FiLOdiritto 15°
insieme dal 2001 la legge, il diritto, le risposte
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Di trojan-microspia, e-mail che non sono corrispondenza e della colpa veniale di chi usa server stranieri

26 ottobre 2016
Monica Alessia Senor, media LAWS

Di Monica Senor

Il caso

In un'indagine su di un'associazione per delinquere finalizzata allo spaccio di sostanze stupefacenti, gli inquirenti inserivano un trojan all'interno di un PC collocato all'interno di un Internet Point utilizzato dagli indagati per accedere ai loro account di posta elettronica aperti sul provider hotmail.com.

Attraverso il keylogger gli inquirenti acquisivano le password di accesso a tali account e le usavano per prendere visione dei messaggi di posta elettronica inviati e ricevuti nonché di quelli salvati nella cartella "bozze" (sistema usato dai membri dell'associazione come metodo di comunicazione sicura).

La sentenza

"*Poco rilevante, nel caso in esame, è l'utilizzo da parte degli inquirenti di un programma-virus (il c.d. trojan) inserito all'interno dei computer degli internet point frequentati dagli odierni ricorrenti. L'uso del trojan [omissis]è stato limitato, infatti, da quanto risulta dalle sentenze di merito all'acquisizione delle password di accesso agli account di posta elettronica … Si è usato il programma informatico, in altri termini, così come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali. Normalmente, invece, il trojan viene inserito al fine di visualizzare in tempo reale l'attività che veniva svolta su un determinato schermo …*".

"*Va anche aggiunto che nel caso che ci occupa siamo al di fuori della tutela costituzionale della corrispondenza. Indipendentemente che si vogliano ritenere le e-mail spedite e ricevute intercettabili o sequestrabili, non si tratta di corrispondenza … la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito …*".

I due passaggi citati, al di là del loro notevole impatto intrinseco, sono i caposaldi attorno a cui si sviluppa il percorso argomentativo della Corte di Cassazione, il quale si articola nel seguente iter logico:

1. un keylogger è equiparabile ad una microspia;
2. nel caso di specie, il keylogger è stato usato come una semplice microspia perché non ha svolto, come fanno normalmente i trojan, un'attività di monitoraggio in tempo reale dell'attività svolta sullo schermo (schermo?), per cui il suo utilizzo nell'attività di indagine è "poco rilevante";
3. peraltro, i messaggi di posta elettronica non rientrano nel concetto di corrispondenza costituzionalmente tutelata;
4. nel caso di specie, in ogni caso, le e-mail inviate e ricevute sono state acquisite applicando la disciplina delle intercettazioni ed il decreto autorizzativo del G.I.P. copre dunque in termini di garanzie l'operato della Procura;
5. par quanto concerne, invece, le e-mail salvate nella cartella "bozze" all'interno degli account di posta elettronica degli indagati aperti sul provider americano hotmail.com, trattandosi di un'attività di indagine che non rientra nelle intercettazioni di flussi di comunicazioni telematiche, non è necessaria l'autorizzazione del G.I.P.;
6. non rientrando tali bozze neppure nel concetto di corrispondenza non occorre neppure il rispetto della

Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

procedura di cui all'art.254 c.p.p.;

7. né, infine, può trovare applicazione l'art.254 *bis* p.p. in quanto, pur trattandosi di dati informatici, essi non sono da considerare detenuti dal fornitore del servizio di posta elettronica sui suoi server situati all'estero, bensì dal singolo utente che possiede la password di accesso all'account di posta.

Conclude la Cassazione scrivendo che: "… *basterebbe che l'utente si "poggi" su un server straniero per poter sottrarsi alla giurisdizione del proprio Paese. Il che, evidentemente, non può essere*."

Il commento

Esistono sentenze (per fortuna la maggior parte!) in cui le argomentazioni giuridiche conducono e giustificano il dispositivo e sentenze in cui un dispositivo prestabilito viene giustificato da motivazioni, spesso illogiche e partigiane, camuffate da argomentazioni giuridiche.

La sentenza in commento è della seconda specie e lascia attoniti.

Partiamo dalla fine.

La frase "*Ed allora basterebbe che l'utente si "poggi" su un server straniero per poter sottrarsi alla giurisdizione del proprio Paese*" fa rabbrividire!

Anziché essere tutori e paladini dei nostri diritti fondamentali, i Giudici di legittimità alimentano una cultura del sospetto che mette a rischio il concetto stesso di Stato di diritto e la presunzione di innocenza.

Sia chiaro, sin da subito: l'utente che sceglie di affidarsi ad un servizio cloud straniero non si sottrae affatto alla giurisdizione italiana. La giurisdizione permane immutata per qualsiasi fatto di reato commesso in tutto o in parte sul territorio italiano; cambiano, semmai, le regole da applicare per ottenere valide prove da portare in giudizio.

Certo, si dovranno seguire procedure di acquisizione probatoria più laboriose perché l'Autorità giudiziaria dovrà verosimilmente fare ricorso a rogatorie internazionali, ma bypassare con meschine argomentazioni giuridiche le regole previste dal codice di procedura penale a garanzia del giusto processo solo perché più faticose significa violare *in nuce* i diritti fondamentali dei cittadini.

Non è un approccio nuovo. Anzi, è esattamente la stessa ragione fieramente sbandierata dalle Procure per giustificare l'uso dei captatori informatici. In sintesi, si sostiene che non potendo più ricorrere alla storica collaborazione con gli operatori telefonici nazionali a causa dell'ampia diffusione di sistemi di comunicazione legati alla rete Internet, i cui fornitori di servizi sono prevalentemente allocati all'estero, i trojan rappresentano il sistema più facile ed immediato per acquisire alla sorgente elementi di prova utili per il perseguimento e la repressione dei crimini. Il fatto che i captatori informatici possano non essere compatibili con il dettato normativo ordinario e con le garanzie costituzionali è ritenuto un fattore del tutto irrilevante rispetto al fine perseguito.

Che però lo stesso tipo di ragionamento sia avallato dalla magistratura giudicante è cosa davvero preoccupante.

Chi scrive trova gravissimo che la Corte di Cassazione minimizzi le caratteristiche di un trojan come quello utilizzato nel caso di specie (che, si rammenta, era stato installato in un Internet Point pubblico con la conseguenza che sono stati acquisite le digitazioni sulla testiera non solo degli indagati, ma anche quelle di tutti gli onesti cittadini che frequentavano in quel frangente il locale), definendolo una comune microspia.

C'è una sostanziale differenza di funzioni tra un keylogger ed una cimice ed è una differenza che si ripercuote sui diritti potenzialmente compromessi dall'uno o dall'altra.

FiLOdiritto 15°
insieme dal 2001 la legge, il diritto, le risposte
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Come noto, la capacità intrusiva dei captatori non può essere neanche lontanamente paragonata a quella delle tradizioni microspie atte ad intercettare.

Né può dirsi che le garanzie difensive siano da considerare rispettate sol perché agli atti vi è un decreto autorizzativo del giudice che "copre" qualsiasi attività di indagine, a prescindere dalla sua esatta collocazione all'interno dei (tassativi) mezzi di ricerca della prova previsti dal codice di rito. Se è vero, infatti, che l'intervento del G.I.P. rappresenta la massima tutela per l'indagato perché garantisce una valutazione indipendente e *super partes*, è altresì vero che esso è richiesto in tema di intercettazioni perché si tratta di un'attività di indagine estremamente invasiva che viene svolta all'insaputa dell'indagato.

I presupposti che regolano perquisizioni e sequestri sono diversi e, sebbene sia sufficiente un decreto del Pubblico Ministero, si tratta di un'attività investigativa che viene preventivamente comunicata all'indagato e, qualora si tratti di dati informatici, richiede l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (art.247, comma 1 *bis*, c.p.p.).

Eseguire, grazie ad un captatore informatico, un'operazione di perquisizione e sequestro, travestendola giuridicamente da intercettazione al fine di poter indagare senza avvisare l'indagato, è lesivo dei diritti dell'indagato tanto quanto procedere senza decreto alcuno.

Ancor più sorprendente è che il nostro massimo organo giurisdizionale affermi che le e-mail non sono corrispondenza e ne neghi espressamente la tutela costituzionale.

Un conto, infatti, è dire che il disposto di cui all'art.254 c.p.p. si applica solamente al sequestro di corrispondenza presso i fornitori di servizi postali, un altro affermare *tout court* che le e-mail non sono corrispondenza.

In realtà, come visto, la legittimazione dell'uso del keylogger in quanto mera cimice (al fine di non violare i principi espressi dalle Sezioni Unite n. 26889/16) e l'affermazione che le bozze di e-mail in cloud non sono corrispondenza (al fine di non applicare il disposto di cui all'art.254 *bis* c.p.p.), sono percorsi argomentativi finalizzati unicamente a preservare l'acquisizione di prove che altrimenti avrebbero dovuto essere dichiarate inutilizzabili.

Ma il castello giuridico costruito dalla Cassazione non regge e lo dimostra la fallacia dell'analogia usata dalla stessa Corte a sostegno della sua tesi.

Si legge in sentenza (pagina 43) che la detenzione consiste nell'avere la disponibilità di una cosa e la disponibilità sulle bozze delle e-mail la esercita non il provider del servizio bensì l'utente che è in possesso della password per accedere all'account di posta: "*È come avere la detenzione di un bene 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*".

Bene. Ammettiamo che l'analogia calzi. Ora chiediamoci: se quel parcheggio non fosse in Italia, ma negli U.S.A., l'Autorità giudiziaria italiana come dovrebbe procedere per perquisire e sequestrare l'area di pertinenza dell'indagato, sebbene recintata e chiusa a chiave e di sua esclusiva disponibilità?

La risposta a questa semplice domanda vale più di tante disquisizioni giuridiche.

Redatto il 17 ottobre 2016

Articolo pubblicato in: Diritto penale, Diritto dellâ€™informazione, Diritto dell'informatica

FiLOdiritto 15°
insieme dal 2001 la legge, il diritto, le risposte
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

TAG: *investigazioni, indagini, Privacy, New Media, trojan*

Avvertenza