

MOTIVAZIONI E CONTENUTI DEL DISCIPLINARE TECNICO

Alla norma per la regolamentazione dei captatori informatici viene allegato un disciplinare tecnico.

L'ambito dei captatori informatici risulta particolarmente spinoso poichè la possibilità tecnica di creare informazioni false piuttosto che non riportare o rendicontare informazioni acquisite è molto elevata e va già in conflitto con le pratiche internazionali di acquisizione delle evidenze in formato digitale attraverso l'acquisizione di memorie di massa da dispositivi elettronici.

La presente proposta di legge nell'ambito della regolamentazione d'uso dei captatori informatici, necessita di forti garanzie per essere inattaccabile sul piano della veridicità dei dati acquisiti e portare i dati stessi in sede di dibattito tecnico e giudizio. La storia della computer forensics e delle indagini digitali ci insegna quanto sia importante e necessario il rispetto e l'adozione delle best practices. La storia più recente insegna infatti come in caso di 'fragilità' gli elementi di prova acquisiti vengono completamente invalidati.

Il disciplinare tecnico si pone come obiettivo quello di regolamentare tutti i profili di tipo tecnologico-procedurale nonché tecnico-scientifico inerenti alla implementazione, utilizzo nei vincoli stabiliti della proposta di legge, dei captatori informatici.

Tale disciplinare tecnico funge da riferimento tanto per i produttori di captatori informatici quanto per gli omologatori come per tutte le parti coinvolte, andando a stabilirne con dovizia di dettaglio quali siano gli elementi funzionali nonché di garanzia rivolti a garantire l'integrità e la validità temporale sia delle informazioni acquisite a mezzo captatore che del software stesso.

Per governare la complessità tecnica e tecnologia vedendo garantiti i requisiti stabiliti per legge, si rende necessario senza ogni ombra di dubbio, la disponibilità di regolamentazione tecnica di dettaglio, al pari di quanto già fatto ad esempio per la PEC, lo SPID o il PCT.

Il disciplinare tecnico in particolar modo deve regolamentare i seguenti aspetti del captatore informatico:

- **Architettura informatica e moduli funzionali**

Definizione dei moduli funzionali di un sistema informatico per captatori quali a) sistema di gestione b) modulo captatore c) sistema di comunicazione d) sistema di inoculazione e) sistema di registrazione f) sistema di controllo dei log

- **Requisiti di compliance rispetto a standard internazionali**

Definiti i requisiti ISO/IEC IS-15408 Common Criteria EAL2, usati comunemente per tecnologie per la sicurezza dello stato, come vincoli minimi di qualità e sicurezza dei software captatori.

- **Requisiti tecnici e vincoli operativi di omologazione**

Definiti i requisiti tecnici con cui devono essere documentate ed eseguite le procedure di omologazione, con particolare attenzione alla “ripetibilità certa” del processo tecnico di creazione di un agente software speculare a quello utilizzato in una investigazione specifica, in modo analogo a quanto già avviene per le certificazioni dei software usati nei giochi a premi

- **Requisiti e modalità di custodia dei codici sorgenti del software**

Definizione requisiti, procedure e tempistiche di deposito dei codici sorgenti del software da parte dei produttori

- **Realizzazione di registro captatori informatici e definizione precisa dei dati ivi raccolti**

Definizione delle tipologie di informazioni, con dovizia di dettaglio, che dovranno essere comunicate al registro captatori informatici da parte sia dei produttori che dei software installati presso i centri di controllo di AG/PG

- **Processo e procedura di generazione, uso e verifica presso centro di controllo di PG/AG dei captatori informatici per le singole investigazioni**

Definizione delle procedure con cui è possibile “generare” un captatore da inoculare in un dispositivo bersaglio, quale le sue limitazioni funzionali relative alle autorizzazioni giuridiche concesse e quali le informazioni correlate obbligatorie.

Definizione delle procedure tramite cui le parti possano effettuare una analisi preliminare di congruità e validità delle procedure attuate presso i centri di controllo di AG/PG secondo un percorso tecnico-procedurale garantista ma soprattutto ripetibile.

- **Modalità procedurali-contrattuali per consentire alle parti di ottenere l'accesso alla copia del captatore utilizzato nella specifica investigazione garantendone i vincoli di riservatezza**

Definizione dei requisiti procedurali sia per i produttori che per le parti per potere accedere allo/agli specifici captatori informatici utilizzati in una investigazione specifica, ivi inclusi i requisiti “contrattuali” di garanzia della riservatezza a tutela dei produttori.

- **Modalità di validazione della integrità e di analisi del registro/log di operatività del captatore eseguibile dalle parti**

Definizione delle modalità con cui le parti possano verificare l'integrità dei log di operatività del captatore, delle sue capacità funzionali effettive nonché di tutte le attività da questo eseguite autonomamente o governato da un operatore di PG/AG sino alla sua disinstallazione.

- **Verifica della validazione del captatore mediante interrogazione al registro captatori**

Definizione delle tipologie di interrogazione dei dati presenti nel registro nazionale dei captatori dalle parti con lo scopo di validazione preliminare per riscontro di eventuali anomalie (es: uso di captatori non certificato o uso di captatori istanziati da procure diverse o uso di captatore con capacità tecniche maggiori a quelle definite nelle autorizzazioni del GIP).

- **Verifica della validità del processo di omologazione con sua ripetibilità indipendente**

Definizione di tutte le modalità con cui le parti possano richiedere e ri-eseguire il processo di omologazione, ivi inclusa l'ispezione dei codici sorgenti software e la ri-costruzione della copia esatta del captatore informatico utilizzato nella specifica investigazione. Particolare attenzione viene posta alla tutela del segreto industriale dei produttori e alla attribuzione di responsabilità giuridico-contrattuali dei periti tecnici di parte in merito ad accordi di riservatezza.

In considerazione della completa immaterialità degli strumenti definiti nonché delle informazioni acquisite, l'assenza di un singolo requisito tecnico procedurale definito dal captatore può completamente invalidare l'esecutibilità e integrità dei principi giuridici/procedurali definiti nella proposta di legge.

Per tali motivi è fondamentale che il disciplinare tecnico sia non solo tecnicamente ineccepibile ma pubblicamente disponibile, soggetto a continua revisione da parte della comunità di esperti di settore, con rilascio periodico di aggiornamenti tecnici-funzionali-procedurali.