EDITORIALE

La difficile vita dell'agente ... "captatore"

Con la recente sentenza della cassazione n. 27100 del 26 giugno 2015 si è riaperto il dibattito sull'utilizzabilità dell'agente "captatore" che successivamente, il 5 luglio, ha acquisito una dimensione mondiale a causa del caso "Hacking Team". Il problema delle garanzie delle attività svolte dal programma informatico che opera per finalità di polizia, del tutto simile ad un *trojan*, era già conosciuto dagli esperti di *digital forensics* ed ora, grazie alla pluralità di seminari pubblici che sono seguiti alla nota vicenda, è alla portata di tutti.

Per mezzo di esso gli investigatori riescono a rilevare e a registrare tutto ciò che avviene nel dispositivo in cui è installato. Come lavora? Essendo a tutti gli effetti un trojan esso per definizione contiene istruzioni "maligne", dove l'aggettivo in questo caso assume il senso di "estranee" ovvero le istruzioni inducono un comportamento non previsto dalla macchina che ne è vittima. Il *trojan* quindi esegue operazioni per le quali il computer, tablet, smartphone non sono stati progettati; da qui nasce il timore sulle garanzie di operabilità, essendo stato "alterato" lo stato di funzionamento normale. Anche i risvolti pratici non sono aspetti di secondo ordine: il *trojan* apre a tutti gli effetti una vulnerabilità che altri, semmai prima di lui, hanno cercato di aprire. A questo punto già si insinua il dubbio che potremmo perderne il controllo completo. Inoltre, il *trojan* può essere sviluppato da un'azienda privata, allora la questione si complica non poco perché il controllo si può perdere del tutto. Vale la pena ricordare che tale situazione non può accadere nelle intercettazioni tradizionali, per intenderci quelle telefoniche, dove il gestore della rete opera su richiesta dell'Autorità Giudiziaria e tutte le sue attività sono tracciate. E dove, soprattutto, l'intercettazione è "pulita" nel senso che viene effettuata sulla rete, fuori dall'ambito del terminale dell'utente, e realizzata come copia integrale del traffico.

Queste considerazioni, sintetizzate per esigenze redazionali, sono state già analizzate all'interno di questa rivista ("***CALEA II, Risks of Wiretap Modifications to Endpoints***", n.2/2014) quando è stata richiamata la proposta di modifica al **CALEA Act**, la legge sulle intercettazione degli USA: l'idea di base è molto semplice e sposta la discussione su un piano sicuramente più interessante ed evoluto. Visto che il *trojan* non fornisce garanzie circa un risultato che non sia influenzato dallo stesso *trojan*, perché non mettersi d'accordo con i produttori del sistema operativo di tali dispositivi per aprire canali di tele-controllo in modo regolamentato? Lo studio di 19 esperti mondiali di comunicazioni, cifratura e intercettazioni circa i rischi derivanti dalle modifiche che si vorrebbero introdurre nel CALEA Act, pubblicato il 17 marzo 2013, afferma che obbligare i creatori di software, i *service provider* e tutti gli attori responsabili per i "punti finali" delle comunicazioni digitali (computer, tablet o smartphone) a riscrivere il codice e riprogettare l'*hardware* per facilitare le intercettazioni (legali) non farebbe altro che rendere più facile il lavoro dei *cyber*-criminali.

Se questo non bastasse, la recente sentenza della cassazione 27100/2015 ha anche stabilito che le fonti di prova possono essere non utilizzabili. Nel caso specifico il ricorrente contestava, per violazione di legge e vizio di forma, l'intercettazione d'urgenza telematica disposta dal PM tramite agente intrusore di tutto il traffico dati e di tutte le conversazioni tra presenti, mediante l'attivazione del microfono e della videocamera dello *smartphone*. La Cassazione ha ritenuto fondato lo specifico ricorso perché l'attivazione del microfono dà luogo ad un'intercettazione ambientale, ma l'art. 266, comma 2, cod. proc. pen., nel contemplare l'intercettazione di comunicazioni tra presenti, si riferisce alla captazione di conversazioni che avvengano in un "determinato" luogo, individuato *ab origine*, e non ovunque. Il decreto autorizzativo deve individuare, con precisione, i luoghi nei quali dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo ammissibile un'indicazione indeterminata o addirittura l'assenza di ogni indicazione.
Simile considerazione viene fatta circa le riprese effettuate da remoto attraverso la telecamera dello *smartphone*. Occorre verificare che non siano state effettuate videoregistrazioni all'interno di luoghi di privata dimora o, comunque, tali da imporre la necessità di tutelare la riservatezza personale. In caso contrario le videoregistrazioni, ai fini dei procedimento penale, sono acquisite illecitamente e sono perciò inutilizzabili.

Da ultimo anche il Garante della privacy è intervenuto, proprio portando ad esempio la citata sentenza che confermerebbe le preoccupazioni dallo stesso già espresse, a proposito dell'inutilizzabilità degli elementi di prova ottenuti con tecniche investigative atipiche, non circondate da sufficienti garanzie, in occasione dell'emendamento proposto al decreto-legge anti-terrorismo - poi stralciato - che avrebbe legittimato le intercettazioni da remoto. ©

Giovanni Nazzaro