GIURISPRUDENZA PENALE

"Liberi tutti" nell'utilizzo del trojan di Stato?

di ***Valentino Fracasso***

Sommario. **1.** La vicenda processuale, la tesi del Tribunale del Riesame, la tesi difensiva e le argomentazioni della Corte di Cassazione. – **2.** La potenziale portata della sentenza: "*liberi tutti*" nell'uso delle funzionalità del trojan diverse dall'attivazione del microfono e della videocamera? – **3.** La captazione da remoto di dati informatici statici: una tipologia di indagine non riconducibile ad alcun mezzo di ricerca della prova attualmente disciplinato dal Codice di Procedura Penale. – **3.1** Lo *screenshot* non è una perquisizione. – **3.2** Lo *screenshot* non è una acquisizione di un documento informatico ex art. 234 c.p.p. – **3.3** Lo *screenshot* non integra un'attività di accertamento o rilievo ex art. 354 c.p.p. – **3.4** Lo *screenshot* non è una intercettazione telematica. Il *vulnus* della sentenza in commento: la tesi secondo cui un *file* "aperto" sarebbe espressivo di un comportamento comunicativo. – **4.** L'ulteriore conferma dell'assenza di una disciplina legale della c.d. *on line search* anche mediante *screenshot*: i lavori parlamentari sui contenuti tecnici del c.d. *trojan* di Stato in vista dell'adozione della c.d. "riforma Orlando" e la c.d. Legge "Spazzacorrotti". – **5.** La verifica della possibile sussumibilità dell'esito dell'*on line search* nella c.d. prova atipica, alla luce dei principi di diritto sanciti dalla sentenza *Prisco* emessa dalle Sezioni Unite nel 2006. – **5.1** L'applicazione all'*on line search* dei principi della sentenza *Prisco*: la violazione diretta dell'art. 14 della Costituzione. – **5.2** L'ulteriore violazione dei principi della sentenza *Prisco*: la presenza di una norma penale che vieta (anche le) condotte coincidenti con l'*on line search*. – **6.** L'inutilizzabilità costituzionale dei documenti captati mediante *on line search*.

1. La vicenda processuale, la tesi del Tribunale del Riesame, la tesi difensiva e le argomentazioni della Corte di Cassazione.

La pronuncia si colloca nell'ambito di una vicenda cautelare personale concernente un'ipotesi di associazione per delinquere finalizzata alla commissione di frodi in materia di IVA e accise, con successivo riciclaggio o auto-riciclaggio (contestato al ricorrente) dei proventi. Il materiale d'indagine risultava in larga parte costituito da intercettazioni telefoniche e telematiche. Tra i vari motivi di ricorso prospettati dalla difesa avverso l'ordinanza del Tribunale del Riesame che aveva confermato l'applicazione della misura cautelare, vi era l'illegittimità del provvedimento per inosservanza di norma processuale stabilità a pena di inutilizzabilità. Tale censura era stata mossa

con riferimento all'attività di estrazione mediante *software trojan* (o captatore informatico) di un *file Excel*, da un dispositivo in uso all'indagato, contenente un prospetto contabile nel quale sarebbero state ricapitolate le operazioni illecite.
Tale *file* sarebbe stato captato dal *trojan* mediante c.d. *screenshot*, scattato proprio mentre il documento informatico era aperto ed in corso di redazione da parte dell'ignaro indagato.
Il Tribunale del Riesame ha qualificato lo *screenshot* come una vera e propria intercettazione telematica, precedentemente autorizzata dal GIP, sul presupposto che i flussi di dati *in fieri* e cristallizzati (mediante *screenshot*) nel momento stesso della loro creazione – lunga perifrasi per indicare il *file Excel* su cui l'indagato stava lavorando al momento dell'intercettazione – pur non costituendo una comunicazione in senso stretto integrerebbero un c.d. comportamento comunicativo che, in quanto tale, può formare oggetto di intercettazione telematica previa autorizzazione del Giudice (esistente nel caso deciso).
La tesi dei Giudici del Riesame è stata censurata dal ricorrente sostenendo che l'attività svolta (i.e. lo *screenshot*) altro non sarebbe che il frutto di una perquisizione informatica *de facto*, tuttavia, svolta in palese violazione della specifica disciplina prevista dall'art. 247 c.p.p. e proprio per tale ragione il "risultato" dell'attività intercettativa non potrebbe essere "salvato e recuperato" ricorrendo all'istituto della prova atipica previsto dall'art. 189 c.p.p.
L'illegittimità della perquisizione informatica *de facto* deriverebbe in sostanza dal contenuto dell'art. 14 della Costituzione, la cui violazione nel caso di specie implica, secondo la difesa, l'inutilizzabilità ai fini di prova dello *screenshot*.
La Corte di Cassazione ha "convalidato" il ragionamento proposto dal Tribunale del Riesame ed ha così rigettato la censura mossa dalla difesa.
La Corte ha quindi confermato la tesi secondo cui un *file* in corso di redazione da parte dell'ignaro utente-indagato-intercettato debba esser assimilato ad un comportamento comunicativo e come tale sia intercettabile (previa autorizzazione del Giudice di fase) e in concreto "immortalabile", come avvenuto nel caso analizzato, tramite *screenshot*.
In sostanza l'attività svolta nel caso di specie mediante il *trojan* (i.e. lo *screenshot* del *file Excel*) rientrerebbe nell'alveo delle intercettazioni telematiche, di cui all'art. 266 bis c.p.p.
Da ultimo, i Giudici di legittimità hanno osservato anche che la particolare modalità di captazione rilevante nel caso deciso – *screenshot* eseguito tramite *trojan* – non ha nulla a che vedere con la ricerca ed estrapolazione di un *file* preesistente nel dispositivo informatico "infettato". Siamo dunque al cospetto, così si afferma, di un'attività di ricerca della prova totalmente diversa dalla perquisizione informatica evocata dalla difesa dell'indagato.

2. La potenziale portata della sentenza: "*liberi tutti*" nell'uso delle funzionalità del trojan diverse dall'attivazione del microfono e della videocamera?

Il passaggio della sentenza – peraltro molto breve e sintetico – poc'anzi ricordato, parrebbe aprire, forse in maniera un po'inconsapevole, ad un'interpretazione che legittimerebbe tutte le attività di *online surveillance*[1] o quanto meno quella oggetto della sentenza (lo *screenshot*), sul presupposto che tali attività sarebbero riconducibili al modello legale delle intercettazioni telematiche già disciplinate dal Legislatore: tesi affascinante, specie per gli Uffici Requirenti, ma oggettivamente non percorribile.

Per giungere a tale conclusione è necessario comprendere *i)* quale sia, ove esistente, il regime legale di tale attività di ricerca della prova, *ii)* in subordine ed in assenza di una specifica disciplina, se sia qualificabile come un mezzo di ricerca della prova atipico da cui scaturiscono prove atipiche che, come tali, per divenire processualmente ammissibili, debbono rispettare i principi di diritto sanciti dalla nota sentenza resa dalle Sezioni Unite nel 2006, imputato *Prisco*, *iii)* ove non ricorrano i requisiti di legittimità sanciti dalla predetta pronuncia, stabilire da quale vizio processuale siano afflitti i materiali probatori acquisiti con tali modalità.

3. La captazione da remoto di dati informatici statici: una tipologia di indagine non riconducibile ad alcun mezzo di ricerca della prova attualmente disciplinato dal Codice di Procedura Penale.

La particolare modalità di captazione del *file Excel* oggetto della pronuncia della Corte di Cassazione, rientra nella più ampia categoria delle cosiddette perquisizioni *on line*, definizione elaborata dalla dottrina[2] per individuare un insieme di operazioni volte ad esplorare e monitorare un sistema informatico mediante infiltrazione segreta all'interno dello stesso, che consente di acquisire dati salvati nel *computer*/dispositivo bersaglio (e quindi già esistenti) e/o di captare in tempo reale flussi di dati o dati in corso di formazione.

Più precisamente, attraverso l'installazione, in locale o da remoto, - e soprattutto all'insaputa dell'utente - di uno specifico *software* (il *virus trojan*) sul *computer*/dispositivo oggetto di osservazione, è infatti possibile,

---

[1] *La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli screenshot tramite captatore informatico*, di G. Frova in Sistema Penale

[2] Si segnalano *La perquisizione on line tra esigenze investigative e ricerca atipica della prova*, di L. Battinieri, in *Sicurezza e Giustizia,* numero IV, 2013, pagg. 44 e ss.; *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, di S. Colaiocco, in *Archivio Penale*, n. 1 – 2014, pag. 1 e ss.; *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, di F. Iovene, pubblicato in data 22 luglio 2014 su www.penalecontemporaneo.it

cumulativamente od alternativamente, ed ogni qual volta l'utente si colleghi ad *internet*,

- "perquisire" l'*hard disk*/il dispositivo o l'*account* cui lo stesso è associato e ottenere copia dei dati in esso contenuti, estrarre copia del contenuto di *file* aperti e di quel che viene digitato sulla tastiera (c.d. *screenshot*): queste attività sono ricondotte alla categoria della c.d. *on line search* o *one time search* che potremmo tradurre, con una perifrasi, captazione da remoto di dati informatici statici;
- rilevare e registrare i siti *internet* che vengono visitati, intercettare comunicazioni VoIp (es. Skype), intercettare *e-mail* e *chat*, attività che integrano la cosiddetta captazione da remoto di flussi informatici;
- attivare le periferiche audio e/o video eventualmente presenti sul *device* bersaglio, per sorvegliare il luogo in cui lo stesso si trova, così da eseguire un'intercettazione ambientale. Tale specifica funzionalità del *trojan* era stata ampiamente analizzata dalla Corte di Cassazione nelle sentenze rese dalla Sezione Sesta (n. 27100 del 26 maggio 2015) e dalle Sezioni Unite (n. 26889/2016, imputato *Scurato*). E giova anticipare (meglio *infra*) che i principi espressi dalla sentenza *Scurato* hanno tracciato il solco in cui si è inserita dapprima la c.d. "Riforma Orlando" e poi la successiva Legge c.d. "Spazzacorrotti", che hanno regolamento l'utilizzo dei *software trojan,* seppur limitatamente ad alcune tipologie di reato ed alla specifica modalità operativa consistente nell'attivazione delle periferiche audio-video del dispositivo intercettato.

È bene ricordare l'ovvio: un programma informatico – quale è il *trojan* – è concepito per eseguire le operazioni per cui è stato programmato (i.e. intercettare scambi di *mail*, eseguire gli *screenshot* dei *file* aperti, copiare i *file* presenti sull'*hard disk* o nel *cloud*, attivare il microfono e/o la telecamera ecc.) e starà poi a chi materialmente controlla l'operatività del *software* decidere se e quando dar corso, contestualmente o meno, ad una o più di queste specifiche modalità operative.

Il punto – sorvolato dalla sentenza in commento – è che ognuna di queste possibili (e cumulabili) funzionalità del *trojan*, impone di verificarne la riconducibilità ad un preciso modello legale previsto dal Legislatore italiano. In questa sede ci si focalizzerà sulla modalità oggetto della sentenza in commento ovvero lo *screenshot*.

3.1 Lo *screenshot* non è una perquisizione.

Come detto l'*on line search* cui lo *screenshot* è riconducibile, viene associata in dottrina alle cosiddette perquisizioni *on line*, "etichetta" quanto mai fuorviante se rapportata a tale tipo di attività investigativa.

L'*on line search*, infatti, non ha nulla a che vedere con l'istituto della perquisizione disciplinata dagli artt. 247 e ss. c.p.p.: le perquisizioni sono indirizzate alla ricerca del corpo del reato e delle cose pertinenti al reato che,

in caso di ritrovamento, devono essere necessariamente sequestrate. Inoltre, si tratta di un'attività sì a sorpresa, ma garantita, che prevede la notifica dell'atto, il diritto a nominare un difensore di fiducia/diritto ad un difensore d'ufficio, il diritto a farsi assistere nel corso dell'atto.
Mentre la captazione da remoto di dati informatici statici (ad esempio anche mediante *screenshot*), prescinde dalla ricerca del corpo del reato o di cose pertinenti al reato, non sfocia necessariamente nel sequestro e, soprattutto, si tratta di un'attività che deve rimanere ignota all'indagato. Peraltro, anche le novità introdotte dalla L. n. 48 del 2008 in tema di perquisizioni informatiche o telematiche, non fanno venir meno le caratteristiche tipiche delle perquisizioni poc'anzi ricordate.
Giusto per fugare ogni dubbio, le captazioni di dati informatici da remoto nulla hanno a che vedere con le ispezioni - anche telematiche ed informatiche introdotte dalla L. n. 48 del 2008 - attività quest'ultima finalizzata a "fotografare" una situazione di fatto suscettibile di modifica, poiché attraverso i *software* di *on line search* non si vuole svolgere quell'attività descrittiva, quindi statica, che caratterizza le ispezioni, bensì si procede ad una raccolta di dati ed informazioni di pertinenza dell'indagato all'insaputa di quest'ultimo.

3.2 Lo *screenshot* non è una acquisizione di un documento informatico ex art. 234 c.p.p.

Parimenti l'*on line search* non può essere ricondotta all'acquisizione di documenti, obiettivo in astratto raggiungibile "forzando" il richiamo a "*qualsiasi altro mezzo*" contenuto nell'art. 234 c.p.p., richiamo che sicuramente ricomprende i documenti informatici.
Infatti, bisogna ricordare che i dati informatici non sono documenti, tanto è vero che vengono acquisiti attraverso le modalità dell'accertamento tecnico irripetibile.
E bisogna altresì rammentare che l'acquisizione documentale in ogni caso concerne documenti già esistenti, mentre nel caso dell'*on line search* è possibile captare non solo i *file* già esistenti, ma anche quelli che verranno costituiti o che sono in corso di formazione, stante il protrarsi nel tempo di tale attività di indagine.

3.3. Lo *screenshot* non integra un'attività di accertamento o rilievo ex art. 354 c.p.p.

Analogamente non può essere invocato l'art. 354 comma 2 c.p.p., come invece risulta aver fatto il Giudice d'appello nell'ambito di una nota vicenda giudiziaria poi definita dalla Corte di Cassazione mediante sentenza che ha accertato l'incompetenza per territorio (Cassazione – Sezione Prima Penale, n. 25368/2021).

La ricerca della prova mediante *screenshot* non ha nulla a che spartire con l'attività di messa in sicurezza informatica dei dati contenuti nel *computer* dell'indagato-intercettato prevista dall'art. 354 c.p.p., operazione che materialmente potrebbe essere eseguita – sempre che ne ricorrano i presupposti processuali - effettuando la copia forense dei dati contenuti nel dispositivo.
Quindi nel caso oggetto della sentenza qui commentata, si è andati ben al di là dei meri "*accertamenti e rilievi*" (anche di natura informatica) disciplinati dall'art. 354 c.p.p.
"Accertamenti e rilievi" che in ogni caso andrebbero eseguiti con modalità *forensic,* ma ciò non è evidentemente avvenuto nel caso analizzato ove, pacificamente, non sono state seguite le metodologie di estrazione e copia dei *file* maggiormente utilizzate nella prassi (ossia la copiatura dell'*hard disk* del *computer* o di un *server*[3] o di singoli *file*), e men che meno si è dato corso alla realizzazione della *bitstream image*[4] e alle operazioni di *hashing*[5], uniche modalità che garantiscono con certezza la genuinità dei dati estratti.
E si tratta di modalità dirimenti, posto che il Legislatore ordinario avendo presente l'estrema fragilità del dato informatico, non a caso ha previsto una serie di garanzie e sanzioni processuali, introdotte dalla Legge n. 48/2008[6],

[3] Operazione normalmente eseguita attraverso il *software* Encase, il comando *dd* nei sistemi operativi UNIX, i sistemi *hardware Logicube Forenisc* o *Talon* con cui è possibile di fatto clonare, senza alterarlo, l'*hard disk* di un *computer* o di un *server* e, con gli ultimi due, è altresì possibile "marchiare" con due distinti algoritmi i *file* contenuti sul supporto originale e quelli copiati; se i due algoritmi applicati a tali dati generano una stringa di *bit* identica, allora si ha la certezza tecnica dell'identità di contenuto tra originale e copia.

[4] Attraverso tale procedimento, si realizza una "copia-immagine" del supporto originale, ossia una replica esatta e identica, *bit* per *bit*, che riproduce anche le informazioni precedentemente cancellate e non sovrascritte contenute all'interno dello spazio non allocato di un *file system* (dati che non verrebbero copiati in maniera identica nel corso di un semplice processo di duplicazione dei *files*). La copia *bit stream* è unanimemente ritenuta uno strumento fondamentale e imprescindibile, per le procedure di acquisizione e l'analisi di dati informatici (vedi *Cyberspazio e diritto*, 2007, pagg. 329 e ss.).

[5] L'operazione di *hashing* consiste nel generare una sorta di marchio digitale che contraddistingue univocamente il dato informatico e ne garantisce l'integrità; consiste nell'applicazione di una formula matematica (algoritmo del tipo "funzione di *hash*") al supporto digitale e alla copia: i valori dei due calcoli coincidono solo se vi è assoluta rispondenza tra l'originale e la copia.

[6] Ci si riferisce, segnatamente, *(i)* al dovere di conservare inalterato il dato informatico originale nella sua genuinità: garanzia oggi assicurata per le ispezioni dall'art. 244 comma 2 c.p.p., per le perquisizioni dall'art. 247 comma 1bis c.p.p. ove tali mezzi siano stati disposti dall'Autorità Giudiziaria, nelle perquisizioni e nei sopralluoghi su iniziativa e di Polizia Giudiziaria, si vedano gli artt. 352 comma 1bis c.p.p. e 354

in relazione ai mezzi di ricerca del documento informatico e che di fatto rimandano alle *best practice* della c.d. *forensic*[7].
In definitiva anche l'art. 354 c.p.p. non legittima e/o disciplina lo strumento investigativo dello *screenshot*.

3.4 Lo *screenshot* non è una intercettazione telematica. Il *vulnus* della sentenza in commento: la tesi secondo cui un *file* "aperto" sarebbe espressivo di un comportamento comunicativo.
L'attività di indagine svolta mediante *software* che consentono la captazione da remoto di dati informatici statici – lo *screenshot* del *file* Excel nel caso oggetto della sentenza in commento - non può essere ricondotta nemmeno (e soprattutto) al modello delle intercettazioni telematiche di cui all'art. 266 bis c.p.p.
E invece questa è proprio la posizione, decisamente ardita a parere di chi scrive, proposta dalla sentenza qui analizzata che qualifica un *file* di testo su cui si sta lavorando – dunque non allegato ad una *mail* o condiviso in una *chat* o su un *social network* – alla stregua di un comportamento comunicativo e, proprio in quanto tale, intercettabile anche attraverso la modalità *screenshot*, conclusione che sarebbe coerente con quella giurisprudenza di legittimità che consente l'intercettazione dei comportamenti comunicativi anche in ambito domiciliare.
Così non è: basta "mettere in fila" le definizioni elaborate dalla stessa Corte di Cassazione *(i)* di intercettazione, *(ii)* di intercettazione telematica e soprattutto *(iii)* dell'oggetto di qualunque tipo di attività intercettativa, per cogliere la notevole (per usar un eufemismo) forzatura operata dalla sentenza.
L'unica definizione di intercettazione ad oggi presente nell'Ordinamento è quella elaborata dalle Sezioni Unite nel 2003 con la Sentenza *Torcasio*, ove per intercettazione si intende la "*captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti*" (Cass. Sez. Un., 25.5.2003, n. 36747, *Torcasio*).
Il solco tracciato dalla sentenza *Torcasio* è stato portato avanti anche nel campo delle intercettazioni telematiche o informatiche disciplinate dall'art.

comma 2 c.p.p.; *(ii)* nonché al dovere di impedire l'alterazione dell'originale: garanzia prevista negli artt. 244 comma 2, 247 comma 1bis, 352 comma 1bis, 354 comma 2 c.p.p.; *(iii)* a quello di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale: artt. 354 comma 2 e 254 bis c.p.p.; *(iv)* al dovere di assicurare la non modificabilità dei dati acquisiti: art. 254 bis c.p.p.; *(v)* ed infine, alla facoltà di apporre sigilli informatici sulle cose, *rectius* sui dati sequestrati: art. 260 c.p.p.
[7] In tal senso si veda *Documento informatico e giusto processo*, di P. Tonini, in *Diritto penale e processo*, n. 4/2009, pagg. 401 e ss.

266 *bis* c.p.p., a mente del quale l'intercettazione telematica altro non è che la captazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.
In merito all'oggetto delle intercettazioni telematiche (i.e. *cosa si intercetta?*) la giurisprudenza di legittimità si è da tempo espressa in prima battuta con la pronuncia a Sezioni Unite con la sentenza *D'Amuri* (Cass. Sez. Un., 23.2.2000 n. 6), poi ribadita dalla sentenza *Virruso* (Cass. Sez. 5, 14.10.2009 n. 16556).
La sentenza *Virruso*, in particolare, ha chiarito che "*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 altrimenti al cospetto "***non*** **[di]** ***un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma*** **[…] [di]** ***"un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer***".
Se l'oggetto dell'intercettazione di cui all'art 266 *bis* c.p.p. è da individuarsi nel flusso di dati relativo a sistemi informatici o telematici, tuttavia – e la Corte di Cassazione è chiara sul punto - questo deve essere di tipo comunicativo, come peraltro espressamente affermato dalla stessa norma.
Ecco allora che diviene dirimente cogliere in maniera chiara quando si sia al cospetto di una comunicazione oppure, viceversa, di un comportamento non comunicativo; poco importa se posti in essere in un ambiente reale o informatico-telematico.
La Corte di Cassazione, partendo dall'insegnamento della Corte Costituzionale (Corte Cost., 2.05.2002 n. 135), definisce "*comportamenti comunicativi*" quegli "***atti finalizzati a trasmettere il contenuto di un pensiero*** *con la parola, i gesti, le espressioni fisiognomiche o altri atteggiamenti idonei a manifestarlo, mentre sono comportamenti "non comunicativi"* […] *tutti quelli, diversi dai primi, che rappresentano la mera presenza di cose o persone ed i loro movimenti, senza alcun nesso funzionale con l'attività di scambio o trasmissione di messaggi* ***tra più soggetti***" (Cass. Sez. III, 21 .11.2019 n. 15206). Definizione analoga e speculare si rinviene anche per il "mondo digitale": sul punto basti ricordare la posizione espressa dalla Corte di Cassazione nella sentenza *Virruso* poc'anzi citata.
Di conseguenza è – o dovrebbe essere – evidente la non riconducibilità alle intercettazioni telematiche delle attività di captazione da remoto di **dati informatici statici che non formano oggetto di un flusso comunicativo diretto/promanante a/da terzi**.
Se queste sono le coordinate esegetiche, la tesi perorata nella sentenza in commento risulta decisamente "fuori rotta".

In definitiva, lo *screenshot* e/o l'*on line search* svolte mediante *trojan*, allo stato, non rientrano in alcuna delle attività di ricerca della prova sin qui ricordate ma, come si dirà a breve, l'inesistenza di una disciplina legale di tali penetranti tecniche investigative è stata certificata – a scanso di equivoci – dal Legislatore stesso in occasione delle recenti riforme in materia di intercettazioni.

4. L'ulteriore conferma dell'assenza di una disciplina legale della c.d. *on line search* anche mediante *screenshot*: i lavori parlamentari sui contenuti tecnici del c.d. *trojan* di Stato in vista dell'adozione della c.d. "riforma Orlando" e la c.d. Legge "Spazzacorrotti".

L'inequivocabile conferma dell'assenza di una disciplina legale dell'*on line search* in tutte le sue possibili forme ivi compreso lo *screenshot*, è stata offerta proprio dal Legislatore in occasione dell'*iter* che ha portato alla promulgazione del D.Lgs. n. 216/2017 (c.d. riforma Orlando) e poi dalla L. n. 3/2019 (c.d. Spazzacorrotti).

Il D.Lgs. n. 216/2017 pur prevedendo per la prima volta la possibilità di utilizzare un captatore informatico (o *trojan horse*) come mezzo di ricerca della prova, limita tale possibilità alle sole comunicazioni telefoniche/telematiche e alle conversazioni tra presenti da effettuarsi nel contesto di indagini relative ad alcune tipologie di reato.

Il presupposto dell'utilizzo di tale strumento, e dunque l'oggetto dell'attività di intercettazione mediante *trojan*, rimane, in ultima analisi, l'esistenza di una forma di comunicazione telefonica/telematica/tra presenti.

E i lavori parlamentari della c.d. Riforma Orlando – relazione illustrativa e relazione tecnica – non lasciano dubbi in merito all'intenzione del Legislatore[8] e soprattutto esplicitamente confermano che l'*on line search* – ivi compresa la modalità *screenshot* - non forma oggetto dell'allora introducenda disciplina del *trojan*[9].

---

[8] http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0472_F002.pdf&leg=XVII#pagemode=none , si vedano in particolare le pagg. 9 e 10 della relazione illustrativa del decreto legislativo.

[9] *"16. L'utilizzo del cosiddetto "trojan", - o, appunto, captatore informatico -, pur ampiamente praticato nella realtà investigativa, non è stato in precedenza oggetto di alcuna regolamentazione a livello normativo. La legge di delega stabilisce in proposito, alla lettera e), di "disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili", secondo i seguenti criteri:*

[...] Come si ricava dal chiaro tenore della delega e dai sopramenzionati criteri per la sua attuazione) ***il delegante ha inteso regolamentare uno solo degli usi del captatore informatico, quale modalità specifica di esecuzione delle intercettazioni tra presenti.*** *Ed ha ad oggetto esclusivamente i dispositivi mobili portatili. '* ***Lo strumento, infatti, consistendo in un malware*** *«occultamente*

La L. n. 3/2019 (c.d. "Spazzacorrotti") nulla ha aggiunto o modificato su questo profilo, posto che si è limitata ad estendere l'uso del captatore informatico ai reati contro la Pubblica Amministrazione ove siano puniti con pena non inferiore nel massimo a cinque anni di reclusione.
In definitiva oggi l'*on line search* in tutte le sue possibili forme operative è priva di qualsivoglia disciplina legale[10], non-scelta che distingue (in peggio) l'Italia da quanto fatto a livello Legislativo e a livello giurisprudenziale nella maggior parte dei Paesi occidentali[11]; assenza di disciplina che, a scanso di equivoci, è stata certificata dalla comunicazione inviata il 18 luglio 2019 dal Garante per la protezione dei dati personali al Presidente del Consiglio, al Ministro della Giustizia ed ai Presidenti del Senato e della Camera[12].
Preso atto del vuoto legislativo non rimane che verificare, si passi il termine, "l'ultima spiaggia", ovvero se l'ammissibilità di tale mezzo di ricerca della prova e l'utilizzabilità a fini probatori dei dati carpiti mediante *screenshot*, rispettino i principi di diritto statuiti dalle Sezioni Unite nella nota senza *Prisco* in materia di mezzi atipici di ricerca della prova e di prove atipiche.

---

installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva» ***consente operazioni ulteriori e diverse*** *quali: la captazione del traffico dati (sia in entrata che in uscita); l'attivazione della telecamera installata ab origine sul dispositivo; la "perquisizione" degli hard disk; la possibilità di estrarre copia integrale del loro contenuto; la intercettazione di tutto quanto digitato sulla tastiera; la possibilità di fotografare le immagini ed i documenti visualizzati; oltre che consentire la geo-localizzazione del dispositivo.* ***Si tratta dunque di un complesso di operazioni (alcune delle quali già praticate ove consentite dalla legislazione vigente*** [altre, evidentemente, non sono previste dalla legislazione vigente]***) che la tecnologia consente dì effettuare, ma che il delegante non ha inteso regolare, limitando l'ambito dell'intervento normativa alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile (smartphone, tablet ecc.) e non anche di dispositivi fissi****."*

[10] A ciò si aggiunga che tale tecnica di ricerca della prova non pare essere contemplata e consentita nemmeno dalla vasta platea di norme che prevedono le c.d. indagini preventive previste dal Legislatore per prevenire la commissione di reati gravissimi (si pensi alle disposizioni di cui agli artt. 226 comma 1 disp. att. c.p.p., 226 D.Lgs. n. 271/1989, nonché alle previsioni contenute nella L. n. 38/2006, e nel D.L. n. 7/2015 in materia di terrorismo e infine va rammentato l'art. 9 della L. n. 146/2006).

[11] Sul punto si segnala *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, di F. Iovene, pubblicato in data 22 luglio 2014 su www.penalecontemporaneo.it, in particolare le pagg. 2-7. Ed estesamente sull'elaborazione della giurisprudenza costituzionale tedesca si veda *Dalla data retention alle indagini ad alto contenuto tecnologico* di R. Flor e S. Marcolini, ed. Giappichelli, 2022, pagg. 127 – 132.

[12] Cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9107773

5. La verifica della possibile sussumibilità dell'esito dell'*on line search* nella c.d. prova atipica, alla luce dei principi di diritto sanciti dalla sentenza *Prisco* emessa dalle Sezioni Unite nel 2006.

La sentenza delle Sezioni Unite *Prisco* (n. 26795 del 2006) contiene, la ricostruzione della disciplina delle video riprese nei luoghi di privata dimora, attività di ricerca della prova che, allora come oggi, era ed è priva di una disciplina normativa e la cui legittimità e spendibilità processuale devono essere vagliate alla luce della corretta interpretazione dell'art. 189 c.p.p. che prevede la c.d. prova atipica.

Ai nostri fini, la sentenza rileva poiché impone di verificare se l'attività di indagine, per quanto atipica, e quindi non regolamentata da alcuna norma, non sia anche vietata da altra norma dell'Ordinamento e *in primis* dalla Costituzione[13].

Detto altrimenti, l'art. 189 c.p.p. – che disciplina la c.d. prova atipica - non conferisce *ex se* una patente di ammissibilità di ogni attività atipica di ricerca della prova posta in essere dalla Polizia Giudiziaria, ma legittima solo quelle attività che *(i)* non determinino una violazione diretta di un diritto oggetto di tutela da parte della nostra Costituzione e *(ii)* parimenti, non siano da qualificarsi come illecite alla stregua di altre norme previste dal nostro Ordinamento.

[13] La sentenza, dopo aver ripercorso il lungo dibattito dottrinale e giurisprudenziale sulle cosiddette prove incostituzionali con riferimento alla corretta interpretazione dell'art. 189 c.p.p., ha stabilito che non possono considerarsi ammissibili come prove atipiche le prove acquisite in violazione dell'art. 14 Cost.

La Corte, infatti, ha chiarito che:

- «*prima dell'ammissione, le prove atipiche non sono prove, perciò* ***se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le sorreggono*** *ci si deve interrogare innanzitutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità*»;
- «***i mezzi di ricerca della prova acquisiti in violazione dell'art. 14 Cost. devono considerarsi inammissibili****. Infatti,* ***l'art. 189 c.p.p.****, in coerenza con l'art. 190 c.p.p. che impone al Giudice di escludere le prove vietate dalla Legge,* ***presuppone logicamente la formazione lecita della prova e solo in questo caso la rende ammissibile****. Il presupposto è implicito, dato che per il Legislatore non poteva che essere lecita un'attività probatoria non disciplinata dalla Legge…..è anche vero che* ***non può considerarsi <<non disciplinata dalla Legge>> la prova basata su un'attività che la legge vieta come nel caso delle riprese visive di comportamenti non comunicativi avvenuti in ambito domiciliare***».

5.1 L'applicazione all'*on line search* dei principi della sentenza *Prisco*: la violazione diretta dell'art. 14 della Costituzione.

Applicando al caso dell'*on line search* - eseguita, anche ma non solo, mediante *screenshot* - il metodo e i criteri espressi dalle Sezioni Unite Prisco del 2006, emerge che questa tecnica investigativa lede a più livelli la sfera privata di ogni individuo e fa emergere la certa violazione di fonti di rango costituzionale e internazionale, ovvero *(i)* l'inviolabilità del domicilio tutelata dall' art. 14 Cost., *(ii)* la tutela della riservatezza assicurata dagli artt. 2 Cost., 8 CEDU, 7 Carta dei Diritti Fondamentali dell'Unione Europea – CDFUE, *(iii)* la tutela dei dati personali ai sensi degli artt. 8 CDFUE e 16 Trattato Fondativo dell'Unione Europea – TFUE.

Per non dilatare troppo il campo, vale la pena focalizzarsi sul rapporto tra *on line search* e il diritto all'inviolabilità del domicilio sancito dall'art. 14 Cost., così come interpretato dalla Corte Costituzionale, dalla giurisprudenza nazionale alla luce delle norme della CEDU e in coerenza con le decisioni adottate dalla Corte di Strasburgo[14].

Il punto di partenza di questa verifica è da individuarsi nella corretta definizione del concetto di domicilio che né la Costituzione, né il Codice di Procedura Penale forniscono e che invece si rinviene nell'art. 614 c.p.

Quest'ultima norma è stata oggetto di una giurisprudenza evolutiva della Corte Costituzionale (si pensi a Cort. Cost. n. 88/1987 che ha ricondotto l'abitacolo di un'autovettura alla sfera di tutela del domicilio) volta ad espanderne la portata e conseguentemente le tutele previste per il domicilio a livello costituzionale.

Ha contribuito a questa interpretazione evolutiva anche la Corte di Strasburgo che, da un lato, ha interpretato l'art. 8 CEDU come garanzia non solo dell'inviolabilità degli spazi fisici definibili come domicilio, ma altresì come diritto a non subire interferenze nel godimento dello stesso (Corte eur. Grande Camera, 19 febbraio 1998, Guerra ed altri contro Italia); dall'altro ha esteso il concetto di domicilio sino a ricomprendervi le sedi sociali, le filiali e gli altri locali di pertinenza di una società (Corte eur. 16 luglio 2002, Società Colas Est ed altre c. Francia).

Alla luce della giurisprudenza costituzionale e pattizia, nonché degli spunti offerti dalla dottrina, sono tre le caratteristiche che consentono di qualificare un luogo fisico come domicilio e che debbono essere contestualmente esistenti: *(i)* lo *ius includendi se* ovvero il diritto ad entrare, permanere ed

[14] In dottrina è stato proposto di qualificare l'*on line search* ed altre tecniche di indagine di natura informatica come potenzialmente lesive del diritto alla *privacy* tutelabile ai sensi dell'art. 2 Cost. o dell'artt. 7 e 8 Cedu, si veda S. Signorato, *Le indagini penali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, pagg. 73 e ss; G. Caneschi, *Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico*, DPC, n. 2/2019, pag. 420.

uscire da un determinato luogo, *(ii)* lo *ius admittendi ac excludendi alios*, *(iii)* il luogo sia deputato ad essere *abitativo* o, secondo la giurisprudenza CEDU, destinato a svolgere la propria attività lavorativa.
Ciò detto, gli spazi virtuali che si delineano all'interno di un dispositivo informatico o in rete (su *internet* o nel *Cloud*) sono pacificamente dei "luoghi" suscettibili di tutela legale, ivi compresa quella penale.
Diversamente ragionando non si spiegherebbe l'introduzione dell'art. 615 ter c.p. nel Codice Penale, fattispecie di reato volutamente costruita sulla falsariga della violazione del domicilio "fisico" e volta a tutelare il "domicilio informatico", così infatti si legge nella relazione al disegno di legge della (in allora futura) L. n. 547/1993 che ha introdotto tale ipotesi di reato nell'Ordinamento. Tale impostazione è stata poi ribadita dalla dottrina[15] e dalla giurisprudenza di legittimità[16] formatasi negli anni successivi all'entrata in vigore della norma che ha identificato nel "domicilio informatico" il bene giuridico protetto dall'art. 615 ter c.p.[17]
Ricordato che il "domicilio informatico" è suscettibile di tutela penale, bisogna domandarsi se anche questo "luogo" possieda quelle caratteristiche, sopra ricordate, idonee a far "scattare" le tutele dell'art. 14 Cost. e la risposta è certamente positiva posto che il domicilio informatico,

(i) implica uno *ius includendi se* ovvero il diritto di accedere, rimanere legittimamente ed uscire in/da un determinato sistema informatico o

---

[15] *Sull'accesso abusivo al sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, R. Flor, in Dir. Pen. proc., 2005, pag. 81 e ss.
[16] Cass. Sez. IV Pen. n. 3607/1999; Cass. S.U. n. 4694/2012; Cass. S.U. n. 17325/2015; Cass. S.U. n. 41210/2017.
[17] Giova ricordare che la dottrina ha proposto "configurazioni" più ricche ed articolate del bene giuridico protetto dell'art. 615ter c.p. che, pur includendolo, vanno ben oltre il concetto di "domicilio informatico", si veda in particolare *Dalla data retention alle indagini ad alto contenuto tecnologico* di R. Flor e S. Marcolini, ed. Giappichelli, 2022, pagg. 147 – 162. Sintetizzando, auspicabilmente bene, lo stimolante pensiero degli Autori, si può dire che il bene giuridico protetto dall'art. 615ter c.p. sia la *cybersecurity* nei suoi tre elementi costitutivi ovvero *Confidentiality*, *Integrity* e *Availability* (c.d. CIA-Triad). *Cybersecurity* cui l'Ordinamento riconosce una tutela muti-livello assicurata da una pluralità di fattispecie penali ivi compreso l'art. 615ter c.p. cui gli Autori attribuiscono una funzione portante all'interno dell'arsenale delle norme penali poste a tutela del predetto bene giuridico.
In estrema sintesi, tutelare la *cybersecurity* significa proteggere *(i)* la componente infrastrutturale della stessa (i.e. *device, hardware*, *software* e reti), *(ii)* la componente informazionale che riguarda la persona/l'ente e non necessariamente di carattere personale, *(iii)* la componente personale in senso stretto che riguarda la c.d. *data protection* ossia la tutela dei dati personali. Quest'ultima è oggi presidiata dalle disposizioni penali contenute nel GDPR, mentre le prime due componenti della *cybersecurity* di cui *supra (i)* e *(ii)* sono sostanzialmente "coperte" dagli artt. 615ter, 615quater, 615quiquies, 617quater, 617quiquies e 617sexies c.p.

luogo virtuale (es. profilo *Facebook*, archivio *Cloud*, *casella mail*, *chat* ecc.);

(ii) parimenti contempla uno *ius includendi ac exludendi alios*: si pensi alle impostazioni di *privacy* di un *account* di un *social network* o alla possibilità di bloccare/sbloccare utenti sgraditi/graditi di un sistema di messaggistica o più semplicemente ai sistemi di protezione tramite *password* del proprio *device* o *account*;

(iii) ospita attività tipiche della vita domestica o di uno spazio di lavoro[18]: basta pensare all'uso che ciascuno di noi fa dello *smartphone*, decine se non centinaia di volte al giorno, per avere certezza del fatto che il telefono contiene molte più informazioni, anche riservatissime, della propria vita personale e lavorativa di quante ne contenga l'immobile in cui si vive o una cassaforte posta all'interno di quest'ultimo.

Chiarito che i dispostivi informatici e gli "spazi" telematici "ospitano" certamente uno o più domicili informatici - su ogni *smartphone* o dispositivo informatico ognuno di noi quasi sempre ha almeno un *account mail*, probabilmente più *account* dei vari *social media* ecc. - e che questi ultimi sono da considerarsi domicili anche ai fini della applicazione dell'art. 14 Cost., alla luce dei principi dettati dalla sentenza *Prisco* bisogna domandarsi se un mezzo atipico di ricerca della prova in astratto capace di comprimere l'inviolabilità del domicilio, fisico o informatico, sia da qualificarsi come direttamente lesivo dell'art. 14 Cost.

Per rispondere alla domanda è necessaria una breve esegesi della norma costituzionale che, come noto, estende al domicilio le tutele della libertà personale ovvero la riserva di Legge e di giurisdizione.

Il primo profilo da chiarire è se le indagini informatiche sfuggano o meno alle tutele previste dall'art. 14 Cost., posto che la Costituzione assicura al domicilio le garanzie previste per la libertà personale indicando solo il caso delle ispezioni, perquisizioni e sequestri quali possibili forme di compressione di tale libertà. Detto altrimenti: quello contenuto nella norma costituzionale è un elenco tassativo o esemplificativo?

Domanda dirimente soprattutto ove si ricordi che buona parte delle indagini informatiche, ivi compresa l'*on line search*, si svolgono mediante atti atipici o comunque al di fuori degli schemi delle perquisizioni, delle ispezioni e dei sequestri.

La Corte Costituzionale ha risposto alla domanda ben prima che le indagini digitali prendessero piede, rimodellando in due direzioni il sistema di tutela previsto dall'art. 14 Cost. ovvero *(i)* ampliando il perimetro delle nozioni di ispezione, perquisizione e sequestro, *(ii)* qualificando il catalogo contenuto nell'art. 14 Cost. come non tassativo sul presupposto che il Costituente non

[18] *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, di S. Colaiocco, in *Archivio Penale*, n. 1 – 2014, pagg. 8-11.

poteva prendere in considerazione tecniche investigative a suo tempo inesistenti (Cort. Cost. n. 135/2002).
Dunque, ciò che rileva non è l'inclusione o meno del *nomen* dell'attività di indagine nell'elenco dell'art. 14 Cost., bensì l'idoneità della stessa a violare il domicilio, sia esso fisico o informatico.
Superata l'obiezione del presunto "numero chiuso" dei mezzi di indagine rilevanti ai fini dell'applicazione delle garanzie dell'art. 14 Cost., ciò che rileva è che tale attività sia effettuata "*nei soli casi e modi previsti dalla Legge*".
L'*on line search* è certamente lesiva del domicilio informatico tutelato a livello costituzionale, è priva di qualsivoglia base legale, come peraltro confermato anche dalla dottrina[19], e non si può quindi pensare di estendere *tamquam non esset* e per analogia le norme dettate dal Legislatore per altre tipologie di attività di indagine a questa metodologia investigativa.
La sostanziale violazione diretta dell'art. 14 Cost. in uno con l'assenza di una disciplina legale, preclude, alla luce dei principi di diritto fissati nella sentenza *Prisco*, la possibilità di qualificare *l'on line search* come un mezzo atipico di ricerca della prova idoneo a generare prove atipiche ma utilizzabili processualmente.

5.2 L'ulteriore violazione dei principi della sentenza *Prisco*: la presenza di una norma penale che vieta (anche le) condotte coincidenti con l'*on line search*.

L'esistenza dell'art. 615 ter c.p. costituisce, sempre a mente della sentenza *Prisco*, un ulteriore fattore ostativo alla spendibilità processuale dei risultati dell'attività di *on line search*.
Come poc'anzi ricordato, la fattispecie di cui all'art. 615 ter c.p. individua come oggetto di tutela uno spazio definibile come "domicilio informatico", spazio che acquista una propria autonomia e separazione dall'esterno grazie all'esercizio dello *ius excludendi* che, normalmente, si concretizza anche nell'uso di *password* o di altri sistemi di protezione (es. il *firewall*). La Corte di Cassazione ha altresì chiarito che il sistema informatico costituisce uno dei luoghi di espressione della personalità dell'individuo, all'interno del quale l'interessato conserva i dati personali la cui diffusione ed utilizzo possono essere solo da lui decisi (cfr. Cass. Sez. V, 18 dicembre 2012, Valenza).
Identificato il bene giuridico e l'oggetto della tutela penale, giova ricordare che tale fattispecie sanziona *(i)* l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza, da intendersi come accesso alla conoscenza dei dati o informazioni contenuti nel sistema, effettuato da remoto (la condotta dell'*hacker*) o "da vicino", *(ii)* la

[19] *Dalla data retention alle indagini ad alto contenuto tecnologico* di R. Flor e S. Marcolini, ed. Giappichelli, 2022, pag. 138; *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* S. Signorato, ed. Giappichelli, 2018, pagg. 293 – 294.

permanenza nel sistema contro la volontà o all'insaputa di chi può esercitare il diritto di esclusione.
La norma, in definitiva, punisce condotte che coincidono perfettamente anche con l'attività investigativa di *on line search* che, quindi, oltre ad esser lesiva dell'art. 14 Cost. ed esser priva di base legale, è addirittura vietata dall'Ordinamento e sanzionata penalmente, con ciò integrando l'altro requisito alternativamente previsto dalla sentenza *Prisco* ai fini dell'ammissibilità di una prova atipica e "a monte" di un'attività atipica di ricerca della prova.
La presenza del delitto di cui all'art. 615 ter c.p. rappresenta, come già osservato da attenta dottrina, «*un ostacolo insormontabile* ***per considerare ammissibile l'utilizzo dei programmi spia al fine di captare il contenuto di un dispositivo informatico****, in quanto non si è in presenza di un'area «non disciplinata dalla Legge» - ciò che solo permetterebbe l'applicazione dell'art. 189 c.p.* ***– ma di condotte considerate dall'ordinamento stesso e dal codice penale non solo vietate, ma anche sanzionate penalmente»***[20].
Se, come la giurisprudenza ha più volte affermato, la semplice illiceità dell'attività di ricerca della prova non vale a renderne inutilizzabile il risultato, nel caso in esame il problema investe ulteriori e più delicati profili, in quanto l'attività - priva di base legale - di *on line search* viola non una "semplice" norma di Legge ordinaria, bensì incide su una libertà costituzionalmente protetta,[21] a tacer del fatto che da un punto di vista oggettivo integra la fattispecie di cui all'art. 615 ter c.p.
In uno scenario del genere è l'intera equità del procedimento penale – intesa in relazione ai principi di cui all'art. 6 CEDU – che appare compromessa, trattandosi di prove acquisite in violazione di diritti fondamentali garantiti dalla Convenzione Europea dei Diritti dell'Uomo (cfr. Khan v. the United Kingdom, § 34; P.G. and J.H. v. the United Kingdom, § 76; Allan v. the United Kingdom, § 42), e segnatamente del diritto al rispetto della vita privata di cui all'art. 8 CEDU. E ciò alla luce di tutte le descritte circostanze del caso concreto e, in particolare, alla luce del rispetto dei diritti di difesa del ricorrente e dell'importanza processuale della prova in oggetto (Gäfgen v. Germany [GC], § 165).
Da ultimo rimane da capire quale sia la sorte processuale dei *file* e/o dei documenti informatici non oggetto di trasmissione o condivisione, carpiti mediante *on line search* e nello specifico attraverso lo *screenshot*.

[20] *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, di S. Colaiocco, in *Archivio Penale*, n. 1 – 2014, pagg. 11 e 12.
[21] *Sorveglianza e perquisizione on line su materiale informatico* di M. Trogu, in *Le indagini atipiche* a cura di A. Scalfati, Giappichelli, 2014, pag. 433.

6. L'inutilizzabilità costituzionale dei documenti captati mediante *on line search*.

Dall'attività di ricerca della prova sin qui analizzata – priva di disciplina legale, direttamente lesiva dell'art. 14 Cost. e, da un punto di vista oggettivo, idonea ad integrare il delitto di cui all'art. 615 ter c.p. - non possono che discendere delle prove (*rectius* fonti di prova) non ammissibili e in ogni caso inutilizzabili a fini probatori.

La conclusione è il frutto della diretta e lineare applicazione dei principi scolpiti dalla Corte Costituzionale che, in maniera costante, ha dichiarato l'inutilizzabilità dei risultati probatori di un'attività di ricerca della prova direttamente lesiva di un diritto costituzionalmente garantito quale è, nel nostro caso, l'inviolabilità del domicilio fisico ed informatico, così dando vita alla categoria della c.d. inutilizzabilità costituzionale.

Si tratta di un istituto che trova la propria origine nella sentenza della Corte Costituzionale n. 34 del 1973 in materia di intercettazioni telefoniche, pronuncia in cui la Corte aveva avvertito "*il dovere di mettere nella dovuta evidenza il principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino, non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito*".

Principio ribadito, successivamente, nella sentenza n. 120/1975 in cui la Corte aveva chiarito che "*nessun effetto probatorio*" può derivare da intercettazioni effettuate fuori dai casi consentiti dalla Legge o in difformità delle relative prescrizioni, le quali debbono "*ritenersi come inesistenti*" con la conseguenza che "*nessun effetto può derivare da intercettazioni siffatte" le quali dunque "sono assolutamente inidonee a produrre alcun effetto*" anche indiretto.

E ancora la Corte Costituzionale ha poi confermato che "*non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo e del cittadino*" (Cort. Cost. n. 81/1993).

Venendo ad un tema "prossimo" a quello analizzato, la Consulta – con una pronuncia che ha tracciato il solco in cui si è poi inserita la sentenza *Prisco* – ha precisato che l'ipotesi della videoregistrazione domiciliare che non abbia carattere di intercettazione di comunicazione può esser disciplinata soltanto dal Legislatore nel rispetto delle garanzie dell'art. 14 Cost. e, quindi, in assenza di una disciplina legislativa, costituisce un'ipotesi di violazione del domicilio al di fuori dei casi previsti dalla Legge, cioè una prova atipica, tuttavia inammissibile perché incostituzionale (Cort. Cost. n. 135/2002).

E coerentemente, la Corte ha precisato che, in assenza di una norma che consenta o disciplini l'attività investigativa nel domicilio così da rispettare la riserva di Legge e di giurisdizione prevista dall'art. 14 Cost., la ripresa domiciliare è "*radicalmente vietata, proprio perché lesiva dell'inviolabilità del*

domicilio, sancita dal comma 1 dello stesso art. 14 Cost.; mentre i risultati delle riprese effettuate in violazione del divieto rimarrebbero inutilizzabili" (Cort. Cost. n. 149/2008).

La Corte di Cassazione si è, via via, accodata alla rotta tracciata dalla Corte Costituzionale, sancendo, a più riprese, l'inutilizzabilità processuale degli elementi di prova acquisiti *(i)* in violazione di diritti soggettivi tutelati in maniera specifica dalla Costituzione e *(ii)* al di fuori dei casi e delle modalità previste, in ossequio alla Carta costituzionale, dalla Legge (Cass. S.U. 16 maggio 1996, Sala; Cass. S.U. 25 marzo 1998, Manno; Cass. S.U. 24 settembre 1998, Gallieri; Cass. S.U. 23 febbraio 2000, D'Amuri; Cass. S.U. 28 marzo 2006, Prisco; Cass. S.U. 13 gennaio 2009, Racco).

Scendendo dal piano costituzionale a quello della Legge ordinaria, l'inutilizzabilità dei documenti (statici) captati mediante *on line search*, può esser formalizzata processualmente attraverso l'art. 191 c.p.p. che punisce con questa sanzione l'attività posta in essere in violazione di "*divieti stabiliti dalla legge*".

Divieti che in caso di possibili prove atipiche - frutto "a monte" di mezzi di ricerca della prova atipici – non possono che esser individuati da norme extraprocessuali (come si desume *a fortiori* da Cass. Sez. Quinta, n. 35681/2014[22]).

Peraltro, diversamente ragionando, si cadrebbe nel paradosso che, stante l'assenza di norme processuali che disciplinano l'*on line search*, gli esiti di tale attività atipica sarebbero sempre leciti ed utilizzabili anche se posti in violazione di altre norme dell'Ordinamento (i.e. l'art. 615ter c.p.) o, peggio ancora, dell'art. 14 della Costituzione. Così non può essere.

Per amor di completezza, vale la pena ricordare che per "salvare" i risultati probatori dell'attività di *on line searche* (mediante *screenshot*) non si può certo attingere alla radicata giurisprudenza costituzionale e di legittimità che, applicando il principio *male captum, bene retentum*, ha ritenuto legittimo e dunque processualmente spendibile, il sequestro di beni scaturito da una perquisizione o da un'ispezione illegittima.

Senza necessità di addentrarsi nel complesso dibattito sulla configurabilità nel nostro Ordinamento della c.d. inutilizzabilità derivata (o, stessa cosa, sull'applicabilità della teoria del *frutto dell'albero avvelenato*), è evidente che nel caso dell'*on line search* si versi in uno scenario decisamente diverso dal binomio perquisizione illegittima-sequestro valido.

[22] Pronuncia che ha affermato l'inutilizzabilità, in quanto acquisite in violazione dell'art. 615 bis c.p., le prove ottenute attraverso interferenza illecita nella vita privata: nel caso di specie si trattava di una registrazione illecitamente effettuata da un coniuge delle conversazioni intrattenute, in ambito domestico, dall'altro coniuge con un terzo.

La perquisizione (o l'ispezione) è un mezzo di ricerca della prova previsto a livello costituzionale e puntualmente disciplinato così da dare concreta attuazione alla riserva di Legge e di giurisdizione.
L'*on line search* è, invece, priva di una disciplina legale di qualsivoglia rango, viola direttamente l'art. 14 Cost. e integra l'elemento oggettivo del reato di cui all'art. 615 ter c.p.. A ciò si aggiunga che la materiale captazione del *file* da parte del *software trojan* non equivale al sequestro obbligatorio del corpo del reato o delle cose pertinenti.
Semplificando: l'inoculazione del *virus* informatico non sta alla captazione del *file* come la perquisizione illegittima sta al sequestro ex art. 253 c.p.p.
In definitiva, non è difficile cogliere che nel caso dell'*on line search* siamo ben oltre il *male captum*, ragion per cui non vi è spazio per giustificare l'utilizzabilità a fini processuali dei *file* appresi dal *trojan* di Stato nei modi più vari ed al di fuori delle ipotesi previste dalla Legge.