Corte di Cassazione, Sezione IV Penale, sentenza n. 40903 del 28 giugno 2016 e depositata il 30 settembre 2016

In un'indagine per associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti, gli inquirenti inserivano un *trojan* all'interno di un computer collocato all'interno di un Internet Point utilizzato dagli indagati per accedere a unico *account* di posta elettronica su "hotmail.com". Attraverso il *trojan* gli inquirenti acquisivano la *password* di accesso a tale *account* e la usavano per acquisire i messaggi di posta elettronica inviati e ricevuti nonché di quelli salvati nella **cartella "bozze"**, usata come sistema di "parcheggio" delle comunicazioni scambiate tra i membri dell'associazione.

di Milto Stefano De Nozza

E-MAIL PARCHEGGIATE SU *SERVER* ALL'ESTERO, SIMILITUDINE CON IL *CLOUD COMPUTING*: LA PAROLA DELLA CASSAZIONE

Milto Stefano DE NOZZA, Magistrato in servizio presso la Procura della Repubblica di Brindisi, applicato alla D.D.A. di Lecce, Magistrato responsabile della sala intercettazioni della Procura di Brindisi, Componente della commissione per il noleggio dei servizi di supporto alle attività di intercettazione, Magistrato di riferimento per l'informatica della Procura di Brindisi su incarico del Consiglio Superiore della Magistratura, Magistrato referente per i rapporti con la associazione antiracket Salento.

Continua incessante l'opera della giurisprudenza di legittimità tesa ad offrire, o quanto meno a tentare di offrire, il corretto inquadramento normativo delle sempre più numerose e sofisticate metodologie di captazione che l'evoluzione della tecnologia delle comunicazioni fornisce alle investigazioni, all'interno di un contesto, quale quello domestico, caratterizzato, altresì, da un incessante dinamismo delle contrapposte "tecnologie di elusione".

La Suprema Corte, invero, riunita nella sua più alta composizione, aveva già riconosciuto – almeno per ciò che riguarda i procedimenti di criminalità organizzata – la legittimità dell'uso del *virus* autoinstallante nell'attività di indagine, anche "*nei luoghi di privata dimora di cui all'art. 614 c.p., pur se non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa*"[1].
All'indomani del pronunciamento della Cassazione, l'interrogativo postosi dall'interprete nel turbinoso dibattito che ne era seguito, risultato essere tanto serrato quanto complesso era stato l'*iter* argomentativo seguito dalla Corte medesima, riguardava la possibilità, non nuova, di estendere il sigillo di legittimità offerto alle attività di intercettazione realizzate mediante il *trojan* per reati di criminalità organizzata anche alle indagini per crimini comuni.

Si è già avuto modo di evidenziare[2] come il supremo collegio, sebbene abbia certamente voluto limitare il proprio *dictum* ai soli procedimenti per delitti di criminalità organizzata, perché così richiesto nella ordinanza di remissione, non ha inteso negare, per ciò solo, contestualmente ed implicitamente, la legittimità del *trojan* laddove impiegato nei procedimenti per delitti comuni.
Resta fermo, tuttavia, così come precisato nel percorso motivazionale seguito dalla Corte, che l'utilizzo del *virus* autoinstallante per investigazioni afferenti procedimenti di criminalità comune necessiti di una prescrizione ulteriore, da contenersi nel decreto autorizzativo, avente ad oggetto l'indicazione del luogo in cui eseguire le attività di captazione; luogo che, salvo il sussistere del presupposto di legge, non potrà ricadere, pena l'inutilizzabilità delle stesse, nei luoghi di privata dimora, in linea con l'interpretazione fornita da solida giurisprudenza di legittimità dell'art. 614 c.p.

Allo stato dell'arte si può, quindi, affermare come l'uso del *trojan* sia da ritenersi sempre legittimo nell'ambito di un procedimento per delitti di criminalità organizzata, e che tanto possa dirsi anche per i reati comuni, a patto e condizione che nella richiesta del P.M., nel decreto del G.I.P. e/o nel decreto di esecuzione del P.M. vengano assicurate alcune necessarie precauzioni (*ex multis*, l'utilizzo del G.P.S. installato sul medesimo telefono; il dare disposizione alla P.G. di procedere all'ascolto in tempo reale delle intercettazioni e, conseguentemente, di sospendere la captazione non appena l'indagato abbia agganciato la cella della propria abitazione; nonché disattivare, comunque, l'intercettazione non appena la P.G. abbia la percezione che il soggetto stia per accedere in altri luoghi di privata dimora non previamente identificabili) evidentemente volte ad impedire potenziali captazioni nei luoghi di privata dimora.

Ebbene, a distanza di soli due mesi dal deposito delle motivazioni della sentenza Scurato, la IV Sezione della Suprema corte ritorna, con la sentenza in commento, sui rapporti tra la disciplina dei mezzi di ricerca della prova e la tecnologia delle comunicazioni, affrontando due tematiche di assoluto interesse investigativo e processuale: il regime acquisitivo delle *e-mail* c.d. "parcheggiate" e il *cloud computing*[3].

1 Cass. pen., Sez. Un., 28 aprile 2016, n. 13, *Scurato*;
2 M. S. DE NOZZA, *Intercettazioni mediante trojan: la decisione delle Sezioni Unite*, in "Sicurezza e Giustizia", 2016, n. III/MMXVI, pp. 17 ss.
3 Cass. pen., sez. IV, 28 giugno 2016, n. 40903;

Una compiuta analisi delle questioni appena citate necessita, tuttavia, di una preliminare disamina dell'orizzonte storico-fattuale su cui si è stagliata la sentenza in commento. Le indagini avevano disvelato l'esistenza di una associazione a delinquere di stampo transnazionale finalizzata al traffico di sostanze stupefacenti. Era emerso, altresì, come tutti gli indagati erano soliti mantenere i contatti attraverso la medesima postazione di un internet point, dal quale accedevano ad un'unica e comune casella di posta elettronica. Gli organi inquirenti avevano individuato le credenziali di accesso all'*account* – le quali risultavano in possesso di tutti gli indagati – grazie all'installazione di un *trojan* nel *client* che gli stessi erano soliti usare all'interno dell'*internet point* monitorato dagli investigatori.

Il flusso di comunicazioni – nelle parole stesse della decisione – avveniva per il tramite di una modalità "*singolare, ma non sconosciuta alla casistica criminale*", vale a dire attraverso il parcheggio delle *e-mail* nella "cartella bozze" dell'*account* comune di posta elettronica: la *mail*, quindi, veniva scritta, non inviata, ma semplicemente salvata nel *file* "bozze", per poi essere successivamente letta da altro indagato in occasione di un accesso successivo. La Suprema corte qualifica questa singolare modalità di comunicazione quale *"scambio comunicativo differito, in quanto sebbene la mail non [venga] inoltrata al destinatario, questi ne [prende] direttamente cognizione accedendo all'account di posta elettronica del mittente con la password di questi"*.
Ne discendere a parere della Corte che siffatto scambio di comunicazione, in quanto differito, debba esulare dal perimetro operativo delle intercettazioni, per essere correttamente ricompreso in quello del sequestro dei dati informatici.

Ad imporre una siffatta soluzione vi sarebbero, secondo i supremi giudici, perspicue ragioni logico-sistematiche.
Precisamente la Corte, senza esitazione alcuna, afferma, che per le *e*-mail c.d. parcheggiate *"si [è] in presenza di una attività che ricorda quella del sequestro di dati informatici e perciò si tratterebbe di una attività di indagine che non rientra nella disciplina delle intercettazioni e non necessita di alcuna autorizzazione del gip"*.
Escludere, tuttavia, la possibilità di acquisire tale flusso di dati mediante lo strumento delle intercettazioni, pone, a tutta evidenza, un problema interpretativo di una certa rilevanza, relativo ai potenziali effetti dirompenti e pregiudizievoli che, in applicazione della disciplina del sequestro, l'obbligo di notifica all'indagato produrrebbe sulle indagini in corso.
Così risolta la questione relativa alla cornice normativa di riferimento, i giudici di legittimità affrontano e risolvono, in termini negativi, una seconda e conseguente problematica, concernente l'attivazione della procedura della rogatoria attiva per il decreto di sequestro dei dati contenuti nelle *e-mail* parcheggiate (nel caso di specie l'*account* di posta elettronica era gestito da una società statunitense il cui *server* era allocato in territorio americano – *@hotmail*).
A tanto si dovrebbe ricorrere, nell'ottica della difesa, ai fini della corretta esecuzione del decreto di sequestro, perché acquisire i dati di un *server* allocato fisicamente nel territorio di uno Stato estero, comporta una limitazione della sovranità di quest'ultimo.

La risoluzione del quesito ha imposto alla Corte una riflessione preliminare sul tema del *cloud computing*, risultata essere di assoluto pregio esplicativo. Dal tema fuoriescono, chiaramente, tutti i casi di attività acquisitiva di dati contenuti in indirizzi di posta elettronica gestiti da società che si avvalgono di *server* allocati nel territorio dello Stato Italiano, per la manifesta ragione che in simili casi verrebbero meno i presupposti operativi della rogatoria attiva.
La Corte definisce il *cloud computing "quale tecnologia che permette di elaborare, archiviare e memorizzare dati grazie all'utilizzo di risorse hardware e software distribuite nella rete (si pensi per fare gli esempi più comuni a dropbox. Google drive. Icloud)"*.
In altri termini, il *cloud computing* attiene al fenomeno, in costante evoluzione, di spazi di memoria virtuale (anche molto estesi) generati da *server*, il cui accesso è consentito al solo titolare di credenziale e *password* e nei quali vengono archiviate foto, documenti di qualunque formato e genere, nonché video e numerose altre informazioni.
Si tratta, in buona sostanza, di un'area nella quale l'utente salva documenti personali, la cui acquisizione – laddove gli stessi appaiano decisivi e rilevanti per una attività d'indagine in corso – deve, evidentemente, avvenire nel pieno rispetto delle regole processuali, ai fini della utilizzabilità del risultato di prova acquisito.
La Suprema corte chiarisce, quindi, come il decreto di sequestro ex art. 254 e ss. c.p.p. avente ad oggetto le *e-mail* parcheggiate di un *account* straniero non richieda, a pena di inutilizzabilità, il ricorso alla rogatoria attiva in quanto *"la detenzione consiste nell'avere la disponibilità di una cosa, ossia nell'avere la possibilità di utilizzarla tutte le volte che sui desideri pur nella consapevolezza che essa appartiene ad altri"*;
Spiega che, in ragione di tanto, anche se i dati sono conservati in un *server* allocato all'estero, essi devono considerarsi fisicamente presenti sul territorio italiano, nonché nella piena disponibilità dell'indagato, atteso che il potere di disporre dei dati conservati in uno spazio di memoria virtuale lo esercita solo e soltanto chi è in possesso della relativa *password*[4].
A tutta evidenza, spiega la Corte, i dati contenuti in uno spazio virtuale di memoria, anche se generato da un server allocato all'estero, sono detenuti dal titolare delle credenziali di accesso e non dalla società che gestisce il *server* che genera lo spazio di memoria virtuale; ne consegue, come nel caso portato all'attenzione della Corte, che la piena disponibilità da parte dell'indagato dei documenti memorizzati virtuali in territorio nazionale, trascina con sé, quale naturale e logica conseguenza, la sola attivazione della procedura di sequestro senza rogatoria.

Ciò posto, la Corte prende posizione anche sulla modalità acquisitiva delle *e-mail* già inviate e/o ricevute, giungendo alla conclusione che per esse la cornice di copertura normativa possa e debba essere solo quella offerta dagli artt. 266 bis c.p.p., equiparando, quindi, il regime acquisitivo delle *e-mail* già ricevute e/o inviate con quella delle *e-mail* che vengono inviate e/o ricevute nel corso delle indagini.
Sul punto, invero, è dato ravvisare una radicale divergenza di prospettiva tra gli interpreti del diritto e in numerose altre decisioni della Suprema Corte secondo il regime acquisitivo delle *e-mai già inviate o ricevute* ricade sotto la copertura normativo del sequestro.

4 Sul punto la Corte fa ricorso ad una similitudine semplice, ma molto efficace: "è come avere la detenzione di un bene e che venga parcheggiato all'interno di un'area di proprietà altrui, in cui si disponga di un'area esclusiva recintata e chiusa a chiave. Quel bene è nella detenzione di chi ha la chiave non del proprietario del parcheggio che gli ha concesso l'area". Cass. pen., 28 giugno 2016, cit.

La Corte respinge, anzitutto, e a chiare lettere, l'orientamento prospettato da autorevole dottrina, secondo cui laddove non vi sia "contestualità" tra il momento in cui si invia un *e-mail* ed il momento in cui la stessa viene acquisita, il regime acquisitivo delle *e-mail* già inviate e/o ricevute, proprio perchè flusso di dati già esaurito, debba ricadere sotto l'egida del sequestro[5].
Rifiuta, altresì, l'altro criterio prospettatosi nel panorama giuridico, che fa leva sulle "modalità di effettuazione dell'atto", per cui se l'attività di acquisizione è svolta in maniera occulta, il regime normativo sarebbe quello delle intercettazioni, viceversa, se l'attività di acquisizione è compiuta a sorpresa, la disciplina applicabile sarebbe quella del sequestro.

Precisamente, nell'ottica della citata *opinio,* laddove l'acquisizione del flusso informativo avvenga mediante la duplicazione della casella di posta elettronica da parte del gestore, con il conseguente inoltro di tutte *le e-mail* al *server* della Procura della Repubblica, si sarebbe in presenza di una intercettazione di flussi informatici ex art. 266-bis c.p.p.; se, invece, l'acquisizione avvenga presso la società che gestisce la corrispondenza elettronica, ovvero accedendo direttamente al computer dell'interessato, l'attività di apprensione si tradurrebbe in una attività di sequestro.

Come accennato, tuttavia, la Suprema corte è persuasa di altra opinione. Essa rifiuta, difatti, tanto il "criterio della contestualità" quanto quello della "modalità di effettuazione dell'atto", per aderire al "criterio dell'inoltro".
Di seguito il passaggio argomentativo della decisione sul punto "*in realtà, alla luce del dettato normativo sopra richiamato, nella giurisprudenza di questa Corte di legittimità, anche a Sezioni Unite, si rinvengono elementi per poter affermare che il discrimen perché ci sia stato o meno flusso informativo - e quindi debba essere applicata la disciplina delle intercettazioni e non quella del sequestro - è nell'avvenuto inoltro del e-mail da parte del mittente. perciò ritiene il collegio che quanto alle e-mail inviate o ricevute la risposta da fornire al quesito circa l'esistenza o meno di una flusso informativo sia positiva*".

Ciò posto, pare opportuno tirare le somme di quanto fin'ora esaminato.
Con evidente complessità i giudici offrono due distinte soluzioni con riferimento al regime acquisitivo delle *e-mail* parcheggiate, e per ciò che riguarda le *e-mail* già inviate e/o già ricevute.
Si ritiene, tuttavia, di non poter condivide le conclusioni offerte dalla sentenza in commento.
È bene osservare come una pedissequa applicazione del "criterio dell'inoltro" farebbe dipendere il regime normativo applicabile da variabili indeterminate. Gli esempi, invero, potrebbero essere molteplici e numerosi così come quelli prospettati dalla Corte come ostativi all'applicazione del criterio della contestualità. Basti pensare alla caduta di potenza della rete da cui derivi il mancato recapito di una *e-mail* spedita ma mai giunta al destinatario, o anche per avvenuta cancellazione del relativo indirizzo di posta elettronica.
Il "criterio della contestualità" (attualità della comunicazione rispetto all'atto acquisitivo) appare, viceversa, effettivamente idoneo ad offrire i maggiori crismi di oggettività; per cui allorquando la captazione della *e-mail* avvenga *on real time,* ovvero in maniera contestuale alla sua trasmissione, dovrebbe ritenersi applicabile la disciplina delle intercettazioni; laddove, invece, l'acquisizione avvenga *off line,* si dovrebbe applicare la disciplina del sequestro.
A ben guardare il criterio temporale permette anche di risolvere i casi limite individuati dalla Corte quali ipotesi dimostrative della fallacia del criterio predetto.
Ed invero, in caso di *account* sotto intercettazione, le *e-mail* inviate ma non consegnate, ovvero le *e-mail* inviate, consegnate ma non lette, vengono comunque acquisite in tempo reale, vale a dire nello stesso istante del loro invio, al pari di quanto accade nelle ipotesi in cui vi sia un conversazione durante la quale un interlocutore rende una affermazione che non viene percepita dalla controparte per caduta di potenza della rete. In simili casi nessuno dubbio può, né potrebbe essere sollevato, in merito alla applicabilità della disciplina delle intercettazioni anche per le parole pronunciate ma non percepite dal destinatario.
Le perplessità diventano, quindi, palesi e non facilmente arginabili.

Le *e-mail* parcheggiate, costituendo uno scambio di comunicazione, nelle parole della Corte, "differito", non possono essere acquisite con lo strumento delle intercettazioni telefoniche. La sentenza in commento ritiene sufficiente lo strumento del sequestro, mancando, quasi a voler tenere un contegno omissivo, di prendere consapevolezza in ordine al fatto che il flusso comunicativo viene volontariamente differito solo per ragioni (criminose) di elusione di eventuali investigazioni in corso.
Le *e-mail* già inviate e/o ricevute possono essere acquisite con lo strumento delle intercettazioni, al pari delle *e-mail* che vengono inviate e/o ricevute in corso di attività di captazione.
Le soluzioni offerte, se possono convincere con riferimento al regime acquisitivo delle *e-mail* parcheggiate, non si prestano a tanto per ciò che riguarda le *e-mail* già inviate e/o già ricevute; quest'ultime, infatti – al contrario delle *e-mail* che vengono inviate e/o ricevute in corso di attività di captazione che rappresentano, evidentemente, il prodotto di un flusso di comunicazioni in essere e che, quindi, giustificano l'ovvio ricorso all'intercettazione, in quanto prodotto di un flusso digitale esaurito, ben dovrebbero essere acquisite con lo strumento del sequestro.
In attesa di un'ultima parola delle Sezioni Unite, questo è il sistema ad oggi delineato.

Un sistema inutilmente complesso nel quale il caso (nella misura in cui si abbia o meno la "sfortuna" di essere sotto intercettazione contestualmente allo scambio comunicativo tradizionale tramite *e-mail*), o soprattutto lo scaltro indagato e/o imputato (che opti, al fine di eludere le attività captative, per il salvataggio delle *e-mail* nella "cartella bozze"), sembra poter scegliere la disciplina da applicare (sequestro o intercettazione). ©

5 Il criterio temporale proposto dalla dottrina non convince la Corte in ragione dei dubbi che situazione ricorrenti potrebbero creare all'operatore del diritto: si pensi al caso di ritardo nella consegna del messaggio dal server del mittente a quello del destinatario, ovvero al caso di e-mail ricevuta ma non letta. In simili evenienze il criterio della contestualità temporale non offrirebbe all'interprete una soluzione ragionevole.