2° COMMISSIONE GIUSTIZIA DEL SENATO

AUDIZIONE 12/01/2023

INDAGINE CONOSCITIVA SUL TEMA DELLE INTERCETTAZIONI: AUDIZIONI DEL PRESIDENTE DELL'ASSOCIAZIONE NAZIONALE DEI MAGISTRATI, DEL PRESIDENTE DELL'UNIONE DELLE CAMERE PENALI ITALIANE E DI UN CONSULENTE DI INFORMATICA FORENSE

Prof. Ing. Paolo Reale

Esperto di informatica forense

Firmato digitalmente da

PAOLO REALE

O = Ordine degli Ingegneri della Provincia di Roma
C = IT

SOMMARIO

1 PREMESSA SUL CORRETTO APPROCCIO ALL'ANALISI DEL FUNZIONAMENTO DEI SISTEMI INFORMATICI 3

1.1 LA VERIFICA DELL'EFFETTIVO FUNZIONAMENTO VS LA SUA DESCRIZIONE 4
1.2 LA FISICITÀ VS LA "VIRTUALITÀ" 5

2 SINTESI SULLA CLASSIFICAZIONE DELLE PRESTAZIONI NELL'AMBITO DELLE INTERCETTAZIONI 6

2.1 LE PRESTAZIONI OBBLIGATORIE 6
2.2 LE PRESTAZIONI FUNZIONALI ALLE INTERCETTAZIONI 7

3 COSA È UN CAPTATORE INFORMATICO, O TROJAN 8

4 PUNTI APERTI 11

4.1 IL NUMERO DI CAPTATORI UTILIZZATI 11
4.2 IL TAVOLO TECNICO ISTITUITO DAL DECRETO MINISTERIALE 12
4.3 OBBLIGHI DEI FORNITORI DELLE PRESTAZIONI 12
4.4 LA CERTIFICAZIONE DA PARTE DI UN SOGGETTO TERZO QUALIFICATO 13
4.5 IL TRACCIAMENTO DELLE OPERAZIONI SVOLTE CON IL CAPTATORE INFORMATICO 14

5 CONCLUSIONI 16

6 ALLEGATI 17

6.1 ARTICOLO "INTERCETTAZIONI LEGALI SOLO SE 'CERTIFICATE'" PUBBLICATO SU SICUREZZA E GIUSTIZIA N. 2 ANNO 2021 DI GIOVANNI RUSSO 17
6.2 ARTICOLO "EXODUS, ECCO I DISASTRI CHE POSSONO CAUSARE GLI SPYWARE" PUBBLICATO SU START MAGAZINE IL 31.03.2019 DI UMBERTO RAPETTO 23
6.3 ARTICOLO "QUANDO GLI SPYWARE POSSONO DIVENTARE ARMI MINACCIOSE" PUBBLICATO SU "IN TERRIS" IL 21.07.2021 DI UMBERTO RAPETTO 25
6.4 ARTICOLO "LIA CERTIFICATION: LA PRIMA CERTIFICAZIONE INDIPENDENTE DEGLI APPARATI PER LE INTERCETTAZIONI" PUBBLICATO SU SICUREZZA E GIUSTIZIA N. 4 DEL 2018 27

7 NOTE SULL'AUTORE 29

1 PREMESSA SUL CORRETTO APPROCCIO ALL'ANALISI DEL FUNZIONAMENTO DEI SISTEMI INFORMATICI

Si considera utile, in premessa, fornire alcune premesse sull'approccio al cosiddetto "mondo digitale" in modo fornire una migliore chiave di lettura per confrontarsi con i sistemi di tipo informatico. Questa necessità nasce dal fatto che, molto spesso, chi non è esperto della materia tende ad interpretarla, e quindi a formulare ipotesi e ragionamenti, e anche a trarre delle conclusioni, come se fosse sempre possibile assimilarla all'esperienza del mondo fisico, e quindi senza cogliere appieno le sostanziali differenze che sussistono tra questi due ambienti.

L'esperienza del mondo fisico ci consente spesso di comprendere, anche senza spiegazione, il funzionamento di un oggetto, o di un meccanismo, ma questo non è tipicamente possibile, né vero, nel "mondo digitale". Volendo fare un esempio, è banale per chiunque osservare il funzionamento di una maniglia, in quanto muovendola possiamo osservare l'effetto di muovere lo scrocco, così come premendo lo scrocco possiamo constatare la presenza della molla che lo fa tornare in posizione di chiusura: questi semplici elementi ci consentono di cogliere già il funzionamento. Per quanto ciò non possa essere esteso a qualunque tipo di meccanismo, è comunque vero che nella maggior parte dei casi la fisicità dello stesso consente (magari grazie ad uno smontaggio o consultando il disegno): di "osservarlo", di "toccarlo", di "comprenderlo" nel suo funzionamento.

Ma quali siano le azioni "digitali" che si scatenano al semplice "click", p.es., di un link giunto tramite una mail, o come sia effettivamente composta "digitalmente" la stessa mail, o quali siano le effettive interazioni, anche con Internet, di un'applicazione installata su un cellulare, è qualcosa di assolutamente impossibile per un "non addetto ai lavori", e in molti casi lo è anche per gli stessi "addetti ai lavori". Ciò deriva dal fatto che il "dato informatico" è invisibile, di per sé astratto: può essere un livello di tensione trasmesso su una linea elettrica, o un segnale luminoso trasmesso su una fibra ottica, o uno stato elettrico all'interno di un 'chip' elettronico… nessuno di questi è "visibile", deve essere quindi opportunamente acquisito e rappresentato, tramite un'attività di rilevazione e/o con opportuni strumenti.

A titolo esemplificativo, lo stesso captatore può essere un ottimo esempio: un'applicazione che si "traveste" in modo tale da apparire come un'app differente, e che una volta installata esegue comandi e attività di cui l'utente è completamente ignaro e che non ha neppure modo di comprendere a posteriori in quanto "invisibili". Già questo dovrebbe essere sufficiente a cogliere che, in ambito informatico, non è sufficiente "osservare": nell'esempio del trojan, se si osserva proprio l'app installata, si potrà notare che questa consente di effettuare operazioni che nulla hanno anche vedere con l'effettiva funzionalità di catturare le conversazioni, ben celata e invisibile.

Si vogliono quindi introdurre qui alcuni concetti base, che sono più dei "caveat", da intendersi nel senso che se non si colgono pienamente questi aspetti, si corre il rischio di trarre conclusioni astratte, difformi da quello che realmente avviene all'interno di un sistema informatico.

1.1 LA VERIFICA DELL'EFFETTIVO FUNZIONAMENTO VS LA SUA DESCRIZIONE

Da quanto descritto in precedenza, in generale un sistema informatico è assimilabile ad una "scatola nera", nell'accezione utilizzata in ambito scientifico per indicare un oggetto i cui meccanismi interni sono inaccessibili o volutamente omessi. Per contro, i sistemi a Scatola Bianca o a Scatola Chiara sono trasparenti, nel senso che il loro funzionamento interno è visibile, accessibile e comprensibile.

È inevitabile che sistemi trojan non possano essere trasparenti, in quanto se così fosse sarebbero facilmente riconoscibili, identificabili, e neutralizzabili, con buona pace della funzione a cui dovrebbero assolvere.

Tuttavia, è possibile immaginare che sistemi così invasivi -come i trojan- possano essere completamente secretati nel loro funzionamento di dettaglio e che nessuno, al momento, eccetto ovviamente il produttore, possa accedere al reale funzionamento di questi strumenti?

Per sopperire a questa lacuna vengono richieste sommarie descrizioni, auto-dichiarazioni di conformità alle normative vigenti, ma sono ormai diversi i casi in cui, anche non volendo mai mettere in discussione la buona fede e il rigore di chi opera nel settore, si sono create situazioni di totale difformità tra la descrizione e il funzionamento reale, l'esistenza di fasi di processo non previste né spiegate, lacune realizzative che potevano consentire accessi non autorizzati ai dati, e altro ancora. Chi scrive un programma può generare, anche involontariamente, situazioni differenti da quelle volute, oppure lasciare (involontariamente o meno) delle vulnerabilità, o altro ancora.

In assenza dei dettagli di funzionamento, la ricostruzione di cosa fa esattamente un'applicazione informatica può essere complessa al punto da diventare sostanzialmente impossibile. Sicuramente esistono tecniche di "*reverse engineering*", strategie di "*testing*" e verifica, e altre ancora, ma queste non sempre consentono una completa ricostruzione dell'effettivo funzionamento, quando questo è l'obiettivo, come nel caso specifico.

In questi casi, anche per tutela del segreto industriale e degli investimenti che stanno dietro lo sviluppo di questi sistemi, si dovrebbe fare ricorso a procedure di certificazione, per garantire gli standard di produzione in generale, ma anche per verificare la conformità di quanto dichiarato rispetto al prodotto effettivo.

Volendo fare un esempio, proprio relativo al captatore, è pacificamente noto, ampiamente descritto dai media che hanno trattato il caso, che in una specifica situazione reale il sistema di captazione era stato esposto, peraltro in una sede istituzionale, in modo semplicissimo: "*i dati intercettati escono dal cellulare e vengono trasmessi al server di Roma. "In mezzo" non c'è niente, è come un tubo*".

La realtà, emersa attraverso un complesso lavoro di analisi informatica, attingendo a competenze specifiche di alto livello, dispendio di tempo in molti test e prove, e anche incappando in modo fortuito in una serie di casistiche favorevoli, è che il sistema **non funzionava affatto come descritto**!

Nel mondo digitale per stabilire il funzionamento "reale ed effettivo" di un qualunque sistema, occorre qualcosa di più che una descrizione, o una osservazione limitata ai soli effetti più macroscopici.

1.2 LA FISICITÀ VS LA "VIRTUALITÀ"

L'esperienza fisica tende a far ritenere importante la collocazione materiale di un oggetto, piuttosto che la sua ben più importante collocazione "informatica" nel mondo di Internet. Nel mondo digitale è vero il contrario.

Gli esempi non mancano, anche recenti: quanto avvenuto con la clamorosa *débâcle* dei sistemi sanitari della Regione Lazio in agosto 2021 (ma si possono citare anche quelli negli USA relativamente all'attacco ransomware all'oleodotto, e altri ancora) fa capire che i criminali informatici che hanno messo KO il sistema non hanno MAI messo piede presso qualunque struttura fisica della regione, eppure hanno devastato tale sistema. **Non è importante "dove" si trovi fisicamente un sistema, ma "come" si può accedere a questo**.

In alcuni casi, come p.es. quando le informazioni vengono conservate nel cosiddetto "*cloud*", non è neppure possibile comprendere DOVE questi dati siano effettivamente e fisicamente conservati, in quanto sono distribuiti secondo logiche di sicurezza e di resilienza, di fatto "sparpagliati" nel mondo fisico, ma accessibili e visibili in modo unitario solo tramite il canale informatico, esclusivamente nella sua dimensione virtuale.

Anche questo è un passaggio chiave nella comprensione dei sistemi informatici: sapere "dove si trova un server" è un'informazione limitatamente utile. Ben più utile è comprendere "chi" può accedere, "come" può accedere attraverso internet, "quali sistemi di sicurezza" impediscono l'accesso agli estranei, quali sistemi di tracciamento consentono la ricostruzione di cosa sia avvenuto, e via discorrendo.

Se è vero che chi ha "fisicamente" in gestione un dispositivo digitale, p.es. un server, può accenderlo e spegnerlo, o magari scollegarlo dalla rete togliendo i relativi cavi, non è altrettanto vero che sia noto "cosa stia elaborando" e "come", e "chi" lo stia controllando nei suoi contenuti informatici, e la consapevolezza del suo contenuto e nel suo stesso funzionamento!

2 SINTESI SULLA CLASSIFICAZIONE DELLE PRESTAZIONI NELL'AMBITO DELLE INTERCETTAZIONI

2.1 LE PRESTAZIONI OBBLIGATORIE

Il complesso degli impianti, sistemi, operazioni e servizi tecnici inservienti alla fruizione dei contenuti e dei dati associati, captati e veicolati dagli operatori di comunicazioni elettroniche e/o dagli Internet Service Provider (Tel.co) in esecuzione delle prestazioni obbligatorie di cui al Decreto Ministeriale 28 dicembre 2017, per la ricezione, registrazione, conservazione e trascrizione delle operazioni di intercettazione di conversazioni, di comunicazioni o di flussi informatici ed elaborazione della documentazione storica del traffico e dei dati associati, per la ricezione, visualizzazione, registrazione, conservazione e fruizione dei contenuti, dei dati, dei servizi e applicazioni web veicolati dagli Internet Service Provider e infine per la vigilanza e manutenzione finalizzate al corretto funzionamento degli impianti e sistemi installati.

1. la fornitura di **informazioni anagrafiche dell'utenza intestataria del contratto**, in termini di informazioni che l'operatore ha registrato per l'attivazione del servizio, eventualmente comprendendo le informazioni di fatturazione, con l'indicazione della data in cui si è risolto il contratto;

2. **l'intercettazione delle comunicazioni**, mediante fornitura dei contenuti e dei metadati ad essi associati, intesa come intercettazione delle comunicazioni sia a livello di accesso, cioè indipendentemente dai servizi usufruiti dall'utenza come appunto la telefonia o la connessione dati, sia a livello di servizio come, ad esempio, del solo servizio e-mail;

3. **il tracciamento delle comunicazioni**, inteso come fornitura dei soli metadati che accompagnano i contenuti delle comunicazioni intercettate;

4. **la localizzazione dell'utenza**, valida solo per la telefonia mobile, che si suddivide in localizzazione standard associata alla comunicazione e localizzazione di precisione che prescinde dalle comunicazioni dell'utente;

5. **l'identificazione dell'utenza**, intesa come il risalire all'identificativo tecnico che è stato utilizzato dall'utenza, valido sia per le connessioni dati per le quali dall'IP si vuole risalire al numero di telefono oppure all'hot-spot che ha fornito l'accesso, sia per lo stalking telefonico (in questo caso si ricorre all'override);

6. **la sospensione o la limitazione dei servizi**, come ad esempio nel caso delle e-mail in cui si inibisce temporaneamente l'accesso;

7. **la documentazione integrale del traffico storico**, con la fornitura delle informazioni prescritte dal dlgs n. 109 del 30 maggio 2008(7);

8. **il sequestro dei contenuti**, intesi come contenuti a disposizione dell'operatore e tecnicamente sequestrabili come, ad esempio, le email in precedenza inviate/ricevute e conservate dall'utente sul server email oppure i messaggi in segreteria telefonica.

2.2 LE PRESTAZIONI FUNZIONALI ALLE INTERCETTAZIONI

Diversi da quelli forniti dagli operatori Tel.co si intendono, invece, i sistemi elettronico/informatici e i servizi ad essi connessi, finalizzati all'acquisizione, veicolazione, geolocalizzazione, registrazione e fruizione dei segnali audio video e dei flussi di comunicazione comunque oggetto di captazione. In particolare, si tratta dei servizi di installazione, manutenzione, vigilanza sul corretto funzionamento degli impianti e sistemi inservienti alle intercettazioni e degli interventi tecnici per l'accesso ai luoghi di installazione e captazione e per la dissimulazione delle attività di intercettazione.

Le attività funzionali sono quelle di intercettazioni informatiche o telematiche (passive); intercettazioni informatiche o telematiche (attive attraverso captatore elettronico, cioè trojan); intercettazioni ambientali audio; intercettazioni ambientali video; intercettazioni ambientali audio/video; intercettazioni ambientali veicolare; intercettazioni ambientali veicolare Audio/Video + GPS; sistema di localizzazione, comprensivo di client per la visualizzazione; analisi dati.

Ossia tutte quelle possibili grazie alle nuove tecnologie, ai malware, ai rilevatori di tracciamento, che si aggiungono alle prestazioni cosiddette obbligatorie.

3 COSA È UN CAPTATORE INFORMATICO, O TROJAN[1]

Il *Trojan Horse* è un programma maligno mascherato da qualcosa di benigno (il nome, infatti, deriva da Cavallo di Troia, in esplicito riferimento alla leggenda Greca). La Corte di Cassazione, che ha più volte trattato l'argomento, l'ha definito "captatore informatico" ma in realtà questo applicativo racchiude in sé una moltitudine di funzioni che lo rendono uno strumento che va oltre la semplice operazione di captazione. Il captatore informatico rappresenta senza ombra di dubbio la nuova frontiera delle intercettazioni di comunicazioni essendo in grado di assumere il controllo dell'apparato su cui viene installato e consentendo così all'operatore remoto di poter svolgere molteplici funzioni.

Generalmente questi sistemi possono essere distinti in due componenti principali:

1. Un applicativo che viene installato sul dispositivo dell'utente, che si occupa di inviare dati e/o ricevere comandi;

2. Un sistema composto da più componenti, che si occupa di offuscare il transito dei dati, di ricevere e memorizzare i dati inviati dal client e inviare comandi verso il quest'ultimo, al fine ultimo di depositare su un server presso la Procura di riferimento i dati intercettati, per la consultazione dell'Autorità Giudiziaria.

Esistono oggi diverse tipologie di captatori utilizzati dall'AG, con caratteristiche differenti e possibilità di accesso ai dati differenti: esistono trojan che sono in grado esclusivamente di attivare/disattivare il microfono per registrare quanto avviene come se il telefono cellulare fosse una 'cimice mobile', fino ad arrivare a trojan più invasivi che possono -in alcuni casi- acquisire i cosiddetti 'privilegi di amministratore' del dispositivo stesso, in tal modo potendo quindi accedere a qualsiasi risorsa anche con possibilità di modifica/cancellazione.

Di seguito si sintetizzano le funzionalità a cui è possibile avere accesso tramite i captatori informatici:

- **Ascolto da remoto delle conversazioni ambientali captate dal microfono del telefono infettato.**

L'operatore, dalla sua consolle, può inviare un comando all'apparato sotto controllo in modo tale che esso attivi il microfono interno e registri conversazioni e suoni da esso captati. Queste registrazioni saranno memorizzate all'interno di file audio che verranno successivamente inviati attraverso la rete Internet.

- **Attivazione della fotocamera integrata nell'apparato infettato.**

[1] Sostanzialmente tratto dall'articolo "*L'intercettazione dei servizi radiomobili avanzati, l'acquisizione forense dei siti web e i cyber attacchi nell'indagine e nel processo penale*" di Marco Zonaro, pubblicato sul testo "*Copia forense e trojan - La nuova frontiera della genuinità della prova legale digitale nel processo penale italiano*" a cura di Mario Antinucci.

Inviando un apposito comando, l'operatore può attivare entrambe le videocamere presenti sul telefonino, o l'unica telecamera presente sul computer, in modo da ricevere alternativamente le immagini da esse riprese. Le fotografie scattate dalle videocamere verranno inviate alla consolle virtuale dell'operatore non appena la comunicazione dati diviene disponibile. Gli scatti fotografici possono avvenire anche in sequenza e in maniera totalmente silenziosa.

- **Lettura di messaggi SMS e MMS.**

Una volta installata nel telefono, l'applicazione è in grado di inviare all'operatore tutti i messaggi SMS e MMS contenuti nella memoria utente del dispositivo. Grazie all'utilizzo della rete Internet l'invio dei messaggi non potrà essere visualizzato dall'utente.

- **Lettura del contenuto delle chat relative a sistemi di messaggistica istantanea multimediale.**

L'efficacia del captatore informatico è dimostrata dalla possibilità di inviare all'operatore il contenuto di tutte le chat scambiate dall'utente utilizzando sistemi di messaggistica istantanea multimediale (WhatsApp, Telegram, Hangout, Skype, e molte altre). Oltre i messaggi testuali l'operatore può acquisire anche gli allegati multimediali. Il captatore informatico sopperisce, in questi casi, all'impossibilità di intercettare le conversazioni che avvengono con tali applicativi, utilizzando i convenzionali sistemi di intercettazione.

- **Geolocalizzazione del dispositivo.**

Un apposito comando inviato dalla consolle virtuale consente all'operatore di attivare, in modalità stealth, il ricevitore GPS del dispositivo radiomobile sul quale il captatore informatico è stato inoculato, in modo tale da ricevere da quest'ultimo, periodicamente, le sue coordinate polari. Utilizzando questi dati, con l'ausilio di una cartografia, l'operatore è in grado di visualizzare la posizione dell'utente utilizzatore del telefono.

- **Ispezione e scaricamento delle immagini e dei filmati memorizzati nel dispositivo.**

Il captatore informatico consente all'operatore di scaricare, da remoto, tutto il contenuto delle cartelle multimediali afferenti alle immagini e dai filmati che sono stati acquisiti mediante le fotocamere integrate nel telefono su cui il captatore stesso è stato installato.

- **Ispezione dei contenuti di navigazione Internet.**

L'operatore può chiedere al telefono sottoposto al controllo del captatore informatico di ricevere la cronologia di navigazione sulla rete Internet effettuata con tutti i browser installati sul dispositivo. Questa ricerca consente di evidenziare tutti i siti Web visitati, correlati con data e ora di connessione, e di estrapolare eventuali contenuti di interesse investigativo.

Quelle summenzionate sono le più importanti funzionalità che il captatore informatico mette a disposizione degli investigatori; come si può ben intuire esso rappresenta un potentissimo strumento che non si può definire solo "di ascolto" bensì un dispositivo virtuale che è anche in grado di controllare totalmente l'apparato su cui è installato.

Altra caratteristica importante di questo tipo di sistemi di intercettazione è quella di **poter essere disattivati o addirittura disinstallati da remoto senza lasciare alcun tipo di traccia della loro presenza: se l'operatore, durante le operazioni di monitoraggio, dovesse rendersi conto che l'utilizzatore sospetti di essere monitorato potrà lanciare un comando di rimozione totale del Trojan installato in modo tale che un'eventuale analisi approfondita del dispositivo sotto controllo non ne rilevi più alcuna traccia.**

Il captatore informatico, in pratica, altro non è che un applicativo installato nel telefono o nel computer sotto controllo e in quanto tale può essere rilevato da un'approfondita analisi compiuta da un tecnico esperto di Mobile Forensics. Va considerato, infatti, che qualunque tipo di captatore informatico venga installato all'interno di un telefono o di un computer, esso altro non è che un software che necessariamente deve interagire con il sistema operativo del dispositivo.

Il problema principale legato all'utilizzo del captatore informatico è costituito dall'attuale impossibilità di operare un controllo effettivo a posteriori delle operazioni che con esso è possibile effettuare; mediante questo strumento, infatti, non è solo possibile ispezionare il contenuto di un determinato dispositivo ma è anche possibile alterarne i dati. **Va da sé che ciò non significa necessariamente che gli utilizzatori di questo potente strumento di intercettazione lo impieghino in maniera impropria ma il fatto stesso che un tale utilizzo possa essere possibile implica che debbano essere messi in atto tutti gli opportuni accorgimenti al fine di garantire e certificare le operazioni che con esso possono essere compiute**.

Nel caso del captatore informatico, quindi, **dovrebbe essere previsto che il sistema a cui esso si collega sia dotato di uno strumento di registrazione delle operazioni compiute (c.d. file di LOG) non modificabile né cancellabile; ogni singolo comando inviato al captatore, deve essere rintracciabile così come la risposta che esso produce deve essere registrata e possibilmente firmata digitalmente. Solo in questo modo potrà essere possibile, a posteriori, controllare efficacemente ogni singolo risultato prodotto**.

4 PUNTI APERTI

4.1 IL NUMERO DI CAPTATORI UTILIZZATI[2]

Nel 2016 la Lawful Interception Academy, congiuntamente alla rivista giuridico-tecnica 'Sicurezza e Giustizia' e la Procura di Reggio Calabria hanno condotto un'analisi qualitativa dei dati statistici prodotti annualmente dal Ministero di Giustizia[3]. Nel nostro paese, infatti, le spese di giustizia si articolano su tre capitoli di spesa, di cui il n. 1363 è relativo alle intercettazioni. Nell'ambito degli interventi di spending review (DL n. 98 del 2011, art. 37, co. 16) è previsto che, a decorrere dall'anno 2012, il Ministro della giustizia presenti alle Camere, entro il mese di giugno, una relazione sullo stato delle spese di giustizia.

Dall'approfondimento, è emerso che la metodologia utilizzata per questa ricognizione statistica è affetta da molte **criticità**, tra cui la mancata indicazione della durata delle intercettazioni e delle relative proroghe e, soprattutto, dalla constatazione che le spese tracciate tramite fattura fanno riferimento all'anno solare in cui vengono liquidate, con il rischio di confondere il numero degli intercettati che si riferisce all'anno in corso con le spese sostenute che invece fanno riferimento ad attività chiuse, quindi relative agli anni precedenti, ma fatturate nell'anno in corso.

Detto in altri termini, non risulta metodologicamente corretto accostare la spesa al numero di prestazioni, poiché non fanno riferimento alle medesime variabili temporali.

Inoltre, in merito alle spese di intercettazione rientrano anche quelle attività effettuate per le c.d. operazioni speciali (Videosorveglianze, localizzatori GPS, ecc.), di contro nel Mod 37/INT il numero dei provvedimenti per questo tipo di operazioni non trova collocazione. Sarebbe utile, così come avviene già in alcuni uffici di Procura della Repubblica, istituire il Registro Operazioni Speciali (R.O.S.) all'interno del registro intercettazioni, dove già trovano ubicazione i R.I.T. Ciò permetterebbe di monitorare queste operazioni, il cui costo è spesso rilevante.

E' ipotizzabile, ma non è descritto nella relazione, che il numero dei giorni relativi alla durata delle singole prestazioni provenga dalla fatturazione effettuata dagli operatori di telecomunicazioni. La relazione, crediamo correttamente ed in linea con questa ipotesi, distingue tra le righe questa diversa provenienza nei due punti di seguito elencati, dove per "attento monitoraggio" probabilmente fa riferimento proprio ad una sorgente diversa da quella dei dati statistici disponibili alla Direzione generale di Statistica:

- *Dall'analisi dei **dati statistici** a disposizione del Ministero della giustizia (Direzione generale di Statistica) i bersagli intercettati negli ultimi 5 anni risultano essere nella media di circa 130.000 annui,*

[2] Tratto da atto depositato presso la Commissione Giustizia della Camera, audizione dell'Ing. G. Nazzaro del 16.03.2021: https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/005/116/LIA_Audizione_Camera_16-03-2021.pdf

[3] Cfr. "Limiti circa l'utilizzabilità delle statistiche nazionali sulle intercettazioni" di G. Nazzaro e T. De Giovanni, su 'Sicurezza e Giustizia' n.3 del 2016 (rif. https://www.sicurezzaegiustizia.com/limiti-circa-lutilizzabilita-delle-statistiche-nazionali-sulle-intercettazioni/)

di cui l '85% degli stessi fanno riferimento alla categoria delle prestazioni funzionali alle intercettazioni di tipo telefonico, il 12% a quelle di tipo ambientale e il 3% a quelle di tipo telematica.

- *Considerato che, dall'esito di un **attento monitoraggio**, la durata media delle suddette prestazioni risulta essere di 57,74 giorni per le prestazioni funzionali alle intercettazioni di tipo telefonico, di 72,04 giorni per quelle di tipo ambientale e di 73,87 giorni quelle di tipo telematica, moltiplicando la durata complessiva con la tariffa massima giornaliera per categoria di prestazione funzionale, come da listino allegato, si ottiene il totale della spesa complessiva annua per categoria di prestazione funzionale alle intercettazioni.*

La statistica ha una funzione molto importante, perché riesce a sintetizzare in poche cifre il lavoro svolto, affinché possa essere generalizzato ed accostato a modelli di comparazione. Lo scopo della statistica è offrire quel giusto dettaglio di realtà per poter intervenire, sanare o risolvere, contribuire al miglioramento ma **deve potersi basare su dati trasparenti e verificabili**.

4.2 IL TAVOLO TECNICO ISTITUITO DAL DECRETO MINISTERIALE

Il decreto ministeriale del 28.12.2017, disposizione di riordino delle spese per le prestazioni obbligatorie di cui all'art. 96 del d.lgs. n. 259 del 2003**,** all'art 7, prevedeva uno specifico tavolo tecnico per il monitoraggio del sistema delle prestazioni obbligatorie.

Il Tavolo tecnico permanente, ferme restando le competenze delle singole amministrazioni, dell'Autorità giudiziaria e delle Autorità indipendenti:

- monitora il sistema delle prestazioni obbligatorie in relazione alla qualità, all'efficienza e alla sicurezza dei servizi forniti, affinché sia garantita un'esecuzione ottimale, uniforme e razionale;
- monitora le modalità di trasmissione e gestione delle comunicazioni amministrative relative alle prestazioni obbligatorie, promuovendo, ove necessario, la diffusione di prassi operative omogenee da parte di tutti gli operatori coinvolti nel circuito amministrativo;
- valuta l'opportunità di un aggiornamento del listino;
- valuta l'introduzione di meccanismi di tipo forfettario nella determinazione dei costi complessivi delle prestazioni obbligatorie.

Detto tavolo, che avrebbe dovuto e potuto coinvolgere i cosiddetti *stakeholder* del complessivo processo, non risulta ad oggi essere mai stato avviato.

4.3 OBBLIGHI DEI FORNITORI DELLE PRESTAZIONI

Quanto previsto agli artt. 3 e 4 del decreto ministeriale del 6.10.2022, pubblicato sul n 23 del Bollettino Ufficiale del Ministero della Giustizia, del 15.12.2022, costituisce l'insieme dei cosiddetti "obblighi" in capo a chi fornisce le prestazioni di intercettazione.

Si tratta di numerose disposizioni che devono appunto essere assicurate dai fornitori, anche relative alle garanzie di sicurezza nella conservazione e gestione dei dati.

Al di là dello specifico contenuto, che per alcuni passaggi sarebbe meritevole di essere meglio approfondito sotto il profilo tecnico, in funzione di ambiguità da risolvere, o di aspetti che non tengono adeguatamente conto della natura informatica delle prestazioni richieste, la criticità maggiore legata a queste disposizioni è che **la normativa non prevede né verifiche né controlli sull'effettiva adesione o conformità, e in generale il loro puntuale rispetto**.

Un approccio di questo tipo, come è evidente, consente di agire solo *ex post*, ovvero quando si verifica o viene riscontrato un problema, con gli effetti deflagranti e forieri di sfiducia in un contesto in cui dovrebbe essere applicata la massima attenzione e diligenza.

Richiamandosi a contesti differenti, si vuole qui ricordare come la manutenzione dell'auto deve essere certificata da un'ispezione ("revisione") ogni due anni, come analogamente la caldaia a gas di un'abitazione deve essere corredata di apposito libretto compilato dal personale specializzato che opera le necessarie verifiche nei tempi previsti, anche con il controllo dei fumi e il rilascio di un bollino, o ancora un autovelox, che deve essere sottoposto a tarature puntuali di legge, pena la decadenza del rilievo prodotto dallo strumento.

4.4 LA CERTIFICAZIONE DA PARTE DI UN SOGGETTO TERZO QUALIFICATO

Diversamente dagli esempi citati sopra, per quanto attiene alla disciplina delle intercettazioni, siano queste effettuate col captatore informatico che con il tradizionale ascolto delle conversazioni telefoniche, non esiste obbligo alcuno che il sistema sia certificato, o comunque oggetto di ispezioni e verifiche.

Eppure, il tipo di attività svolto da questi sistemi è, per sua natura, invasivo a diversi livelli della vita personale e della privacy delle persone, che -si ricorda- non possono anche non essere necessariamente oggetto di indagine: si faccia riferimento a captazioni che avvengono in presenza di altri soggetti, diversi dal target, che rimangono quindi casualmente oggetto di attenzione e raccolta di informazioni, con la compressione dei relativi diritti, pur in assenza di alcuna ipotesi di reato.

Senza considerare che, comunque, questi sistemi -per loro natura, come detto, di tipo 'black box'- non sono noti in modo puntuale nel loro funzionamento neppure al committente, come la Procura di riferimento, ancor meno al soggetto intercettato, che per poter comprendere cosa sia avvenuto non dispone né di documentazione tecnica né di altre forme di certificazione, se non la mera dichiarazione asettica e succinta di un asserito 'rispetto della vigente normativa'.

Come suggerisce l'ex Procuratore Nazionale Antimafia Dott. Giovanni Russo in un articolo recente (a disposizione in allegato 6.1), basterebbe guardare ai modelli internazionali di valutazione della sicurezza informatica: esaminare i sistemi nel loro complesso, valutandoli rispetto ad altri fattori come, ad esempio, la tipologia di dato, la sua importanza sotto il profilo della sicurezza, il luogo di conservazione, la natura e le prerogative dei suoi fruitori.

L'aggregazione di tali standard internazionali, sulla base delle finalità da perseguire e del settore di pertinenza, è alla base dei c.d. accreditamenti o certificazioni condotte da enti terzi (in quanto diversi sia dall'utilizzatore che dal produttore), valorizzando di conseguenza l'intera filiera sotto i profili della qualità e dell'affidabilità.

Per contro, deve essere evidente che le società che operano in questo settore, estremamente innovativo e dinamico, hanno l'assoluta necessità di tutelare il proprio segreto industriale, per il quale vengono investiti capitali economici ed umani, in termini di competenze di alto livello. In quest'ottica va quindi inquadrata l'esigenza di mantenere il massimo segreto e riserbo sul funzionamento di dettaglio di questi stessi sistemi. Questo è quindi un altro fattore che deve essere comunque tenuto in considerazione nella valutazione delle possibili soluzioni.

Spesso si è portati a valutare erroneamente che tale forma di garanzia o certificazione sia già in qualche modo contemplata nella dichiarazione di aderenza ai requisiti elencati nei relativi bandi di gara e nei loro allegati tecnici. In realtà, l'elencazione di requisiti tecnici dei bandi non può essere mai così dettagliata da considerare tutti gli aspetti necessari, ad esempio come quello della sicurezza, del trattamento, degli standard ETSI per l'inoltro dei dati ai sistemi dell'autorità giudiziaria, ecc. Nella maggior parte dei casi, quindi, si procede sulla base di una semplice autodichiarazione del fornitore, che ha il solo scopo pratico di manlevare i pubblici uffici dalle verifiche preliminari, altamente specialistiche sotto il profilo tecnico, che questi ultimi non sarebbero in alcun modo in grado di svolgere.

Il principale vantaggio di una certificazione anche nel settore delle intercettazioni sarebbe quello di fornire una preventiva garanzia circa la legalità (intesa come rispondenza alle regole tecniche più avanzate) dell'intero sistema delle intercettazioni, evitando di dover ricostruire ogni volta l'intera filiera di gestione del dato intercettato, con benefici anche sotto il profilo della riduzione dei tempi processuali.

In Italia, peraltro, esiste già una prima certificazione indipendente degli apparati per le intercettazioni, la "LIA Certification" costruita dal suo direttore Giovanni Nazzaro, che opera secondo lo standard 17020:2021, che specifica i requisiti per la competenza degli organismi che effettuano l'ispezione nonché i requisiti per l'imparzialità e la coerenza delle loro attività di ispezione.

Tuttavia, l'assenza di obblighi normativi a riguardo, o anche di richieste specifiche da parte dell'AG, rende tale possibilità a tutt'oggi inapplicata per la maggior parte delle società che operano nel settore.

4.5 IL TRACCIAMENTO DELLE OPERAZIONI SVOLTE CON IL CAPTATORE INFORMATICO

Se, da un lato, lo strumento deve offrire le dovute garanzie nei confronti dello Stato e dei suoi cittadini, dall'altro lo strumento deve essere utilizzato nel rispetto dei diritti dell'intercettato.

Ma, considerato che il trojan può essere cancellato da remoto senza lasciare tracce, e che non esistono strumenti di tracciamento previsti per questi strumenti, che possibilità esistono *ex post* per ricostruire esattamente come sia stato usato lo strumento, quando il microfono è stato acceso e dove, quali informazioni sono state visionate ed eventualmente esfiltrate etc.?

Alcune situazioni reali, in cui è stato possibile affrontare questi aspetti, hanno consentito di verificare come vi siano enormi difficoltà, se non in alcuni casi l'impossibilità, di ricostruire a posteriori le attività svolte, anche semplicemente il calendario di attivazione e disattivazione del microfono.

In altri casi non è stato neppure possibile ricostruire puntualmente il percorso dei file dal terminale al server.

E' necessario quindi che questi strumenti abbiano anche un relativo registro 'sicuro' in ci vengono tracciate tutte le attività: 'sicuro' nel senso che debba essere tracciata ogni attività, quando e da chi, senza omissioni, e proteggendo tale registro in modo che il suo contenuto sia reso immodificabile e la sua integrità sempre verificabile.

5 CONCLUSIONI

Si ritiene doveroso evidenziare che, sebbene siano noti sia alla cronaca che all'Autorità Giudiziaria (che ha aperto le relative indagini) alcuni casi di gestione difforme di questi sistemi di captazione informatica, o di problematiche di sicurezza nell'accesso e ancora alla disponibilità di dati intercettati su sistemi esteri, al momento non esistono indicazioni in merito ad un eventuale dolo o abuso.

Ciò, tuttavia, non diminuisce, ma semmai deve far aumentare l'attenzione su questi strumenti, proprio per la loro peculiare invasività, perché non può essere lasciato spazio agli errori, anche generati in assoluta buona fede. La fiducia delegata dai cittadini e dalle istituzioni all'utilizzo di questi strumenti è sempre in discussione, e non può essere minata, anche solo da un'operazione effettuata con superficialità.

Sotto il profilo squisitamente teorico -comunque- esiste la possibilità, in astratto, che i dati possano essere manipolati, o che sia in discussione la loro genuinità. A questo proposito, volendo affrontare in modo tecnico il tema, ovvero accertare tale avvenuta manipolazione, i limiti che si trovano oggi sono:

- Mancanza della conoscenza della gestione puntuale dei dati
- Impossibilità a ricostruire il sistema e il suo funzionamento
- Difficoltà a ricostruire le operazioni svolte.

Inoltre, i captatori, come strumenti informatici, possono essere anche programmati per rispondere a requisiti ulteriori, quali, ad esempio (compatibilmente con i limiti del dispositivo e della tecnologia adottata):

- La possibilità di inibire l'ascolto in zone geografiche predefinite;
- La possibilità di accedere solo a precise risorse e/o informazioni presenti sul dispositivo, in modo selettivo e non generalizzato.

Richiamando il contenuto di questa note, si vogliono qui sintetizzare i punti relativi ai captatori informatici che, ad avviso di questo Consulente, sono meritevoli di essere presi in carico dal legislatore al fine di risolvere le problematiche esistenti ed indirizzare quelle potenziali:

1. In funzione della peculiarità di questo strumento, definire una disciplina *ad hoc*, diversa da quella prevista per le intercettazioni telefoniche;
2. Definire una forma di garanzia terza per questi strumenti, sotto forma di certificazione o altro, al fine di avere la certezza che effettivamente il loro funzionamento sia puntualmente conforme agli obblighi previsti dalla normativa;
3. Prevedere che il sistema a cui esso si collega sia dotato di uno strumento di registrazione delle operazioni compiute non modificabile né cancellabile; ogni singolo comando inviato al captatore deve essere rintracciabile, così come la risposta che esso produce deve essere registrata e possibilmente firmata digitalmente;
4. Attivare il tavolo tecnico previsto dal decreto ministeriale, al fine di monitorare in modo costante ed efficace l'utilizzo di questo strumento.

6 ALLEGATI

6.1 ARTICOLO "INTERCETTAZIONI LEGALI SOLO SE 'CERTIFICATE'" PUBBLICATO SU SICUREZZA E GIUSTIZIA N. 2 ANNO 2021 DI GIOVANNI RUSSO

https://www.sicurezzaegiustizia.com/intercettazioni-legali-solo-se-certificate/

Il principale vantaggio di una certificazione anche nel settore delle intercettazioni sarebbe quello di fornire una preventiva garanzia circa la legalità (intesa come rispondenza alle regole tecniche più avanzate) dell'intero sistema delle intercettazioni, evitando di dover ricostruire ogni volta l'intera filiera di gestione del dato intercettato, con benefici anche sotto il profilo della riduzione dei tempi processuali. Si avrebbero inoltre vantaggi nello snellimento delle procedure di gara: in moltissimi altri settori industriali la certificazione indipendente di prodotto costituisce già un requisito legale o contrattuale. Infine, si avrebbe finalmente la disponibilità di un'elencazione oggettiva di caratteristiche che permetterebbe ai pubblici uffici una più semplice scelta del prodotto più adeguato alle specifiche esigenze del momento.

1. Introduzione

E' ben nota la rilevanza investigativa e probatoria delle intercettazioni, un tempo prettamente telefoniche e, più recentemente, anche telematiche e ambientali.

Esse permettono l'acquisizione di elementi probatori (non solo conversazioni ed altri tipi di comunicazione, ma anche documenti, immagini, video ecc.) che sono il frutto della diretta (e inconsapevole) produzione dei soggetti intercettati. Forniscono, cioè, informazioni "di prima mano", di grande interesse giudiziario, perché caratterizzate, il più delle volte, da spontaneità e veridicità e perché correlate a manifestazioni comunicative private, idonee a rivelare le reali motivazioni e finalità dell'agire umano.

Con la rivoluzione digitale, le relazioni comunicative hanno assunto un ruolo centrale, potremmo dire "essenziale" in tutti gli ambiti della vita quotidiana e, quindi, anche nei contesti criminali.

Se nel 2017 The Economist, con qualche ritardo, poteva affermare che "*The world's most valuable resource is no longer oil, but data*", risulta evidente che al giorno d'oggi le informazioni rappresentano certamente l'oggetto del desiderio dei moderni delinquenti, che hanno sostituito grimaldelli, piedi di porco e ordigni esplosivi con nuovi e sofisticati strumenti digitali (virus, worm, trojan malware, adware, ransomware) oppure, più semplicemente, hanno imparato ad approfittare di password deboli o di siti internet non sicuri.

Ma la ricerca informativa è anche il "terreno di caccia" degli apparati investigativi e giudiziari, il cui compito è prevenire la commissione dei reati e sanzionare gli autori dei crimini.

L'inviolabilità della libertà e della segretezza delle comunicazioni, proclamata come principio dall'art. 15 della Costituzione, deve trovare oggi una sua declinazione anche digitale, realizzando quella che il mondo

anglosassone definisce come “cyber security”, assicurata dall’insieme degli strumenti, delle tecnologie e delle procedure atti a garantire disponibilità, confidenzialità e integrità ai dati e ai sistemi informatici.

Una “barriera” virtuale tra il mondo esterno e le informazioni in formato digitale che ognuno di noi produce, detiene, scambia. Cresce, dunque, di giorno in giorno, l’esigenza di individuare metodologie e competenze in grado di assicurare la sicurezza informatica dei sistemi, anche complessi, per fronteggiare forme sempre più dirompenti di compromissione di micro e macro ecosistemi digitali, ad esempio, con dati esfiltrati o criptati con richiesta di riscatto.

Ma si impone, parallelamente, la necessità di realizzare efficaci attività di indagine penale, nell’ambito dell’area legale autorizzata dal secondo comma del citato art. 15 Costit.

2. Le intercettazioni legali

Come il chirurgo, in condizioni di necessità e, se possibile, previo consenso della persona interessata, opera col bisturi una lesione nei tessuti del corpo umano, per tutelare il bene superiore della vita, il sistema giustizia dello Stato può intervenire, lacerando la sfera della privacy di un determinato soggetto, per ragioni di interesse investigativo. L’autorizzazione a ledere, momentaneamente e per le sole esigenze di giustizia, il diritto alla libertà e alla segretezza delle informazioni delle comunicazioni è fornita dalla Costituzione in presenza di due condizioni.

Innanzitutto deve sussistere una previsione legislativa che faccia da guida, da argine e che orienti la dimensione della “violazione” in quell’area di riservatezza, calibrandone gli effetti nell’ambito delle finalità costituzionalmente riconosciute e rilevanti. Nel caso di specie, le finalità rilevanti che consentono questa compressione della libertà di comunicare (senza che altri ascoltino) nascono dall’esigenza penalistica di garantire l’ordine sociale attraverso la punizione di chi commette dei reati.

La seconda condizione è costituita dall’esistenza di un provvedimento del magistrato, cioè una valutazione, caso per caso, della ricorrenza dei presupposti previsti dalla legge e della oggettiva pertinenza di questa compressione in relazione ai fini costituzionalmente garantiti che sono concorrenti. Il magistrato verifica la sussistenza dei presupposti, disciplinati nel codice di procedura penale dagli articoli 266 e seguenti, ivi compresa la necessità/indispensabilità di un così rilevante tipo di intromissione nella sfera personale tutelata rispetto alle finalità investigative.

La mutevolezza delle capacità comunicative e trasmissive che, come cittadini, sperimentiamo quotidianamente impone al legislatore di adeguare periodicamente le regole procedurali, affinché le descritte garanzie costituzionali siano assicurate anche in presenza di innovazioni tecnologiche.

In particolare, vengono in considerazione i recenti interventi legislativi (il Decreto Legislativo 29 dicembre 2017, n. 216 e il decreto-legge 30 dicembre 2019, n. 161 convertito con legge 28 febbraio 2020, n. 7): essi, nel riconoscere il ruolo delle intercettazioni come strumento di indagine necessario, si propongono di fissare il giusto equilibrio tra la segretezza della corrispondenza e di ogni altra forma di comunicazione e il diritto all’informazione.

Vengono introdotte alcune novità come quella che vieta "sempre" la pubblicazione, anche parziale, del contenuto delle intercettazioni non acquisite, quella che interviene nell'ambito dell'art. 266 c.p.p. e, in particolare, in relazione all'impiego del captatore nei luoghi qualificabili come domicilio, per il quale è richiesta adeguata motivazione in seno al decreto autorizzativo. Si assiste, altresì, al potenziamento del ruolo del Pubblico Ministero sul vaglio delle intercettazioni: egli dovrà anche vigilare affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone. Viene previsto un archivio digitale, gestito e tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica dell'ufficio che ha richiesto ed eseguito le intercettazioni.

L'intervento legislativo, quindi, è chiamato a tenere conto delle novità nel campo delle attività tecniche di captazione, rese possibili dalla disponibilità non solo dei nuovi strumenti tecnologici in senso stretto ma anche dallo sviluppo di una nuova dimensione di espressione degli spazi comunicativi intra e inter relazionali. Ci si riferisce alle svariate piattaforme di comunicazione (ad es. i social network) in relazione alle quali assumono sempre maggiore importanza le intercettazioni telematiche che consentono di penetrare questi nuovi ambiti relazionali restituendo, anche a livello storico, una grande quantità di informazioni generate con le nostre attività, attraverso i computer e, soprattutto, attraverso i devices portatili. Questi strumenti, peraltro, sono funzionali anche ad un'altra esigenza umana, cioè quella della memorizzazione, ovvero della custodia di documenti e attività in genere che l'utilizzatore compie o alle quali è interessato. L'accesso captativo a questi strumenti consente quindi non solo di registrare e ascoltare in tempo reale o differito le conversazioni, ma consente anche di ricostruire, a mesi o anni di distanza, una traccia storica delle attività svolte dal "bersaglio" (relazioni e contatti che il soggetto ha avuto, compresi i contenuti che sono lì depositati). Si tratta, a ben vedere, di una sorta di estensione digitale della personalità.

Proprio nella rilevanza di tale impatto sembra di poter invenire il fondamento della previsione dell'obbligo di distruzione del materiale costituito da verbali, registrazioni di comunicazioni intercettate etc., non rilevanti: non vengono dettate regole esclusivamente di tipo formale ma si cerca, in qualche modo, di affrontare, il più vicino possibile, il contenuto informativo, per differenziarlo in base alla concreta utilità che la sua conoscenza rivesta nell'ambito delle indagini (e del dibattimento), restituendo la parte irrilevante a quella sfera di riservatezza della persona che ne è titolare, tutelata per diritto ma violata per ragioni di giustizia.

Il tema denuncia tutta la sua delicatezza: il legislatore ha saputo individuare regole aggiornate che mettano in sicurezza, in chiave adeguatamente moderna, i valori che sono alla base del principio costituzionale sopra indicato? E l'applicazione pratica che di quelle regole fanno magistrati, polizia giudiziaria e tecnici addetti alle operazioni materiali di intercettazione garantisce effettivamente che la compressione del diritto di ognuno di noi ad una sfera di riservatezza (entro la quale liberamente atteggiarsi comunicativamente con gli altri e entro la quale manifestare, liberamente, la nostra personalità) sia la minima possibile?

3. Criticità vere e presunte

Da più parti sono stati sollevati rilievi e rimostranze circa l'impiego dello strumento intercettativo, sia con riferimento al ricorso in via generale a tale mezzo di indagine, sia con riguardo alle concrete modalità di esecuzione dello stesso.

Al netto delle posizioni meramente strumentali, finalizzate alla paralisi o alla delegittimazione di specifiche indagini, va osservato che la enorme dimensione di dati che vengono sottratti, seppur per ragioni di giustizia, alla vita di migliaia di persone, assume valore certamente degno di attenzione. Non possono, pertanto, essere tollerate sbavature.

Ebbene, taluni episodi assurti agli onori della cronaca, sia pure frammentariamente, hanno potuto ingenerare la convinzione che non tutti i meccanismi siano attuati in maniera soddisfacente. In attesa di conoscere i risultati degli approfondimenti svolti al riguardo, anche nell'ambito di procedimenti penali, vanno comunque rilevate alcune "zone d'ombra" che sarebbe necessario contrastare.

In primo luogo, mancano regole uniformi per la realizzazione delle operazioni di intercettazione. Non esiste un mansionario né un catalogo delle prestazioni che disciplinino in dettaglio le azioni da porre in essere nelle fasi pre e post intercettazione (oltre che, ovviamente, nell'esecuzione delle operazioni di captazione in senso stretto). Eppure sarebbe importante poter contare su di un "disciplinare", considerando che l'ufficio di Procura, per poter effettuare le attività tecniche di intercettazione, deve necessariamente rivolgersi alla galassia delle innumerevoli aziende, presenti sul mercato e che offrono servizi di questo tipo, ognuna delle quali segue proprie regole e prassi.

In secondo luogo, per ragioni prevalentemente "tecniche", possono verificarsi anomalie nella continuità dei flussi delle attività di captazione, che comunque non sono sempre sicure, fondandosi, anche se per necessità tecniche, su di un trasferimento del dato captato attraverso più punti.

Altri aspetti di opacità possono riguardare la modalità di custodia dei dati acquisiti, soprattutto con riferimento alla fase di smistamento dall'operatore telefonico all'azienda incaricata delle intercettazioni e, da questa, all'ufficio di Procura.

Alcune problematiche sono sorte anche con riguardo alle tecniche di inoculazione dei captatori informatici, dovendosi prevenire casi di "infezioni massive", nonché con riferimento alla effettiva rimozione del virus, una volta terminata l'intercettazione autorizzata (non è accettabile che il virus, ancorché "inattivato", venga lasciato all'interno del dispositivo target).

Sono ben evidenti, in tale scenario, le difficoltà, per i circa 140 Procuratori del nostro Paese, di esercitare una efficace azione di controllo sul sistema dei flussi sopra sommariamente descritti. Un groviglio abbastanza complicato, insomma, e tale da rappresentare, nel suo complesso, una struttura critica.

Nella migliore delle ipotesi, infatti, il Procuratore, attraverso la struttura dedicata alle intercettazioni (il "CIT"), potrà assicurare in maniera rigorosa la correttezza degli aspetti burocratici/procedurali (l'esattezza del bersaglio da attingere, la conformità all'autorizzazione del Gip delle attività da delegare, il rispetto delle scadenze, ecc.), ma non potrà certamente espletare alcun effettivo controllo circa le risorse e le soluzioni tecnologiche di volta in volta adottate. Neppure i pregevoli decaloghi, che qualche Procura con più spiccata sensibilità e più avanzate competenze in questo settore ha avuto cura di predisporre (e che sono stati diffusi a tutti gli uffici di Procura nell'ambito della condivisione delle best practises), possono ritenersi una soluzione appagante. Questo decalogo, che contiene una serie di condizioni che gli operatori incaricati delle intercettazioni devono assicurare prima di iniziare le attività, finisce per collocarsi – infatti – sul piano delle iniziative meramente formali per due motivi: la Procura non dispone di alcuno strumento efficace e completo

per un controllo della veridicità dei titoli vantati dal contraente, né della effettività degli impegni assunti; può agire soltanto ex post, ovvero quando emerge già la patologia.

La seconda ragione è che oggettivamente un decalogo astratto, a fronte della velocità con la quale mutano i sistemi tecnologici (soprattutto in questo settore vengono ideati ogni settimana nuovi prodotti, nuovi software, nuove applicazioni ecc.), rischia di diventare obsoleto anche a pochi mesi dalla sua stesura o sottoscrizione.

4. Il valore dell'accreditamento o della certificazione

In realtà, basterebbe guardare ai modelli internazionali di valutazione della sicurezza informatica: esaminare i sistemi nel loro complesso, valutandoli rispetto ad altri fattori come, ad esempio, la tipologia di dato, la sua importanza sotto il profilo della sicurezza, il luogo di conservazione, la natura e le prerogative dei suoi fruitori. Non a caso uno degli elementi di maggiore novità introdotti dal Regolamento (UE) 2016/679 sulla protezione dei dati è stata la previsione di una valutazione di impatto, cioè una valutazione del rischio, con conseguente gestione, che dipendesse proprio dai suddetti fattori.

In tutti i settori in cui tali sistemi informatici lavorano, dal manufatturiero all'agroalimentare, dal chimico al meccanico, la scelta della migliore prassi o soluzione da applicare tiene conto delle esigenze di sicurezza: gli enti internazionali di standardizzazione come ISO, ITU, ETSI, ecc., con la loro documentazione tecnica, hanno infatti profilato le casistiche d'uso. L'aggregazione di tali standard internazionali, sulla base delle finalità da perseguire e del settore di pertinenza, è alla base dei c.d. accreditamenti o certificazioni condotte da enti terzi (in quanto diversi sia dall'utilizzatore che dal produttore), valorizzando di conseguenza l'intera filiera sotto i profili della qualità e dell'affidabilità.

In tutti i Paesi in cui l'accreditamento è stato introdotto è aumentata la competitività e l'intero sistema socio-economico ne ha beneficiato, dalle istituzioni alle imprese, ai consumatori, in termini di reputazione e di performance.

Nel dettaglio, come ricordato dal nostro ente di certificazione nazionale Accredia, diversi potrebbero essere i vantaggi: nel caso delle istituzioni, o della Pubblica Amministrazione più in generale, si possono ottenere benefici in termini di riduzione della legislazione nazionale aggiuntiva e di semplificazione dei controlli diretti nei confronti di organizzazioni pubbliche o private che possiedono la certificazione.

5. Le intercettazioni legali come servizi informatici da certificare

E' dunque paradossale rilevare che le intercettazioni, intese come servizi informatici noleggiati dalla Pubblica Amministrazione, non possono riferirsi ad alcuno standard internazionale, che comprenda le varie peculiarità, a differenza di quanto avviene in tanti altri settori.

Spesso si è portati a valutare erroneamente che tale forma di garanzia o certificazione sia già in qualche modo contemplata nella dichiarazione di aderenza ai requisiti elencati nei relativi bandi di gara e nei loro allegati tecnici. In realtà, l'elencazione di requisiti tecnici dei bandi non può essere mai così dettagliata da considerare

tutti gli aspetti necessari, ad esempio come quello della sicurezza, del trattamento, degli standard ETSI per l'inoltro dei dati ai sistemi dell'autorità giudiziaria, ecc. Nella maggior parte dei casi, quindi, si procede sulla base di una semplice autodichiarazione del fornitore, che ha il solo scopo pratico di manlevare i pubblici uffici dalle verifiche preliminari, altamente specialistiche sotto il profilo tecnico, che questi ultimi non sarebbero in alcun modo in grado di svolgere.

Il principale vantaggio di una certificazione anche nel settore delle intercettazioni sarebbe quello di fornire una preventiva garanzia circa la legalità (intesa come rispondenza alle regole tecniche più avanzate) dell'intero sistema delle intercettazioni, evitando di dover ricostruire ogni volta l'intera filiera di gestione del dato intercettato, con benefici anche sotto il profilo della riduzione dei tempi processuali. Si avrebbero inoltre vantaggi nello snellimento delle procedure di gara: in moltissimi altri settori industriali la certificazione indipendente di prodotto costituisce già un requisito legale o contrattuale. Infine, si avrebbe finalmente la disponibilità di un'elencazione oggettiva di caratteristiche che permetterebbe ai pubblici uffici una più semplice scelta del prodotto più adeguato alle specifiche esigenze del momento. In tal modo si raggiungerebbero tre obiettivi importanti.

1. Garantire al cittadino che le modalità tecniche delle captazioni, della trasmissione e della custodia delle sue comunicazioni rispettino elevati e costanti standard qualitativi, idonei ad assicurare l'effettività dei precetti delle norme di rango costituzionale e ordinario. In altri termini, dare a tutti la certezza che l'intero "processo" dell'attività intercettativa sia presidiato da meccanismi tecnici – validati ab inizio e costantemente monitorati – che garantiscano l'integrità, la continuità, la non manipolabilità, la non replicabilità, la confidenzialità delle comunicazioni.
2. Garantire ai Procuratori della Repubblica di poter disporre, già all'atto della scelta dell'azienda a cui affidare le attività intercettative, di elementi valutativi affidabili; attribuire ai predetti Procuratori – attraverso le competenze del soggetto certificatore – strumenti per verificare in maniera continuativa e attendibile le modalità attraverso le quali viene posto in esecuzione il mandato intercettativo che egli ha conferito, sulla base dell'autorizzazione del GIP, alla Polizia Giudiziaria. Attraverso la certificazione del "processo" intercettativo, in altri termini, il Procuratore ottiene la garanzia scientifica che ogni istante dell'attività invasiva avvenga senza intromissioni, interferenze, errori, dimenticanze, negligenze, trascuratezza ecc.
3. Garantire all'operatore incaricato di eseguire le intercettazioni, di avere un qualificato e competente interlocutore con il quale potersi permanentemente interfacciare, anche a fronte di ogni nuovo evento che si manifesti e che richieda una "decisione" di tipo tecnologico.

Lo strumento necessario per il raggiungimento dei tre obiettivi è la certificazione – a cura di soggetto terzo qualificato e accreditato – dell'intero processo di intercettazione e captazione delle informazioni: esso, fin dall'avvio dell'installazione, anzi fin dalla scelta degli strumenti tecnologici, da quelli hardware al software, deve essere validato dal punto di visto scientifico così che se ne certifichi la idoneità a realizzare un'attività conforme ai parametri di legge.

Dal punto di visto organizzativo la individuazione dei soggetti certificatori, da abilitare a tale funzione in materia di intercettazione, potrà essere compiuta dal Ministero della Giustizia, eventualmente per macro aree territoriali, oppure potrà essere rimessa alla discrezionalità dei singoli Procuratori della Repubblica, attingendo tale figura nell'ambito di elenchi previamente validati dallo stesso Ministero.©

6.2 ARTICOLO "EXODUS, ECCO I DISASTRI CHE POSSONO CAUSARE GLI SPYWARE" PUBBLICATO SU START MAGAZINE IL 31.03.2019 DI UMBERTO RAPETTO

Fonte: https://www.startmag.it/innovazione/exodus-ecco-i-disastri-che-possono-causare-gli-spyware/

EXODUS, ECCO I DISASTRI CHE POSSONO CAUSARE GLI SPYWARE

Italiani infettati da uno spyware (software che raccoglie informazioni) sviluppato da un'azienda italiana (eSurv), distribuito sui dispositivi Android, usato dalle procure e capace di bypassare i filtri di sicurezza Google. Si chiama Exodus ed è stato identificato da un gruppo di ricercatori. Ecco l'approfondimento di Umberto Rapetto

Un vecchio Carosello un tempo diceva "A scatola chiusa compro solo Arrigoni", sottolineando che solo in certi casi si poteva prescindere dal sincerarsi della bontà dell'acquisto, della rispondenza alle proprie aspettative o necessità, della sua sostanziale conformità a quanto dichiarato dal venditore.

Lo Stato – dall'Autorità giudiziaria alle Forze di Polizia fino ad arrivare all'Intelligence – quel vecchio spot non l'ha visto.

La necessità di avere gli strumenti per rincorrere indagati in procedimenti penali o sospetti di chissà quale minaccia in danno al Paese ha portato ad acquisire (e a incentivare la produzione) di soluzioni tecnologiche dalle mille controindicazioni.

La gente non telefona più e non si scambia SMS, sfuggendo alle tradizionali intercettazioni? Niente paura. Salta subito fuori qualcuno (e guai a preoccuparsi di chi sia e quali obiettivi reconditi possa avere) che ha già il "tool" che risolve il problema. In pochissimo tempo il mercato dei software di supporto alle indagini sono sbocciati come i fiori all'arrivare della bella stagione.

Chi li acquista (o ad esser precisi li noleggia, pagando la licenza d'uso di quel programma) non sa cosa ha comprato, ma ne conosce superficialmente solo alcune funzionalità. Una volta scoperto che quel software è in grado di produrre un certo risultato, perché preoccuparsi se ci sono tremende controindicazioni?

Ad una consistente domanda istituzionale si è subito contrapposta una rigogliosa offerta di "spyware" dalle miracolose proprietà, che – a differenza dei farmaci – non sono corredati dal "bugiardino" che dopo posologia ed altre prescrizioni ne sconsiglia l'eventuale utilizzo per possibili effetti collaterali.

Questi prodotti – il cui costo è sempre stellare – consentono di vampirizzare pc, tablet e smartphone, addentandone il contenuto, fagocitando le informazioni di interesse investigativo, eviscerando mille segreti e non trascurando nemmeno quel che con le indagini non ha alcuna attinenza. La trasfusione di file avviene tra il dispositivo "donatore" e il server messo a disposizione da chi ha sviluppato il marchingegno virtuale.

Dati, dati e ancora dati vengono memorizzati chissà dove, viaggiando su Internet (attraversando chissà quanti e quali Paesi per via della strutturale "liquidità" della Rete delle Reti che non ha… linee dirette), restando nella disponibilità dell'"architetto" che ha progettato il prelievo e che poi metterà a disposizione del committente (ad esempio una Procura della Repubblica) succulenti report.

Il latifondista istituzionale, radioso per la soddisfacente mietitura e trebbiatura digitale, non si preoccupa certo della "pula" e ancor meno della "paglia" che è rimasta al mezzadro (in questo caso rappresentato dalla società produttrice dello spyware) e tanto meno è in grado di sapere se i sacchi consegnati contengono tutto il raccolto commissionato.

Chi tra i committenti è davvero capace di conoscere quel che davvero fanno le istruzioni e i filtri che sono l'ossatura di un programma complesso e imperscrutabile?

Chi tra i committenti conosce il prestatore d'opera, dal caposquadra titolare dell'azienda aggiudicatrice dell'incarico fino all'ultimo bracciante hi-tech che con il suo falcetto ha forgiato comandi e azioni dello spyware?

Chi tra questi ha valutato le conseguenze indesiderate della dispersione di quel software che potrebbe essere un pericoloso anticrittogamico che finisce sulla tavola anche di chi con le indagini non c'entra nulla?

Le domande potrebbero susseguirsi in un impietoso crucifige, in cui ogni riga del testo sarebbe una martellata sui chiodi destinati a trafiggere gli arti di chi in storie come queste ha pesantissime responsabilità. Fermiamoci qui.

Chi vuol sapere cosa è successo e, perché no?, capirci qualcosa è presto accontentato.

Questo genere di programmi somigliano ai paguri che occupano conchiglie altrui. Uno dei modus operandi più comune è infatti quello di inserirli, adeguatamente camuffati, all'interno di "app" di potenziale uso comune. Queste applicazioni vengono caricate sui diversi "store" dove gli utenti cercano quel che serve loro andando a privilegiare opportunità economiche o addirittura gratuite.

Il soggetto – nel mirino degli investigatori o delle "barbe finte" – riceve un messaggio sul proprio smartphone da un utente che apparentemente risulta essere un amico o un parente, regolarmente inserito nella rubrica telefonica dell'apparato. La comunicazione è il semplice invito a provare una certa "app" e il testo è farcito di buone considerazioni in ordine all'utilità e all'efficacia del programmino suggerito. Il link presente nel messaggio permette di trovare subito la "app" e un semplice clic ne consente l'installazione.

Da quel momento lo smartphone ha caricato a bordo l'intruso e sarà controllato da remoto da chi ha congegnato la trappola.

La "app avvelenata" rimane online sullo "store" e gli sfortunati avventori (estranei a procedimenti penali in corso o ben lontani dal target che gli 007 si sono prefissati) che – semplicemente colpiti dal nome o dalla descrizione – ne riconoscono una possibilità di utilizzo, finiscono con l'intossicare il proprio telefonino con l'attivazione dello spyware nascosto nel programma appena installato.

I responsabili di simili disastri ricordano i produttori di liquori di una volta, quelli che sull'etichetta riportavano la dicitura "fornitori della Real Casa". Il lavorare per le Istituzioni più delicate del Paese ha garantito loro "regie patenti" che hanno permesso l'agire indisturbati nel forgiare strumenti di pericolosità inaudita e in grado di violare qualunque diritto. La giustificazione dello sviluppo di "software investigativo" probabilmente ha sviluppato persino un senso di riconoscenza nei loro confronti…

Tiriamo comunque le somme.

Mille italiani "fregati" da questo spyware? Pochi, fortunatamente pochi. Probabilmente le "app" usate come guscio erano di infima qualità e non hanno catturato l'interesse dei tanti collezionisti di applicazioni di ogni genere… Alla fine possiamo dire che poteva andare peggio.

6.3 ARTICOLO "QUANDO GLI SPYWARE POSSONO DIVENTARE ARMI MINACCIOSE" PUBBLICATO SU "IN TERRIS" IL 21.07.2021 DI UMBERTO RAPETTO

Fonte: https://www.interris.it/rubriche/opinione/spyware-armi/

Il coltello da cucina nasce per tagliare il pane o la carne. Se lo brandisce un assassino probabilmente la posata – fino a quel momento "innocua" – diventa uno **strumento di morte**.

I **software di controllo** servono per contrastare il terrorismo, ma se li si adopera per spiare avversari politici, attivisti per i diritti umani, presunti dissidenti o semplici giornalisti quei programmi diventano una **minaccia per la libertà** di espressione, per l'indipendenza dell'informazione, per la democrazia, per il futuro della civiltà contemporanea.

Un certo tipo di arsenale accomuna realtà antitetiche ed acerrimi nemici che – arroccati a iperboliche distanze ideologiche – si rivolgono al medesimo fornitore per farsi dispensare le armi per **acquisire la supremazia** della conoscenza, per scovare segreti, per intimidire, per ricattare, per **condizionare le scelte**.

Israele e **Arabia Saudita**, a dispetto della spigolosa facciata delle storiche ostilità e dell'assenza di relazioni diplomatiche, hanno avuto incontri segreti a Vienna, Cipro e Riyadh. Da una parte del tavolo gli israeliani rappresentanti commerciali di TSO, dall'altra gli acquirenti arabi della "specialità della casa" ovvero il **sistema Pegasus**. *Pecunia non olet* e nell'effervescente universo del business i principi passano facilmente in secondo piano….

Avvezzi a considerare venditrice di morte l'**industria bellica**, dovremmo includere in quel ruolo anche chi sviluppa i cosiddetti "RCS" o *remote control system*, quei software che – inoculati come una venefica dose per endovena nei circuiti elettronici – acquisiscono il **controllo a distanza di un dispositivo informatico** (computer, tablet, smarphone…).

Inutile però scandalizzarsi se Israele guadagna con certe discutibili invenzioni e a servirsi di certe soluzioni sono il governo messicano o quello dell'Azebarijan. Le stesse cose, magari con nomi diversi, le produciamo anche noi in Italia e persino la magistratura ne fa un uso non sempre consapevole delle **incontenibili potenzialità** che certe applicazioni *hi-tech* sono capaci di estrinsecare.

Le vicende di Hacking Team o il più recente caso Exodus testimoniano che non siamo diversi dai soggetti verso i quali adesso si riversano impetuose **ondate di sdegno**.

Questi spyware (o trojan, chiamateli come preferite) si installano facilmente su qualunque aggeggio sia nella disponibilità della persona presa di mira. Il recapito della "polpetta avvelenata" avviene attraverso l'invio di un SMS o di un "WhatsApp", oppure mediante una mail o con **qualunque altra opportunità di messaggistica**, persino facendo ricorso ad una qualunque pagina web.

Una volta accomodatosi sul dispositivo "target" questo genere di software ne prende il **dominio assoluto**, governandone tutte le funzioni e utilizzando senza limiti la globalità degli accessori a bordo. Il tizio da colpire viene "tradito" dal microfono e dalla telecamera che riteneva inoffensivi, lascia a chi agisce in suo danno la possibilità di leggere la posta elettronica e **frugare in ogni angolo della "memoria"**, registra inconsciamente telefonate e conversazioni per poi spedirle a "chi di dovere", comunica involontariamente la propria posizione così da consentire il continuo e costante pedinamento…

Chi gestisce questa infamia può anche "caricare" su quel dispositivo una ampia serie di contenuti che non sono mai stati né visti, né acquisiti o conservati dal legittimo possessore di un telefonino o di un PC. E quest'ultimo potrà essere anche incriminato per la disponibilità di *file* che lo incastrano senza che lo sventurato abbia mai saputo della loro esistenza e ancor meno della loro presenza all'interno del telefono o del disco fisso del computer.

Le brutali esecuzioni di **Giulio Regeni** e **Jamal Khashoggi** sono soltanto due delle tante pagine insanguinate dei nostri tempi.

Le Nazioni Unite dovrebbero adottare provvedimenti severi, ma l'inerzia nell'affrontare beghe colossali e l'incompetenza tecnica per comprendere la gravità di queste situazioni riducono una **questione di inestimabile caratura** ad un evento capace di galleggiare solo qualche giorno sui mezzi di informazione.

Il fragore del silenzio istituzionale è allineato al disinteresse che precedenti abnormi esperienze non sono riuscite nemmeno a scalfire. Se ne riparlerà, con *nonchalance*, tra qualche mese al verificarsi del prossimo **scandalo**…

6.4 ARTICOLO "LIA CERTIFICATION: LA PRIMA CERTIFICAZIONE INDIPENDENTE DEGLI APPARATI PER LE INTERCETTAZIONI" PUBBLICATO SU SICUREZZA E GIUSTIZIA N. 4 DEL 2018

Fonte:

https://www.sicurezzaegiustizia.com/wp-content/uploads/2019/01/SeG_IV_MMXVIII_Certificazione_LIA.pdf

La LIA ha definito il primo processo di Certificazione in Italia dedicato agli apparati e ai servizi utilizzati in ambito delle intercettazioni telefoniche, telematiche e ambientali. In sintesi l'iniziativa: 1) permette di adottare la metodologia della "certificazione di terza parte" già ormai utilizzata in quasi tutti gli altri settori merceologici; 2) consente di verificare, anche periodicamnete, le qualità tecniche dei sistemi utilizzati per la ricezione delle intercettazioni; 3) garantisce che non si perda ulteriore tempo nei processi o nelle fasi di verifica a garanzia del prodotto acquistato o noleggiato; 4) tutela gli interessi di tutti interessati (cliente, fornitore, utilizzatore finale).

Durante l'ultima edizione della LIA si è riportato all'attenzione dei presenti un principio piuttosto rilevante, che con il tempo sembrava essere stato accantonato nel nostro paese, secondo il quale il sistema legale – che consente le intercettazioni giudiziarie – è un sistema che deve essere garantito a monte. E' il caso, ad esempio, dell'avvocato difensore che, nell'ambito di determinati processi, intende ricostruire l'intera filiera di gestione del dato intercettato. Appare indubbiamente un onere complesso, delicato e che richiede tempo e che, quindi, non potrebbe essere svolto a valle, e che dovrebbe essere effettuato per ogni singola attività investigativa supportata da apparati deputati alla ricezione delle intercettazioni. Il fattore di complessità aumenta poi con il numero di apparati utilizzati, forniti da società private distinte.

La garanzia richiesta a monte dovrebbe essere assicurata per tempo, cioè prima che le attività abbiano inizio, attraverso la giusta competenza, poiché la gestione del dato intercettato non riguarda solo la sicurezza informatica ma anche requisiti funzionali e operativi del particolarissimo settore, senza trascurare la responsabilità con la quale si opera, perché il dato intercettato va a costituire una prova nel processo, ed infine dovrebbe essere rivalutata a periodi temporali costanti poiché sia i sistemi informatici sia la tecnologia di comunicazione subiscono importanti aggiornamenti periodici. A tutti gli effetti tale garanzia si configura, quindi, come una vera e propria attività specialistica continuativa.

La garanzia o la certificazione di possesso di determinate qualità è una dichiarazione, spesso intesa quale atto di natura giuridica, di conoscenza di fatti e qualità verificati nella realtà, rilasciata da un soggetto qualificato in forma scritta contenuta in un documento chiamato appunto attestato. Nel settore commerciale la certificazione è un processo compiuto per mezzo di attività da parte di un soggetto che è indipendente rispetto ai due principali attori che sono l'offerente e l'acquirente. Nel settore ancora più specifico della

lawful interception, il processo di certificazione deve contemplare la verifica di possesso, nella pratica ed a intervalli regolari, di qualità e comportamenti attesi e afferenti a molte discipline diverse tra loro per natura.

Spesso si è portati a valutare erroneamente che, nel settore specifico delle intercettazioni, tale forma di garanzia o certificazione sia già in qualche modo contemplata dalla dichiarazione di aderenza ai requisiti elencati nei relativi bandi di gara e nei loro allegati tecnici. Ciò generalmente non può essere vero in quanto l'elencazione di requisiti così dettagliati non può rientrare in un contratto di natura commerciale, in quanto sarebbe facilmente contestabile in fase di esecuzione dello stesso da una delle due parti e le controversie amministrative fondate su argomentazioni tecniche non sarebbero facilmente risolvibili. Inoltre, se le qualità non fossero verificate nel dettaglio dall'acquirente, si scadrebbe in una semplice autodichiarazione di certificazione del fornitore. Ecco perché, in moltissimi altri settori industriali, una certificazione indipendente di questo tipo costituisce già un requisito legale o contrattuale ed unico strumento per una valutazione completa del prodotto. Tale certificazione può essere richiamata negli allegati tecnici dei relativi bandi di gara in modo da sollevare l'acquirente da eventuali controversie, che quindi sarebbero gestite separatamente tra il fornitore ed il soggetto certificatore.

In genere, la responsabilità del soggetto certificatore non è trascurabile: infatti, in quanto dichiarazioni di conoscenza, le certificazioni producono gli effetti giuridici stabiliti dall'ordinamento, a prescindere dalla volontà di chi le rilascia.

In tale contesto, per rispondere alla sollecitazione esposta in premessa, la LIA ha definito il primo processo di Certificazione in Italia dedicato agli apparati e ai servizi utilizzati in ambito delle intercettazioni telefoniche, telematiche e ambientali. La Certificazione LIA è rivolta esclusivamente all'Industria di tale settore, tuttavia, è importante evidenziare che la certificazione consentirà indirettamente agli utilizzatori di tale tecnologia, quindi alle Procure della Repubblica, di poter meglio comprendere sia il suo funzionamento sia il grado di aderenza alle disposizioni legislative nazionali ed internazionali, alle best practices tecniche applicate in ambito security e privacy, nonché ai requisiti funzionali richiesti dall'Autorità Giudiziaria e standardizzati dall'ETSI.

La metodologia utilizzata è frutto di un lungo studio, con un periodo di osservazione di circa 20 anni, basato sugli standards internazionali ISO e ETSI a cui sono state integrate le conoscenze specifiche del settore in Italia ed i comportanti attesi dall'Industria e dai suoi Clienti. La certificazione LIA fornisce una valutazione descrittiva e numerica (espressa in percentuali) per rappresentare l'aderenza a quattro aree distinte di possesso di determinati requisiti: 1. Funzionali, 2. di Sicurezza, 3. di Privacy o di trattamento del dato, 4. di Compliance. Qualora l'azienda sottoposta a certificazione risultasse non certificabile per una o più inadempienze anche su una sola delle suddette aree, la certificazione in quanto "processo" prevede la possibilità di recuperare tale situazione. Il report completo, tuttavia, registrerà ogni modifica intervenuta durante il processo di certificazione. ©

7 NOTE SULL'AUTORE

Paolo Reale
Certificato RMB-2040-IT19
INGEGNERE ESPERTO IN AMBITO FORENSE
CONSULENZE TECNICHE IN
INFORMATICA E TELECOMUNICAZIONI

Lead Auditor

Paolo Reale si è laureato nel 1994 con il massimo dei voti in Ingegneria Elettronica presso l'Università di Pisa, presentando una tesi in Robotica pubblicata nel 1995 al simposio INRIA/IEEE sulle tecnologie emergenti, proseguendo l'iter formativo successivamente presso la Scuola Superiore G. Reiss Romoli de L'Aquila.

Ha prestato servizio nell'Esercito Italiano come Ufficiale nell'Arma delle Trasmissioni, operando in qualità di docente presso la Scuola Telecomunicazioni (interforze) delle FF.AA.

Ha operato inizialmente nell'industria, seguendo lo sviluppo della produzione di dispositivi elettronici a microprocessore, proseguendo con le attività di *project management*, e assumendo ruoli di livello manageriale, per l'ingegnerizzazione di processi e sistemi di controllo per le grandi aziende di ICT, con particolare attenzione alle tematiche di tutela delle informazioni aziendali e della privacy. Su queste tematiche ha anche dedicato un iter di approfondimento specifico con il corso di alta formazione per DPO, organizzato dal CNF e dal CNI con il patrocinio del Garante per la protezione dei dati personali.

Esercita da anni l'attività di Consulente, al servizio di Aziende e Privati, della Polizia Giudiziaria e del Giudice (Perizie e Consulenze d'Ufficio), mettendo a disposizione l'esperienza e le competenze acquisite nell'ambito delle telecomunicazioni, dell'informatica e più in generale dei sistemi di *Information and Communication Technology*.

Da luglio 2017 è professore straordinario nell'ambito del corso di laure triennale di "*Diritto dell'impresa, del lavoro e delle nuove tecnologie - Indirizzo: Diritto della società digitale*", Università UNINETTUNO, presta docenze presso Organizzazioni, Ordini e Università. Si citano i moduli di "Digital Forensics" per il Master di II livello in Criminologia presso l'Università LIUC e per il Master di II livello in Criminologia Sociale presso l'Università di Pisa. Partecipa come *Key note speaker* a conferenze internazionali su temi legati alle telecomunicazioni e all'Informatica Forense (*digitalforensics, computer forensics, mobile forensics*).

Collabora con la rivista 'Sicurezza e Giustizia', di cui è anche membro del Comitato di Redazione. E' anche nel comitato scientifico della manifestazione internazionale "Treviso Forensics 2018". E' iscritto all'Albo degli Ingegneri della Provincia di Roma con abilitazione a tutti i settori professionali (a-b-c), eletto Consigliere presso l'Ordine di Roma nel 2022, dal 2013 al 2022 è stato Presidente della Commissione ICT.

Nel 2014 ha fondato, insieme ad altri esperti del settore, l'Osservatorio Nazionale di Informatica Forense (ONIF – www.onif.it). Da gennaio 2015 ne è anche il primo Presidente, confermato anche per il secondo triennio. Tra gli incarichi affidati e svolti si contano casi di particolare rilevanza, anche mediatica. Per ulteriori informazioni si suggerisce di visitare il sito www.paoloreale.it