Accertamenti induttivi tra le "nuvole": la frontiera del *Cloud computing*

Lo sviluppo di sistemi di conservazione dei dati su piattaforme delocalizzate sulla rete dalle quali è possibile accedere da qualunque parte del globo impone talune riflessioni sulla necessità di fondere l'approccio tradizionale di ricerca delle prove con le moderne tecniche dell'informatica investigativa.

di **MARCO STELLA*** e **IVAN DI PIETRO****

Introduzione

Con ordinanza n. 17420 del 30 agosto 2016 la Corte di Cassazione, accogliendo un ricorso avanzato dall'Agenzia delle Entrate, ha stabilito l'utilizzabilità di file informatici rinvenuti presso un "terzo" al fine di adottare l'accertamento induttivo nei confronti di un contribuente infedele.

Nel caso di specie, il "terzo" in questione era un fornitore, presso il quale sono state rinvenute, su supporto informatico, evidenze digitali di transazioni non dichiarate.

L'episodio in sé potrebbe sembrare confinato a meri aspetti procedurali nell'ambito delle ordinarie attività ispettive condotte dall'Amministrazione finanziaria.

Tuttavia, la generica indicazione del "terzo" quale depositario di documentazione rilevante ai fini tributari consente di estendere le prescrizioni della Suprema Corte a scenari assai più avveniristici e attuali, sia da un punto di vista operativo, che in relazione alle procedure tecniche di acquisizione del dato.

Supponiamo, infatti, che il "terzo" sia un cosiddetto *Cloud Service Provider* (CSP), ossia il fornitore di servizi telematici offerti tramite una piattaforma informatica remota. Si pensi, in particolare, ai diffusi sistemi di *cloud storage*, ossia a quelle piattaforme che consentono di memorizzare file di vario genere, in modo che quest'ultimi risultino accessibili, in maniera sincronizzata, da diversi dispositivi.

Nulla vieta che un contribuente scelga di conservare gli archivi contenenti la propria contabilità ovvero quella "parallela" su servizi di questo genere.

Alla luce di quanto affermato dalla Suprema Corte, pertanto, anche simili evidenze digitali, opportunamente acquisite e preservate, qualora costituiscano indizi gravi, precisi e concordanti, potrebbero essere posti alla base di un accertamento induttivo.

Peraltro, l'utilizzo di simili sistemi non appare nemmeno così inusuale, come dimostrato, ad esempio, dagli esiti di una recente operazione della Guardia di Finanza, che ha consentito di individuare uno strumento *software*, specificatamente rivolto ad una categoria professionale, in grado non solo di tenere una contabilità parallela, ma anche di occultarla agli occhi dei verificatori, conservandone una copia su un servizio remoto offerto dalla casa produttrice, utilizzabile anche per ripristinarne i contenuti nel caso in cui il professionista avesse optato per la cancellazione sicura della contabilità "in nero" sui propri sistemi locali.

Considerazioni di natura tecnica

L'acquisizione documentale fatta sul *cloud* non esime dall'adozione delle buone pratiche connesse alla corretta gestione delle evidenze digitali. Anzi, rispetto alle tradizionali attività di informatica investigativa, meglio nota come *digital forensics*, l'individuazione e l'acquisizione di *file* su servizi di *cloud storage* comporta maggiori difficoltà, dovendo adottare metodologie tipiche sia della *computer forensics*, ossia del trattamento di memorie presenti presso il contribuente, che della *network forensics*, connessa all'analisi dell'interazione dell'utente con servizi remoti.

Per prima cosa, nello scenario che stiamo analizzando va evidenziato il carattere ubiquo dell'informazione, che non risiede più esclusivamente all'interno del pc del

soggetto sottoposto a verifica, ma anche su una moltitudine di altri dispositivi eterogenei, tipicamente rientranti nella categoria dei dispositivi *mobile* (*smartphone*, *tablet*), nonché, naturalmente, presso l'infrastruttura telematica del CSP.

Lo scopo dell'informatica investigativa è quello di individuare i cosiddetti *artifact*, ovvero le "prove digitali" dell'interazione dell'utente con una certa applicazione. Gli stessi documenti sono degli *artifact*, ma oltre al dato in sé, assumono valore investigativo anche i meta-dati che rappresentano una preziosa fonte di informazioni utili a dimostrare i tempi e i modi con cui l'utente e il sistema hanno interagito. Un tipico esempio di meta-dato è la data di creazione di un file.

Per poter individuare le possibili fonti di *artifact* in un contesto in cui si ipotizza l'uso di sistemi di *cloud storage* per la memorizzazione della contabilità "in nero", occorre per prima cosa ripercorrere le modalità di accesso al dato, che può avvenire attraverso:

- un'applicazione *web*. In questo caso l'utente si autentica su un portale *web* e accede, tramite un'apposita interfaccia predisposta dal CSP, ai propri documenti. Gli *artifact* rilevanti in questo scenario sono da rintracciarsi all'interno del *browser*, il *software* per la navigazione *web*;
- un *client desktop*, che consiste in un programma installato su un pc che interagisce in maniera automatica con il servizio di *cloud storage*. Tipicamente, applicativi di questo tipo predispongono una cartella di *file* che, ipotizzando di disporre di una connessione telematica persistente, è costantemente sincronizzata con lo spazio di memorizzazione concesso dal CSP. In pratica, quando si inserisce un file nella cartella, un servizio automatico di sincronizzazione avvia il contestuale *upload* sul sistema remoto. Viceversa, a seguito del caricamento di un file sulla piattaforma remota, il servizio scarica (*download*) una copia del *file*. In questo caso gli *artifact* sono costituiti dagli stessi *file* conservati in locale, acquisibili con le normali tecniche prescritte dalla *computer forensics*. Un'analisi più approfondita degli specifici *client* (es. Dropbox, Google Drive, One Drive, ecc.) può consentire di rilevare anche meta-dati di interesse investigativo, come la cronologia di pregressi *upload/download* riferiti anche a *file* cancellati (a tal proposito, si veda, tra le altre, la presentazione di M. Epifani tenuta per il Clusit Security Summit del 2014[1]);
- una *mobile app:* i sistemi di *cloud storage* esprimono la loro potenza nell'interazione con i dispositivi *mobile*. Quest'ultimi, essendo dotati di risorse di memoria limitate, accedono al *file* remoto *on demand*. In locale, infatti, viene mantenuto il solo elenco dei *file* disponibili (un altro esempio di meta-dato); il contenuto vero e proprio viene scaricato, in forma temporanea, solo a seguito di una specifica richiesta. A causa di tale tipo di interazione con il servizio *cloud*, il solo accesso allo *smartphone* non consentirebbe di acquisire massivamente i contenuti remoti. In questo caso, tuttavia, l'*artifact* di interesse è costituito dai dati che il dispositivo usa per autenticarsi presso il servizio. Infatti, a parte un primo *login* che l'utente effettua *una tantum*, gli accessi successivi avvengono in maniera automatica, poiché all'interno del dispositivo viene memorizzato il cosiddetto *token* di autenticazione: un insieme di dati che identificano univocamente l'utente. Esistono strumenti di *digital forensics* in dotazione alle Forze di Polizia che consentono di estrarre tale *token* dal dispositivo e di riutilizzarlo tramite un apposito *software* di analisi per accedere ai contenuti remoti e acquisirne una copia garantendone l'integrità;
- una *application programming interface (API).* In questo caso l'interazione dell'utente non è diretta, ma mediata da un'applicazione realizzata *ad hoc*. Una API, infatti, è un modulo *software* che può essere integrato all'interno di un applicativo personalizzato. Potrebbe essere questo il caso, ad esempio, del programma di occultamento utilizzato dai soggetti sottoposti a verifica nel corso della citata operazione. In questo caso gli *artifact* dipendono dal tipo di applicativo ma, in linea di massima, possono essere identificati con i *log* delle connessioni al servizio, dominio di azione di quella parte della *digital forensics* nota come *network forensics*.

Ovviamente, i *file* sono anche conservati presso il "terzo" (il CSP) e, proprio come nel caso della sentenza della Corte di Cassazione, possono essere utilizzati per l'accertamento.

Occorre, tuttavia, tenere in debito conto anche in questo caso le peculiarità tecniche connesse all'utilizzo di sistemi di *cloud storage*:

- virtualizzazione dei sistemi: le piattaforme *cloud* hanno avuto un grande successo soprattutto per la loro flessibilità, nel senso che le risorse fisiche disponibili (memoria, potenza di calcolo) vengono assegnate dinamicamente all'utente, in base alle specifiche esigenze. In pratica, se l'utente ha bisogno di raddoppiare lo spazio di memorizzazione, grazie al *cloud* ciò può essere fatto dal CSP senza riservare nuove risorse fisiche (es. installando un nuovo disco), ma riallocando dinamicamente lo spazio di *storage* già disponibile. La conseguenza di tale architettura è una sorta di indeterminazione circa la posizione fisica del *file* di inte-

resse. In altri termini, i file possono essere distribuiti, in maniera dinamica e parzialmente prevedibile, su apparati fisici geograficamente separati, anche a livello globale;
- *multi-tenancy:* sempre in virtù della flessibilità dell'allocazione delle risorse, queste sono condivise tra più utenti (*tenant*). Conseguentemente, una richiesta di accesso avanzata nei confronti del CSP dovrebbe poter fare affidamento sulla possibilità di isolare le risorse allocate ad altri utenti che nulla hanno a che vedere con il procedimento in corso e di cui bisogna preservare la *privacy*;
- internazionalità: non è detto che il CSP operi sul territorio nazionale. Peggio, lo stesso CSP potrebbe a sua volta appoggiarsi ad altri CSP, creando così una catena di dipendenze, a livello internazionale, che mina profondamente la capacità di una Forza di Polizia di ottenere il necessario supporto in tempi compatibili con le indagini.

CLOUD COMPUTING

È un sistema telematico per il trattamento dei dati condivisi tra più postazioni per il quale non è sempre agevole individuare una sfera spaziale certa. Le informazioni sono consultabili e acquisibili pertanto in condizioni di parità su tutti i mezzi con i quali può avvenire l'accesso

Riflessioni di natura tecnico-professionale

Come detto, la Suprema Corte di Cassazione, accogliendo il ricorso dell'Amministrazione finanziaria, nella sentenza in esame ha ribadito l'orientamento di legittimità secondo il quale la contabilità "in nero", costituita da documenti informatici, assume rilevanza probatoria, sia pure meramente presuntiva.

Da ciò ne discende che la pronuncia della Suprema Corte ha, di fatto, confermato due importanti principi: da una parte, i *file* informatici costituiscono elemento probatorio, sia pure presuntivo, "*legittimamente valutabile in relazione all'esistenza delle operazioni non contabilizzate (Corte Cass., n. 20902 del 2014)*"; dall'altra, l'inattendibilità delle scritture contabili e quindi l'accertamento induttivo dei ricavi può essere fondato "*su documentazione reperita presso terzi e su annotazioni elaborate da terzi*"[2].

Pertanto si continua a ritenere acquisibili ed utilizzabili gli elementi documentali reperiti presso soggetti terzi rispetto al verificato, non sussistendo – nell'ordinamento italiano – un generale divieto di acquisizione ed utilizzazione di detta documentazione. Sul punto la stessa Corte di Cassazione, con la sentenza n. 9108 del 6 giugno 2012, ha, fra l'altro, confermato la legittima acquisizione della documentazione reperita presso terzi. In tal senso, infatti, viene specificato che "*nessun pregiudizio al diritto di difesa subisce, peraltro, il terzo che dai documenti acquisiti nel corso della verifica risulti avere intrattenuto rapporti commerciali con il contribuente verificato; dall'altro che il contribuente, nei cui confronti l'Amministrazione finanziaria emetta avvisi di accertamento fondati in tutto od in parte sulla documentazione od informative acquisite presso terzi, è posto comunque in grado di esercitare in modo pieno e senza alcun limite il proprio diritto di difesa*".

La legittimità dell'operato dei verificatori va valutata, in ultima istanza, rispetto alle modalità del suo esercizio. Ciò che rileva è l'attendibilità delle prove e non i luoghi in cui sono state acquisite.

Di contro e ad ulteriore precisazione per affrontare il contesto in esame, in altre pronunce[3] la Suprema Corte ha valutato come non legittimo l'accertamento induttivo posto in essere esclusivamente in base a dati ritenuti, nei fatti, non attendibili, in quanto desunti da un *software* aziendale strutturalmente e funzionalmente non correlato alle scritture contabili obbligatorie.

L'ufficio è dunque legittimato a utilizzare, nei confronti del contribuente sottoposto ad accertamento, documenti informatici rinvenuti presso terzi qualora sussistano ulteriori elementi indiziari da cui sia possibile dedurre consequenzialmente che la contabilità ufficiale non è veritiera.

In tal senso, la stessa Cassazione[4] aveva peraltro già affermato che, se fosse precluso agli organi verificatori di prendere visione e, se del caso, acquisire atti e dati fiscalmente rilevanti nei confronti di terze persone (non menzionate nel provvedimento di autorizzazione), "*sarebbe agevole per il contribuente infedele sottrarre alle verifiche la propria documentazione fiscale, bastando a ciò il semplice accorgimento di conservarla presso un'altra persona*".

Quanto sopra in una logica di coerenza interna del sistema tributario, in quanto tale sistema è mosso proprio dall'esigenza contraria, diretta a potenziare gli strumenti di accertamento, in modo da creare i presupposti per garantire l'osservanza dei doveri tributari[5] imposti a tutti nella più ampia cornice dell'art. 53 della Costituzione.

Con riferimento inoltre ai servizi di tipo "*cloud*", la Suprema Corte di Cassazione – valutando gli aspetti relativi alla competenza territoriale sulla fattispecie delittuosa di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-*ter* c.p. – ha osservato[6] che, in questo caso, l'azione telematica viene realizzata attra-

verso una connessione tra sistemi informatici distanti tra loro, cosicché gli effetti di un'interazione con tali sistemi possono esplicarsi in un luogo diverso da quello in cui un utente si trova. In aggiunta, l'operatore, sfruttando le reti di trasporto delle informazioni, è in grado di interagire contemporaneamente sia sul computer di partenza sia su quello di destinazione.

La giurisprudenza di legittimità continua con la constatazione che "*(...) nel cyberspace i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio). Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione*".

Del resto, come già accennato, la "*dimensione aterittoriale*" si è incrementata da ultimo con la diffusione dei dispositivi mobili (*tablet*, *smartphone*, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo.

Viene anche osservata l'oggettiva difficoltà di individuare il luogo nel quale le informazioni sono collocate qualora i dati sono archiviati su *cloud computing* o resi disponibili da *server* che sfruttano tali servizi.

In tal senso e a maggior corroborazione di quanto già trattato nelle considerazioni di natura tecnica, è stato anche specificato che un sistema telematico per il trattamento dei dati condivisi tra più postazioni (come potrebbe essere il *cloud computing*) assume carattere unitario e, per la sua capacità di rendere disponibili le informazioni in condizioni di parità a tutti gli utenti abilitati, il luogo di ubicazione della postazione remota dalla quale avviene l'accesso assume, di per sé, una rilevanza giuridica suscettibile di essere opportunamente analizzata.

Conclusioni

Il tema dell'"accesso" ai dati, nel senso più ampio del termine, detenuti da terzi ed il loro utilizzo – a parere di chi scrive – ricomprende, per molti versi, anche la ricerca di elementi probatori tipici di un'attività di controllo in ambito di polizia economico-finanziaria.

In sintesi, se si considera uno scenario operativo in cui occorre acquisire un dato informatico di possibile interesse operativo, qualora quest'ultimo sia utilizzato e conservato attraverso un servizio di tipo *cloud computing*, non appare corretto ritenere che lo stesso dato si trovi solo nei *server* gestiti dal *Cloud Service Provider*, poiché il sistema stesso è "ubiquitario" e "diffuso" sul territorio. Contestualmente è compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate per l'accesso al *cloud*, tanto che – come sopra argomentato – le tracce delle operazioni compiute all'interno della rete e le informazioni relative agli accessi sono reperibili, in tutto o in parte, sia nei *server* che nel *client*.

In conclusione, occorre porre l'attenzione su un tema di estrema attualità in cui vi è la necessità di fondere l'approccio più tradizionale di tipo operativo con quello più marcatamente tecnico della *cloud forensics*, tenendo nella dovuta considerazione l'evoluzione tecnologica dei sistemi informatici e delle relative tecniche di investigazione.

* **Marco Stella,** *Maggiore della Guardia di Finanza, in servizio presso il Comando Generale.*

** **Ivan Di Pietro,** *Capitano della Guardia di Finanza, in servizio presso il Comando Generale.*

Note

1 M. Epifani, *Cloud Forensics – Tecniche di acquisizione e analisi*, 2014, *[Online]*. Disponibile: *https://www.securitysummit.it/.*

2 G. Antico, "*I files rinvenuti presso terzi possono legittimare l'accertamento induttivo – commento*", Fisco, 2016 – D. De Marco, "*File informatici "compromettenti" giustificano il ricorso all'induttivo*", Fisco Oggi, 2016, *[Online]*. Disponibile: *http://www.fiscooggi.it/.*

3 Una fra tutte, Corte Cass., sentenza 6 luglio 2016, n. 13728.

4 Corte Cass., sentenza 12 ottobre 2005, n. 19837.

5 A tal proposito, si richiama l'articolo 39, comma 3, del D.P.R. n. 633 del 1972 che consente al contribuente di conservare elettronicamente le fatture create in formato elettronico e quelle cartacee, sotto certe condizioni, anche all'estero. Infatti "*il luogo di conservazione elettronica delle stesse, nonché dei registri e degli altri documenti previsti dal presente decreto e da altre disposizioni, può essere situato in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza. Il soggetto passivo stabilito nel territorio dello Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, compresi quelli che garantiscono l'autenticità e l'integrità delle fatture di cui all'articolo 21, comma 3, siano stampabili e trasferibili su altro supporto informatico.*"

6 Corte Cass., sentenza 24 aprile 2015, n. 17325.