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

I captatori informatici a tre anni di distanza dalla sentenza Scurato delle Sezioni unite penali

24 Aprile 2019
Vincenzo Giglio

Abstract
Lo scritto fa il punto sullo stato dell'arte a distanza di tre anni dalla decisione delle Sezioni unite che hanno legittimato l'uso dei captatori informatici come strumento di intercettazione nei procedimenti di criminalità organizzata.
The paper focuses on the state of the art three years after the decision of the Joint Sections that legitimized the use of spyware as an instrument of interception in organized crime proceedings.

Indice
1. Premessa
2. Le rassicurazioni
3. Tre anni dopo
4. Qualche osservazione conclusiva

1. Premessa

Tre anni fa, le Sezioni unite penali emisero la sentenza 26889/2016, Scurato.
Due furono i punti di diritto affermati nell'occasione:
«***Limitatamente ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un "captatore informatico"*** *in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone, ecc.) – anche nei luoghi di privata dimora ex articolo 614 codice penale, pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa*».
«***Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'articolo 51, commi 3-bis e 3-quater, codice di procedura penale, ma anche quelli comunque facenti capo a un'associazione per delinquere, ex articolo 416 codice penale,*** *correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato*» [1].
Le Sezioni unite diedero in tal modo via libera all'uso di spyware del tipo Trojan Horse per scopi intercettivi.

Si tratta di veri e propri «***virus informatici che solitamente vengono installati da remoto inviando una e-mail o un sms al bersaglio prescelto*** *(un personal computer, uno smartphone o un tablet), beninteso all'insaputa di chi ne fa uso. Una volta completata l'operazione, il suo regista dispone di molteplici opzioni ed in particolare: il* ***controllo a distanza del dispositivo infettato*** *(l'operatore può servirsene senza limiti, compiendovi ogni tipo di attività); la* ***visualizzazione di tutte le operazioni*** *compiute dal detentore; la* ***visualizzazione e l'estrazione di tutti i dati*** *contenuti nel dispositivo; la sua messa fuori uso; l'* ***attivazione del microfono e della webcam del dispositivo*** *e quindi la possibilità di ottenere riprese audio e video. In sostanza,* ***l'operatore ha il completo controllo non solo delle attività informatiche compiute dall'utilizzatore del dispositivo ma anche dei suoi movimenti e delle sue comunicazioni. Quasi della sua vita, si potrebbe dire***» [2].

2. Le rassicurazioni

In vista dell'imminente decisione della questione sui captatori, il Procuratore generale presso la Suprema Corte depositò una memoria, offrendo alla riflessione delle Sezioni unite un articolato contributo.

Qui interessa ricordare soltanto due tra le tante proposizioni del PG. Entrambe decisamente metagiuridiche.

La prima: «*Egli constata la straordinaria velocità dei progressi delle tecnologie della captazione e, in parallelo, di quelle volte all'elusione della captazione (fondate in massima parte sulle tecniche di criptazione). Ne trae la convinzione che l'impiego di virus informatici, più che al potenziamento delle intercettazioni, serve in realtà a recuperare l'efficacia perduta o compromessa delle tecniche tradizionali. Invita quindi le Sezioni unite ad inserire anche questa esigenza nel complesso balance degli interessi e dei valori in gioco*» [2].

La seconda, verosimilmente dettata dalla consapevolezza di molteplici e non trascurabili preoccupazioni e rilievi provenienti dall'accademia e dalla società civile: «***La molteplicità di funzioni dei programmi informatici di cui si discute non deve indurre a credere di essere di fronte a strumenti onnipervasivi e onnipotenti****, suscettibili di dar vita ad un potere invasivo esercitabile senza limiti o in forme incontrollabili sotto il profilo tecnico o giuridico. Al contrario* ***è seriamente ipotizzabile l'apposizione di limiti tecnici preventivi all'impiego dei virus informatici*** *(ad es., inibendo a priori l'operatività di alcune delle loro molteplici funzioni acquisitive). Inoltre, ciò che più conta in questa sede, è possibile dettare i limiti giuridici delle modalità di utilizzo dei captatori (ad es. escludendo che i programmi di on line surveillance possano essere utilizzati per effettuare videoriprese o che i programmi on line search siano impiegati per acquisire dati, al di fuori o in contrasto con le regole in tema di perquisizioni e sequestri). Ancora una volta, dunque, come avviene del resto in altri delicatissimi campi dell'esperienza umana,* ***sono la legge ed il diritto a fissare i confini delle possibilità offerte dalla tecnologia****, commisurandole ai principi dello Stato democratico di diritto, ai diritti individuali ed alle esigenze e sensibilità della collettività*».

La decisione Scurato recepì largamente entrambe le suggestioni del PG: «***Le minacce che derivano alla società ed ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticare tecnologie e di notevoli risorse finanziarie*** - *ed oggi, anche dalla crescente diffusione ed articolazione su scala mondiale delle organizzazioni terroristiche le cui azioni sono finalizzate ad attentare alla vita ed alle libertà delle persone ed alla sicurezza collettiva* - ***richiedono una forte risposta dello Stato con tutti i mezzi che la moderna tecnologia offre*** - *e la vigente legislazione, nonché i principi costituzionali, consentono - per adeguare l'efficacia investigativa all'evoluzione tecnologica dei mezzi adoperati dai criminali.* ***Per quel che riguarda l'eventualità che lo strumento captativo in argomento possa produrre, in casi estremi, esiti lesivi della dignità umana, va osservato*** - *come opportunamente prospettato dai rappresentanti della Procura generale nella memoria in atti* - ***che si tratta di un pericolo che ben può essere neutralizzato con gli strumenti di cui dispone l'ordinamento****; ad esempio, «facendo discendere dal principio personalistico enunciato dall'articolo 2 della Costituzione, e dalla tutela della dignità della persona che ne deriva, la sanzione di inutilizzabilità delle risultanze di "specifiche" intercettazioni che nelle loro modalità di attuazione e/o nei loro esiti abbiano acquisito "in concreto" connotati direttamente lesivi della persona e della sua dignità***».

Il PG e le Sezioni unite mandarono così a tutti noi due messaggi forti e chiari:

- la lotta alla criminalità organizzata di ogni tipo ben giustifica un deciso aggiornamento delle tecniche investigative di contrasto;
- l'ordinamento e i suoi principi "nucleari" offrono tutti gli strumenti necessari per evitare che le nuove tecnologie sfuggano di mano agli operatori e diventino mezzi di violazione dei valori essenziali della persona umana.

> **Le Sezioni unite furono per la verità piuttosto parche nell'individuazione concreta delle trincee e degli sbarramenti di tutela ma uno non rinunciarono ad indicarlo. L'eventuale straripamento delle agenzie investigative e degli organi inquirenti poteva essere arginato attraverso la sanzione dell'inutilizzabilità dei risultati delle intercettazioni.**

In sintesi: beni umani primari come l'inviolabilità del domicilio, la libertà e la segretezza della corrispondenza e di ogni altra forma comunicazione, il diritto di libera manifestazione del pensiero sono adeguatamente tutelati dalla forza intrinseca del nostro ordinamento e dalla capacità dei suoi interpreti di tramutare quella forza in statuti garantistici coerenti alla sfida delle nuove tecnologie.

3. Tre anni dopo

Il tempo passato dalla decisione Scurato è ormai sufficiente per un bilancio dei suoi effetti e per la "taratura" della credibilità delle sue proposizioni di fondo.

…Le modifiche legislative

Il **Decreto legislativo 216/2017**, attuativo della Legge di delega 103/2017, **ha legittimato normativamente il ricorso ai captatori informatici**, interpolando il secondo comma dell'articolo 266 codice di procedura penalee aggiungendovi il nuovo comma 2-bis.

Ha modificato inoltre il comma 1 dell'articolo 267, così rendendo obbligatoria l'indicazione specifica nel decreto autorizzativo delle ragioni che rendono necessario l'uso del captatore.

Il decreto deve inoltre includere, quando autorizza intercettazioni collegate a delitti non compresi tra quelli descritti nei commi 3-bis e 3-quater dell'articolo 51 codice di procedura penale, i luoghi e il tempo in cui è consentita la captazione dei segnali vocali mediante l'attivazione del microfono.

È stato inoltre aggiunto il nuovo comma 2-bis, applicabile ai casi d'urgenza in cui è il pubblico ministero ad autorizzare interinalmente le intercettazioni tra presenti. La norma gli consente di disporre l'intercettazione mediante l'inserimento di un captatore su un dispositivo elettronico portatile ma solo nei procedimenti per i delitti indicati nei citati commi dell'articolo 51. È tuttavia imposta al PM una motivazione aggravata che dia conto dell'impossibilità di procedere per le vie ordinarie.

È stato ancora aggiunto un inciso al comma 4 che riguarda il caso in cui il PM procede alle operazioni di intercettazione non personalmente ma avvalendosi di un ufficiale di polizia. Se così accade, l'ufficiale è tenuto ad informare il primo dei contenuti delle comunicazioni e conversazioni captate prima di redigere i brogliacci. Questa disposizione serve a consentire al PM di avere il controllo in tempo reale dei risultati progressivamente acquisiti così che si ottemperi al divieto, posto dal nuovo comma 2-bis dell'articolo 268, di trascrivere anche sommariamente conversazioni o comunicazioni irrilevanti.

Alle modifiche introdotte direttamente nel corpo dell'articolo 267 bisogna aggiungere quelle che hanno interessato l'articolo 89 att. codice di procedura penale e realizzano i criteri di delega indicati nell'articolo 1 comma 84 lettera a) nn. 4 e 5.

Nel nuovo testo, **l'articolo 89 prevede infatti che, in caso di uso del captatore informatico, il verbale delle operazioni indichi il tipo di programma impiegato (che deve essere conforme ai requisiti tecnici stabiliti con decreto del Ministro della giustizia) e i luoghi in cui si svolgono le comunicazioni e conversazioni.**

Stabilisce inoltre che le comunicazioni intercettate siano trasferite esclusivamente verso gli impianti delle Procure della Repubblica e che, alla fine delle operazioni, il captatore deve essere disattivato e reso inservibile.

Ulteriori modifiche hanno riguardato l'articolo 270 codice di procedura penale al quale è stato aggiunto il comma 1-bis che ha escluso l'utilizzabilità a fini di prova dei risultati delle intercettazioni tra presenti acquisiti tramite captatore informatico per reati diversi da quelli cui si riferisce il decreto autorizzativo, fatta eccezione per il caso in cui siano indispensabili per l'accertamento di delitti per i quali sia obbligatorio l'arresto in flagranza.

All'articolo 271 è stato infine aggiunto il comma 1-bis che rende inutilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore nel dispositivo bersaglio e ogni altro dato acquisito oltre i limiti di luogo e di tempo fissati nel decreto autorizzativo.

Ulteriori modifiche sono state apportate dalla Legge 3/2019 (cosiddetta **legge spazzacorrotti**) che ha inserito riferimenti ai delitti dei pubblici ufficiali contro la pubblica amministrazione nell'articolo 266 comma 2-bis e nell'articolo 267 comma 1, terzo periodo.

…**Il crescente ricorso ai captatori informatici**

Come era prevedibile, investigatori e inquirenti stanno facendo un uso sempre più largo di intercettazioni mediante captatori informatici.

Le cronache giudiziarie riportano incessantemente, e spesso entusiasticamente [3], l'esito di inchieste condotte con questa modalità. Se ne loda l'efficacia, si inneggia alla bontà della scelta legislativa di estenderne l'uso ai reati contro la pubblica amministrazione e ci si rattrista che una decisione così ovvia non sia stata presa prima.

…La giurisprudenza

Non si vuole qui fornire un aggiornamento con caratteri di sistematicità.

Ci si limita quindi a una rapidissima sottolineatura delle linee interpretative di maggiore rilievo.

L'uso dei captatori, in generale, continua ad essere avallato senza alcuno scossone significativo e senza che siano stati finora sollevati dubbi sulla sua compatibilità costituzionale.

La scure dell'inutilizzabilità si è talvolta abbattuta su risultati intercettivi ottenuti con i Trojan, anche in vicende di particolare clamore mediatico (si veda Cassazione penale, Sezione 6, 45486/2018, che ha appunto dichiarato l'inutilizzabilità, per difetto di consistenza indiziaria e violazione dei termini di durata delle indagini, delle intercettazioni svolte nel procedimento che ha coinvolto l'imprenditore Alfredo Romeo nel caso CONSIP).

Non è stato tuttavia messo in discussione il granitico indirizzo (tra le tante, Cassazione penale, Sezione 6, 54535/2016) che nega l'esistenza di qualunque forma di inutilizzabilità derivata sicché «*una volta affermata l'inutilizzabilità di una certa captazione, la sanzione non precluderebbe l'uso del suo risultato come notitia criminis e quindi, ad esempio, come legittimo input per la richiesta di una nuova sequenza intercettiva o per altre attività investigative. Il frutto dell'albero avvelenato non sarebbe perciò considerato avvelenato anch'esso e non sarebbe condannato alla distruzione ma rimarrebbe a disposizione degli inquirenti per gli scopi predetti*» [2].

La stessa considerazione vale per un altro aspetto di non poco momento.

È ovviamente il pubblico ministero a stabilire la cornice iniziale del procedimento, spetta a lui comporre la contestazione iniziale.

Ne deriva che è un organo di parte, sia pure pubblico, a determinare solitariamente, attraverso le imputazioni formulate, le condizioni che legittimano il ricorso ai captatori informatici.

C'è di più. Se i successivi vagli giurisdizionali sconfessassero la configurazione iniziale delle accuse ed escludessero le fattispecie alle quali è legata la possibilità normativa di usare i captatori, i relativi risultati rimarrebbero pienamente utilizzabili poiché, per costante giurisprudenza, ciò che conta è che le intercettazioni siano state autorizzate in un momento in cui erano presenti le condizioni di legge, tra le quali una contestazione provvisoria per una fattispecie compresa nel catalogo dei reati che consentono l'uso dei Trojan. **Le cose possono poi cambiare, le cornici scelte dal PM possono essere smentite, ma i risultati delle intercettazioni rimangono fermi e pronti all'uso**.

Si chiude segnalando infine che in questi tre anni sono anche spuntate decisioni (il pensiero va a Cassazione penale, Sezione 6, 40903/2016 [4]) che ha addirittura avallato l'uso dei captatori per l'acquisizione delle credenziali di accesso ad un account di posta elettronica e delle mail conservate in bozza) che sembrano massimamente incoerenti agli auspici delle Sezioni unite.

> **Che dire? Si fatica a scorgere nella produzione giurisprudenziale di legittimità il baluardo a difesa dei diritti umani preconizzato dalla sentenza Scurato.**

…La cronaca più recente

È di questi giorni la notizia [5] di un'indagine condotta dalla Procura della Repubblica di Napoli che ha ad oggetto l'uso asseritamente indebito di uno spyware, sviluppato da un'azienda calabrese.

Sembrerebbe, a giudicare dai resoconti di stampa, che questo virus, distribuito su dispositivi Android, e infettato subdolamente attraverso app accessibili su Google Play Store, abbia infettato migliaia di PC, tablet e smartphone dopo essere riuscito ad eludere i sofisticati sistemi di controllo interno di Google.

La cosa inquietante e al tempo stesso surreale è che il software sarebbe stato in realtà sviluppato per scopi intercettivi e come tale venduto a numerosi uffici italiani di Procura.

Senza contare che l'azienda che lo produce sembrerebbe avere tra i suoi clienti primarie aziende pubbliche e private e numerosi enti locali.

Chiaro che si tratta di un'inchiesta che sta muovendo adesso i suoi primi passi sicché la tesi accusatoria deve essere ancora verificata attraverso plurimi vagli giurisdizionali.

Eppure queste considerazioni di prammatica non eliminano l'inquietudine e, soprattutto se valutate congiuntamente alle non poche vicende affini che la cronaca ci ha consegnato negli scorsi anni [2], rendono attuale una volta di più la domanda *Quis custodiet ipsos custodies*?

4. Qualche osservazione conclusiva

È nella percezione comune che si vive in anni in cui lo spettro del Grande fratello orwelliano si agita sempre più freneticamente.

Come se ognuno si sentisse spiato e al tempo stesso fosse curioso dei segreti altrui.

Le istituzioni pubbliche appaiono tutt'altro che estranee al fenomeno. Lo cavalcano, vi partecipano, vi intravedono un *passepartout* buono per tutti gli usi cui si può ricorrere per la lotta al nemico di turno (che cambia secondo la sensibilità e le priorità elettorali della maggiornza in sella, fermo restando che uno, due, tanti nemici sono necessari nel nostro tempo per coagulare consensi e definire linee ideologiche e politiche).

> **Si viene così abbandonando o minimizzando progressivamente i capisaldi della democrazia, si impoveriscono garanzie essenziali di libertà, si chiede di rinunciare a porzioni sempre più grandi di beni che invece dovrebbero essere indisponibili e si offre in cambio sicurezza sociale, spesso contro pericoli artificiosamente creati o aumentati.**

È proprio il caso di parlare di realtà potenziata.

Non sembra uno scambio conveniente ma piuttosto un patto leonino.

Per visualizzare la sentenza clicca qui.

Note

[1] Per una riassunzione del dibattito, interpretativo e non solo, che precedette e seguì la decisione Scurato, sia consentito il rinvio a V. Giglio, *I virus informatici per scopi intercettivi nei procedimenti di criminalità organizzata: mezzi di cura o agenti patogeni?* e, dello stesso autore, *Captatori informatici per scopi intercettivi: il dibattito dopo la sentenza Scurato delle Sezioni unite penali*, entrambi reperibili su questo portale agli indirizzi: https://www.filodiritto.com/articoli/2016/06/i-virus-informatici-per-scopi-intercettivi-nei-procedimenti-di-criminalit-organizzata-mezzi-di-cura-o-agenti-patogeni.html e https://www.filodiritto.com/articoli/2017/01/captatori-informatici-per-scopi-intercettivi-il-dibattito-dopo-la-sentenza-scurato-delle-sezioni-unite-penali.html

[2] V. Giglio, *I virus informatici…*

[3] Un esempio tra tutti: **G. Pipitone,** *Sanità Umbria, l'incontro tra l'arrestato e la presidente registrato dal trojan: così l'Anticorruzione ha blindato l'inchiesta*, Il Fatto Quotidiano, edizione web del 13 aprile 2019, reperibile al seguente link: https://www.ilfattoquotidiano.it/2019/04/13/sanita-umbria-lincontro-tra-larrestato-e-la-presidente-registrato-dal-trojan-cosi-lanticorruzione-ha-blindato-linchiesta/5107726/

[4] **V. Giglio,** *Captatori informatici per scopi intercettivi…*

[5] M. Piras, *Tutti gli affari di eSurv, la società dello spyware Exodus*, Startmag, 1 aprile 2019, reperibile al link:
https://www.startmag.it/innovazione/tutti-gli-affari-di-esurv-la-societa-dello-spyware-exodus/

Letture consigliate

Recentemente il Garante per la protezione dei dati personali ha pubblicato sul suo sito web una segnalazione al Parlamento e al Governo sulla disciplina
delle intercettazioni mediante captatore informatico. Per visualizzare il documento, clicca qui.

TAG: *captatori informatici, trojan, penale, privacy, costituzionale*
