Con il trojan si può intercettare anche il cellulare dei parlamentari?

La legge **n. 3 del 9 gennaio 2019** (c.d. “spazza corrotti”), nel modificare gli artt. 266 e 267 del codice di procedura penale, ha ampliato l’utilizzo delle **intercettazioni** anche per i **delitti dei pubblici ufficiali contro la pubblica amministrazione** puniti con la pena della reclusione non inferiore nel massimo a cinque anni.

È noto che tra le diverse forme di intercettazione vi possono essere quelle c.d. “ambientali” cioè quelle in grado appunto di “intercettare” conversazioni tra presenti in un determinato ambiente.

Ultimamente, gli strumenti in uso sono diversi e tra questi grande risalto mediatico (dopo il caso del **CSM**) è stato rivolto ai *trojan*.

Grazie ai *trojan* qualsiasi apparato telefonico mobile può diventare uno strumento di intercettazione ambientale.



Tra le varie criticità dell’uso dei ***trojan*** **come intercettazione,** possiamo tenere in considerazione due temi principali.

Il primo, ovviamente, riguarda la tutela dei dati personali

Invero, già con deliberazione del luglio 2016 il CSM aveva recepito le migliori prassi da seguire in caso di compilazione dei "brogliacci" e cioè quello di evitare che venissero annotate "intercettazioni irrilevanti" (cioè intercettazioni palesemente estranee alle esigenze investigative e/o processuali, alla dimostrazione dei fatti costituenti reato e alla relativa responsabilità) capaci però di divulgare e quindi trattare dati personali senza alcuna valida base giuridica e talvolta a divulgare dati particolari (ex sensibili) irrilevanti ai fini delle indagini.

Sul punto il CSM, nella citata deliberazione, aveva stilato un protocollo virtuoso per effettuare quella attività di filtro per la connaturale esigenza di ricercare il giusto equilibrio tra valori costituzionali, nessuno dei quali è tanto prevalente da imporre automaticamente il sacrificio dell'altro.

Ultimamente, il ricorso ai *trojan* come strumento di intercettazione è stato ampiamente criticato dallo stesso Garante.

Nei vari interventi sul caso "**exodus**", Soro ha avuto modo di affermare che *"E' un fatto gravissimo. La notizia dell'avvenuta intercettazione di centinaia di cittadini del tutto estranei ad indagini giudiziarie, per un mero errore nel funzionamento di un captatore informatico utilizzato a fini investigativi, desta grande preoccupazione e sarà oggetto dei dovuti approfondimenti, anche da parte del Garante, per le proprie competenze. La vicenda presenta contorni ancora assai incerti ed è indispensabile chiarirne l'esatta dinamica…Ciò che, tuttavia, emerge con evidenza inequivocabile è la notevole pericolosità di strumenti, quali i captatori informatici, che per quanto utili a fini investigativi*

rischiano, se utilizzati in assenza delle necessarie garanzie anche soltanto sul piano tecnico, di determinare inaccettabili violazioni della libertà dei cittadini…Tali considerazioni erano state da noi rivolte al Governo, in sede di parere tanto sullo schema di decreto legislativo di riforma della disciplina intercettazioni che ha normato il ricorso ai trojan, quanto sullo schema di decreto attuativo che avrebbe, appunto, dovuto introdurre garanzie adeguate nella scelta dei software da utilizzare. E' indispensabile trarre, da questa vicenda, la determinazione necessaria per impedire ulteriori violazioni in futuro, nella consapevolezza di come non possano tollerarsi errori in un campo così sensibile, perché incrocia il potere investigativo e il potere, non meno forte, della tecnologia. Strumenti investigativi così delicati devono certamente essere disponibili gli organi inquirenti come prevede la legge, ma nel rispetto di garanzie elevate per tutelare la libertà dei cittadini"

Il secondo tema ha profili prettamente processuali di utilizzabilità delle intercettazioni da *trojan*

Invero, il richiamato caso del CSM ha evidentemente sottolineato che uno dei vari pericoli dell'**intercettazione** (diremmo "indiscriminata") è che questa **possa essere dichiarata inutilizzabile,** laddove ad esempio si verifichino intercettazioni di conversazioni di parlamentari.

Infatti, il regime previsto dalla Legge 20 giugno 2003, n. 140 in merito art. 68 Cost. distingue le **intercettazioni del parlamentare** in "**dirette**", "**indirette**", "**casuali o fortuite**" (sulla distinzione fra intercettazioni "*dirette*"/"*indirette*", da una parte, e "*casuali*" o "*fortuite*", dall'altra, si possono citare le seguenti sentenze della Corte Costituzionale n. 114

e n. 113 del 2010, n. 390 del 2007; ordinanza n. 263 del 2010).

Sappiamo che per poter intercettare direttamente o indirettamente un parlamentare, deve essere richiesta **l'autorizzazione preventiva**, **a pena di inutilizzabilità**, alla Camera di appartenenza.

In quelle c.d. "casuali o fortuite"esse non andrebbero immediatamente trascritte, ma *meramente indicate* nel brogliaccio con la dicitura "***conversazione casualmente captata con parlamentare***", dandone immediata informativa al pubblico ministero per le sue valutazioni, cioè per verificare se le intercettazioni siano in realtà indirette o dirette e quindi potenzialmente inutilizzabili ovvero sia necessaria **un'autorizzazione successiva**.

Invero, nel caso di intercettazioni casuali è prevista la possibilità di **autorizzazione successiva** a mente dell'art. 6 della Legge 20 giugno 2003, n. 140, laddove sia necessario utilizzare contro il parlamentare quelle intercettazioni già acquisite e rispetto alle quali, proprio per il carattere imprevisto dell'interlocuzione del parlamentare, l'autorità giudiziaria non avrebbe potuto, neanche volendo, munirsi preventivamente dell'autorizzazione della Camera d'appartenenza.

Incidentalmente, deve essere chiarito che le intercettazioni seppur inutilizzabili per il parlamentare sono perfettamente producibili nel processo riguardanti il terzo, cioè il soggetto intercettato insieme al parlamentare (sul tema si veda Corte di Cassazione Penale, Sez. II, ud. 16.11.2012, dep. 22.2.2013, n. 8739)

A questo punto è bene considerare che anche l'intercettazione da *trojan* deve rispettare le tutele di protezione delle comunicazioni e conversazioni del parlamentare.

Seguendo la lettura costituzionalmente orientata offerta dalla

recente sentenza n. 38/2019 della Corte Costituzionale sull'art. 68, terzo comma, Cost. (sul tema dei tabulati telefonici riguardante un parlamentare); potremmo considerare applicabile tale impianto argomentativo anche all'utilizzo dei *trojan* (equiparabile in tutto e per tutto ad intercettazioni vecchio stile) e per la quale deve essere sempre richiesta alla Camera, alla quale il parlamentare appartiene o apparteneva, l'autorizzazione ad utilizzare le conversazioni o comunicazioni intercettate, anche frutto di procedimenti riguardanti terzi.

Sul punto osserviamo che l'art. 68 costituisce una maggiore garanzia della libertà e della segretezza di ogni forma di comunicazione, già assicurata dall'art. 15 Cost.

Invero, la *ratio* della garanzia prevista all'art. 68, terzo comma, Cost. non mira a tutelare un diritto individuale (la riservatezza del parlamentare), ma a proteggere la libertà della funzione che il parlamentare esercita, in conformità alla natura stessa delle immunità parlamentari, volte primariamente alla protezione dell'autonomia e dell'indipendenza decisionale delle Camere rispetto ad indebite invadenze di altri poteri, e solo strumentalmente destinate a riverberare i propri effetti a favore delle persone investite della funzione (sentenza Corte Costituzionale n. 9 del 1970).

Inoltre, l'art. 68, terzo comma, Cost. stabilisce chiaramente la necessità dell'autorizzazione della Camera d'appartenenza «per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza».

Si tratta, in tal caso, di un'autorizzazione preventiva, che precede il compimento dell'atto d'indagine.

La Corte Costituzionale (nella sentenza n.38/2019) ha, poi, precisato che l'autorizzazione deve essere preventivamente

richiesta non solo se l'atto d'indagine sia disposto direttamente nei confronti di utenze intestate al parlamentare o nella sua disponibilità (intercettazioni cosiddette "**dirette**"), ma anche tutte le volte in cui la captazione si riferisca a utenze di **interlocutori abituali del parlamentare**, **o sia effettuata in luoghi presumibilmente da questo frequentati**, al precipuo scopo di conoscere il contenuto delle conversazioni e delle comunicazioni del parlamentare stesso.

Ai fini della richiesta preventiva dell'autorizzazione, ciò che conta, in altre parole, non è la titolarità dell'utenza o del luogo, ma la direzione dell'atto d'indagine (sentenza Corte Costituzionale n. 390 del 2007).

Come ricordato dalla stessa Corte Costituzionale (sentenza n.38/2019) la tutela della corrispondenza di cui all'art. 15 Cost. riguarda tutti i soggetti dell'ordinamento, e deve riguardare anche i **dati "esterni"** di una comunicazione cioè quei dati ricavabili da qualsiasi strumento che consente, in virtù dell'evoluzione tecnologica, il tracciamento di localizzazioni e spostamenti dei titolari di apparati mobili.

Ancora, il significato da attribuire a «conversazioni o comunicazioni», induce a ritenere che al contenuto di una conversazione o di una comunicazione, siano accostabili, e risultino perciò protetti dalle garanzie costituzionali, anche i dati puramente storici ed esteriori, in quanto essi stessi "fatti comunicativi".

Del resto, il termine «comunicazioni» ha, tra i suoi comuni significati, quello di «contatto», «rapporto», «collegamento», evocando proprio i dati.

Pertanto, il *trojan* (come già argomentato per il "tabulato telefonico" nella citata sentenza n.38/2019) può aprire squarci di conoscenza sui rapporti di un parlamentare, specialmente istituzionali, «di ampiezza ben maggiore rispetto alle esigenze di una specifica indagine e riguardanti altri

soggetti (in specie, altri parlamentari) per i quali opera e deve operare la medesima tutela dell'indipendenza e della libertà della funzione» (sentenza Corte Costituzionale n. 188 del 2010).

https://www.key4biz.it/con-il-trojan-si-puo-intercettare-anche-il-cellulare-dei-parlamentari/262991/

Hackers Favoring Shimmers Over Skimmers for ATM Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dpk4Sfi-GYM/hackers-favoring-shimmers-over-skimmers-atm-attacks

---

Telcos Pwned: Multi-Wave Attacks Stealing 'Obscene Amount of Data' From Providers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/FwvSVtGf9ZA/telcos-pwned-multi-wave-attacks-stealing-obscene-amount-data-providers

Cyberwar Usa-Iran, Teheran assicura: ‘Nessun attacco americano è riuscito’

Secondo quanto riporta il *New York Times*, **Washington** ha sferrato un’offensiva cyber lo scorso giovedì contro l’**Iran** prendendo di mira sistemi che vengono impiegati per l’impostazione di azioni militari e per il controllo dei lanci di missili di **Teheran**.

I servizi segreti **Usa** credono ci sia proprio l’Iran dietro l’attacco alle **petroliere** nel **Golfo del’Oman**.

L’attacco dello **Us Cyber Command** è stato portato a termine lo stesso giorno in cui il presidente **Donald Trump** ha fermato i raid aerei contro stazioni radar e batterie missilistiche di **Teheran**.

La risposta dell’Iran

L’Iran intanto ha negato che i cyberattacchi ai suoi sistemi di difesa rivendicati nelle scorse ore dagli Stati Uniti abbiano avuto successo.



"Nessun attacco da parte degli Usa è stato condotto con successo", ha scritto su **Twitter** il ministro delle Telecomunicazioni di **Teheran**, **Mohammad Javad Azari Jahromi.**

"*Lo scorso anno abbiamo sventato non uno ma 33 milioni di attacchi con lo scudo* ***Dejpha***", ha aggiunto il ministro iraniano, sostenendo che il suo Paese *"sta affrontando il cyber terrorismo – come Stuxnet".* **Stuxnet** è un virus informatico di sospetta produzione israeliana e americana che ha danneggiato in passato impianti nucleari di **Teheran**.

Cybercom

Trump ha dato una significativa autonomia a **CYBERCOM**, il commando delle forze armate statunitensi per le operazioni cyber, e lo ha autorizzato a condurre attacchi offensivi contro avversari stranieri durante la sua presidenza. La nuova strategia consente al commando di condurre alcune delle sue operazioni senza consultare i funzionari della Casa Bianca o altre agenzie governative.

Secondo il **Wall Street Journal,** attuali ed ex funzionari statunitensi dicono che l'Iran potrebbe tentare di lanciare attacchi cibernetici contro gli Stati Uniti alla luce delle ostilità.

Nel 2016, il Dipartimento di Giustizia ha accusato sette iraniani di aver presumibilmente coordinato attacchi

informatici finanziari che hanno portato centinaia di migliaia di clienti a non poter accedere ai propri account e decine di milioni di dollari spesi dalle aziende che tentano di rimanere online attraverso questi attacchi.

https://www.key4biz.it/cyberwar-usa-iran-teheran-assicura-nessun-attacco-americano-e-riuscito/262770/

New Attack Delivers FlawedAmmyy RAT Directly in Memory

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bqbzRiZl-pY/new-attack-delivers-flawedammyy-rat-directly-memory

---

Mac Malware Delivered via Firefox Exploits Analyzed

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/u3-O6WxbFU4/mac-malware-delivered-firefox-exploits-analyzed

---

Ex-Senate Aide Sentenced to 4 Years in Prison for Data Leak

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/qHgQhSzMYEo/ex-senate-aide-sentenced-4-years-prison-data-leak

---

Massive Data Breach at Canada Credit Union Giant Desjardins

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/aLXDI1aYVQE/massive-data-breach-canada-credit-union-giant-desjardins

---

Mozilla Patches Second Firefox Zero-Day Used in Cryptocurrency Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/lMKWlbWCRD4/mozilla-patches-second-firefox-zero-day-used-cryptocurrency-attacks

Russia-Linked Hackers Hijack Infrastructure of Iranian Threat Group

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ZJ9lOg_1Tv4/russia-linked-hackers-hijack-infrastructure-iranian-threat-group