Mercoledì 6 Dicembre 2017
Nuova serie - Anno 27 - Numero 287 - Spedizione in A.P. art. 1 c.1 L. 46/04, DCB Milano
* *Offerta indivisibile con* Marketing Oggi *(ItaliaOggi € 1,20 + Marketing Oggi € 0,80)*

Uk £ 1,40 - Ch fr. 3,50
Francia € 2,50 **€2,00***

9 771120 606007 71206

www.italiaoggi.it

ItaliaOggi

QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO

L'occhio del fisco nel cellulare

La Guardia di finanza è autorizzata a cercare indizi di evasione anche tra i contenuti di tablet, applicazioni di messaggistica e chat archiviati nel cloud

La Guardia di finanza cercherà i segnali di evasione anche su tablet, smartphone, applicazioni di messaggistica e chat, andando a spulciare documenti e materiali che vengono archiviati sul cloud. Lo prevede la nuova circolare operativa sui controlli. Personale qualificato in Data Analysis verificherà i contribuenti che utilizzano sistemi informatici avanzati e complessi di protezione e archiviazione dei dati.

LE FIAMME GIALLE SI SPECIALIZZANO NELL'ESTRAZIONE DEI DOCUMENTI INFORMATICI

A caccia di evasori anche nelle memorie degli smartphone

La Guardia di finanza cercherà i segnali di evasione anche nel cloud. Non sfuggiranno alle attenzioni dei militari delle fiamme gialle neppure i tablet, gli smartphone, i client di posta elettronica e le applicazioni di messaggistica e chat.

Alla ricerca e alla estrazione di documenti informatici in chiave antievasione la nuova circolare operativa n. 1/2018 sui controlli, diramata dal comando generale delle fiamme gialle, dedica infatti una particolare attenzione.

All'interno del corposo manuale viene ribadita, con forza, l'assoluta importanza di procedere all'acquisizione di tutti gli elementi utili alle attività di natura tributaria, che i contribuenti che adottano sistemi digitali complessi, ovvero che operano nel segmento della c.d. economia digitale oppure che si avvalgono dei sistemi cc.dd. Cloud, potrebbero aver celato all'interno di questi strumentazioni informatiche.

L'evoluzione continua e senza sosta delle tecnologie digitali di archiviazione e di protezione dei dati – si pensi ad esempio ai sistemi di cifratura e criptatura dei files – impongono ai reparti operativi della Guardia di finanza l'impiego di militari in possesso di specifiche qualifiche. Si tratta di personale qualificato Cfda (Computer forensics e data analysis) che verrà impiegato per le verifiche su contribuenti che utilizzano sistemi informatici avanzati e complessi di protezione e archiviazione dei dati.

Il manuale operativo suddivide queste particolari tipologie di verifiche e di ricerche di dati ed indizi di evasione in due differenti tipologie di approcci in funzione dello stato di funzionamento dei dispositivi che si intende acquisire nel corso delle attività.

Si tratta nello specifico delle static analysis, che verranno effettuate quando l'acquisizione è stata eseguita su dispositivi spenti (c.d. post mortem) e delle live analysis, comprendente tecniche di analisi su sistemi attivi per tutti quei dati che si perderebbero spegnendo il dispositivo (Ram, chiavi di cifratura contenute nella memoria temporanea, server, cloud storage ecc.).

A seconda del tipo di approccio da utilizzare nel corso della verifica sui sistemi informatici del contribuente cambiano ovviamente le modalità di acquisizione e ricerca dei dati.

Nel primo caso i militari procederanno con le operazioni di analisi sulla copia forense del dato informatico o del documento digitale acquisito e non anche sull'originale, in virtù del fatto che occorre preservarne l'integrità ai fini dell'eventuale ripetibilità e riproducibilità.

Nel secondo scenario invece, con i sistemi attivi e funzionanti ed al preciso fine di non compromettere l'irripetibilità degli atti, i militari procederanno sempre in contraddittorio con il soggetto sottoposto a verifica o con un suo delegato.

Per quanto riguarda invece gli scenari che si possono presentate durante le operazioni di verifica su sistemi informatici di una certa complessità, il nuovo manuale operativo delle fiamme gialle fornisce una serie di esempi tipici.

Fra questi figurano le ricerche di file cancellati, la ricerca di determinati tipi di file (documenti di testo, piuttosto che documenti contabili digitali oppure e-mail), la ricostruzione della cronologia delle operazioni eseguite sul sistema oppure a quella dell'utilizzo di specifiche applicazioni come browser o client di posta o, ancora, applicazioni di messaggistica e chat.

In altre circostanze, si legge ancora nel nuovo manuale operativo, le analisi e le ricerche da effettuare sono direttamente correlate da un punto di vista tecnico e degli strumenti da utilizzare dal sistema in cui le prove possono essere celate. Da questo punto di vista si pensi ad esempio agli smartphone o ai tablet oppure ad analisi da svolgersi su sistemi cloud o virtualizzati.

Tutte le operazioni effettuate dai militari operanti dovranno essere attentamente documentate e verbalizzate in modo chiaro e preciso, per poter consentire a chiunque di ripetere le medesime analisi che, laddove correttamente eseguite, forniranno i medesimi risultati.

Il manuale sulle verifiche fiscali pone inoltre l'accento sulla possibilità di acquisire dati informatici detenuti presso soggetti terzi diversi dal verificato.

Tale situazione, che si presenta piuttosto spesso nella pratica, trova un preciso supporto da parte della giurisprudenza della Corte di cassazione che di recente (sentenza n. 17420 del 30 agosto 2016) ha ribadito che i file contenuti su supporto magnetico, rinvenuti presso un soggetto terzo, costituiscono elemento probatorio, sia pure presuntivo, atto a comprovare l'esistenza di una contabilità parallela, tale da legittimare l'accertamento induttivo.

Andrea Bongi