mancata loro adozione, potendone derivare, invece, eventualmente, effetti sull'attendibilità della prova rappresentata dall'accertamento eseguito.

[15] Tale riflessione potrebbe far emergere il discorso sull'utilizzabilità della prova, in assenza della predetta regola (obbligo di redigere il verbale). In tema di prove assunte in dispregio di diritti fondamentali v. Corte cost., 7 maggio 2008, n. 149; Corte cost. 24 aprile 2002, n. 135; Corte cost., 19 luglio 2000, n. 304; Corte cost., 18 giugno 1998, n. 229; Corte cost., 9 luglio 1996, n. 238; Corte cost., 11 marzo 1993, n. 81; Corte cost., 6 aprile 1973, n. 34. In argomento cfr. ARICÒ, *Riflessioni in tema di inutilizzabilità delle prove nel nuovo processo penale*, in *Annali dell'istituto giuridico dell'Università di Salerno*, 1993, 28; CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, 1188; CONTI, *Inutilizzabilità*, in *Enc. giur.*, XVII, Roma, 2004, 9; ID. *Accertamento del fatto* e *inutilizzabilità nel processo penale*, cit., 151 ss.; CORDERO, *Tre studi sulle prove penali*, Milano, 1963, 63 e 149; ID., *Procedura penale*, Milano, 2003, 630 ss.; DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Milano, 2008, 75 ss.; GALANTINI, voce *Inutilizzabilità*, in *Enc. dir.*, I, Milano, 1997, 700; LOZZI, *Lezioni di procedura penale*, Torino, 2004, 226; NOBILI, sub *art. 191*, in *Commentario codice di procedura penale*, a cura di Chiavario, II, cit., 409-413; PIERRO, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali*, Napoli, 1992, 172; RICCIO, *Le perquisizioni nel codice di procedura penale*, Napoli, 1974, 181 ss.; ID., *La procedura penale. Tra storia e politica*, Napoli, 2010, 31 ss.; SIRACUSANO, *Le prove*, in Siracusano-Galati-Tranchina-Zappalà, *Diritto processuale penale*, Milano, 2004, 343; volendo, VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011, 3-5; 97 ss.

[16] Il legislatore, peraltro, non può prevedere in maniera tassativa specifiche modalità tecniche, sia perché

verificare in concreto se l'attività in questione possa qualificarsi come attività ripetibile o meno anche alla luce dell'evoluzione tecnologica[17].

Un adempimento di questo tipo sarebbe, di fatto, necessario per garantire un efficace controllo *a posteriori* dell'operato degli inquirenti da parte della difesa e del giudice. In questa prospettiva, ad esempio, la difesa potrebbe affidare ad un proprio consulente tecnico o ad un perito (chiedendone l'ammissione) il compito di verificare se le tecniche di recupero e di analisi informatica abbiano alterato o danneggiato dati; non bisogna dimenticare, appunto, che eventuali alterazioni di dati potrebbero inficiare la fase valutativa del giudice, compromettendone la correttezza[18].

Infine, spostando l'attenzione sullo *screenshot* – non nelle situazioni in cui vi sia la possibilità di procedere da parte dei soggetti di polizia giudiziaria, secondo quanto previsto dalla l. 48/2008 – occorrerebbe ragionare sull'impronta di *hash* dei documenti informatici[19], in modo da certificare la conformità all'originale degli stessi[20].

Viceversa, una consapevolezza della giurisprudenza, non ancora acquisita, sulla gestione informatica dello *screenshot* porterebbe ad un'inattendibilità

---

soggette a variazioni in forza della natura del dato ricercato e dello stato del dispositivo (spento, acceso, operativo *on line*), sia in forza del progresso tecnologico.

[17] SIGNORATO, *Le indagini digitali. Profili Strutturali di una metamorfosi investigativa*, cit., 143 ss., prospetta l'opportunità della videoripresa per l'attività di acquisizione dei dati informatici, in quanto «è sempre immanente il rischio di una loro alterazione involontaria in sede investigativa».

[18] Cfr. GIUNCHEDI, *Le malpractices nella digital forensics. Quali conseguenze sull'inutilizzabilità del dato informatico?* in *Arch. pen.*, III, 2013, 835, in dottrina si è osservato come «la potenziale proficuità dell'indagine, però, non può andare a discapito della genuinità della prova»; vista la consapevolezza di non poter realizzare un contraddittorio nel momento dell'acquisizione della prova digitale, sia per l'urgenza a volte dell'accertamento informatico, sia per evitare pericoli di manipolazione del sistema informatico con inquinamento dei dati ad opera dell'indagato, «l'unica garanzia possibile è un controllo *ex post* fondato sulla verifica della correttezza della metodologia utilizzata, senza alcun onere probatorio in capo alla parte che eccepisce una deviazione dal modello operativo».

[19] L'impronta *hash* viene utilizzata in diverse applicazioni per certificare la conformità all'originale di un documento. Per ogni singolo file, l'impronta hash viene generata applicando uno specifico algoritmo (funzione di hash) che permette di ottenere stringhe di lunghezze diverse a seconda della stringa utilizzata. La sequenza di numeri e lettere viene generata leggendo in sequenza ciascun singolo *byte* del file preso in esame ed eseguendo una serie di passaggi matematici formando delle impronte intermedie legate fra loro, per poi ottenere alla fine l'impronta definitiva. Esistono numerosi algoritmi di *hashing* con proprietà e livelli di complessità differenti: il metodo mediamente più utilizzato è SHA256 che genera una stringa lunga 64 caratteri. L'impronta hash viene apposta a garanzia dell'integrità di un file al suo originale e per certificare la conformità di un documento. Tramite l'impronta hash un file informatico avrà una sola impronta per tutto il suo contenuto: se viene modificato anche solo un carattere o spazio del contenuto l'impronta hash sarà diversa. L'impronta hash non è invertibile, ovvero da un'impronta hash non è possibile ricavare il contenuto del file iniziale.

[20] In merito alla funzione di hash cfr. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e dir.*, 2010, 500.

dello stesso, pur rientrando nella prova documentale *ex* art. 234 c.p.p.
Siffatta visione risulta valida, in particolare, ove gli elementi probatori relativi allo *screenshot* non possano o non vengano riconosciuti in sede processuale: ad esempio testimonianza sull'autenticità e genuinità dello *screenshot*. I fatti processuali, difatti, possono essere provati attraverso diversi strumenti probatori.
Anche la procedura di riconoscimento del documento è utile per verificarne la provenienza (art. 239 c.p.p.), nel senso che attraverso essa possa riannodarsi il documento rappresentativo al soggetto esaminato, ai fini della veridicità e genuinità dello stesso. La sottoposizione del documento per il riconoscimento alle parti private o ai testimoni, come facoltà e non obbligo del giudice, ha una portata, però, più ampia[21].
Il termine «provenienza», si è osservato, comprende non solo quello dell'accertamento sulla paternità in senso stretto ma ha il pregio di stabilire l'identità del documento acquisito[22].
Il documento deve possedere, dunque, i requisiti di idoneità o autenticità, ma la stessa non deve emergere necessariamente dal medesimo.

3. *Lo screenshot mediante captatore informatico.* È evidente come nell'ambito della disciplina delle intercettazioni[23] si assiste ad un conflitto tra

[21] In argomento, VELE, *La prova documentale nel processo penale*, Bari, 2022, 47.
[22] CALAMANDREI, *La prova documentale*, Padova, 1995, 39-40, secondo cui lo strumento del riconoscimento ha l'obiettivo non solo di individuare l'autore, ma anche quello di stabilire l'identità del documento presentato rispetto a quello prodotto, o anche solo posseduto o veduto.
[23] Sul tema, in generale, v. CAMON, *Le intercettazioni nel processo penale,* Milano, 1996; FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997; CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. e proc. pen.,* 1991, 143 ss.; RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001; sia consentito rinviare anche a VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011. Sulla riforma "Orlando", fra i molti, cfr. BENE, *La riforma parziale (e il gorilla invisibile)*, in *L'intercettazione di comunicazioni*, a cura di Bene, Bari 2018, p. 15 ss.; CAMON, *Forme, destinazione e regime della documentazione*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra-Orlandi, Torino, 2018, 63 ss.; CAPRIOLI, *La nuova procedura di selezione delle comunicazioni rilevanti*, in *L'intercettazione di comunicazioni*, cit., 125 ss.; CONTI, *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa*, in *Giur. it.,* 2018, 1754 ss.; GIOSTRA, *Il segreto estende i suoi confini e la sua durata*, in *Nuove norme in tema di* intercettazioni, cit., 2018, 131-132; DINACCI, *Intercettazioni, e riservatezza tra ampliamenti di disciplina, inconcludenze operative e restrizioni difensive*, in *Le nuove intercettazioni*, a cura di Mazza, Torino, 2018, 27 ss.; GIULIANI, *Intercettazioni, tutela della riservatezza e procedimento* de libertate, in *Nuove norme in tema di intercettazioni*, cit., 31 ss.; VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione,* in *Le nuove intercettazioni*, cit., 139 ss.; volendo, VELE, *Riforma delle intercettazioni, riservatezza, e selezione*

valori costituzionalmente protetti – autorità e libertà – dovendo, perciò, il legislatore, con adeguata tecnica normativa, bilanciare mediante corrette regole processuali la tutela dell'interesse pubblico sotteso alla giurisdizione penale e l'interesse soggettivo ad una compressione di diritti fondamentali soltanto in presenza di situazioni determinate e tassative.
Uno strumento di intercettazione che viene impiegato come mezzo di ricerca della prova è il captatore informatico (*trojan horse*).
Nella sostanza si tratta di un "*malware*", definito come un software invasivo, che si nasconde all'interno di un'applicazione o di un file apparentemente legittimo al fine di ingannare l'utente e consentire l'accesso non autorizzato al sistema o di svolgere azioni dannose.
Nella quasi totalità dei casi questo software non viene tecnicamente identificato e riconosciuto come una potenziale minaccia dai sistemi antivirus o di protezione installati sui singoli dispositivi.
Questo software è in grado di impossessarsi di informazioni estremamente riservate contenute in qualunque apparato di comunicazione elettronico.
Difatti, una volta inserito il malware nel dispositivo target, quest'ultimo è in grado di captare conversazioni tra presenti – intercettando a distanza tramite il microfono del dispositivo – quanto di copiare la rubrica dei contatti, la galleria di foto o video, le password memorizzate, così come potenzialmente qualsiasi altro documento presente a prescindere dal suo formato od estensione.
In sostanza è in grado di acquisire il controllo effettivo del dispositivo elettronico e delle sue periferiche.
Questo "agente" subdolo, proprio perché si insidia all'interno di un dispositivo ed in esso opera acquisendo molteplici informazioni[24], è disciplinato dagli artt. 266 ss. codice di procedura penale[25], ancorché la disciplina andrebbe

dei dati, in *Proc. pen. e giust.,* 2019, 1526 ss.

[24] Sulla potenzialità investigative del virus e sua funzione cfr. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, 12 ss. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova, 2021.

[25] L'uso del captatore informatico è previsto dall'art. 266, co. 2 c.p.p., secondo cui l'intercettazione tra presenti «può essere eseguita anche mediante inserimento di captatore informatico su dispositivo elettronico portatile». Il comma 2-*bis* del medesimo articolo prevede però che tale modo di intercettazione è sempre consentito nei procedimenti per i delitti di cui all' art. 51, co. 3-*bis* e co. 3-*quater* c.p.p. : per tali delitti non è necessario che sussista il fondato motivo che in loco si stia svolgendo l'attività criminosa, mentre tale requisito risulta necessario per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore nel massimo a cinque anni di reclusione. Secondo l' art. 267, co. 1 c.p.p., il decreto che autorizza l'uso del captatore informatico espone con autonoma valutazione le ragioni che rendono necessaria in concreto tale modalità per lo svolgimento delle indagini e se si procede per delitti diversi da quelli di cui all' art. 51, co. 3-*bis* e co. 3- *quater* c.p.p., i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono. Nei casi

perfezionata.
Epperò, stando al tema *screenshot* non mancano dubbi sull'utilizzabilità dello stesso, allorquando un file contenente un comportamento non comunicativo in senso stretto sia fotografato sul dispositivo elettronico in virtù del *malware* inoculato.
Tanto è vero che la Corte di cassazione ha evidenziato come tale «attività investigativa non ha riguardato l'estrapolazione dal supporto digitale di documenti informatici preesistenti all'attività intercettiva, bensì esclusivamente la captazione di flussi di dati in fieri, cristallizzati nel momento stesso della loro formazione».
Per il giudice di legittimità «tale attività di mera "constatazione" dei dati informatici in corso di realizzazione, pur non costituendo una "comunicazione" in senso stretto, costituisce certamente, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione - previo provvedimento autorizzativo dell'autorità giudiziaria - nonché la videoregistrazione, dunque anche la fotografia, nel caso di specie mediante screenshot della schermata»[26].
Inoltre, la Suprema corte, nella rappresentata situazione, specifica che non è stata effettuata alcuna perquisizione e perciò sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266-*bis* c.p.p., effettuate mediante l'installazione di un captatore informatico (c.d. "*trojan horse*") all'interno di un computer collocato in un luogo di privata dimora.
Siffatta interpretazione genera dubbi, anche alla luce del recente chiarimento sviluppato dal giudice delle leggi[27], poiché per intercettazione si intende la cap-

---

d'urgenza l' art. 267, co. 2-*bis* c.p.p. prevede che il pubblico ministero possa disporre l'intercettazione mediante captatore informatico nelle situazioni previste dal comma 2 del medesimo soltanto nei procedimenti per i delitti di cui all' art. 51, co. 3-*bis* e co. 3-*quater* c.p.p.

[26] Cfr., Cass., Sez. I, 7 ottobre 2021, n. 3591, secondo cui non è stata ravvisata alcuna perquisizione, essendo mancata qualsiasi ricerca e successiva estrapolazione di materiale preesistente dal supporto informatico e non rileva che in tale prospetto in fieri figurino dati preesistenti alla sua formazione, ciò risultando necessitato dalla natura del medesimo, riportante poste di contabilità, ex se riepilogative di operazioni economiche già effettuate ovvero in corso di realizzazione, delle quali si aggiorna annotazione e memoria. Sicché, come già affermato dalla suprema Corte, sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266-*bis* c.p.p., effettuate mediante l'installazione di un captatore informatico (c.d. "*trojan horse*") all'interno di un computer collocato in un luogo di privata dimora" (Cass., Sez. 5, n. 48370, 30 maggio 2017, Occhionero, Rv. 271412).

[27] Cfr., Corte cost., 22 giugno 2023, n. 170, secondo cui debbono ricorrere due condizioni affinché si abbia intercettazione: la prima, di ordine temporale, è che «la comunicazione deve essere in corso nel momento della sua captazione da parte dell'*extraneus*»; la comunicazione va colta quindi «nel suo momento "dinamico", con conseguente estraneità al concetto dell'acquisizione del supporto fisico che reca memoria di una comunicazione già avvenuta (dunque, nel suo momento "statico"). La seconda condizione attiene alle modalità di esecuzione: l'apprensione del messaggio comunicativo da parte del terzo

tazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti e, poi, perché l'oggetto dell'intercettazione di comunicazioni informatiche o telematiche previsto dall'art. 266-*bis* c.p.p. è il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi[28].

Di conseguenza, non si può prescindere dall'elemento della partecipazione di una pluralità di soggetti, peculiarità propria della "comunicazione" in senso stretto.

La Corte di cassazione, invece, con tale indirizzo, amplia il concetto di comportamento comunicativo ai fini dell'art. 266-*bis* c.p.p., ricomprendendovi tutti i flussi di dati (bit) a prescindere dal loro contenuto e dallo scambio reale di comunicazione o conversazione tra due o più soggetti; in sostanza, si tiene in considerazione il solo limite della captazione contestuale, al di là della percezione dei flussi informatici percepiti, potenziando le attività investigative in contrasto con le garanzie a tutela dei diritti fondamentali.

Peraltro, in questa chiave, non può sottacersi che lo *screenshot* fuoriesce dall'attività tipica di intercettazione, anche se effettuata durante l'operatività del *trojan horse*.

Si è sostenuto come questo mezzo di ricerca della prova non è stato percepito dalla politica legislativa con razionalità e con consapevolezza della sua particolare natura tecnologica e delle relative potenzialità investigative[29].

Su questo terreno, lo strumento del captatore informatico[30], di fatto, consente

---

deve avvenire in modo occulto, ossia all'insaputa dei soggetti tra i quali la comunicazione intercorre». Sul punto, vedi, altresì, Cass., Sez. un., 28 maggio 2003, n. 36747.

[28] Cass. Sez. V, 14 ottobre 2009 n. 16556, secondo cui «per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro [...] non potendo ritenersi sufficiente l'elaborazione del pensiero e l'esternazione, anziché mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato», trovandosi invece dinanzi non a «un "flusso di comunicazioni", richiedente un dialogo con altri soggetti,» ma ad «"un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer». In argomento cfr., Cass., Sez. un., 23 febbraio 2000, n. 6, D'Amuri.

[29] A tal proposito cfr., VELE, *Ambito d'applicazione dello strumento intercettazioni. Uso dei risultati in altri procedimenti*, in *www.lalegislazionepenale.eu*, 2020.

[30] Sulla recente riforma in tema di captatore informatico si rinvia al commento di DANIELE, *L'illusione di domare il captatore informatico*, in *www.lalegislazionepenale.eu*, 2020.

Più in generale, sull'argomento cfr. Cass., Sez. un., 28 novembre 2016, n. 26889, in *www.giurisprudenzapenale.com*; BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.,* 2016, 2274 ss.; BARROCU, *Il captatore informatico: un virus per tutte le stagioni*, in *Dir. pen. e proc.,* 2017, 379 ss.; CAMON, *Cavalli di troia in Cassazione*, in *Arch. n. proc. pen.,* 2017, 76 ss.; CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *www.archiviopenale.it*, 2016,

contemporaneamente di visionare e/o reperire contenuti *on line,* in controtendenza ad attività di ricerca c.d. a sorpresa, le quali si caratterizzano per l'essere manifeste, con applicazione delle dovute garanzie; consente naturalmente l'intercettazione, presso qualunque luogo e domicilio, con problematiche a monte di individuazione dei citati ambiti e a valle di limitazione dell'operatività negli stessi, cioè di gestione esecutiva della captazione tra presenti qualora l'ambito delimitato risultasse diverso da quello predeterminato[31]. Il captatore informatico risulta, quindi, particolarmente invasivo e compressivo dei diritti fondamentali; caratteristiche, queste, che non sono bilanciate a sufficienza dalla prudenziale inutilizzabilità dei dati acquisiti nel corso delle operazioni preliminari all'inserimento dello strumento sul dispositivo elettronico portatile, nonché dei dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo (art. 271, co. 1-*bis* c.p.p.); anche in questo caso, infatti, sarebbe stata apprezzabile una disposizione più chiara nello stabilire l'inutilizzabilità di tutti gli elementi acquisiti mediante il captatore, tranne soltanto le comunicazioni o conversazioni tra presenti[32].

331 ss.; CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Dir. dell'inform. e dell'inf.,* II, 2016, 88 ss.; FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico),* in *www.archiviopenale.it*, 2016, 348 ss.; FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. e giust.,* 2016, 21 ss.; GAITO-FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *www.archiviopenale.it*, 2016, 309 ss.; LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, 7 ottobre 2016; PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *www.archiviopenale.it*, 2016, 354 ss.; SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 237 ss.

[31] Cfr., VELE, *Ambito d'applicazione dello strumento intercettazioni. Uso dei risultati in altri procedimenti*, cit.

[32] In questi termini, VELE, *Ambito d'applicazione dello strumento intercettazioni. Uso dei risultati in altri procedimenti*, cit.