GIUSTIZIA INSIEME

Processo Penale

Il Trojan horse nel processo penale

di Pierluigi Di Stefano

28 ottobre 2020

ABSTRACT

Warning: Undefined array key "abstract" in
/var/www/vhosts/giustiziainsieme.it/httpdocs/print/articolo_pdf.php on line **334**

Warning: Undefined array key "sommario_indice" in /var/www/vhosts/giustiziainsieme.it/httpdocs/print/articolo_pdf.php on line 335

Il Trojan horse nel processo penale

di Pierluigi Di Stefano

Sommario: 1. Regime di utilizzabilità dei messaggi inviati a mezzo Sms, WhatsApp o email acquisiti tramite *Trojan* - 2. Mezzi e tempi di acquisizione della messaggistica - 3. L'utilizzabilità

della messaggistica acquisita con le intercettazioni - 4. Regime della acquisizione della messaggistica pregressa - 4.1. Segue: messaggistica come “documento informatico” - 4.2. Segue: l’acquisizione “in presenza” del supporto informatico con i dati – il rapporto tra supporto e dati in esso contenuti - 4.3. Segue: l’acquisizione dei dati “da remoto”. La perquisizione ed il sequestro on-line - 5. L' utilizzabilità della messaggistica memorizzata - 6. Utilizzabilità nei confronti dei terzi - limite della riservatezza e diritto al segreto della corrispondenza - 7. I dubbi sulla ammissibilità dell’acquisizione indiscriminata di messaggistica a mezzo di *Trojan.*

1. Regime di utilizzabilità dei messaggi inviati a mezzo Sms, WhatsApp o email acquisiti tramite *Trojan*

Il tema di cui discutere riguarda un importante aspetto del rapporto fra nuove tecnologie ed attività di indagine penale ed una delle questioni più “calde” soprattutto in relazione a vicende (per tutte l’*affaire* “Palamara”) in cui l’acquisizione di quantità impressionanti di messaggi di esponenti delle istituzioni ha manifestato la capacità dirompente di indagini sempre più efficaci ma invasive della sfera della riservatezza ed i cui esiti finiscono per andare ben al di là della vicenda per la quale sono iniziate.

Interessa soprattutto la messaggistica prodotta mediante applicazioni dedicate essenzialmente agli smartphone: innanzitutto la dominante Whatsapp, ma anche Messenger, Telegram, Viber, Signal etc. Le questioni più rilevanti che si pongono, comunque, sono riferibili anche ai mezzi di comunicazione digitale più “*tradizionali*” quali posta elettronica e sms**[1]**.

Tra gli effetti della “*rivoluzione digitale*” vi è l’ utilizzazione da parte di chiunque di tecnologie informatiche giungendosi alla sostanziale indispensabilità dei dispositivi portatili individuali nei quali spesso vengono riversate informazioni rappresentative dell’intera vita personale e professionale dell’utilizzatore: è diventato di uso universale ciò che fino a pochi anni fa era comunque limitato al minor numero di persone che facevano uso assiduo di pc. Ed è diventato universale soprattutto l’utilizzo della messaggistica istantanea per comunicare (messaggi scritti, vocali registrati, emoticons quali novelli geroglifici) anziché della classica telefonia.

E qui si pone la peculiarità che rende assai rilevante per le indagini penali accedere alla messaggistica di tale tipo: non solo è possibile intercettare in modo classico i messaggi che verranno inviati nella fase dell’ascolto autorizzato dal giudice, ma è anche possibile conoscere cosa si è detto (o, meglio, scritto) in precedenza: basta accedere alle chat passate, di norma memorizzate nei dispositivi. (Quasi) come se, in passato, si fossero registrate le proprie telefonate degli ultimi anni, mantenendole tutte direttamente accessibili nella memoria dei

dispositivi.

Ed anche la possibilità di accesso a tali chat è semplificata grazie a più efficaci tecnologie di intrusione nei dispositivi informatici individuali mediante l'utilizzo di programmi di accesso da remoto operanti senza essere rilevabili dall'utente bersaglio ("*captatore informatico*", gergalmente "*Trojan (horse)*", chiarissima la metafora del cavallo di Troia).

Quindi, certamente vi sono grandi possibilità per le indagini penali, che in passato potevano tuttalpiù confidare sui "*tabulati*" per ricostruire i precedenti contatti telefonici del titolare dell'utenza ma non i relativi contenuti (salvo per gli sms, che però non hanno mai avuto una estensione d'uso paragonabile agli altri sistemi di messaggistica operanti su internet).

Ma, nel contempo, si realizza un livello di intrusione nella vita privata inimmaginabile in passato e, quindi, vi è il rischio di gravi danni per i diritti fondamentali della persona.

Tali nuove opportunità di indagine hanno avuto ulteriore spazio con la più recente normativa (D.Lgs. n. 216 del 2017, L. n. 3 del 2019, D.l. n. 161 del 2019) che, con riferimento al sistema delle intercettazioni, ha ampliato i fenomeni criminali per i quali si ritiene opportuno una maggiore libertà di azione degli inquirenti, anche mediante accesso ai dispositivi informatici: ora, anche per i più gravi delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione sono applicabili le disposizioni in passato limitate ai soli procedimenti per criminalità organizzata e terrorismo.

Questo significa che, per questi reati, oltre ad essere semplificate le condizioni per procedere alle già invasive intercettazioni, le operazioni di ascolto possono essere effettuate anche nel domicilio del soggetto intercettato con il "*captatore informatico*"**[2]**.

Ad oggi, non esistono disposizioni in tema di prova che siano specifiche per la messaggistica, pur se questa certamente pone problemi del tutto peculiari.

La giurisprudenza sinora ha inquadrato agevolmente la messaggistica alla quale ha applicato le regole probatorie preesistenti in tema di documenti, corrispondenza, perquisizione, sequestro ed intercettazioni a seconda delle situazioni. Questa applicazione appare certamente adeguata per l'interesse alla conduzione delle indagini ma appare poco soddisfacente quanto alla tutela della riservatezza, come segnalato da varia dottrina.

In particolare, la giurisprudenza ha equiparato i messaggi elettronici archiviati alla posta "*cartacea*" custodita dal destinatario dopo il suo ricevimento.

Tale posta "*ricevuta*", per l'evidenza del dato normativo e della relativa interpretazione (secondo il testo dell'art. 254 cod. proc. pen. rientrano nella "*corrispondenza*" i plichi in transito presso i gestori del servizio e non quella, ricevuta o in copia di quella spedita, conservata dal destinatario o dal mittente), è sempre stata considerata alla stregua di una comune documentazione per la quale può essere disposto il sequestro in base alle norme generali.

Se, però, tale equiparazione appare in teoria ovvia e corretta, sul piano concreto, proprio per la impressionante quantità di messaggi che ormai chiunque manda, riceve e conserva, il paragone non regge più: tutto è amplificato, sia sotto il profilo della utilità probatoria che della necessità di tutela della riservatezza perché la messaggistica archiviata può contenere informazioni dettagliate su tutti i profili più intimi della persona (relazioni, opinioni, abitudini, vizi etc).

La mancanza di una normativa che tenga conto di tali nuove situazioni si fa sentire, considerando che le disposizioni ultime del codice di rito in ordine alla gestione dei dati informatici risalgono al 2008, tempi sostanzialmente remoti per le tecnologie di comunicazione informatica e, soprattutto, ben prima della generalizzata disponibilità dei dispositivi individuali tipo smartphone, dei sistemi di messaggistica via rete e della maggiore disponibilità dei sistemi di intrusione nei sistemi informatici**[3]**.

La soluzione normativa appare opportuna perché il lavoro della giurisprudenza per adattare le disposizioni esistenti risente inevitabilmente del tipo di approccio al problema.

È chiaro che i temi di utilizzabilità si pongono all'attenzione dei giudici di cassazione per la decisione in casi concreti, quando la messaggistica è stata già materialmente acquisita: una tale situazione può portare ad interpretazioni più "conservative"**[4]** che privilegino la massima estensione dei poteri inquisitori rispetto ad interpretazioni che, per rispettare anche gli altri interessi in gioco, comportino l'inutilizzabilità di quanto ormai raccolto nel processo**[5]**.

Le soluzioni normative, invece, ben si prestano a ridefinire il giusto equilibrio tra gli opposti interessi e disciplinare un'eccessiva pervasività dell'accesso ad informazioni che rappresentano ogni aspetto della vita dei "bersagli" (che, si rammenta, non sono necessariamente gli indagati; persino la vittima potrebbe trovarsi la propria vita "in piazza")**[6]**.

Tali normative, però, non sembrano essere in discussione e, anzi, i più recenti interventi tendono a privilegiare essenzialmente il perseguimento di obiettivi securitari, operando contro il rischio di "dispersione" delle prove**[7]**. Mentre il legislatore del codice di rito del 1989, se a conoscenza dei futuri fenomeni, probabilmente avrebbe ben diversamente disciplinato l'equilibrio tra esigenze securitarie e diritti dei singoli, come testimoniano le garanzie del codice originario in

tema di intercettazioni, chiaramente forti rispetto alla semplice telefonia fissa e sostanzialmente "analogica", quello attuale sembra privilegiare l'esigenza del momento, come avvenuto con il D.L. 30 dicembre 2019, n. 161, convertito con modificazioni dalla L. 28 febbraio 2020, n. 7, che ha ampliato al massimo l'utilizzabilità delle intercettazioni in diverso procedimento, sostanzialmente cancellando il divieto dell'art. 270 cod. proc. pen. la cui imperatività era appena stata riaffermata dalla nota Sezioni Unite Cavallo del 28 novembre 2019, in tal modo introducendo la sostanziale illimitatezza delle cd "intercettazioni a strascico"**[8]**; e come avvenuto con le varie disposizioni che hanno ampliato le possibilità di ricorso ad intercettazioni ambientali anche nel domicilio.

2. Mezzi e tempi di acquisizione della messaggistica

Per individuare quale sia la disciplina positiva dell'acquisizione dei messaggi, secondo la corrente interpretazione della giurisprudenza di legittimità, va considerato che ci si trova di fronte a diverse tipologie di prove a seconda del modo in cui tale acquisizione avviene (il riferimento è soprattutto alla messaggistica immediata ma lo stesso vale anche per la posta elettronica):

- Il discrimine essenziale utilizzato in giurisprudenza è se l'indagine sia mirata all' acquisizione di messaggi già scambiati che, quindi, siano stati archiviati localmente (lasciati nel dispositivo di ricezione o copiati su altri supporti) o, invece, sia mirata alla captazione di messaggi durante la loro spedizione/invio, quindi con captazione in tempo reale. La diversità di tali casi rinvia chiaramente alla differenza tra (sequestro di) documenti ed intercettazioni.

Quanto ai "*mezzi di ricerca della prova*" costituita dai documenti "*messaggi memorizzati*", si deve distinguere tra:

- la consegna diretta agli inquirenti /al giudice dei messaggi da parte di chi ne è in possesso;

- la apprensione fisica del dispositivo elettronico per poi estrarne il contenuto (perquisizione e sequestro);

- l'intrusione dall'esterno con l'uso di metodiche informatiche di collegamento e controllo da remoto dei dispositivi informatici per gestirli/osservare/copiare (praticamente il "*Trojan*")**[9]**. Tale ultimo sistema risulta oggi disciplinato espressamente dalla legge quale possibile strumento per l'esecuzione di intercettazioni delle comunicazioni tra presenti ("*l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*"); la limitatezza di una tale previsione non è di

poco conto, potendo essere interpretata nel senso di lasciare, per il resto, la piena libertà di accesso da remoto ai sistemi informatici se al solo fine di prelevare dati e non per utilizzare il microfono o comunque "spiare" l'ambiente (ad es. con videocamera o gps)**[10]**.

In definitiva, l'utilizzabilità del materiale acquisito è condizionata dalla modalità di raccolta.

Anticipando, in sintesi, quanto si svilupperà dopo:

- Per le conversazioni effettuate con messaggistica immediata (con *Trojan* o altro mezzo), oggetto di intercettazione ex artt. 266 e ss. cod. proc. pen., valgono i medesimi limiti delle intercettazioni di conversazioni. Il mancato rispetto di limiti e regole produce, secondo le specifiche previsioni delle intercettazioni, l'inutilizzabilità del materiale indebitamente raccolto.

- Per le chat pregresse, acquisite nei vari possibili modi, non vi sono limiti per tipologia di reato ed è sufficiente che si proceda sulla scorta di una notizia di reato che abbia dei minimi caratteri di concretezza. Inoltre, non vi sono limiti alla utilizzazione in altri procedimenti e forme di protezione particolari per prevenire l'indebita diffusione del materiale. In compenso, per il caso dell'acquisizione mediante sequestro probatorio, vi è la possibilità di rivolgersi al giudice per il riesame del provvedimento del p.m..

3. L'utilizzabilità della messaggistica acquisita con le intercettazioni

Sviluppando tali punti facendo riferimento al "diritto vivente", si parte dal dato che la giurisprudenza sostanzialmente non sembra dubitare della netta distinzione tra l'intercettazione diretta dei messaggi e la loro acquisizione mediante sequestro.

Le varie decisioni note fanno riferimento al momento in cui interviene la captazione:

poiché l'intercettazione *"… postula infatti, per sua natura, la captazione di un flusso di comunicazioni nel momento stesso in cui si realizzano, cosicché il provvedimento di autorizzazione del giudice risulta necessario in quanto finalizzato, in via preventiva ed in relazione al quadro accusatorio, alla verifica dell'esistenza di gravi indizi di reato, in una prospettiva di indispensabilità per la prosecuzione delle indagini preliminari*" Cass. VI, n. 28269 del 28.5.2019, tale forma di acquisizione della prova non potrà che riguardare le comunicazioni successive all'inizio delle operazioni di ascolto/captazione.

Ovvio, tanto da non dovere spiegarne le ragioni, che la "*conversazione*" sia tale anche senza la necessaria immediatezza della catena dello scambio di messaggi; è tipico di una tale forma di comunicazione che la risposta possa certamente seguire nel tempo, non perdendo la natura di "

conversazione" **[11]**.

In definitiva, l'utilizzabilità delle "*chat*" e, comunque, di tutta la corrispondenza informatica (email o altra forma), captata in tale modo segue le regole ben strutturate degli articoli 266 e ss. cod. proc. pen.: quanto alla previa autorizzazione, alla possibilità di disporle solo per taluni reati, alla necessaria preesistenza di un quadro indiziario ed alla necessità ai fini delle indagini, al rispetto delle date modalità di esecuzione e dei sistemi di selezione di quanto utile per il processo e di protezione dalla indebita diffusione del materiale.

In particolare, per tale materiale è prevista "*la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche*", presumibilmente costituite dalla registrazione o sequenza di istantanee dello schermo del dispositivo intercettato.

Quanto detto prescinde dal mezzo tecnico utilizzato per l'intercettazione dei messaggi. Comunque, per quanto riguarda la messaggistica tipo whatsapp, allo stato, per i sistemi di crittografia maggiormente in uso, non appaiono possibili modalità diverse dal captatore informatico (è necessario "entrare" nell'apparecchio).

È poi plausibile che nel corso delle operazioni eventualmente condotte con il *Trojan* gli inquirenti sfruttino il mezzo anche per acquisire le chat/email memorizzate prima dell'inizio delle operazioni di captazione; per queste, comunque, non sarà applicabile la disciplina delle intercettazioni per la loro diversa natura bensì la disciplina di cui appresso.

4. Regime della acquisizione della messaggistica pregressa

Ben più complessa la questione giuridica relativa all'acquisizione delle conversazioni/messaggi di posta elettronica etc conservati nei dispositivi informatici. La massa di informazioni e l'ampiezza del coinvolgimento dei diritti personali coinvolti da tali indagini può fare ritenere inappagante la applicazione pura e semplice delle norme, pur se apparentemente calzanti, in tema di perquisizione e sequestri, anche di corrispondenza.

Le questioni rilevanti riguardano in particolare la modalità di acquisizione "*occulta*" e la possibilità di contenere il materiale sequestrato entro l'ambito ragionevole per le indagini in atto.

4.1. Segue: messaggistica come "documento informatico"

Non sembra dubbio che, nell'inquadrare la messaggistica memorizzata tra i mezzi di prova, la disposizione di carattere generale per definirne la natura intrinseca sia quella dell'art. 234 cod.

proc. pen.: si è in presenza di una prova documentale consistente nella rappresentazione di "*fatti, persone o cose mediante qualsiasi mezzo, ivi compresa la fotografia, la cinematografia, la fotografia qualsiasi altro mezzo*", formata all'esterno del procedimento.

La giurisprudenza lo afferma chiaramente: sono documenti ai sensi dell'art. 234 cod. proc. pen. i "*dati di carattere informatico contenuti nel computer, in quanto rappresentativi, alla stregua della previsione normativa, di cose*": e Cass. III, sent. 37419 del 27.9.12, facendo riferimento all'inequivoca normativa in tema di documentazione digitale, lo ha affermato espressamente proprio per i "*messaggi "WhatsApp" e gli "SMS" conservati nella memoria di un telefono cellulare sottoposto a sequestro*". In termini analoghi anche Cass. V, sent. 1822 del 16.1.2018**[12]** e Cass. III, sent. 8332 del 6.11.2019.

La giurisprudenza ha anche affrontato ed agevolmente risolto la questione dei dati salvati su "*cloud*", ovvero spazi virtuali a disposizione dell'utente posti nel server del gestore del servizio; la questione è stata discussa soprattutto perché tali server sono all'estero.

Sostanzialmente, in quanto spazio informatico di accesso esclusivo da parte del singolo, si afferma che i dati ivi posti rappresentano documenti in diretto possesso dell'utente**[13]**.

Alla natura di documento consegue la applicabilità delle relative disposizioni: in particolare, si applica l'art. 237 cod. proc. pen. che consente l'acquisizione dei documenti "*provenienti*" dall'imputato. La disposizione rileva soprattutto perché, al di là della pacifica possibilità di acquisire i documenti informatici, comprese le chat, consegnati spontaneamente dall'imputato, si aggiunge la possibilità di utilizzare liberamente tutti i documenti informatici da lui provenienti e conservati da terzi; questo vuol dire che le conversazioni memorizzate ed i messaggi di posta elettronica possono essere consegnati anche dall'altro interlocutore**[14]**.

D'altra parte, l'imputato può consegnare le *chat* che riguardano, oltre che lui, gli interlocutori; anche qui, apparentemente, nulla di nuovo, si tratta di quanto è sempre stato possibile per la posta cartacea archiviata. Ma vale il consueto richiamo alla peculiarità della messaggistica informatica; quello che va rimarcato è che l'imputato è in grado di allegare anche spontaneamente tale tipo di documentazione senza alcuna possibilità per il terzo interlocutore di opporre il proprio interesse contrario.

Le questioni di maggior rilievo riguardano, poi, le modalità di accesso alla documentazione al di fuori della ipotesi della spontanea consegna da parte di chi ne ha la disponibilità. Con mezzi "tradizionali" o con il *Trojan*.

4.2. Segue: l'acquisizione "in presenza" del supporto informatico con i dati – il rapporto tra supporto e dati in esso contenuti

Dopo una abbastanza recente evoluzione della giurisprudenza che ha preso atto, soprattutto a seguito delle innovazioni del codice penale e di procedura penale con la legge n. 48 del 2008, che l'oggetto del sequestro è il "*dato informatico*" in quanto documento o comunque in quanto bene sul quale si incentra l'interesse del suo titolare e degli inquirenti ("*è la stessa circolazione dell'informazione che rappresenta lo spossessamento del diritto*"), è finalmente ben chiara la distinzione tra il supporto che contiene i dati - che si tratti dell'intero dispositivo (il telefono, il pc, il server etc) o di una scheda di memoria o di uno spazio virtuale di un server - ed i dati stessi **[15]**.

Tralasciando per ora il tema della possibile eccessività del sequestro di sistemi informatici rispetto ai dati documentali cui l'indagine è mirata, rileva la modalità per giungere alla acquisizione della messaggistica.

Valgono quindi le disposizioni in tema di "*mezzi di ricerca della prova*", utilizzabili pienamente per l'acquisizione diretta dei supporti contenenti la memorizzazione informatica della messaggistica**[16]**:

- Ispezione: l'art. 244 cod. proc. pen. disciplina espressamente anche l'ispezione "*informatica*";

- perquisizione, in particolare quanto alla peculiare forma della "*perquisizione informatica*"; in questo caso, vi è la disposizione speciale dell'art. 247, comma 1 bis, cod. proc. pen., introdotta dalla citata legge del 2008, secondo la quale "*quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ... ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati...*" nonché quella dell' art. 352, comma 1 bis, cod. proc. pen.: "*Nella flagranza del reato, ovvero nei casi di cui al comma 2 ... gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, ...*". L'attività è finalizzata a ricercare cose da sottoporre a sequestro tra cui "*dati, informazioni e programmi informatici*";

- sequestro: oltre alle disposizioni generali che comunque sarebbero applicabili per l'acquisizione dei supporti contenenti i dati, vi sono anche disposizioni specifiche in tema di sequestro di dati informatici presso i fornitori di servizi (art. 254 bis cod. proc. pen.).

Sono invece inapplicabili le disposizioni che riguardano il sequestro di corrispondenza. Come già detto, l'interpretazione corrente e letterale degli artt. 254 (*sequestro di corrispondenza*) e del corrispondente 353 cod. proc. pen. , per quanto riguarda la posta cartacea, è nel senso che la disciplina speciale di tutela della corrispondenza riguarda solo il momento in cui il materiale è "in itinere", ovvero sotto il controllo diretto del soggetto che gestisce il servizio.

Ciò è stato testualmente riferito anche alle forniture di servizi di trasmissione telematica della corrispondenza: in tema di posta elettronica si è chiarito che i messaggi spediti o pervenuti (o, anche, preparati per la spedizione ma non ancora spediti) archiviati nel dispositivo individuale o nello spazio riservato sul server del fornitore del servizio non sono "corrispondenza" e non hanno la relativa tutela. Mutatis mutandis, quanto detto vale anche quanto alla messaggistica salvata negli spazi propri dell'utente privato**[17]**.

In definitiva, in modo non dissimile dal sistema delle intercettazioni, i mezzi tipici di ricerca della prova appaiono pienamente applicabili alla acquisizione della messaggistica archiviata mediante apprensione "in locale" dei supporti da parte del soggetto che ne è in possesso.

Tali norme, a conferma della loro applicabilità, disciplinano espressamente anche le procedure di estrapolazione e selezione dei dati; è comunque evidente, in base al dato testuale, che il fuoco delle disposizioni specifiche non è incentrato sulla tutela della riservatezza bensì sulla garanzia di integrità dei dati.

La giurisprudenza conferma quanto si è detto, sviluppando temi che attengono essenzialmente a proporzionalità ed adeguatezza del sequestro, problema comprensibile perché la assenza di apprezzabile fisicità dei dati rende facile la loro acquisizione al di là di quanto utile e necessario, anche solo per "pigrizia" nel (non operare) la selezione quando si proceda ad una acquisizione massiva.

Si vedano Cass. VI, sent. 24617 del 10.6.15, Cass. V, sent. 38456 del 17.5.2019 e Cass. VI, sent. 41974 del 14.2.2019 le quali, con riferimento ai dati informatici in generale e alla posta elettronica (non alla messaggistica istantanea, evidentemente non in questione in quei casi concreti), ritengono privo di giustificazione di per sè il sequestro di interi sistemi informatici e non dei soli dati rilevanti, salvo quanto (e per il solo tempo) necessario a procedere alla selezione dei dati stessi.

4.3. Segue: l'acquisizione dei dati "da remoto". La perquisizione ed il sequestro on-line

Il tema che appare di particolare rilievo e che, in assenza, per ora, di una significativa casistica giudiziaria nota, allo stato sembra preso in considerazione solo dalla dottrina, riguarda

l'acquisizione a distanza, occulta ed indiscriminata, della messaggistica istantanea archiviata nei dispositivi individuali (non necessariamente portatili).

La stessa discussione, l'elaborazione giurisprudenziale e la introduzione di una norma ad hoc in materia di captatore informatico dimostra quanto sia pervasivo ex sé il controllo effettuato con determinate tecniche.

A ben vedere, non si discute se sia ammissibile o meno la prova "intercettazione", in particolare quella tra persone presenti: premesso che tali intercettazioni sono sempre state consentite, la questione riguarda, né più né meno, il "come" vada installato un microfono.

Il punto è che il rapporto personale tra individuo e dispositivi elettronici, in particolare quelli portatili tipo smartphone, ha la conseguenza che quasi chiunque in età attiva passa la maggiore parte del suo tempo avendo con sé un microfono ed una videocamera collegata alla rete; poiché in tale situazione diviene possibile conoscere il "*tutto*" dell'individuo se solo riesce l'intrusione nel suo apparecchio, il dibattito giurisprudenziale e normativo si è dovuto spingere a discutere sul tema della natura giuridica del come "*collegare i fili*" a tale apparecchio. Se, cioè, tale collegamento sia legittimo ed a che condizioni, in considerazione di tutti i rischi che presenta, in caso di cattivo uso, l'attivazione di un'arma così letale.

E queste semplici osservazioni, portano a chiedersi se, per la parte non disciplinata dalla normativa in tema di intercettazione, l'acquisizione di dati (messaggistica) in modo occulto ed a distanza possa ritenersi una applicazione come un'altra delle regole in tema di perquisizione e sequestro o, per il coinvolgimento di diritti fondamentali (e del diritto al "*domicilio informatico*"), si tratti di una (mezzo di ricerca della) prova non disciplinata dalla legge da valutare anche considerando se vi sia il pieno rispetto di principi di rango costituzionale.

Il novellato articolo 266 cod. proc. pen., adeguandosi alla discussione giurisprudenziale culminata nella nota sentenza delle SS.UU. Scurato del 28 aprile 2016, ha disciplinato " *l'inserimento di un captatore informatico su un dispositivo elettronico portatile*" finalizzato alla " *intercettazione di comunicazioni tra presenti*", ponendosi essenzialmente i soli temi della possibilità di attivare l'ascolto anche quando l'intercettato si trovi all'interno del domicilio e delle modalità tecniche per garantire la sicurezza e segretezza delle operazioni.

La disposizione, però, ha visto in un'ottica molto limitata la funzione del "*captatore informatico*".

In questo ambito rientrano anche i programmi che consentono la gestione da remoto di un apparecchio informatico (prodotto diffusissimo, ad esempio, per l'assistenza informatica da

remoto e con i programmi di collaborazione a distanza). La peculiarità di quelli di interesse ai fini di indagini penali è la capacità da *hacker* del programma di intrufolarsi non percepito e non lasciando segni, consentendo di avere il controllo del dispositivo bersaglio.

Quindi un captatore informatico non è semplicemente uno strumento che si limiti ad utilizzare il microfono: è uno strumento che mette in condizioni il soggetto intrusore di utilizzare l'apparecchio altrui come un comune utente con accesso fisico allo stesso.

Insomma, non solo l'art. 266 cod. proc. pen., considerando la sua portata limitata alla installazione del *Trojan* in un dispositivo portatile, non chiarisce se sia liberamente installabile un captatore informatico in un computer fisso od in altro apparecchio non portatile**[18]**, ma non tiene conto di tutte le altre cose che un tale software spia può fare. Ovvero, e soprattutto, accedere a tutto il contenuto dell'apparecchio con la possibilità di visionarlo e ovviamente copiarlo all'insaputa dell'utente**[19]**.

Nessuna disposizione in materia di intercettazioni sembra applicabile al caso: nulla fa riferimento all'acquisizione del contenuto**[20]**.

Né vi è alcuna disposizione che faccia riferimento alla perquisizione on-line. Sostanzialmente, l'hackeraggio finalizzato "soltanto" ad acquisire i dati del sistema informatico potrebbe sembrare una modalità sostanzialmente in sé libera, da valutare nel contesto dei sistemi di ricerca delle prove preesistenti**[21]**.

Se così è, l'acquisizione delle chat pregresse e memorizzate sarebbe consentita:

- Con il "captatore" autorizzato ex art. 266 cod. proc. pen. senza, però, che operino i limiti delle intercettazioni ma quale comune documento informatico; oppure

- utilizzando un qualsiasi programma di controllo da remoto che venga destinato solo all'accesso ai dati e non all'ascolto dal microfono ("qualsiasi" in quanto vi la previsione di regole tecniche solo per i programmi destinati alle intercettazioni)**[22]**.

L'accesso ai dati effettuato in tale modo andrebbe allora disciplinato alla stregua delle disposizioni esistenti:

- L'art. 246 cod. proc. pen. prevede la consegna del decreto di ispezione a chi è presente nel luogo in cui la stessa va eseguita. Va avvisata la parte che sia presente nel luogo fisico in cui vi è il dispositivo ispezionato?

- L'art. 247 cod. proc. pen. dispone la perquisizione informatica sulla scorta di un decreto motivato. Il dubbio è, allora: si applicano le disposizioni in tema di richiesta alla parte di consegnare quanto oggetto di ricerca? E quelle in tema di perquisizione locale in relazione al luogo fisico in cui è il dispositivo perquisito?

Considerato però che la giurisprudenza tende ad escludere che la perquisizione nulla comporti l'invalidità del sequestro (il nostro sistema non sembra prevedere la regola del "*fruit of the poisonous tree*", per tutte Cass. V, n. 32009 del 12.7.2018), le questioni più rilevanti riguardano la fase del sequestro.

Invero, soprattutto se si procede al di fuori delle operazioni di intercettazione, non sembrano esservi difficoltà particolari ad applicare le comuni regole in tema di sequestro probatorio. Certamente, nel caso di sequestro di iniziativa della polizia giudiziaria, il provvedimento andrà convalidato nei brevi termini dell'art. 355 cod. proc. pen. e comunicato all'interessato. Ma, anche se venga omessa o ritardata la notifica dell'avvenuta convalida, non vi sarà alcuna nullità o inutilizzabilità del sequestro (per tutte Cass. III, n. 6114 del 20.1.2005): semplicemente, non decorrerà il termine per proporre riesame.

La peculiarità, però, è che l'interessato, se non riceve avviso, non potrà comprendere esservi stata la acquisizione dei dati (quindi dei messaggi) dal suo apparecchio.

In definitiva, il sequestro di *chat* con intrusione da remoto nel dispositivo informatico, considerato il quadro normativo e la giurisprudenza, appare ammissibile.

Più avanti, comunque, si valuteranno le pur significative ragioni per una diversa ricostruzione giuridica, in termini di possibile inutilizzabilità dell'acquisizione di dati così effettuata.

5. L'utilizzabilità della messaggistica memorizzata

Una volta qualificata la messaggistica memorizzata quale documento, l'utilizzabilità in sé non sembra discutibile e va quindi considerata sotto il punto di vista della corretta acquisizione della prova:

- il documento informatico riproduttivo delle chat/messaggi può essere acquisito agli atti in quanto consegnato da chi può disporne; ovvero l'imputato od uno dei soggetti che hanno partecipato alla chat (né, ovviamente, è necessario che si tratti di un colloquio cui abbia preso parte l'imputato);

- tale documento può essere stato sequestrato nelle varie forme dette, con l'unica condizione della pertinenza e della necessità per l'accertamento dei fatti. E, secondo la interpretazione "permissiva" quanto all'uso di sistemi di intrusione a distanza per il prelievo dei dati già in memoria, può essere stato sequestrato con una perquisizione da remoto.

Una volta ritualmente acquisiti, i messaggi, in quanto documenti non costituenti intercettazione né corrispondenza, non hanno alcun limite di utilizzazione

- non vi è alcun limite per tipologia di reato;

- non è necessario alcun previo provvedimento del giudice che valuti l'esistenza di un previo serio quadro indiziario e la necessità di ricorrere al dato tipo di prova, pur se per sua natura invasivo;

- non vi è alcun limite alla libera utilizzazione di tale messaggistica al fine di provare altri reati; o in procedimenti non penali (allo stato è certamente ritenuta pacifica l'utilizzabilità nei procedimenti disciplinari nei confronti di magistrati);

- non vi sono le garanzie di conservazione previste per le intercettazioni ma quelle (comunque senza alcuna sanzione di inutilizzabilità) della conservazione dei dati informatici; né le garanzie di trascrizione previa valutazione di rilevanza etc. previste per le intercettazioni;

- non vi sono regole specifiche per contrastare in modo efficace il pericolo di eccessiva e indebita diffusione al di fuori del processo.

E' indiscutibile, quindi, che, secondo la interpretazione che incasella tale tipologia di prove e la loro raccolta nelle disposizioni sulle prove tipiche, questo materiale rappresentativo di informazioni sulla persona non è assistito da alcuna seria tutela alla riservatezza delle comunicazioni, pur essendo probabilmente ancor più invasivo della intercettazione "in diretta" dei messaggi captati nel solo periodo di operazioni autorizzati ex art. 266 cod. proc. pen.: difatti, potrebbero acquisirsi con un *click* ed in pochi minuti anni di relazioni personali.

Tali aspetti sono chiaramente ancora più rilevanti con il sistema di intrusione a distanza.

In giurisprudenza, allo stato, non sembrano porsi particolari problemi in tema di utilizzazione dei messaggi conservati nei dispositivi informatici.

Considerando alcune decisioni più recenti:

- Cass. VI, n. 1822 del 12.11.2019, in un caso (sembra) di acquisizione dei messaggi a seguito di ispezione, afferma che per i messaggi whatsapp e sms rinvenuti in un telefono cellulare

sottoposto a sequestro non è applicabile la disciplina dettata dall'art. 254 cod. proc. pen., in quanto tali messaggi memorizzati non rientrano nel concetto di "corrispondenza".

- Cass. VI, n. 28269 del 28.5.2019 ritiene legittimo il sequestro probatorio di messaggi di posta elettronica già ricevuti o spediti e conservati nelle caselle di posta del computer, in quanto tali comunicazioni hanno natura di documenti ai sensi dell'art. 234 cod. proc. pen**[23]**.

- Cass. VI, n. 12975 del 6.2.2020, in relazione a materiale rinvenuto su server e consegnato su ordine di esibizione, afferma che i messaggi di posta elettronica memorizzati nelle cartelle dell'account o nel computer del mittente ovvero del destinatario, costituiscono meri documenti informatici intesi in senso "statico", dunque acquisibili ai sensi dell'art. 234 cod. proc. pen.

- Cass. V, n. 1822 del 21.11.2017 afferma lo stesso principio con riferimento a messaggi whatsapp e sms contenuti in un telefono cellulare posto sotto sequestro.

Non si rinvengono, invece, decisioni rispetto alla acquisizione di documenti e/o messaggi mediante l'uso del captatore informatico autorizzato per le intercettazioni (caso nel quale appare probabile che sia stata svolta l'attività parallela di ricerca del materiale presente nell'apparecchio – bersaglio)**[24]**.

6. Utilizzabilità nei confronti dei terzi - limite della riservatezza e diritto al segreto della corrispondenza

La possibilità che si proceda alla acquisizione di grandi quantità di messaggi riguardanti un considerevole numero di interlocutori, con contenuti ragionevolmente di natura anche strettamente personale, pone ovviamente il problema di quale possa essere la tutela dei terzi interlocutori rispetto alle loro esigenze di riservatezza soprattutto a fronte di materiale acquisito che non sia rilevante ai fini della prova nel dato processo.

Invero, pur se il problema è di tale rilievo da fare apparire opportuna una diversa regolamentazione, se è vero quanto detto sopra (o, comunque, seguendo le attuali linee giurisprudenziali) non può che applicarsi la disciplina comune.

- Per il caso in cui la messaggistica sia stata acquisita con il mezzo delle intercettazioni, nell'arco temporale delle relative operazioni, si applicheranno le regole corrispondenti dalle quali (anche) il terzo sarà tutelato; difatti, non saranno selezionati e trascritti i messaggi privi di rilievo probatorio e vi è la possibilità di richiedere la distruzione dei messaggi superflui a norma dell'art. 269, comma 2, cod. proc. pen. (prevista espressamente "*a tutela della riservatezza*");

- per il caso in cui la messaggistica sia stata acquisita quale documento proveniente dall'imputato mediante consegna spontanea da parte dello stesso o da parte di un terzo che ne abbia la disponibilità, ricorrendo l'ipotesi dell'art. 237 cod. proc. pen., non vi è alcuna tutela diretta a favore del terzo che risulta interlocutore nei messaggi;

- per il caso, invece, di messaggistica acquisita mediante sequestro probatorio, sarà proponibile la richiesta di riesame del decreto di sequestro da parte di colui che abbia diritto alla restituzione, indagato o terzo.

Sulla tutela rappresentata dal riesame del sequestro probatorio va posta maggior attenzione.

Sulla possibilità che il rimedio possa essere proposto dal soggetto al quale le chat siano state sequestrate, non vi sono dubbi: si tratta di un sequestro di "*dati informatici*" alla cui disponibilità esclusiva tale soggetto (indagato o terzo) ha diritto, quindi è certamente legittimato all'impugnazione (l'art. 257 cod. proc. pen. ritiene legittimati l'"*imputato*", la "*persona alle quale le cose sono state sequestrate*" e "*quella che avrebbe diritto alla loro restituzione*").

La disposizione, però, non consente una tutela del terzo interlocutore. La procedura di riesame reale è strettamente finalizzata alla tutela di chi ha il diritto sul "bene" oggetto del sequestro e non sembra proponibile dal terzo interlocutore il quale potrebbe far valere soltanto un proprio interesse alla riservatezza dei dati/del file riproduttivo della conversazione sequestrata ad altri.

In sede di riesame avverso il sequestro probatorio potrà farsi valere la superfluità del sequestro, essendo sempre necessario che vi sia una specifica funzione probatoria a giustificare la acquisizione da parte dell'organo di accusa. Inoltre, potrà chiedersi il rispetto dei principi di adeguatezza e proporzionalità eventualmente non rispettati in sede di adozione del provvedimento.

Non è casuale come le decisioni più rilevanti sul tema giuridico del principio di proporzionalità ed adeguatezza riguardino proprio l'ipotesi del sequestro probatorio di una massa indistinta di dati informatici per le ragioni ovvie per le quali è assai semplice che si giunga ad un sequestro ridondante di un' impalpabile massa di documenti informatici:

- In tal senso, Cass. VI, n. 24617 del 24.2.2015, Cass. II, n. 26606 del 12.3.2019, nonché Cass. V, n. 38456 del 17.5.2019 e Cass. VI, n. 53168 del 11. 11. 2016 che ammettono il sequestro di un intero sistema informatico se ricorrono ragioni tecniche, dovendosi poi procedere alla estrapolazione dei dati necessari Ai fini della prova con obbligo di immediata restituzione quando sia decorso un tempo ragionevole per l'effettuazione degli accertamenti.

La giurisprudenza nota affronta il tema della proporzionalità e adeguatezza sotto il profilo della utilità e della eccessività sotto un profilo essenzialmente quantitativo.

E' comunque ragionevole ritenere che adeguatezza e proporzionalità vadano valutate anche rispetto allo scopo da raggiungere con il mezzo di prova, il che significa che andrà effettuata anche una comparazione di interessi**[25]**: quindi, così come non si dovrebbe ritenere ammissibile un sequestro di un intero sistema informatico che consente il funzionamento di un ospedale, influendo negativamente sul suo regolare esercizio, al fine della ricerca di una singola falsa certificazione, così si dovrebbe escludere che ricorrano le condizioni di adeguatezza e proporzionalità per procedere ad un sequestro indiscriminato di un intero archivio di messaggi, funzionale alla prova di un reato bagattellare, con il rischio di una rilevante lesione della riservatezza dei soggetti coinvolti (compreso lo stesso indagato).

In pratica, proprio nell'ambito di interesse, il principio di adeguatezza dovrebbe fare ritenere la prevalenza dell'esigenza di escludere eccessivi "*danni collaterali*".

Resta fermo, però, che in favore del terzo cui siano riferiti i messaggi non vi è una tutela processuale per fare valere direttamente il profilo della riservatezza, come previsto dal solo art. 267 cod. proc. pen.

Quindi la possibilità di sequestro delle *chat* pone indubbiamente problemi che il sistema non appare al momento in grado di risolvere efficacemente.

Peraltro, se è in questione la riservatezza, una volta resa conoscibile la messaggistica, il danno dovuto alla diffusione non potrà essere evitato anche da un provvedimento di restituzione che sia successivo a tale diffusione.

7. I dubbi sulla ammissibilità dell'acquisizione indiscriminata di messaggistica a mezzo di *Trojan*

Quanto detto sinora è basato sulla valutazione delle posizioni della giurisprudenza che, pur non sempre affrontando in modo diretto la questione, ha in vario modo ritenuto utilizzabile la messaggistica archiviata nonché ritenuto utilizzabile il captatore informatico anche oltre l'ambito della intercettazione delle comunicazioni tra presenti con uso di sistemi portatili**[26]**. Si è quindi considerato come si sia presenza di prove che trovano corrispondenza nel sistema delle prove tipiche.

Le soluzioni individuate, però, non sono del tutto soddisfacenti; i dubbi emergono soprattutto in dottrina mentre la giurisprudenza, come visto, non sembra aver posto particolare attenzione al

tema del rispetto dei diritti fondamentali che viene in questione della materia in oggetto.

In particolare, gli aspetti critici riguardano la possibilità di acquisire senza reali limiti la messaggistica archiviata, in assenza di alcun previo controllo giurisdizionale (previsto, invece, per le intercettazioni dei messaggi *futuri*), sulla scorta di una qualsiasi notizia di reato e senza alcun limite per la ulteriore utilizzazione del materiale raccolto.

Inoltre, soprattutto in caso di acquisizione massiva di messaggistica/email nei confronti di soggetti particolari (ad es. esponenti delle istituzioni, operatori economici, esponenti politici), su di un materiale che sia ridondante rispetto all'indagine in corso può essere sviluppata un' attività investigativa che vada oltre la mera constatazione di fatti *ictu oculi* penalmente rilevanti e, invece, si trasformi in un'attività "esplorativa" (non consentita, trattandosi altrimenti di una attività ispettiva priva di regole; sul tema che il sequestro probatorio possa muovere solo da specifiche notizie di reato e non essere funzionale ad una ricerca casuale delle stesse, per tutte si veda Cass. VI, n. 41974 del 14.2.2019).

A ciò, poi, si aggiunge il rischio concreto che, in assenza di regole per garantire una seria secretazione di tale tipo di materiale, lo stesso possa essere oggetto di indebita diffusione.

In giurisprudenza si rilevano pochi tentativi di una disciplina diversa:

- Per quanto riguarda il profilo della acquisizione della messaggistica già conservata vi è stata l'unica decisione sopra citata che ha inteso ritenere applicabile la disciplina delle intercettazioni; le ragioni, collegate a dei profili tecnici, non appaiono condivisibili ma il risultato è certamente apprezzabile, consentendo di fare ricorso al più garantito sistema delle intercettazioni. Si tratta, però, di una linea isolata e difficilmente coniugabile con la disciplina positiva delle intercettazioni.

- Per quanto riguarda la possibilità di accesso mediante *Trojan* ai dati e, quindi, alle conversazioni memorizzate, in giurisprudenza vi è qualche accenno all'inquadramento quale prova atipica ex art. 189 cod. proc. pen.. Un tale inquadramento, però, appare fatto in termini non condivisibili. Il riferimento alla disciplina dell' art. 189 cod. proc. pen. sarebbe apprezzabile se si procedesse a verificare che la prova innominata non pregiudichi "*la libertà morale della persona*" (come richiede la disposizione); invece, il ricorso alla categoria della prova atipica è apparso un modo per risolvere (o eludere) il problema che, a qualificare le attività come di perquisizione e sequestro on-line, non risultano pienamente rispettate le garanzie di partecipazione della difesa alle relative attività.

Si considerano, allora, in sintesi i profili critici, quali emergono dalla dottrina, che ostano ad una piena utilizzazione della messaggistica se acquisita con il tramite della perquisizione e sequestro da remoto.

La questione riguarda il mancato rispetto dei diritti fondamentali:

- Innanzitutto, quelli degli articoli 2, 14 e 15 della Costituzione in tema di rispetto del domicilio nonché di libertà e segretezza di qualsivoglia forma di comunicazione, e comunque dei "*diritti inviolabili dell'uomo*" con le connesse riserve di legge e di giurisdizione.

- Poi, gli analoghi diritti riconosciuti dalle fonti sovranazionali, Carta dei Diritti Fondamentali e, soprattutto, l'art. 8 della C. E.D.U. lì dove riconosce, con formulazione anche più ampia, il "*diritto al rispetto della vita privata e familiare, del proprio domicilio e della propria corrispondenza*", escludendo ogni ingerenza dell'Autorità pubblica che non sia giustificata da gravi esigenze di prevenzione reati.

Come noto, proprio in relazione alla diffusione dell'utilizzazione dei sistemi informatici quale luogo "*virtuale*" di gestione delle relazioni sociali e di conservazione della memoria individuale e quant'altro, si giunge a configurare un vero e proprio diritto alla tutela del "*domicilio informatico* ". Appare, ormai, banale considerare che per ampia parte delle persone è mediamente ben più invasiva una incursione nei dispositivi informatici personali che nel domicilio, e di questo non può che prendersi atto ai fini delle necessarie tutele e per contemperare diritti fondamentali ed esigenze securitarie.

In dottrina si citano comunemente due decisioni della Corte costituzionale tedesca del 2008**[27]** e del 2016 per affermare come possa e debba ricostruirsi un tale diritto al domicilio informatico, affermazione sulla quale si può concordare facendo l'ordinamento tedesco riferimento a propri analoghi principi nazionali ed ai nostri medesimi principi fondamentali di rango sovranazionale.

Su questi presupposti va verificata la tenuta di una interpretazione che consenta l'accesso alle conversazioni memorizzate con l'uso degli attuali strumenti processuali.

Il primo profilo riguarda il ritenere soddisfacente il sistema del sequestro e della utilizzazione probatoria senza alcun limite per tipologia di reato.

Come si è già detto, è da considerare che la regola della proporzionalità ed adeguatezza del sequestro viene fondamentalmente utilizzata in sede di applicazione concreta nel senso di limitare il provvedimento a quanto utile, ma non nei termini di escludere che sia "accettabile"

una pesante intromissione nella vita privata per provare una vicenda di poco conto (quale una semplice contravvenzione). E, del resto, per la materia qui di interesse non è in questione la indebita ablazione di un oggetto "palpabile" che, una volta dissequestrato, torna al proprietario così risolvendo il profilo di danno**[28]**. Qui si tratta, ad esempio, della diffusione di informazioni attinenti alla vita privata che la parte ha tutto l'interesse ed il diritto a tenere riservate ma che, una volta uscite dalla sua sfera di controllo, non vi rientreranno più.

Questa è una ragione per dubitare che possa valere la mera equiparazione delle chat archiviate alla posta cartacea.

Del resto vi è da chiedersi cosa avverrebbe se si accendesse ad un archivio personale di registrazione dei propri colloqui con terzi, magari persino audiovideo (cosa del tutto plausibile perché tutti girano con uno "studio di registrazione" in tasca. Il nuovo reato di cui all'art. 617 septies cod. pen. certamente non lo vieta). Verrebbe ritenuto materiale tranquillamente sequestrabile ed utilizzabile in qualsiasi contesto processuale penale e non? Solo perché intercettazione di un "vecchio" colloquio? Non vi sarebbe applicazione delle regole di tutela (anche) della riservatezza di cui agli artt. 266 e ss. cod. proc. pen.?

La giurisprudenza non offre soluzioni diverse da quelle di cui sopra ma il tema richiederebbe un approfondimento**[29]**. L'esito attuale, invero, sembra portare alla violazione dei diritti fondamentali e, soprattutto, ad una non sempre giustificata lesione dei diritti dei terzi.

Fin qui la questione dell'acquisizione delle *chat*, a prescindere dal mezzo.

L'altro profilo sul quale si rinvia alla elaborazione dottrinaria**[30]**, anche in questo caso per l'assenza di chiare prese di posizione della giurisprudenza, vuoi per la scarsa casistica finora portata ai giudici di legittimità, vuoi per la soluzione semplicistica offerta dall'unica sentenza citata alla quale la questione era pur stata posta, riguarda la utilizzabilità della perquisizione *on-line* ed il sequestro da remoto delle *chat*, soprattutto quando, in ragione delle esigenze di segretezza per le coeve operazioni di intercettazioni, si opti per un indefinito ritardo della comunicazione dell'avvenuto sequestro alla parte interessata.

Sotto questo profilo i dubbi posti sono il rischio di elusione delle garanzie minime di tali strumenti di ricerca della prova, rischio che dovrebbe portare a non consentire una simile forma di intrusione, e la impossibilità di ricorrere al concetto di "*prova atipica*"**[31]** in quanto non è comunque consentito eludere un sistema di prova tipizzato (che, come detto, si rinviene nella perquisizione e nel sequestro) solo perché non è possibile offrirne le necessarie garanzie.

Inoltre anche le garanzie previste dall'art. 189 cod. proc. pen. (il giudice deve sentire le parti sull'ammissione della prova) sarebbero inevitabilmente spostate in una fase temporale successiva.

Oltre al tema della ammissibilità della prova così raccolta, va considerato il dubbio sull'esservi un vero e proprio divieto legislativo all'utilizzo del dato tipo di strumento, ovvero l'accesso da remoto.

Difatti, si può affermare che proprio la previsione legislativa esclusivamente di un determinato tipo di utilizzo della intrusione informatica significhi la non legittimità degli usi non previsti.

Ovvero, come già anticipato, certamente si può sostenere che, in quanto lesivo del principio dell'art. 15 della Costituzione, il dato sistema di intercettazione può essere consentito soltanto sulla scorta di disposizioni che siano rispettose della riserva di legge e della riserva di giurisdizione.

Questo, quindi, vorrebbe dire che, per la parte non disciplinata dagli artt. 266 e ss cod. proc. pen., il *Trojan* non potrebbe essere utilizzato.

Gli argomenti contrari sono sicuramente:

- la incomprensibilità, altrimenti, di un implicito divieto di estensione della utilizzabilità del *Trojan* per l'intercettazione ai computer fissi (o dispositivi non portatili);

- la sostanziale natura del *Trojan* non di mezzo di prova ma di una particolare modalità tecnica di raccoglierla; come detto, si può banalizzare dicendo che si tratta semplicemente di una forma di controllo sul modo di installare il microfono, il che non vieta l'utilizzazione di altri dispositivi;

- la previsione nella normativa di prevenzione della pedopornografia dell'accesso da remoto ai sistemi informatici privati senza alcuna forma particolare (in realtà in questo caso vi è una previsione normativa).

A favore, invece, di una tale limitazione va considerato che la recente normativa in tema di captatore informatico utilizzabile per le intercettazioni prevede garanzia su modalità**[32]** e tipologia di dispositivo informatico e l'obbligo di disinstallazione a fine delle operazioni rendendolo inidoneo a successivi impieghi; con tali previsioni, appare difficile affermare che possa essere giustificato il mantenimento di quello stesso strumento informatico per la sola "ispezione" (anche se, a fine operazioni, presumibilmente quel che interessava prendere dal dispositivo è già stato prelevato).

In definitiva, è certamente ragionevole ipotizzare che un esame più accurato di vicende significative possa portare la giurisprudenza a decisioni che valorizzino maggiormente il rispetto dei diritti fondamentali, soprattutto rispetto al coinvolgimento di terze persone; ma, nel contempo, ragionevole ipotizzare (e temere, per un ambito così delicato) di una disparità di decisioni. Si tratta, decisamente, di un ambito che merita una accurata normazione.

[1] Sul tema si vedano: M. Torre, *WhatsApp e l'acquisizione processuale della messaggistica istantanea*, in Dir. Pen. e Proc 9/2020; M. Minafra, *Sul giusto metodo acquisitivo della corrispondenza informatica "statica"*, in Giurisprudenza Italiana, 7/2018; A. Nocera, L'*acquisizione delle chat whatsapp e messenger: intercettazione, perquisizione o sequestro*?, in il Penalista, 12 febbraio 2018; G. Illuminati, *Libertà e segretezza della comunicazione*, in Cass. pen., 2019, 3826

[2] Per un quadro esaustivo della giurisprudenza degli ultimi anni e della normativa in tema di captatore informatico si rinvia a L. Giordano, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della suprema corte,* in Sistema Penale, 4/2020; L. Giordano, *Il ricorso al captatore informatico nei reati contro la pubblica amministrazione, in G. Flora, A. Marandola (a cura di), La nuova disciplina dei delitti di corruzione*, Pacini giuridica, Pisa, 2019, pag. 83 e ss.; L. Giordano, *La disciplina del "captatore informatico", in T. Bene (a cura di), L'intercettazione di comunicazioni*, Cacucci editore, Bari, 2018, pag. 247 e ss.

[3] Tali sistemi certamente non sono nuovi per i computer – l'intrusione abusiva nei sistemi informatici è praticamente nata insieme alle reti di computer - ma comunque sono certamente più efficaci e facilmente utilizzabili per essere ormai situazione ordinaria il collegamento costante alla rete.

[4] In M. Minafra, *Sul giusto metodo acquisitivo della corrispondenza informatica "statica", in Giurisprudenza Italiana, 7/2018*, si osserva: "*Appare, invero, che i giudici di legittimità tengano in maggior conto il principio di conservazione (rectius: non dispersione) della prova piuttosto che la tutela di un rapporto, quello tra individuo e attrezzatura informatica, che coinvolge e necessariamente implica i diritti inviolabili quali la libertà personale, la libertà di domicilio, anche nella sua particolare accezione di domicilio informatico, nonché la libertà e la segretezza della corrispondenza*".

[5] Non è un caso che in materie comparabili le decisioni più "dirompenti" a garanzia della difesa sono derivate da decisioni delle Sezioni Unite (si vedano quelle in tema di tabulati telefonici, sent. Gallieri del 13 luglio 1998 e le due decisioni in tema di art. 270 cod. proc. pen.,

sentt. Esposito del 17 novembre 2004 e Cavallo del 28 novembre 2019), che, per il particolare ruolo loro attribuito, mirano essenzialmente alla decisione sui principi giuridici.

[6] Si veda l'Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali, in Commissione Giustizia al Senato nell'ambito dell'iter di conversione del decreto sulle intercettazioni (**https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9116010**) poi operato con legge 28 febbraio 2020, n. 7: "*I recenti sviluppi del "caso Exodus" ripropongono, sotto aspetti diversi, il tema delle intercettazioni. La notizia dell'accesso agli atti di centinaia di inchieste e dell'intercettazione di altrettanti cittadini del tutto estranei ad indagini dimostra il grado di pericolosità di strumenti investigativi fondati, come nel caso dei trojan, su tecnologie particolarmente invasive. Per un verso, infatti, i software utilizzati a questi fini presentano un'intrinseca pericolosità, potendo "concentrare", in un unico atto, una pluralità di strumenti investigativi, in alcuni casi non lasciando tracce o alterando i dati acquisiti. Si realizza, così una sorveglianza ubiquitaria, ogniqualvolta tali captatori siano installati su dispositivi mobili, che ci accompagnano in ogni momento della vita. Per le loro stesse caratteristiche, dunque, i trojan, sfuggendo alle tradizionali categorie gius-processuali, rischiano di eludere le garanzie* essenziali *sottese al regime di acquisizione probatoria nei sistemi accusatori. ....* ".

La vicenda "*Exodus*" (nome di un software -Trojan utilizzato da soggetti privati delegati ad attività di intercettazione per varie Procure italiane) riguarda l'indagine in cui è emerso il sospetto che talune aziende, anziché limitarsi a far rimbalzare i flussi di comunicazioni intercettati al fine di garantirne l'anonimizzazione, li abbiano raccolti su uno o più server, tra l'altro di incerta collocazione territoriale, procedendo solo successivamente a scaricarli su quelli dislocati presso le sale intercettazioni delle Procure che le avevano disposte. A ciò si aggiungono serie perplessità sul sistema di introduzione del virus nell'apparato elettronico portatile, realizzata attraverso la preventiva infezione di app scaricabili da taluni store, di grande diffusione, con la conseguente infezione a tappeto di tutti coloro che avevano proceduto alla loro installazione, potenzialmente divenuti intercettabili attraverso l'attivazione del virus in tal modo introdotto nel cellulare.

Al di là della rilevanza penale di una tale procedura realizzata, sembra, nei confronti di centinaia di migliaia di utenti, risultavano comunque violate le prescrizioni 10, 25, 26 e 27 di cui al provvedimento del 18 luglio 2013, in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica del Garante per la protezione dei dati personali.

Questa vicenda ha contribuito a fare ritenere necessarie regole tecniche ad hoc per i futuri sistemi di intrusione.

[7] G. Illuminati, op. cit., espone come fosse stato presentato un progetto di legge, poi abortito, che mirava ad una disciplina completa del captatore informatico, considerate le sue varie possibilità, venendo poi approvata solo la minima disciplina riferita alla sua utilizzazione per le intercettazioni di conversazioni

[8] Se tale lettura dell'art. 270 cod. proc. pen. come modificato con la citata normativa sarà confermata (il dubbio sul modo in cui sarà interpretato è d'obbligo per la formulazione non chiarissima), ovvero di non necessità di collegamenti sostanziali al fine di utilizzare le intercettazioni disposte in un dato procedimento per accertare altri reati di cui all'art. 266, comma 1, cod. proc. pen., verosimilmente, vi sarà un vaglio di costituzionalità. Difatti le Sezioni Unite, nella sent. Cavallo del 28 novembre 2019 hanno evidenziato come il requisito del legame ex art. 12 cod. proc. pen. quale condizione per l'utilizzo delle intercettazioni (salvo i casi di eccezionale gravità riconducibili all'art. 380 cod. proc. pen.) sia funzionale alla attuazione della riserva di giurisdizione di cui all'art. 15 Cost., evitando che il decreto autorizzativo del giudice si traduca in una sorta di autorizzazione in bianco.

[9] Queste metodiche di intrusione, vecchie quanto la rete, divengono frequenti con la reazione degli inquirenti alla moltiplicazione dei modi di comunicare consentiti Internet: la soluzione per le indagini di fronte alla fonia Voip (Skype et similia, per intendere) che consentiva di inviare "pacchetti" sulla linea Internet, non intercettabili, venne individuata in sistemi di ascolto inseriti negli stessi computer, nonché della installazione in locale di keylogger, ovvero sistemi di registrazione di quanto digitato dall'utente con trasmissione occulta agli inquirenti. La naturale evoluzione è stata l'utilizzazione di sistemi di accesso remoto che consentono di operare direttamente nel computer bersaglio come da un comune terminale. E' quanto, oggi, si fa soprattutto sugli smartphone.

[10] Si consideri, però, che la scelta normativa di disciplinare una sola modalità di uso, l'attivazione del microfono, e per i soli dispositivi portatili (e "indossabili", trattandosi essenzialmente degli smartphone), oltre che probabilmente connessa al dato che il dibattito giurisprudenziale riguardava quella sola modalità d'uso, ha una chiara ragione: questa particolare modalità di intrusione in tutto ciò che chi ha con sé il dispositivo dice od ascolta, non limita l'intercettazione a sue singole comunicazioni (quelle realizzate attraverso telefono o in un determinato luogo, ove è stato in precedenza collocato uno strumento di captazione) ma in

sostanza (nei limiti temporali in cui lo strumento viene attivato) la estende all'intera sua esistenza e a tutti i tipi di sue relazioni. Quindi, già solo per questo profilo, non sembra possa affermarsi in termini di certezza che la scelta normativa escluda gli altri usi del *Trojan*. Semplicemente, "spiare" da una postazione fissa non pone problemi comparabili.

[11] Non manca una decisione, restata isolata, Cass. IV, n. 40903 del 28.6.2016 che, in riferimento alle email archiviate, ha affermato che " *indipendentemente dal sistema di intrusione utilizzato (quello dell'accesso diretto al computer ovvero occulto attraverso un programma spia), quando si vanno a recuperare e-mail ormai spedite o ricevute siamo di fronte ad un'attività intercettativa*". Invero il caso era peculiare, dei trafficanti comunicavano accedendo in rete ai messaggi in bozza della stessa utenza email; si tratta di una particolare modalità tendente ad una comunicazione occulta consentendo l'accesso contemporaneo a risorse accessibili da internet.

[12] In Giur. it., 2018, 1718, con la già citata nota di M. Minafra secondo cui "*sarebbe riduttivo, oltre che contrario alla stessa lettera della legge, ritenere la disposizione in questione dettata esclusivamente a tutela del segreto epistolare previsto nell'art.15 della Costituzione, dovendosi, piuttosto ritenere, storicizzando, che l'oggetto della protezione apprestata dall'ordinamento sia rappresentato dalla corrispondenza nella sua accezione più ampia, da intendere come ogni particolare forma di comunicazione della quale rappresenta il profilo statico, vale a dire la materializzazione del pensiero comunicato o da comunicare con "qualsiasi" mezzo anche i più innovativi come le piattaforme on-line*".

[13] Per la messaggistica tipo Whatsapp, con la diffusione della "crittografia end to end", che rende illeggibili messaggi al gestore del servizio, l'accesso ai server è ormai inutile. La giurisprudenza ha valutato spesso il caso del sistema BlackBerry che, però, ormai non è più in uso.

[14] Cass. III, n. 38681 del 26.4.2017 "*Per documento proveniente dall'imputato si intende, ai sensi dell'art. 237 cod. proc. pen., il documento del quale è autore l'imputato ovvero quello che riguarda specificamente la sua persona, ancorché da lui non sottoscritto, anche se sequestrato presso altri o da altri prodotto. (Fattispecie in cui la Corte ha ritenuto corretta l'acquisizione da parte del giudice di merito di messaggi inviati attraverso i social networks Whatsapp e Facebook dall'imputato ad una minore, e da questa messi a disposizione della polizia giudiziaria al momento della presentazione della querela).*".

[15] Per questa ragione qui non si fa riferimento alla giurisprudenza precedente che considerava l'attività di estrazione di dati dai supporti di memoria, anche da remoto, quale mera attività di

"copia" e non sequestro, appunto ritenendo che il "dato" non avesse la natura di cosa.

[16] Per una esposizione generale sulle modalità di ricerca della prova digitale, vedi L. Cuomo e L. Giordano, *Informatica e processo penale, in Processo penale e giustizia 4|2017*; S. Aterno, *Digital Forensics (Investigazioni informatiche), in Dig. pen., 2014, p. 217*

[17] Si potrebbe discutere di un eventuale archivio dei messaggi conservato dal gestore del servizio, ma le più recenti tecniche di crittografia adottate da tutti i principali operatori presumibilmente rendono illeggibili tali archivi.

[18] Dalle smartTV con microfono e telecamera, alle telecamere di sorveglianza con microfono installate nei domicili e collegate in rete, ai dispositivi tipo "Alexa" ….

[19] Altro tema, poi, riguarda "chi controlla i controllori". Si veda la vicenda Exodus, sopra richiamata in nota, nonché Brizzi, *il captatore informatico: un "Exodus" verso buone pratiche*?, in IlPenalista, 04 Settembre 2019. L'articolo espone le problematiche sorte, le sollecitazioni provenienti dal Garante per la privacy e le solo parziali soluzioni normative (i "*requisiti tecnici dei captatori tali da garantire che essi si limitino effettivamente ad eseguire le sole operazioni autorizzate*" che sono stati introdotti sembrano riguardare solo il captatore utilizzato per le intercettazioni ambientali).

[20] Invero, l'art. 271 cod. proc. pen. (divieti di utilizzazione) al comma 1-bis dispone "*1-bis. Non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo*". Può ritenersi che il riferimento ai "*dati*" (e non alle conversazioni) "*acquisiti al di fuori dei limiti di tempo … indicati nel decreto autorizzativo*" significhi che non sia consentito l'uso del captatore per acquisire dati se non autorizzato ex art. 266 cod. proc. pen.? Il riferimento, invero, appare troppo generico per trarne una tale conclusione.

[21] Si veda L. Giordano "*dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*", in Diritto penale contemporaneo, quanto a " *L'uso del captatore per la funzione di Keylogger. … La captazione delle e-mail "parcheggiate", di quelle "bozza" e delle "chat" non contestualmente al loro svilupparsi.*

[22] sul tema si veda L. Giordano, *Il ricorso al captatore informatico nei reati contro la pubblica amministrazione*, in G. Flora, A. Marandola (a cura di), La nuova disciplina dei delitti di corruzione, Pacini giuridica, Pisa, 2019, pag. 83 e ss.; Valli *La perquisizione informatica e la*

perquisizione "da remoto". IlPenalista, ottobre 2017. Dalle ampie argomentazioni risulta come, sul piano della normativa codicistica vigente, la perquisizione informatica "*da remoto*" non abbia alcuna disciplina particolare, ma è caratterizzata dalla difficoltà di riconoscere le garanzie difensive previste per quella "*in presenza*". Allo stato della disciplina positiva, quindi, l'evidente necessità di maggiori tutele per un tale tipo di operazione viene risolta con il rilievo della opportunità di uno specifico decreto motivato, non potendosi per il resto che invocare interventi delle SS.UU, che, come avvenuto per i "tabulati" e le videoriprese nel domicilio, hanno di fatto innovato rispetto alla normativa vigente.

[23] Si veda il commento di L. Giordano, *I messaggi di posta elettronica già inviati o già ricevuti dal destinatario e contenuti in una casella di posta elettronica possono essere acquisiti nel procedimento penale con un provvedimento di sequestro, nelle forme di cui agli artt. 253 e ss. c.p.p., oppure è necessario un decreto di intercettazione ex art. 266-bis c.p.p?,* in IlPenalista, settembre 2019.

[24] Invero, almeno allo stato, l'autorizzazione di tali sistemi appare quantitativamente alquanto moderata. Ciò sembra dovuto, più che ad un self restraint all'utilizzo di un'"arma" troppo "letale", fondamentalmente al costo di tale tipo di operazioni ed allo scarso successo dei tentativi di installazione: i sistemi noti (oggi, peraltro, ai fini dell'art. 266 cod. proc. pen. deve trattarsi di "programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia") richiedono una ingenuità dell'utente, indotto con vari trucchi ad aprire messaggi esca che consentono l'installazione del programma; perciò la percentuale di riuscita rispetto ai tentativi di installazione è, ragionevolmente, assai ridotto. Da valutare quale sarà il futuro di questi sistemi: da un lato l'eventuale riduzione dei costi e la maggior semplicità di inserimento, potrebbe portare ad un accrescimento della utilizzazione di tale sistema che ben potrebbe diventare di uso comune per il sequestro a sorpresa delle chat; dall'altra, invece, l'eventuale diffusione di programmi antiintrusione (come del resto sono già gli "antivirus" per i pc) nei dispositivi mobili potrebbe ridurre al minimo tale modalità di acquisizione delle prove.

[25] Sembra in parte orientarsi in questi termini Cass. VI, n. 43556 del 26.9.2019 (la quale parte proprio dalla regola di proporzionalità ed adeguatezza sviluppata per i dati informatici per farne un' applicazione in un caso di sequestro " eccessivo" di un archivio cartaceo). Si veda anche un commento in L. Nullo, "*Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*", in Proc. Pen. e Giust., 3/2020.

[26] Dalla lettura della motivazione, è proprio la situazione che si verificava nella vicenda sottesa alla decisione Cass. V, n. 48370 del 30.5.2017: la difesa considerava come un captatore informatico fosse stato utilizzato anche per l'acquisizione del materiale "statico" contenuto in un computer fisso. La soluzione adottata non è del tutto chiara, ma sostanzialmente si è ritenuto la piena utilizzabilità del materiale così raccolto. S. Aterno, *"La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screen shot. (Intercettazioni),* in Dir. Pen. e Proc. 8/2018, è critico per il ricorso sbrigativo al criterio della "prova atipica" per giustificare il dato tipo di intromissione; svolge quindi argomenti certamente rilevanti sul tema, dando atto di come le altre utilizzazioni del *Trojan*, quelle attualmente non disciplinate, rischiano di portare a *" L'imputato, di fronte ad una delle attività più invasive della propria riservatezza in tutta la storia delle indagini penali (anche preventive e di intelligence), non avrebbe neanche la possibilità di ricevere una notifica e impugnare un provvedimento (anche successivo ed eventualmente con ritardato deposito avverso il tribunale del riesame.* Si veda anche A. Testaguzza, *"Ancora in tema di captatore: le intercettazioni informatiche e telematiche. La Cassazione chiede il bis. (Intercettazioni informatiche e telematiche)",* in Giur. It. 11/2017. Anche la "informaticamente remota" sentenza Cass. V, sent. 16556 del 29.4.10 (cc. 14.10.09) rv. 246954, trovandosi di fronte al caso della captazione da remoto della documentazione memorizzata in un personal computer in uso all'imputato, definì la prova come "atipica".

[27] 27.2.2008, in Riv. Trim. Dir. Pen. Econ. 2009, 695. Si veda: **A. Venegoni**, **L. Giordano**, "*la corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici",* in in Diritto Penale Contemporaneo con riferimento alla Sentenza del 2008 *".... Corte tedesca, del 27 febbraio 2008 .... Dinanzi alle potenzialità operative del nuovo strumento, non era esclusa in assoluto l'ammissibilità di tale strumento d'indagine, ma venivano ritenute insufficienti le garanzie costituzionali a tutela della segretezza delle comunicazioni e dell'inviolabilità del domicilio. Per la prima volta nel panorama giuridico europeo, inoltre, veniva riconosciuta l'esistenza di un nuovo diritto costituzionale: il "diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici", inteso come espressione del più generale "diritto alla dignità" dell'individuo-utente. Questo nuovo diritto, secondo i giudici tedeschi, "protegge la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati". La declaratoria di incostituzionalità scaturiva dal contrasto tra l'attività di intelligence in argomento (la ricerca a distanza dei dati contenuti su dispositivi digitali) rispetto al nuovo diritto fondamentale, che tutela il cittadino*

digitale nell'uso delle tecnologie di informazione e di comunicazione in rete. Gli utenti, secondo questa decisione, godono di una legittima aspettativa di riservatezza rispetto ai dati ricavabili dall'uso della tecnologia informatica e devono essere tutelati contro l'accesso segreto. Il ricorso a nuove forme di investigazione tecnologica implica necessariamente un bilanciamento, da compiere a livello legislativo, con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo" quanto alla sentenza del 2016 "*La decisione, quindi, afferma che il paragrafo 20k del BKAG, che consente l'accesso ai sistemi informatici da remoto (tra i quali ... si citava anche l'accesso a disco rigido di un computer attraverso il meccanismo denomainto "Trojan"), non assicura una protezione sufficiente del nucleo profondo della vita privata*".

[28] Che era, invece, l'impostazione della giurisprudenza che, ancora con le SS.UU Tchmil del 24.4.2008, affermava che "*Una volta restituita la cosa sequestrata, la richiesta di riesame del sequestro, ... è inammissibile per sopravvenuta carenza di interesse, che non è configurabile neanche qualora l'autorità giudiziaria disponga, all'atto della restituzione, l'estrazione di copia degli atti o documenti sequestrati, dal momento che il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni. (Fattispecie relativa a sequestro di un computer e di alcuni documenti)*".

[29] Valutando se sia corretta l'equiparazione alle intercettazioni: non sembra scorretto affermare che la messaggistica istantanea non è affatto equivalente alla corrispondenza cartacea, semplicemente digitalizzata, ma è un equivalente della conversazione orale utilizzando messaggi scritti (e anche brevi messaggi vocali). E' un tipo di comunicazione "Half Duplex", in cui si comunica uno alla volta, comunque pienamente bidirezionale, come una conversazione telefonica.

[30] Si vedano, in particolare, C. Conti, *Sicurezza e riservatezza, in Diritto Penale e Processo, 11/2019* C. Conti, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo", in Diritto Penale e Processo, 9/2018.* In tali interventi si segnala il rilievo delle decisioni delle SSU Prisco e del giudice delle legge, sent, 320/2009 in tema di videoriprese di comportamenti non comunicativi quale esempio di non ammissibilità di prove non disciplinate dalla legge e che violino principi fondamentali (l'art. 14 Cost.), nonché delle decisione delle SSU Pasqua e della Corte costituzionale 20/2017 in tema di accesso occulto, con il sistema del "visto", alla posta del detenuto, da cui si desume il divieto di escludere le garanzie dei mezzi di prova tipici ricorrendo in via elusiva allo schema della prova atipica. Si veda anche M. Minafra, op. cit.

[32] Da vedere, poi, cosà sarà effettivamente sviluppato. L'individuazione di prodotti con caratteristiche ben specifiche e conoscibili renderebbe semplicissimo realizzare software di contrasto.