SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

FONDAZIONE per la FORMAZIONE FORENSE dell'ORDINE degli AVVOCATI di FIRENZE

-

SCUOLA FORENSE

INTERCETTAZIONI TELEFONICHE, TELEMATICHE E CAPTATORE INFORMATICO ALLA PROVA DELLA LEGGE N. 7 DEL 28 FEBBRAIO 2020

9 luglio 2020

Prof. Avv. Stefano Aterno

La norma riformata dalla legge n. 7 del 2020

Art. 266 comma 2 e 2 bis c.p.p.

- *2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un **dispositivo elettronico portatile.** Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita [295 comma 3-bis] solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa [103 5; 615 bis c.p.]*
- *2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su **dispositivo elettronico portatile** è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4*

Perché sul dispositivo elettronico fisso NO ? Solo su portatile ? Si poteva evitare e coprire questa lacuna

E l'art. 266 bis sulle telematiche ? perché non è stato introdotto anche li la disposizione sul captatore ? Peccato però perché il captatore fa anche intercettazioni telematiche

E ora cosa accadrà ? Il captatore è oggi uno strumento che è stato tipizzato. Non è più una prova atipica o un mezzo atipico di ricerca della prova

Un po’ di storia serve a capire meglio il futuro

indagini del 2004 prima apparizione pubblica del captatore 2010

NO AUDIO

SOLO ACQUISIZIONE DI DATI DA UN PC di un ufficio pubblico di PALERMO

Cassazione sez. 5, ***Sentenza*** *n.* 16556 *del* 14/10/2009 Ud. (dep. 29/04/2010) Virruso

È legittimo il decreto del pubblico ministero di acquisizione in copia*, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato* ***presso un ufficio pubblico****, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati.*

La S.C. ha ritenuto corretta **la qualificazione** dell'attività di captazione in questione quale **prova atipica (art. 189 cpp)**, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen

Era il 2012

…….Skype su PC e su cellulari con app Skype

molte intercettazioni telefoniche diventano inutili. Non si sente la voce che corre su reti cifrate

OGGI Encrochat e altri sistemi di cifratura a 360° ancora non scoperti

Elude tutti i controlli intercettazione, NO inoculazione trojan , NO analisi Computer forensics. Effettua controlli ciclici su File System e se trova qualche cosa che non va resetta tutto automaticamente

Le pronunce della Cassazione in tema di Captatore informatico fino ad oggi

- ***Cass. 2010,*** *n.* 16556 *del* 29/04/2010 sul cd captatore informatico, Virruso
- **Gip tribunale di Napoli 2011,** decreto autorizzazione per Caso P4 sul PC in uso ad uno degli indagati (Bisignani)
- **Cass. 2015**, n. 27100 del 26 maggio 2015, Musumeci
- **Cass. SSUU, 2016**, n. 26889 del 28 aprile2016, Scurato (dep. 1 luglio 2016)
- **Cass. Sez. 6, 2017**, n.36874 del 13 giugno 2017, Romeo (caso Consip)
- **Cass. 2017**, n. 48370, del 30 maggio 2017, Occhionero
- **Cass. 2019**, n. 19146, del 2019, Cicciari
- **Cass. SSUU. Civili, 2020**, n. 741 de 2020 sull'utilizzo di captatore informatico in un procedimento disciplinare per reati contro la PA, in epoca antecendente al 1.1.2020
- **Cass. 2016**, n. 40903 del 28 giugno 2016 – uso del trojan per captare le pw di un account email ed entrare nell'account bozze (mancata notifica all'indagato titolare dell'account)

in modalità ambientale NON sono mai state un problema

le Sezioni Unite e le intercettazioni tra presenti - cd itineranti

Cass. SSUU 24 aprile 2016, n. 26889, (dep. 1 luglio 2016), SCURATO

Un'analisi della sentenza della Corte di Cassazione a Sezioni Unite del 24 aprile 2016, n. 26889 (dep. 1 luglio 2016) sulle intercettazioni tra presenti cd itineranti in quanto effettuate attraverso l'uso del captatore informatico. Analisi del problema affrontato dalla Corte Suprema di Cassazione circa l'utilizzo di tale strumento nei procedimenti per delitti di criminalità organizzata e il diverso problema delle intercettazioni tra presenti fuori dai locali di cui all'art. 614 cod. pen.

Il ruolo dell'art. 13 della legge n. 152 del 1991 che consente di non dover provare che in quel domicilio si sta svolgendo l' attività criminosa

In attesa delle necessarie modifiche normative, alcuni rilievi finali e una lieve critica sulle occasioni mancate per fare chiarezza una volta per tutte e rendere più ampio, trasparente e garantito l'uso da parte della magistratura e delle forze di polizia di uno degli strumenti investigativi più utili degli ultimi decenni.

I problemi sorgono per gli screen shot e i files acquisiti da remoto in modo occulto

- La soluzione della PROVA ATIPICA ex art. 189 c.p.p.
- NON REGGERA' ANCORA MOLTO

***Cassazione sez.* 5, *Sent. n.* 16556 *del* 14/10/2009 Ud. (dep. 29/04/2010) Virruso**

Cassazione sez. 5, n. 48370, del 30 maggio 2017, Occhionero

Acquisizione occulta dei dati da remoto: Perquisizione occulta non notificata all'indagato e acquisizione di copia dei dati contenuti del PC/smartphone

QUID IURIS ?

Cass. Occhionero 2017

12. Tale ultima circostanza è smentita, quanto meno in parte, nell'ordinanza impugnata laddove, a contrasto della medesima doglianza prospettata con la memoria depositata dalla difesa dell'Occhionero al tribunale del riesame, riconduce le operazioni della polizia giudiziaria alla captazione in tempo reale di flussi informatici transitati sul computer dell'indagato, con acquisizione di 'dati contenuti nel computer, ovvero – congiunzione disgiuntiva *n.d.r.* - (d)i flussi informatici transitati sui dispositivi', rientrante, quest'ultima, nel concetto di intercettazione. Dal provvedimento impugnato si ricava, in altre parole, che l'agente intrusore impiegato ha captato, comunque, anche un flusso di comunicazioni, richiedente un dialogo con altri soggetti, oltre a documentazione relativa ad un flusso unidirezionale di dati confinati all'interno dei circuiti del *computer*, secondo la distinzione effettuata dalla giurisprudenza di questa Corte (Sez. 5, n. 16556 del 14/10/2009 - dep. 2010, Virruso, Rv. 246954).

13. Se così è, e non vi è ragione di dubitarne, non è necessario addentrarsi nella questione, irrilevante per quanto si osserverà subito dopo, se l'acquisizione dei dati presenti nell'*hard disk* del computer costituisca intercettazione (come ritenuto per i messaggi di posta elettronica, anche se già ricevuti o spediti dall'indagato e conservati nelle rispettive caselle di posta in entrata e in uscita, indipendentemente dal sistema intrusivo adottato dagli inquirenti, cioè tramite accesso diretto al *computer* o inserimento di un programma spia, da Sez. 4, n. 40903 del 28/06/2016, Grassi e altri, Rv. 268228), oppure se integri prova atipica (come ritenuto, allorché attraverso l'installazione di un captatore informatico, si proceda all'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati, dalla già evocata sentenza Virruso; ovvero, ancora, richieda un provvedimento di perquisizione e

CHIAMALA SE VUOI …….

“attività di captazione informatica”

- è assai limitativo parlare oggi solo di “captatore informatico” quando gli strumenti in uso alla criminalità impongono
- nuove e maggiori tecniche di captazione e di elusione degli apparati di cifratura (ormai con i telefoni Encrochat,
- cellulari cifrati olandesi BQ Acquaris, per citare solo alcuni, il solo captatore non serve più a nulla essendo necessari
- nuovi e diversi strumenti di Hacking), pertanto è più corretto e, in previsione futura, più efficace parlare di “attività di
- captazione informatica” al fine di prevedere ed estendere a livello normativo le opportune garanzie menzionate
- proprio dal DL n. 161 anche tutte le altre attività di captazione che la tecnologia rende e renderà possibile nel futuro e
- che non sono basate solo sul captatore ma sullo sfruttamento, in generale e in sintesi, delle vulnerabilità dei sistemi.

(citazione dall’Audizione dell’avv. Stefano Aterno presso la Commissione parlamentare (Senato della Repubblica) del 4 febbraio 2020)

Il punto fondamentale del controllo della Procura sull'attività del Captatore

Ma….chi effettua le operazioni di installazione, controllo, manutenzione ?

INVOCO qui
“La legge del Capitano della nave di Panama”: PROFESSIONALE E SICURO

se

Il 5 luglio 2015……

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Home - Garante Privacy | trenitalia - Cerca con Google | rcs-common/file.rb at master ... | Hacking Team ai clienti: "Non ... | Hacking Team hacked, attack...

www.repubblica.it/tecnologia/sicurezza/2015/07/07/news/hacking_team_galileo-118552287/

hacking team

Più visitati | Come iniziare | Ultime notizie | Delicious/statodiallerta | ANSA.it | I pezzi mancanti

DNSQUERIES | Reverse DNS lookup | Help

NETCRAFT | Services | Risk Rating | Since: August 1996 Rank: 124 Site Report [IT] Kataweb S.p.A

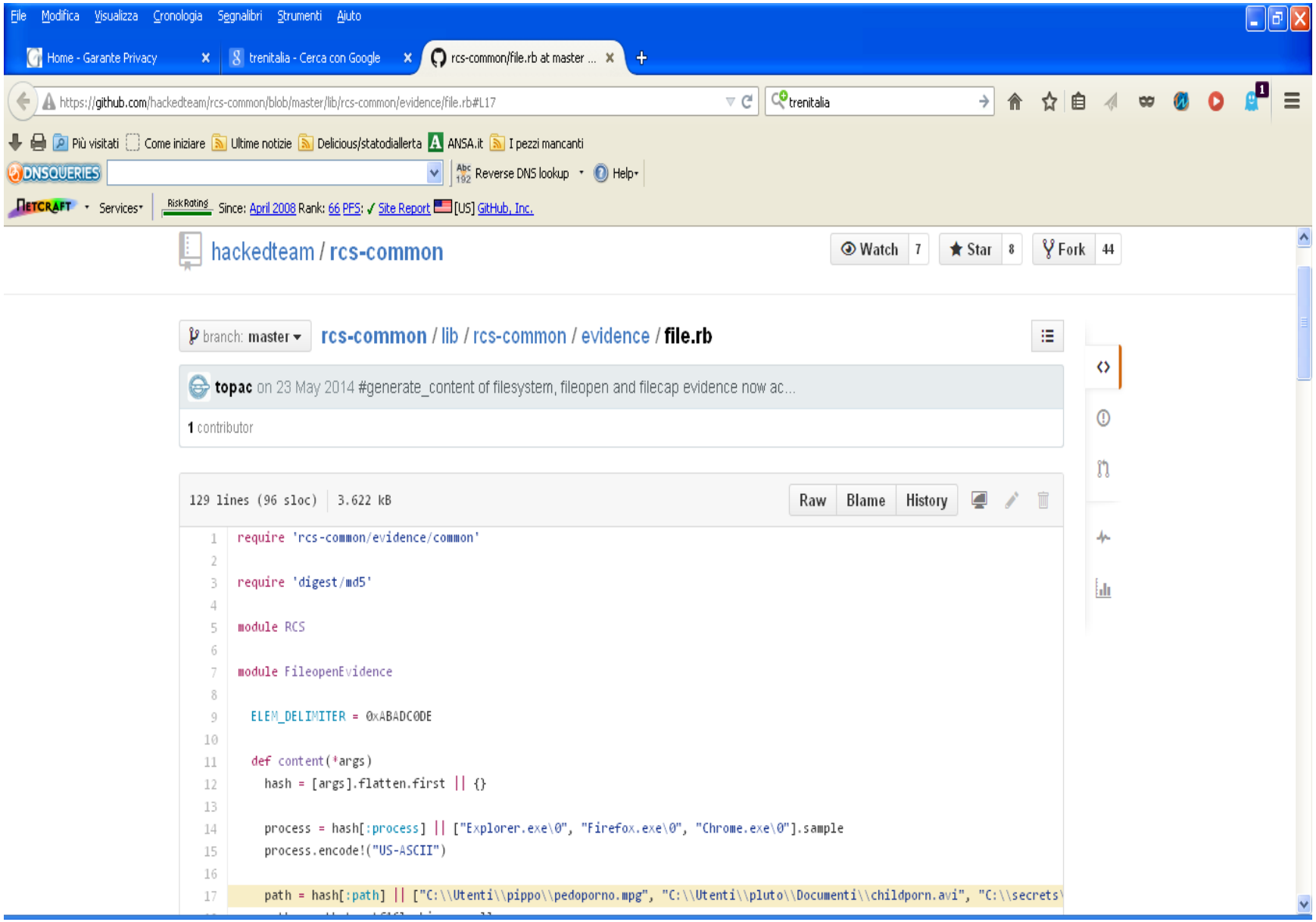
Hacking Team ai clienti: "Non usate il nostro programma-spia". E quello strano account Twitter...

Day after per la società milanese di sorveglianza informatica colpita da un fatale furto di dati e informazioni da 400GB dai quali si evincono e si confermano rapporti con governi e regimi dittatoriali, Sudan incluso. Un misterioso profilo sul social traccia un collegamento con un fatto analogo dello scorso anno contro la britannica Gamma

di SIMONE COSIMI

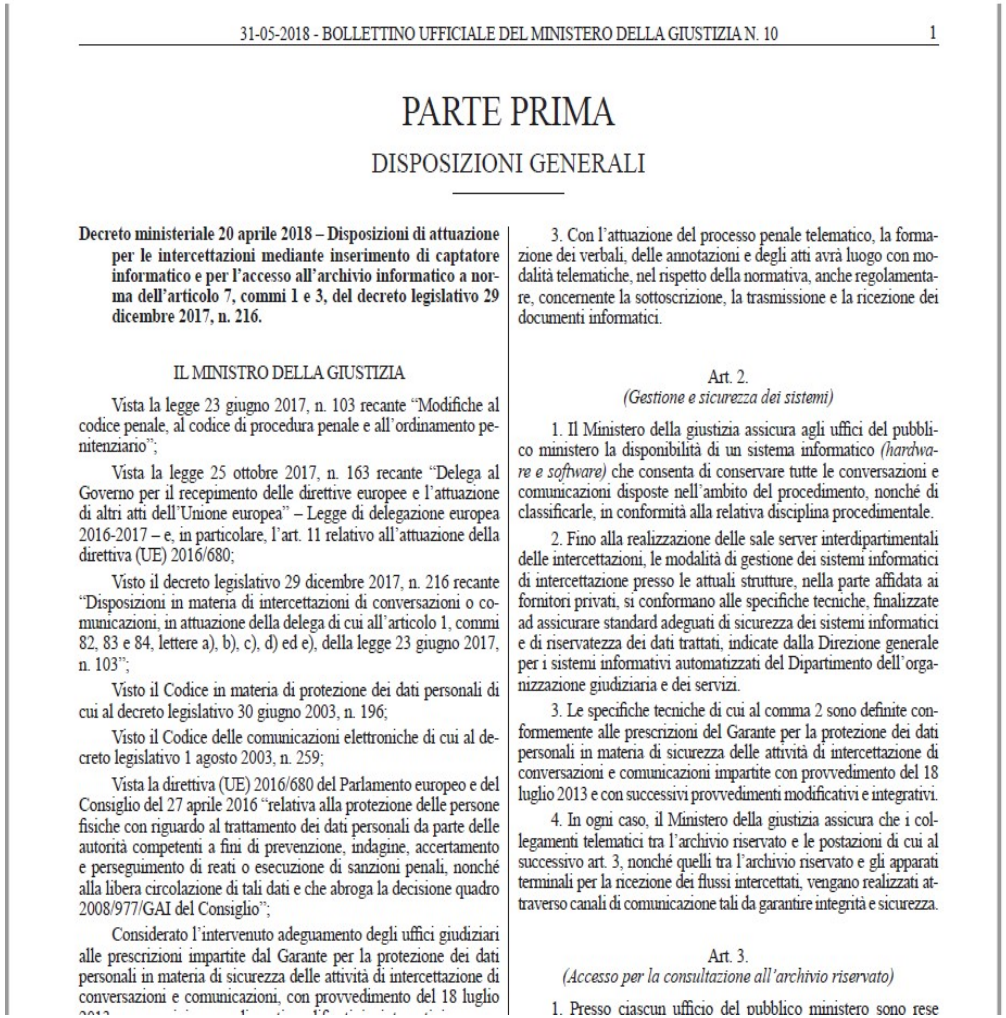
In attesa di scripts.kataweb.it...

2015\rcs-common · GitHub.pdf



L’importanza di un buon regolamento tecnico per evitare altri casi EXODUS art. 89 cpp

Tracciare attraverso idonei file di LOG ogni attività del captatore in modo da verificare il suo funzionamento ed eventuali abusi o errori involontari



PARTE PRIMA

DISPOSIZIONI GENERALI

Decreto ministeriale 20 aprile 2018 – Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l’accesso all’archivio informatico a norma dell’articolo 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216.

IL MINISTRO DELLA GIUSTIZIA

Vista la legge 23 giugno 2017, n. 103 recante “Modifiche al codice penale, al codice di procedura penale e all’ordinamento penitenziario”;

Vista la legge 25 ottobre 2017, n. 163 recante “Delega al Governo per il recepimento delle direttive europee e l’attuazione di altri atti dell’Unione europea” – Legge di delegazione europea 2016-2017 – e, in particolare, l’art. 11 relativo all’attuazione della direttiva (UE) 2016/680;

Visto il decreto legislativo 29 dicembre 2017, n. 216 recante “Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all’articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103”;

Visto il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Visto il Codice delle comunicazioni elettroniche di cui al decreto legislativo 1 agosto 2003, n. 259;

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 “relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;

Considerato l’intervenuto adeguamento degli uffici giudiziari alle prescrizioni impartite dal Garante per la protezione dei dati personali in materia di sicurezza delle attività di intercettazione di conversazioni e comunicazioni, con provvedimento del 18 luglio

3. Con l’attuazione del processo penale telematico, la formazione dei verbali, delle annotazioni e degli atti avrà luogo con modalità telematiche, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.

Art. 2.
(Gestione e sicurezza dei sistemi)

1. Il Ministero della giustizia assicura agli uffici del pubblico ministero la disponibilità di un sistema informatico *(hardware e software)* che consenta di conservare tutte le conversazioni e comunicazioni disposte nell’ambito del procedimento, nonché di classificarle, in conformità alla relativa disciplina procedimentale.

2. Fino alla realizzazione delle sale server interdipartimentali delle intercettazioni, le modalità di gestione dei sistemi informatici di intercettazione presso le attuali strutture, nella parte affidata ai fornitori privati, si conformano alle specifiche tecniche, finalizzate ad assicurare standard adeguati di sicurezza dei sistemi informatici e di riservatezza dei dati trattati, indicate dalla Direzione generale per i sistemi informativi automatizzati del Dipartimento dell’organizzazione giudiziaria e dei servizi.

3. Le specifiche tecniche di cui al comma 2 sono definite conformemente alle prescrizioni del Garante per la protezione dei dati personali in materia di sicurezza delle attività di intercettazione di conversazioni e comunicazioni impartite con provvedimento del 18 luglio 2013 e con successivi provvedimenti modificativi e integrativi.

4. In ogni caso, il Ministero della giustizia assicura che i collegamenti telematici tra l’archivio riservato e le postazioni di cui al successivo art. 3, nonché quelli tra l’archivio riservato e gli apparati terminali per la ricezione dei flussi intercettati, vengano realizzati attraverso canali di comunicazione tali da garantire integrità e sicurezza.

Art. 3.
(Accesso per la consultazione all’archivio riservato)

1. Presso ciascun ufficio del pubblico ministero sono rese

Le Procure devono avere i dati del Trojan subito memorizzati su server «in casa» e fare Audit periodici avvalendosi della PG specializzata presso le società a cui si rivolgono.

1. All'articolo 9 del decreto legislativo 29 dicembre 2017, n. 216, sono apportate le seguenti modificazioni:

Art. 9 (Disposizione transitoria).
 - 1. Le disposizioni di cui agli articoli 2, 3 4, 5 e 7 si applicano ai procedimenti penali iscritti dopo il 31 agosto 2020. 2. La disposizione di cui all'art. 2, comma 1, lettera b), acquista efficacia a decorrere dal 1° settembre 2020. (Omissis).».

Si riporta il testo dell'art. 2 del decreto-legge 30 dicembre 2019, n. 161 convertito, con modificazioni, dalla legge 28 febbraio 2020, n. 7, cosi' come modificato dalla presente legge:
«Art. 2 (Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni). - 1. Al codice di procedura penale, approvato con decreto del Presidente della Repubblica 22 settembre 1988, n. 447, sono apportate le seguenti modificazioni:

c) all'art. 92, comma 1-bis, dopo le parole «conservazione nell'archivio» e' soppressa la parola «riservato».

3. Con decreto del Ministro della giustizia sono stabiliti i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante inserimento di captatore informatico su dispositivo elettronico portatile. 4. I requisiti tecnici sono stabiliti secondo misure idonee di affidabilita', sicurezza ed efficacia al fine di garantire che i programmi informatici utilizzabili si limitano all'esecuzione delle operazioni autorizzate.

Grazie per l’attenzione

resto a vostra disposizione per eventuali domande

Avv. Prof. Stefano Aterno

www.studioaterno.it

s.aterno@studioaterno.it

STUDIO LEGALE
ATERNO