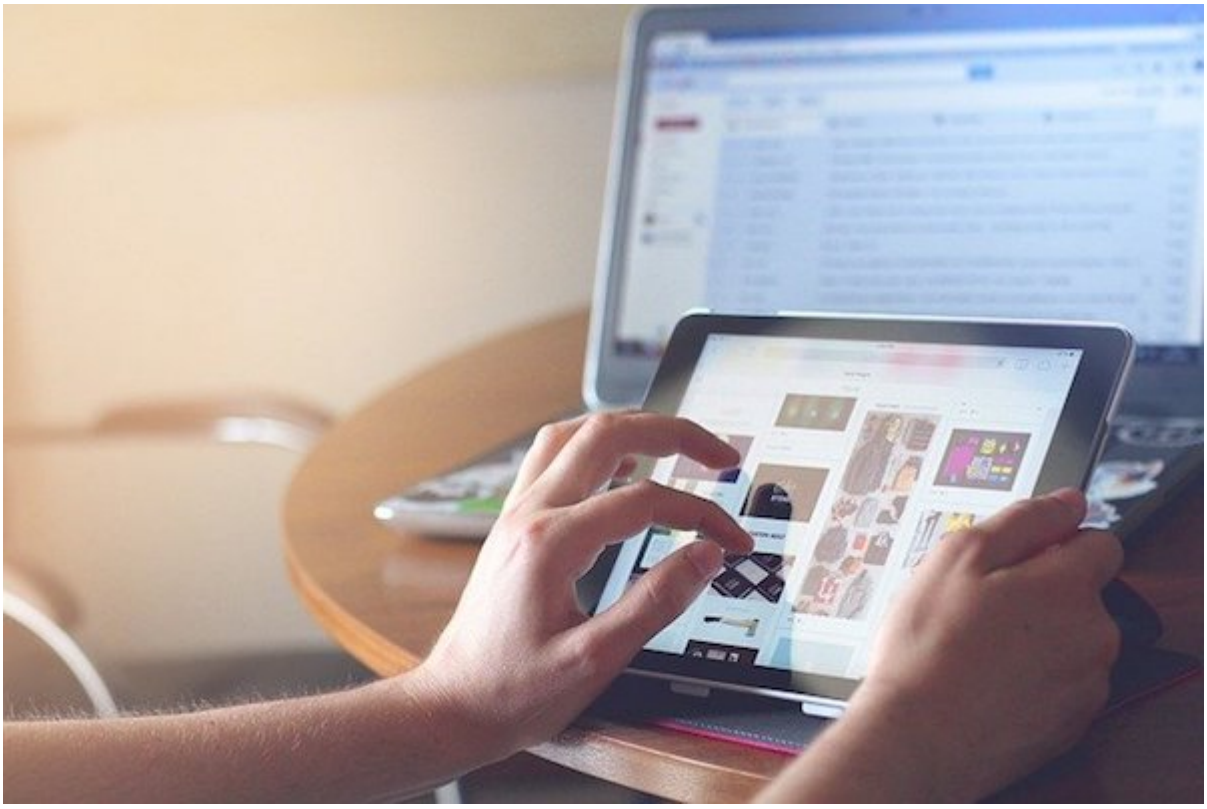
LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

Sequestro informatico: cos’è e come funziona

Autore: Paolo Remer | 26/03/2021



L’acquisizione probatoria dei dati su dispositivi e server è consentita se c’è un decreto del pm che sta indagando: quali sono le condizioni di legittimità?

Si può sequestrare una e-mail, o una conversazione su WhatsApp, o un archivio

digitale tenuto su un cloud estero? Da qualche anno, sì: i reati possono essere commessi in molti modi e spesso anche da remoto. Pensa a uno stalking virtuale, alla diffusione di materiale pedopornografico o al riciclaggio illecito di capitali e valute. Insomma, i crimini non conoscono confini e la nostra legislazione si è adeguata, prevedendo uno strumento specifico per contrastarli in modo efficace. Si tratta del **sequestro informatico: cos'è e come funziona?**

Ora, ti descriveremo le condizioni che legittimano l'acquisizione dei dati contenuti in un computer, su uno smartphone o qualsiasi altro tipo di dispositivo. E non è nemmeno necessario disturbarti di persona, perché i dati possono essere prelevati direttamente dal fornitore del servizio di traffico informatico o telematico. Vedrai che la polizia giudiziaria può compiere anche l'accesso ai server dovunque essi siano dislocati e, perciò, non basta evitare di detenere i dati presso di sé per sfuggire alle investigazioni: ad esempio, una contabilità nera tenuta su un cloud dislocata all'estero non è sfuggita alla Guardia di Finanza, che l'ha acquisita come prova del reato di evasione fiscale su cui stava indagando sotto la direzione della Procura della Repubblica.

Trattandosi di strumenti molto invasivi per la privacy degli interessati, ogni attività di questo genere deve essere autorizzata dal magistrato, che deve anche precisare le modalità di compimento. E servono anche particolari cautele per copiare i dati, mantenerne la fedeltà all'originale e preservarli dal pericolo di cancellazione o di dispersioni.

Sequestro di materiale informatico e telematico

La legge **[1]** consente dal 2008 il sequestro probatorio dei dati detenuti presso i **fornitori di servizi** informatici, telematici o di telecomunicazioni. Il provvedimento è emesso dal pubblico ministero (in breve, il pm) e viene eseguito direttamente presso le società che erogano i servizi di connessione o di stoccaggio dei dati degli utenti. In questo, il sequestro informatico si differenzia dal "classico" sequestro compiuto con una perquisizione fisica dei luoghi nella disponibilità del soggetto di interesse investigativo: il destinatario è diverso. I dati sono tuoi ma il sequestro è rivolto a chi li trasmette o li conserva.

La norma è stata inserita per colmare una lacuna: fino a quel momento, non

esisteva un modo giuridicamente valido per eseguire il **sequestro di dati informatici** conservati su archivi virtuali, o server, situati in luoghi remoti, spesso all'estero, e comunque appartenenti a soggetti diversi da quelli nei cui confronti vengono eseguite le indagini penali.

Fino a quel momento, l'unica norma analoga era quella che riguardava il **sequestro di corrispondenza [2]** che consentiva di intervenire presso gli uffici postali o gli altri fornitori di servizi di comunicazioni, ma la disposizione era "pensata" prevalentemente per i plichi cartacei e non funzionava per quelli digitali, che viaggiano in rete a prescindere dal supporto fisico di trasmissione. Così, il legislatore del 2008 ha precisato che questo tipo di sequestro può avvenire anche se i dati sono «inoltrati per via telematica», come un **messaggio di posta elettronica** e oggi anche il contenuto di una **chat** presente su **WhatsApp** o altri sistemi analoghi di messaggistica istantanea.

La copia forense dei dati

L'acquisizione dei dati può avvenire, oltre che con la loro apprensione diretta, «mediante copia di essi su adeguato supporto». In tali casi, per la validità del sequestro, occorre seguire «una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità». Si tratta della cosiddetta "**copia forense**", molto utilizzata quando si deve sequestrare un cellulare; ma anche quando essa viene realizzata e i dati copiati vengono così acquisiti al procedimento penale, il fornitore dei servizi rimane obbligato a «conservare e proteggere adeguatamente i dati originali», per evitare il pericolo della loro dispersione.

Quindi, la metodologia del sequestro cambia a seconda dei casi: la polizia giudiziaria può acquisire fisicamente i supporti su cui i dati sono detenuti (hard disk, supporti di memoria esterna, server, ecc.) oppure eseguire il sequestro "a distanza" notificando il provvedimento del magistrato al **fornitore di servizi** che in quel momento detiene i dati, li tratta o li custodisce: specialmente in queste ipotesi, occorre preservare la garanzia della loro immodificabilità, perché viene coinvolto un soggetto esterno che non è colpito dalle indagini in corso e nei suoi confronti occorre questo ordine di conservazione dei dati digitali che mantiene sui propri apparati.

Per questo motivo, agli atti del procedimento penale viene acquisita la copia

forense, identica all'originale di cui costituisce una duplicazione eseguita con particolari accorgimenti tecnici (si realizza una "*bit-stream image*", cioè la copia di ogni singolo bit di dati da un dispositivo all'altro, con un metodo che assicuri la genuinità e la fedeltà). In questo modo, si tende a preservare, come ha sottolineato recentemente la Corte di Cassazione **[3]**, l'**integrità probatoria** del dato digitale, che altrimenti sarebbe per sua natura volatile e fragile, in quanto suscettibile di manomissioni o cancellazioni.

Il decreto di sequestro

Il **decreto di sequestro** probatorio informatico è emesso dal pm e deve precisare le modalità di **acquisizione della prova digitale** e della sua conservazione in vista del processo. L'indagato potrebbe infatti contestare l'illegittimità del provvedimento impugnandolo presso il tribunale del riesame **[4]** e chiederne l'annullamento per carenza di presupposti. In tal caso, il sequestro cadrebbe e le cose andrebbero immediatamente restituite.

Il sequestro probatorio è infatti un mezzo di **ricerca della prova** che soggiace ai normali limiti previsti dal Codice di procedura penale **[5]** anche quando riguarda dati digitali o telematici: occorre sempre che essi siano riferiti al reato per cui si procede e precisamente devono essere qualificati o come «**corpo del reato**», cioè le cose sulle quali o attraverso le quali il reato è stato commesso o ne costituiscono il prodotto, profitto o prezzo, oppure come «cose pertinenti al reato necessarie per l'accertamento dei fatti».

La **motivazione** del sequestro probatorio deve perciò riportare, sia pur sinteticamente, la relazione tra la cosa sequestrata e il reato: non è ammesso il sequestro "esplorativo", finalizzato a ricercare una **notizia di reato** che deve esserci già per legittimare il vincolo apposto sui dati informatici **[6]**. Quando questo nesso c'è, è consentita l'acquisizione anche di una grossa mole di dati, nel cui ambito gli investigatori selezioneranno quelli di interesse a fini di prova: ad esempio, la Corte di Cassazione ha ritenuto che i principi di proporzionalità, adeguatezza e gradualità sono rispettati quando si sequestra un intero dispositivo, come un personal computer o uno smartphone, per ricercare un solo file illecito **[7]**.

In alcuni casi, potrebbe essere necessario sottoporre i dati informatici ad accertamenti tecnici irripetibili **[8]** finalizzati alla loro estrazione o elaborazione,

con una modifica irreversibile che non consentirebbe più di riportarli al loro stato originale; dunque, occorre far partecipare l'indagato alle operazioni tecniche, a pena di inutilizzabilità della prova acquisita.

Il sequestro informatico della Guardia di Finanza

La **Guardia di Finanza** ricorre spesso al sequestro di dati informatici e telematici per accertare le violazioni penali alla normativa tributaria, anche quando essi sono detenuti su **cloud e server esteri**: così una **contabilità in nero** non sfugge e può essere prelevata e analizzata pur trovandosi fisicamente in un luogo remoto e diverso dai locali dove è stato effettuato l'accesso finalizzato alla verifica fiscale.

Con una recente sentenza la Cassazione **[9]** ha ritenuto legittima l'**acquisizione dei dati informatici** compiuta dalle Fiamme Gialle su un server dislocato in Olanda: a nulla è valsa l'opposizione del soggetto verificato, che voleva denunciare i finanzieri per il reato di **accesso abusivo** al sistema telematico.

La Suprema Corte ha affermato che i militari hanno esercitato in modo legittimo i poteri loro conferiti dalla legge ed hanno agito in conformità al decreto di sequestro emanato dal pm, che proprio attraverso quell'acquisizione probatoria intendeva verificare la commissione dell'illecito fiscale su cui stava indagando.

Leggi anche: "Se viene la Finanza mi può sequestrare il computer?".

Note

[1] Art. 254 *bis* Cod. proc. pen. **[2]** Art. 254 Cod. proc. pen. **[3]** Cass. sent. n. 34265 del 02.12.2020. **[4]** Art. 257 Cod. proc. pen. **[5]** Art. 253 Cod. proc. pen. **[6]** Cass. sent. n. 37941 del 31.12.2020. **[7]** Cass. sent. n. 24617/2015, n. 16622/2017 e n. 28456/2019. **[8]** Art. 360 Cod. proc. pen. **[9]** Cass. sent. n. 11207 del 24.03.2021.