DIALOGHI DI DIRITTO TRIBUTARIO

TRA ATTUALITÀ E PROSPETTIVE

Aggiornamenti scientifici e valutazioni operative
in materia di Diritto Tributario Telematico:

1) *Documento informatico e firme elettroniche nel diritto tributario: la documentazione extracontabile digitale*

2) *Controlli in ambiente web e prove digitali:* Computer Forensics *e diritto tributario*

3) *Profili fiscali del* crowdfunding *e del* Bit Coin

AVV. FABIO MONTALCINI

AVV. CAMILLO SACCHETTO

AVV. GABRIELE VARRASI

TORINO, 16 GENNAIO 2015

Oggetto della presente indagine e della relazione odierna è il Diritto Tributario Telematico che vede indubbiamente nell'aggettivo telematico il suo baricentro.

Il concetto di telematica, a mente della disciplina e della materia del diritto dell'informatica, è determinata dall'unificazione dei concetti di informatica e telecomunicazioni; tale stretta correlazione può essere indifferentemente analizzata sia alla luce delle valutazione delle telecomunicazioni integrate al servizio dell'informatica (come ad esempio i mezzi di trasmissione, le reti ed i servizi di comunicazione che permettono e facilitano la condivisione delle risorse tra i computer connessi) e sia considerando l'informatizzazione dei sistemi di telecomunicazione (come ad esempio il miglioramento dei metodi di scambio delle informazioni attraverso un potenziamento dei servizi offerti dalle reti di comunicazione attraverso l'uso di software ed hardware adeguati).

Tale innovativo approccio, che nel diritto tributario si riverbera direttamente sul nuovo concetto di trasmissione dell'informazione, di valore probatorio della documentazione utilizzata nonché di determinazione del reddito tassabile, comporta una nuova tipologia di determinazione dei metodi, delle fattispecie e dei concetti propri del diritto tributario che devono essere rivalutati alla luce di tali innovazioni.

In tale ottica si può correttamente affermare di trovarsi di fronte al nuovo concetto di "ambiente fiscale virtuale" (la cui prima fonte normativa tributaria - architrave della archiviazione digitale e della conservazione sostitutiva - è il Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004) in cui, ai fini di una corretta comprensione, risulta necessario riprendere ed analizzare patrimoni concettuali provenienti dal diritto dell'informatica, dal diritto commerciale e dalla *computer forensics*.

1. Documento informatico e firme elettroniche nel diritto tributario: la documentazione extracontabile digitale

In un ambiente fiscale virtuale - alla luce del diritto dell'informatica - merita soffermarsi sul delicato e peculiare ruolo che riveste la gestione della documentazione extracontabile digitale. Per comprendere appieno la questione pare necessario muovere dal concetto di documento informatico.

Il Codice dell'Amministrazione Digitale[1] definisce il documento informatico come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[2].

Muovendo da un'analisi di tale definizione ben si può comprendere come lo stesso concetto di documento, prima configurato come un foglio di carta contenente elementi giuridicamente rilevanti, assuma ora una nuova veste.

Lo stesso concetto di "rappresentazione", utilizzato dal legislatore, vuole indicare come la manifestazione dell'elemento giuridicamente rilevante può non essere limitato alla sola scrittura, bensì può manifestarsi sotto molteplici forme (basti pensare ai files audio e video che sono a tutti gli effetti dei documenti informatici); inoltre la fase di manifestazione del contenuto del documento informatico è ben differente dall'elemento fisico della carta, in quanto prevede, per la sua fruizione, un'attività di interpretazione, attraverso un opportuno software, del codice binario[3] che è la base non solo di ogni file ma di ogni sistema informatico.

Ogni documento informatico risulta inoltre avere una caratteristica di notevole importanza che risulta essere fondamentale nel caso in cui si voglia mantenere la piena utilizzabilità, anche in sede penale, delle evidenze digitali raccolte in sede di verifica fiscale. Tale caratteristica è l'"impronta digitale" del file.

Tale impronta, anche nota con il termine inglese *fingerprint*, è definita come quella "sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima sequenza di un'opportuna funzione di *hash*"[4]; la funzione di *hash* è definita, dal medesimo Decreto, come quella "funzione matematica che genera, a partire da una generica sequenza di simboli binari, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (*bit*) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali"[5].

Da tali definizioni ben si può evincere come due impronte identiche corrispondano a due documenti informatici identici; pertanto il calcolo dell'impronta del file che si vuole acquisire in sede dì

[1] D.Lgs. 7 marzo 2005, n. 82

[2] Art. 1, comma 1, lett. p), D.Lgs. 7 marzo 2005, n. 82

[3] Codice che utilizza un alfabeto composto da due soli simboli (zero e uno).

[4] Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze art. 1, comma 1, lett. m).

[5] Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze art. 1, comma 1, lett. n).

verifica, può garantire, in una fase successiva, per quanto concerne la copia informatica di un documento informatico, quella "conformità all'originale" (prevista dallo stesso Codice dell'Amministrazione Digitale[6] e, a livello di principio, (come richiesto dalla legge 18 marzo 2008, n. 48) l'adozione di "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"[7] (v. *infra*).

Ulteriore strumento che consente di garantire l'integrità del file rispetto all'originale è la firma digitale.

In generale, le firme elettroniche sono degli strumenti atti a garantire un'associazione tra un file ed il suo autore. In particolare la firma elettronica semplice è definita dal Codice dell'Amministrazione Digitale come "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica"[8]; il medesimo Codice definisce inoltre la firma elettronica avanzata come un "insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati"[9] e la firma elettronica qualificata come "un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma"[10].

Spostando l'attenzione sulla firma digitale bisogna rilevare come il Codice la definisca come "un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"[11].

---

[6] Art. 23-bis, D.Lgs. 7 marzo 2005, n. 82.

[7] Art. 247, comma 1-bis, c.p.p.

[8] Art. 1, comma 1, lett. q), D.Lgs. 7 marzo 2005, n. 82.

[9] Art. 1, comma 1, lett. q-bis), D.Lgs. 7 marzo 2005, n. 82.

[10] Art. 1, comma 1, lett. r), D.Lgs. 7 marzo 2005, n. 82.

[11] Art. 1, comma 1, lett. s), D.Lgs. 7 marzo 2005, n. 82.

Per quanto qui di interesse merita porre l'accento sulla garanzia di integrità di un documento informatico o di un insieme di documenti informatici; infatti la firma digitale utilizzando la chiave privata, presente sul dispositivo di firma, al fine di cifrare l'impronta digitale del file che si sta sottoscrivendo, garantisce che tale impronta possa venire, in sede di verifica successiva, decifrato attraverso la corrispondente chiave pubblica al fine di effettuare il controllo di corrispondenza tra l'impronta decifrata e quella generata dal *file* di cui si vuole controllare l'integrità rispetto a quello originario.

Da un tale assunto si può quindi valutare se, in sede di verifica fiscale, utilizzare, dandone atto in sede di verbale, lo strumento della firma digitale in alternativa al mero calcolo dell'impronta del file al fine di garantire la conformità all'originale che potrebbe risultare necessaria per la piena utilizzabilità delle evidenze digitali raccolte alla luce della necessaria garanzia inerente la verifica - anche informatica - della loro attendibilità..

In tal senso si è espressa anche la giurisprudenza della Suprema Corte affrontano più direttamente il tema della documentazione extracontabile digitale. In particolare, nella sentenza 12 febbraio 2010, n. 3388 ha affrontato il tema dell'accesso da parte della Guardia di Finanza presso il Centro Elaborazione Dati (CED) di una società verificata.

La Corte di Cassazione, ha statuito, in sintesi, che le notizie e gli elementi desunti e legittimamente ricavati dall'esame dei supporti informatici e dai *files* elettronici che contengono dati contabili ed extracontabili sono utilizzabili ai fini della determinazione e della rettifica del reddito d'impresa, dovendosi ritenere, a tutti gli effetti, parte integrante della contabilità aziendale. Ciò anche qualora la suddetta documentazione sia acquisita con modalità irrituali, non comportando tale irritualità l'inutilizzabilità della stessa, poiché non sussiste una specifica previsione in tal senso[12].

Sempre la Corte di Cassazione è tornata sull'argomento con l'ordinanza 30 marzo 2012, n. 5226: anche in questo caso è stata riconosciuta l'utilizzabilità dei documenti informatici rinvenuti, data la loro attendibilità e le caratteristiche di gravità, precisione e concordanza degli indizi ivi contenuti, utili per l'elaborazione di apposite presunzioni e per l'applicazione dell'accertamento analitico-induttivo[13].

[12] Sullo specifico punto così il testo della sentenza: "l'acquisizione irrituale di elementi rilevanti ai fini dell'accertamento fiscale non comporta, secondo la giurisprudenza di questa *Corte (…) la inutilizzabilità degli stessi, non sussistendo una specifica previsione in tal senso. Pertanto gli organi di controllo possono utilizzare tutti i documenti di cui siano venuti in possesso, salva la verifica dello loro attendibilità, in considerazione della natura e del contenuto degli stessi*".

Ne consegue che la documentazione extracontabile digitale non può essere ritenuta dal giudice, di per sé, probatoriamente irrilevante circa l'esistenza di operazioni non contabilizzate, se non alla luce della valutazione dell'intrinseco valore digitale della stessa ed attraverso la verifica con gli ulteriori dati acquisiti e con quelli emergenti dalla contabilità ufficiale.

2. Controlli in ambiente web e prove digitali: *Computer Forensics* e diritto tributario

La documentazione extracontabile digitale, come più volte affermato, appare caratterizzata da profili di peculiare complessità, non del tutto risolvibili attraverso i tradizionali canoni normativi, giurisprudenziali e/o dottrinali.

In primo luogo, viene a delinearsi il tema dell'acquisizione "irrituale" di tale documentazione, circa il quale è possibile rifarsi alla non pacifica elaborazione giurisprudenziale in materia di inutilizzabilità delle prove irritualmente acquisite[14].

Tale argomento, tuttavia, appare ben lungi dall'aver trovato una definitiva soluzione, specie con riferimento alla documentazione extracontabile di tipo digitale. Si ritiene in tal senso di particolare significato il passaggio motivazionale contenuto nella ordinanza n. 5226 del 30 marzo 2012 emanata dalla Corte di Cassazione nel quale si afferma che "*i documenti informatici (cosiddetti 'files'),* estrapolati legittimamente *dai computers (…) costituiscono, in quanto scritture dell'impresa stessa, elemento probatorio, sia pure meramente presuntivo, utilmente valutabile, salva la verifica della loro attendibilità*".

L'acquisizione di documentazione extracontabile digitale richiede modalità procedurali di carattere tecnico, nonché conseguenti conoscenze di settore: procedere all'estrazione di *file* da supporti informatici è un'operazione non equiparabile, per complessità e natura, alla manuale "apprensione" di un documento analogico da parte dei funzionari del Fisco.

Da altro lato, emergono rilevanti problematiche di carattere tecnico-operativo, foriere di potenziali riflessi anche sul piano giuridico-tributario, ma prioritariamente riconducibili alla complessa disciplina della *digital forensics.*

---

[13] Infatti, si legge nella pronuncia in rassegna, "i documenti informatici (cosiddetti '*files*'), estrapolati legittimamente dai computers nella disponibilità dell'imprenditore, nei quali sia contenuta contabilità non ufficiale, costituiscono, in quanto scritture dell'impresa stessa, elemento probatorio, sia pure meramente presuntivo, utilmente valutabile, salva la verifica della loro attendibilità".

[14] Sul punto, del resto, la Corte di Cassazione nella sent. n. 3388 del 12 febbraio 2010 rinvia ad altre proprie passate pronunce escludendo che la documentazione acquisita "irritualmente" debba essere considerata inutilizzabile, salvo nelle ipotesi in cui si violino principi di carattere costituzionale.

Essa è la scienza che studia l'*individuazione*, la *conservazione***,** la *protezione*, l'*estrazione*, la *documentazione* e ogni altra forma di trattamento del dato informatico per essere valutato in un contesto giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.

Si può considerare, pertanto, *digital evidence* ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stato trasmesso secondo modalità informatiche o telematiche.

I dati informatici importano metodi di conoscenza e di raccolta per i quali sono necessarie notevoli competenze tecniche, diversi da quelli normalmente seguiti rispetto alle tradizionali risultanze probatorie.

Si tenga conto che immaterialità e fragilità sono caratteri intrinseci del dato digitale.

Di conseguenza, esso è facilmente modificabile, anche per effetto di un semplice accesso.

Per tale ragione, la tutela della genuinità della prova rappresenta aspetto assolutamente centrale della tematica, strettamente collegata a quelli della cristallizzazione del "quadro" informatico attraverso complesse operazioni tecniche e della tracciabilità delle operazioni compiute sul medesimo attraverso la stesura di dettagliati *reports*, idonei ad evidenziare la cosiddetta “catena di custodia” (*chain of custody).*

Pertanto, è bene fissare subito un punto: la *digital evidence* può essere danneggiata o distrutta, seppur involontariamente, da personale non in possesso di conoscenze adeguate: e ciò è tanto più grave in quanto sono in gioco interessi rilevantissimi, costituzionalmente garantiti, come il diritto di difesa.

Si tratta di problematiche di regola implicate sul terreno della prova scientifica, di cui la *digital evidence* rappresenta un sottotipo di recente emersione, a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni originariamente contenute in macchinari alquanto complessi in dati intelligibili da un giudice.

Più in generale, ciò induce ad interrogarsi se siamo in presenza di una nuova dimensione della prova e quale collocazione essa sia destinata a ricevere nell'ambito delle tradizionali partizioni in materia.

In che misura, cioè, debbano essere create a tale proposito nuove categorie a causa di una differente "qualità" della prova o, semplicemente, essere adattate quelle vecchie alle nuove dimensioni del fenomeno.

In relazione a tale tipologia di profili, si procederà nel prosieguo ad enucleare i principali elementi giuridico-tributari e tecnico-informatici relativi al cosiddetto “domicilio informatico” ed all’acquisizione della posta elettronica.

2.1 Il "domicilio informatico”

Trattando del concetto di domicilio merita evidenziare come tale concetto si sia in parte modificato con l’avvento della telematica ed in particolare con la nascita della nuova nozione di domicilio informatico.

Per domicilio informatico si intende la tutela concessa dal legislatore all’inviolabilità di un sistema informatico.

La L. 547/1993 introducendo, nella sezione del codice penale dedicata ai reati contro l’inviolabilità del domicilio (Capo III, Sezione IV del Codice penale), gli articoli 615-*ter*, 615-*quater* e 615-*quinquies* relativi ai sistemi informatici e telematici ha specificato come la normativa introdotta “*trova la sua collocazione tra i reati contro l’inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un’espansione ideale dell’area di rispetto pertinente al soggetto interessato, garantito dall’art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 cod. pen.*”[15].

Nella relazione al disegno di legge, merita sottolinearlo, viene precisato che in questo tipo di reato il bene protetto è assimilabile al domicilio: di qui l’inserimento del reato fra i delitti contro l’inviolabilità del domicilio [16].

Inoltre, dei reati compresi fra l’art. 615-bis e l’art. 615 quinquies (tutti rubricati nella Sezione IV relativa ai delitti contro l’inviolabilità del domicilio), quello di “*accesso abusivo ad un sistema informatico o telematico*” prevede una condotta più affine all’attività di indagine tipicamente tributaria che ricomprende la possibilità di estendere l’ispezione alle apparecchiature informatiche installate nei locali del contribuente in cui si svolga un accesso [17].

La volontà legislativa è stata di non attribuire al sistema informatico la natura di bene protetto in sé, ma di attribuirgli il ruolo di mezzo, di strumento mediante il quale fosse possibile la lesione di beni

---

[15] Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia, www.penale.it/legislaz/rel_ddl_2773_XI_leg.htm, visitato il 12 settembre 2012.

[16] Vero è che il concetto di domicilio è un’entità complessa e la traslazione di tali concetti ad una realtà “volatile” come è quella dell’informatica non è certamente semplice; tuttavia i termini “*espansione ideale dell’area di rispetto pertinente al soggetto interessato*” utilizzati nella Relazione del Ministro di Grazia e Giustizia sovra citata, meritano una riflessione approfondita in particolare quando l’utilizzo dello strumento informatico sia indirizzato alla realizzazione di una serie di attività che trovano un limite o confine nell’altrui possibilità di violazione.

[17] Si tratta di un reato che punisce due condotte alternative: - l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza; - il fatto dì mantenersi all'interno del suddetto sistema contro la volontà espressa o tacita di chi ha diritto di escluderlo. La pena base è la reclusione fino a tre anni e il reato è perseguibile a querela della persona offesa, ma è prevista, tra le altre, una circostanza aggravante (al comma 2, n. 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio. In tal caso, la pena va da uno a cinque anni di reclusione e il reato è perseguibile d'ufficio.

giuridici tradizionali come il patrimonio, i diritti inviolabili e l'inviolabilità del domicilio, inteso come luogo virtuale in cui l'individuo esplica liberamente la propria personalità nelle sue diverse manifestazioni.

In questa prospettiva, l'accesso abusivo deve considerarsi tale tutte le volte in cui sia manifesta la volontà del titolare del domicilio informatico di escludere l'intrusione di terzi estranei.

E' dunque sufficiente l'adozione di un qualsiasi sistema di sicurezza, non solo informatico (password o chiavi di accesso) ma anche semplicemente fisico (la custodia in un locale chiuso del sistema informatico).

Sotto questo aspetto, l'art. 615-ter cod. pen. ha inteso reprimere qualsiasi introduzione in un sistema informatico che avvenga contro la precisa volontà dell'avente diritto e, per rendere penalmente apprezzabile una simile contraria volontà, è da ritenersi sufficiente qualsiasi mezzo di protezione, (anche se facilmente aggirabile da persona mediamente esperta) ma che abbia comunque la caratteristica di rendere palese tale contraria volontà[18].

Sfuggono pertanto alla tutela assicurata dall'art. 615-ter cod. pen. i sistemi informatici "*aperti*", privi di qualsiasi protezione e accessibili, per definizione, a qualsiasi utente[19].

In questo quadro di riconoscimento di una specifica tutela (penalistica) dell'accesso abusivo ai sistemi informatici o telematici e, soprattutto, nell'ottica di riconducibilità dello specifico bene protetto alla tutela dell'inviolabilità del domicilio, occorre interpretare le norme tributarie che consentono le ispezioni ai sistemi informatici utilizzati dai contribuenti.

Innanzitutto, il comma 4 dell'art. 52 del D.P.R. n. 633/1972 è stato oggetto di modifica per consentire espressamente l'estensione dell'ispezione - conseguente ad un accesso domiciliare - non solo a "*tutti i libri, registri, documenti e scritture, compresi quelli la cui tenuta e conservazione non sono obbligatorie, che si trovano nei locali in cui l'accesso viene eseguito*" ma anche a quelli "*che sono comunque accessibili tramite apparecchiature informatiche installate in detti locali*".

L'estensione dell'ispezione ai contenuti dei sistemi informatici del contribuente deve soggiacere, a determinate condizioni, ai regimi autorizzativi previsti in tema di accessi domiciliari?

Una prima analisi riguarda i sistemi informatici considerati dalla norma tributaria.

Il tenore letterale porta a rendere ispezionabili solo le apparecchiature informatiche "*installate nei locali*" in cui viene eseguito l'accesso.

---

[18] Anche lo *jus excludendi alios*, è corollario dell'assimilazione della tutela dei sistemi informatici e telematici a quella del domicilio: non rileva il concreto grado di difficoltà di superamento della misura di sicurezza interposta (quindi anche se realizzata con metodi superabili da persone mediamente esperte), mentre è essenziale che sia manifesta la volontà di escludere i terzi dall'introduzione nel sistema informatico.

[19] A questi casi si possono assimilare tutti quelli nei quali le chiavi di accesso o password siano pubbliche (ad es. all'interno di account/profili o directory condivisi della rete aziendale) o collocate in luoghi aperti al pubblico (ad es. bacheche aziendali).

Questa formulazione (si noti il termine "*installate*") dovrebbe suggerire a considerare compresi nella norma solo quelle apparecchiature funzionanti in pianta stabile nei locali oggetto di controllo.
Si dovrebbe escludere la previsione nella specifica norma, ad esempio, di computer portatili o notebook che si trovano occasionalmente nei luoghi oggetto d'ispezione (in questi casi, stante il mancato consenso del titolare, l'autorizzazione dell'autorità giudiziaria per l'accesso a tali specifici mezzi informatici è necessaria).
Un'altra essenziale valutazione riguarda l'esistenza di misure di protezione tali da impedire l'accesso ai sistemi informatici contro la volontà del loro titolare.
La norma tributaria in esame fa riferimento espressamente ad apparecchiature informatiche "comunque accessibili".
Un sistema "protetto" non può considerarsi "accessibile"- concettualmente e giuridicamente - in quanto i due termini sono antitetici.
Sarebbe, inoltre, difficilmente argomentabile - in ottica logica e sistematica - una lettura nel senso di una libera attività ispettiva di sistemi informatici protetti, quando il comma 3 dello stesso art. 52 del. D.P.R. n. 633/1972 sottopone ad un regime di autorizzazione dell'autorità giudiziaria l'apertura di mobili, casseforti e ripostigli.
La soluzione operativa più corretta potrebbe quindi essere quella di considerare liberamente ispezionabili solo quei sistemi informatici che risultino privi di protezione (fisica o elettronica), mentre per l'accesso ai sistemi informatici protetti si avrà l'assimilazione degli stessi ai luoghi descritti nel comma 3 dell'art. 52 del D.P.R. n. 633/1972, per il cui accesso o apertura coattiva è richiesta la preventiva autorizzazione dell'autorità giudiziaria.

2.2. Acquisizione della posta elettronica

Le ispezioni riguardanti la posta elettronica
Il controllo della posta elettronica del contribuente sta diventando uno strumento sempre più significativo a disposizione dei verificatori nello svolgimento delle ispezioni dei documenti extracontabili.
Fra i documenti la cui tenuta e conservazione non sono obbligatorie, accessibili tramite apparecchiature informatiche soggetti ad ispezione ai sensi dell'art. 52, comma 4, del D.P.R. n. 633/1972 possono rientrare anche le e-mail.
La differente natura giuridica attribuita alle e-mail può influenzare le procedure di ispezione.
In dottrina si discute in particolare su quando un messaggio di posta elettronica possa essere considerato corrispondenza chiusa.

La Guardia di finanza, nella sua circ. n. 1/2008, fornisce alcune interessanti indicazioni operative a riguardo.

Viene evidenziato che "*per quanto riguarda le comunicazioni via e mail intercorse fra l'operatore ispezionato e soggetti terzi, ovvero fra articolazioni interne della stessa struttura imprenditoriale, occorre tenere presente le particolari disposizioni previste per l'acquisizione e l'esame di documentazione contenuta in plichi sigillati o per la quale è opposto il segreto professionale*".

I finanzieri possono acquisire direttamente le comunicazioni via e-mail già "aperte" e visionate dal destinatario mentre quelle non ancora lette o per le quali è eccepito il segreto professionale, vanno acquisite con l'apposito provvedimento di autorizzazione dell'Autorità Giudiziaria previsto dal comma 3 dell'art. 52 del D.P.R. n. 633/1972.

Viene ritenuta necessaria l'autorizzazione del Procuratore della Repubblica presso il Tribunale competente ovvero dell'Autorità Giudiziaria più vicina anche quando il contribuente abbia protetto la propria posta elettronica e non voglia comunicare le credenziali per accedervi.

2.3 Elementi distintivi tra e-mail "visionata" / "aperta" ed e-mail "non visionata" / "chiusa"

Il sistema di comunicazione di posta elettronica è così strutturato:

- ✓ il mittente invia il messaggio, al server del proprio ISP ;
- ✓ il server dell'ISP del mittente trasferisce il messaggio al server dell'ISP del destinatario ;
- ✓ il server dell'ISP del destinatario consegna il messaggio al ricevente.

In linguaggio tecnico una mail non visionata si definisce "non letta" mentre una mail visionata si definisce "letta".

Ogni ISP fornisce un *agente utente*[20] per la gestione della posta elettronica. Caratteristica comune di ogni agente utente è l'apposizione di un *flag* di stato a capo di ogni messaggio ricevuto, il quale ha il compito di contrassegnare lo stato di lettura o non lettura degli stessi.

Alla ricezione di un'e-mail questa si trova nello stato "non letta".

Muovendosi col mouse in corrispondenza della riga che contrassegna la mail e cliccando su di essa oppure ponendosi con i tasti direzionali della tastiera sempre nella medesima posizione e premendo successivamente il tasto INVIO vengono a generarsi due eventi simultanei: si apre il messaggio e si modifica il flag di stato.

[20] L'agente utente è un programma che dispone di una numerosa serie di comandi tali da permettere di leggere ed inviare e-mail. L'ISP può inoltre fornire un servizio webmail di consultazione della propria casella mediante un software all'interno della rete.

Una e-mail si definisce letta nel momento in cui questa ha il suo flag posizionato sullo stato "letta".

Una e-mail si definisce non letta quando il suo flag di stato è impostato come "non letta".

L'utente distingue un messaggio "non letto" da uno "letto" per come si presenta nella schermata principale dell'agente utente: nel primo caso la riga riassuntiva del messaggio[21] è tutta in grassetto, nel secondo caso si presenta nelle dimensioni, e colorazioni, ordinarie.

Il flag di stato è quindi una delle opzioni dell'interfaccia che l'ISP fornisce per dare all'utente un agente utente completo e chiaro. Questo genere d'informazione non è pertanto presente all'interno dell'*header* del messaggio.

A fini investigativi l'*header* è elemento essenziale per l'analisi di un messaggio di posta elettronica: prima dell'acquisizione di un'e-mail è doveroso fare un'accurata analisi dell'*header* e del sistema di comunicazione elettronico che si ha davanti.

Più nello specifico, è importante conoscere quale protocollo di trasferimento è utilizzato.

Il protocollo di trasferimento di messaggi tra utenti (*client-client*) è l'SMTP mentre i due protocolli tuttora utilizzati più frequentemente per la comunicazione client-Server sono il POP3 (Post Office Protocol 3) e l'IMAP4 (Internet Message Access Protocol 4). Per i servizi *webmail* si usa il protocollo HTTP che si appoggia comunque ai due protocolli sopracitati.

Con il protocollo POP3 si viene ad concretizzare perfettamente l'operazione definita di "*scaricamento della posta":* il server dell'ISP possiede tutti i messaggi (sempre contrassegnati come "non letti") e il client su richiesta procede all'acquisizione delle recenti mail ricevute.

Le e-mail "scaricate" sono una copia di quelle presenti nel server e che continueranno a rimanere nello stato "non letto". Per eliminare un messaggio è necessario non solo cancellarlo nel client ma anche sul server (non esistendo nel POP3 meccanismi di sincronizzazione). Con il protocollo di comunicazione IMAP4 è possibile scambiare messaggi anche da terminali diversi di natura diversa, posti in luoghi differenti, mantenendo comunque tutti i dati sempre sincronizzati. Questo protocollo permette di mantenere una copia del messaggio memorizzata nei propri *client* di ogni dispositivo e un'altra copia nel server di posta. Le modifiche applicate localmente alle e-mail sono poi sincronizzate con la copia che si trova nel server. L'header fornisce solo informazioni relative al protocollo di trasfermento tra mittente e destinatario. Per le altre informazioni di protocollo è necessario richiedere direttamente all'ISP.

L'atto di apertura di una e-mail comporta quindi automaticamente il cambio del flag di stato. Attraverso uno dei comandi offerto dall'agente utente è possibile rimarcare il messaggio come non

[21] Sia in un programma client sia in un software webmail nella pagina principale non compaiono tutti i messaggi completi uno dopo l'altro. Per ogni messaggio vengono scelte delle informazioni che valgono come riassunto (mittente, data,ora,flag lettura, oggetto)

letto. Alla prima sincronizzazione il client ordinerà al server di ricambiare il flag del proprio messaggio corrispondente.
L'ISP possiede tutti i privilegi per il mantenimento di file di log relativi a tutti gli scambi di protocollo per tutti i messaggi della casella di posta. Sia da lato *client* sia da lato server un messaggio letto e poi contrassegnato come non letto è visto come messaggio non letto. Il file di log può evidenziare man mano ogni azione effettuata sul messaggio, ma solitamente non è mai memorizzato negli spazi server dagli ISP poiché non gli si dà valore di alcun tipo.
Nel caso in cui venga utilizzata una *webmail* per accedere alla posta elettronica è possibile rilevare tracce di letture di messaggi contrassegnati successivamente come non letti andando a osservare i files presenti nella cache del computer.
All'atto di apertura di un'e-mail nella cache può crearsi un file temporaneo che ne rileva la traccia.
In conclusione, efficienti agenti utenti non scaricheranno mai tutto il messaggio dal server ma soltanto i dati necessari per creare la riga riassuntiva presente nella pagina principale mentre nella fase di apertura del messaggio verrà immediatamente scaricato tutto il corpo del messaggio.

L'*e-mail* non letta dal destinatario rappresenta una forma di corrispondenza, con conseguente equiparazione della stessa a un "*plico sigillato*", non acquisibile da parte dei verificatori senza autorizzazione dell'Autorità giudiziaria.
I principali profili giuridici relativi all'oggetto in esame riguardano il contemperamento dell'esigenze ispettive e la tutela della libertà e segretezza delle corrispondenza così come prevista e disciplinata dall'articolo 15 della Costituzione. Un primo rilevante problema è connesso all'esatta delimitazione del contenuto della libertà tutelata, dall'art. 15 Cost[22].
L'art. 15 Cost. tutela la libertà di comunicare in modo riservato; al fine di identificare le forme di comunicazione ricomprese nella disposizione, assume rilevanza decisiva l'intrinseca caratteristica di "garanzia della segretezza" del mezzo espressivo utilizzato. Caratteristica riscontrabile tutte le volte in cui, non solo la comunicazione sia diretta in modo esclusivo a una persona determinata, ma siano anche state adottate le precauzioni per escludere i terzi dalla conoscibilità del suo contenuto.
Occorre ora evidenziare come la disciplina delle indagini tributarie preveda soltanto un'ipotesi in cui sia espressamente possibile derogare a tale situazione soggettiva costituzionalmente protetta: si tratta del caso contemplato dall'art. 52, comma 3, del D.P.R. n. 633/1972, rappresentato dalla

[22] Il cui testo così recita: *"La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge."*

facoltà di procedere - nel corso di un accesso, e previa autorizzazione del Procuratore della Repubblica - all'apertura coattiva di pieghi sigillati e simili[23].

Da questo confronto testuale emerge la carenza della normativa tributaria in ordine alle garanzie connesse all'unica forma di limitazione della libertà e segretezza delle comunicazioni consentita: l'apertura coattiva di pieghi sigillati e altra corrispondenza è solo soggetta alla condizione che essa avvenga - genericamente - in ricorrenza di un accesso domiciliare, e che sussista l'autorizzazione del Procuratore della Repubblica o dell'autorità più vicina.

In merito si ritiene, tuttavia, che quest'ultima - essendo costituzionalmente vincolata a un provvedimento motivato - dovrà comunque vagliare la sussistenza di fondate ragioni per poter autorizzare l'apertura coattiva di corrispondenza.

Nella nozione di "*corrispondenza*", e quindi nella disciplina di cui al comma 3 dell'art. 52 del D.P.R. n. 633/1972 (in virtù della formula aperta "... e simili" ivi utilizzata) rientrano anche tutte le forme di comunicazione informatica (ad esempio, la posta elettronica), la cui conoscibilità da parte dell'organo ispettivo soggiace perciò alla riserva giurisdizionale.

A tal fine, infatti, non risulta applicabile la deroga contenuta nel comma 9 dello stesso art. 52 del D.P.R. n. 633/1972, secondo cui è consentito all'organo ispettivo - sempre in fase di accesso domiciliare - di asportare (per la successiva autonoma elaborazione) i supporti relativi a «sistemi meccanografici, elettronici e simili» utilizzati dal contribuente, qualora questi non consenta di adoperare (per la stessa elaborazione dei dati) i propri impianti e il proprio personale[24].

---

[23] A questo proposito bisogna precisare che la disciplina fiscale, pur rispettosa della riserva giurisdizionale tassativamente prevista dall'art. 15 Cost,, non sembra in linea con la riserva assoluta di legge stabilita dalla medesima norma costituzionale. L'art. 15, comma 2, Cost., infatti, avverte che la limitazione della libertà e della segretezza delle comunicazioni «può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie previste dalla legge». Il che rende necessario non solo l'intervento dell'autorità giudiziaria, ma anche la puntuale previsione legislativa delle specifiche circostanze capaci di giustificare l'adozione di un provvedimento limitativo di tale situazione soggettiva.

24 Si veda Circolare Operativa GDF del 2008, volume I - parte II - capitolo 3 pag. 94 e ss: *"Al riguardo, il comma 9 dell'art. 52 del D.P.R. n. 633/72, valevole, per quanto si è più volte detto, anche ai fini delle imposte sui redditi, prevede che, in deroga alle disposizioni del comma 7 - che contempla limitazioni, meglio descritte al Capitolo 2 della Parte III della presente istruzione, al ritiro di documenti e scritture - gli operatori dell'Amministrazione che procedono all'accesso nei locali dei soggetti che si avvalgono di sistemi meccanografici, elettronici e simili, hanno facoltà di provvedere all'elaborazione dei supporti fuori dei locali stessi qualora il contribuente non consenta l'utilizzazione dei propri impianti e del proprio personale. Conseguentemente, come dianzi accennato, è possibile riversare, ove necessario, i dati presenti nell'hard-disk dell'elaboratore su supporti appositamente predisposti, ai fini della successiva elaborazione, nonché ricercare ed acquisire quelli contenenti copie c.d. "di sicurezza" dei dati effettuate nei giorni antecedenti all'intervento - al fine di individuare, ove possibile, quelli eventualmente cancellati dal sistema nel momento dell'accesso - e stampare i dati ritenuti maggiormente interessanti, con apposizione della firma dei verificatori stessi e del contribuente, oltre che della data della stampa. Tutte le operazioni dianzi indicate, devono essere di norma poste in essere con l'assistenza di personale specializzato dipendente dal soggetto ispezionato."*

Tale disposizione, se da un lato può consentire l'acquisizione di dati archiviati su supporti informatici, non può tuttavia avallare l'accesso al contenuto di comunicazioni spedite o ricevute per via telematica e contenuti nei predetti supporti.

A meno che non si possa dimostrare che si tratta di messaggi archiviati, per i quali, cioè, è venuta meno la caratteristica della segretezza che accompagna ogni comunicazione dal momento del suo inoltro a quella della sua conoscenza da parte del destinatario, o di messaggi archiviati in modo da non escluderne deliberatamente l'accesso da parte di terzi (ad esempio attraverso l'inserimento di codici dì accesso, parole chiave, ecc., che determinerebbe situazioni perfettamente assimilabili a quelle dei plichi documentali sigillati, per la cui apertura coattiva la normativa fiscale prevede, cioè, l'intervento dell'autorità giudiziaria).

Analogo discorso dovrebbe valere per la novella introdotta dall'art. 2, comma 1, lett. b), del D.Lgs. 20 febbraio 2004, n. 52. A seguito di tale modifica, l'attuale comma 4 dell'art. 52 del D.P.R. n. 633/1972 prevede che "*l'ispezione documentale si estende a tutti i libri, registri, documenti e scritture, compresi quelli la cui tenuta e conservazione non sono obbligatorie, che si trovano nei locali in cui l'accesso viene eseguito, o che sono comunque accessibili tramite apparecchiature informatiche installate in detti locali*".

Quest'ultima disposizione non può essere comunque interpretata in modo da consentire l'accesso libero a forme di corrispondenza transitate e custodite in tali apparecchiature informatiche (il caso delle e-mail è il più indicativo): pena la sua incostituzionalità per contrasto con quanto previsto dall'art. 15, comma 2, Cost., secondo cui ogni deroga alla libertà e alla segretezza delle comunicazioni può avvenire - senza eccezioni - soltanto per atto motivato dell'autorità giudiziaria con le garanzie previste dalla legge.

Diventa dunque essenziale, per una corretta interpretazione e applicazione del nuovo comma 4 dell'art. 52 del D.P.R. n. 633/1972 (nella parte ovviamente in cui introduce la possibilità di estendere l'ispezione alle apparecchiature informatiche installate nei locali del contribuente) distinguere fra i dati che non costituiscono forme di corrispondenza o di comunicazione riservata (e che perciò non godono della protezione costituzionale di cui all'art. 15, comma 2, Cost.) e i dati, invece, che rientrano nella nozione di corrispondenza e non risultano liberamente accessibili ai verificatori fiscali (ma lo potranno essere eventualmente solo previa autorizzazione dell'autorità giudiziaria).

In tale ottica, però, va precisato che non costituisce violazione della libertà e della segretezza delle comunicazioni, l'acquisizione - in sede di accesso - di corrispondenza già aperta e quindi conosciuta dal destinatario, nonché di ogni altro documento privo delle cautele idonee ad assicurarne la non conoscibilità da parte di terzi.

In tali ipotesi, dunque, l'organo ispettivo non sarebbe tenuto a munirsi della preventiva autorizzazione dell'autorità giudiziaria. Proprio sotto il profilo della distinzione tra corrispondenza chiusa o aperta, nelle ipotesi di posta elettronica, si segnala l'interpretazione fornita dalla Suprema Corte[25]. La Suprema Corte, dopo aver affermato la pacifica estensione della tutela penale (e costituzionale) alla corrispondenza informatica o telematica, chiarisce che detta corrispondenza deve considerarsi soggetta alla riserva giurisdizionale di cui all'art. 15 Cost. "*nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi*". E aggiunge che "*quando in particolare il sistema telematico sia protetto da una password, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso*".

Tale orientamento farebbe perciò propendere per la necessità dell'autorizzazione dell'autorità giudiziaria tutte le volte in cui gli organi ispettivi tributari intendono estendere l'ispezione mediante l'accesso alla posta elettronica, tenuto conto che essa è di norma protetta da una chiave d'accesso legittimamente conosciuta solo dal destinatario dell'indirizzo di posta elettronica e dall'amministratore del sistema[26].

2.4 Suggerimenti operativi

Come argomentato, l'acquisizione di ogni tipologia di file digitale deve avvenire mediante tecniche forensi avanzate tali da non comprometterne la genuinità: si deve copiare un file in modo che sia possibile riprodurlo identico in un secondo tempo.

Necessario in tal senso è il supporto costante di un cd. documento di *journal*[27] che registra passo passo le procedure di analisi ed estrazione.

---

[25] Cfr. Cassazione penale (sez. V), sentenza n. 47096 del 19 dicembre 200766

[26] Si veda ancora la Circolare operativa GDF 2008 cit., volume I - parte II - capitolo 3 pag. 94 e ss: "*Per quanto riguarda le comunicazioni via e - mail, intercorse fra l'operatore ispezionato e soggetti terzi, ovvero fra articolazioni interne della stessa struttura imprenditoriale, occorre tenere presente le particolari disposizioni previste per l'acquisizione e l'esame di documentazione contenuta in plichi sigillati, di cui al successivo sottoparagrafo f., o per la quale è opposto il segreto professionale, illustrate al sottoparagrafo g., adattate alle prescrizioni dettate in tema di fatturazione e conservazione dei documenti in forma elettronica, meglio descritte al paragrafo 2.g. del Capitolo 4 della Parte III; per effetto delle richiamate previsioni, le comunicazioni via e - mail già "aperte" e visionate dal destinatario sono direttamente acquisibili dai verificatori, mentre quelle non ancora lette o per le quali è eccepito il segreto professionale, vanno acquisite sulla scorta di apposito provvedimento di autorizzazione dell'Autorità Giudiziaria, ex art. 52, comma 3, del D.P.R. n. 633/72, secondo quanto di seguito illustrato*."

[27] File dove sono registrate minuziosamente tutte le operazioni eseguite.

Nella fase operativa il file deve essere copiato e convalidato con una funzione di *hash* [per la definizione della quale vedi *supra*] e tale copia deve essere sequenziale, bit a bit, senza omettere alcun dato.

Uno degli strumenti di maggior efficacia è il comando Unix *dd*: tale comando effettua qualsiasi riproduzione, di blocco in blocco[28].

La documentazione extracontabile digitale ha un indubbio valore probatorio in campo tributario e penale-tributario ma fa emergere difficoltà applicative, di carattere tecnico-operativo, non risolvibili attraverso i metodi ed i criteri interpretativi classici.

Date le insidie sottese alla fase di acquisizione delle risultanze digitali, sarebbe, dunque, lecito attendersi prese di posizione rigorose da parte della giurisprudenza in ordine all'invalidità delle risultanze informatiche.

Invece, in particolare, si tende ad aggirare la fondamentale funzione di protezione svolta dalle *guidelines* fissate in ambito internazionale per la *computer forensics*, addossandosi alla parte interessata l'onere di dimostrare l'avvenuta effettiva modifica del dato informatico, qualora non sia stata seguita la *best practice* nella fase di raccolta della *digital evidence*.

Secondo un percorso comune anche ad altri campi della *scientific evidence*, il libero convincimento diventa il viatico per legittimare un approccio antiformalistico in tema di prova.

Ebbene, tale ricostruzione va senz'altro reinterpretata.

La risposta ad una prova formata senza il necessario rispetto dell'integrità della stessa è una declaratoria di inutilizzabilità probatoria.

E ciò vale, in particolare, a seguito dell'introduzione nel tessuto normativo, da parte della l. n. 48 del 2008, dei fondamentali principi relativi alla salvaguardia dell'integrità della prova digitale.

Quand'anche non si volesse ritenere che la l. n. 48 del 2008 abbia inteso sancire precisi divieti probatori, ancorché in maniera implicita, con riferimento alle risultanze informatiche inquinate al momento dell'apprensione dei dati, occorre prendere atto della necessità di una diversa ricostruzione sistematica della nozione di inutilizzabilità.

In presenza di prove informatiche, eventuali violazioni relative alle modalità di formazione della prova incidono necessariamente anche sulla sostanza della prova stessa, fino a rendere del tutto inattendibile l'accertamento frutto di tali risultanze.

[28] Un hard disk è logicamente partizionato in blocchi di ugual dimensione. L'accesso ad essi può avvenire in modi diversi ma nel nostro specifico caso evidenziamo l'accesso *sequenziale* [dopo aver letto il blocco 6,verrà letto il blocco 7 e così via…]. Unix è un sistema operativo che interpreta qualsiasi elemento digitale (schede di rete,cartelle, immagini…) come un file. In caso di files danneggiati il programma si arresta. È possibile però usare il comando *dd_resque* per analizzare i files danneggiati e tentarne il recupero o, in extremis, superarli.

I caratteri intrinseci di fragilità e volatilità della prova informatica confermano che le investigazioni in materia, ormai, non possono ritenersi più confinate al limitato settore dei *computer crimes*.
Ancorché di natura digitale, la prova deve sempre soggiacere alle regole che ne determinano il valore.

3. Profili fiscali del *crowdfunding* e del *Bit Coin*

La poliedricità dei fenomeni giuridici di oggi obbliga le diverse discipline a dialogare tra loro.
Gli aspetti innovativi, soprattutto della tecnologia, rendono, a volte, obsoleta l'interpretazione attraverso le lenti delle categorie giuridiche esistenti, che, seppur essenziali come base di partenza, necessitano in queste nuove frontiere del diritto di una qualche forma di rivisitazione, se non completa innovazione.
Basti pensare a internet, un mondo virtuale dove i concetti di "confine" e "Autorità" sono assai lontani dai paradigmi classici.
Alcuni nuovi modi di creazione della ricchezza e alcune nuove transazioni commerciali e, a maggior ragione se a carattere globale e quindi *borderless,* impongono un dialogo tra gli interpreti delle diverse discipline in cui si articola il diritto, in quanto di fronte al "nuovo" e all'"inesplorato", la visione d'insieme può essere sicuramente un punto di forza.
Quanto scritto è ben espresso dal Magnifico Rettore Antonio Uricchio e dal Prof. Claudio Sacchetto nella prime pagine del libro Diritto Tributario Telematico, alle cui intuizioni e riflessioni si rimanda.
Inoltre, queste considerazioni, possono essere ben comprese in due recenti fenomeni, legati all'innovazione e alla tecnologia, quali le monete virtuali (tra cui i *bitcoins*) e il *crowdfunding.*
La quasi assenza di discipline a livello globale induce l'interprete a svolgere la funzione di mediatore tra le consolidate categorie giuridiche e le nuove frontiere del diritto, ponendosi -oltre le ricorrenti problematiche -, sia sul piano sostanziale e di ricostruzione sistematica, che successivamente su quello tributario, nuovi dubbi e cercando di colmare nuove incertezze.
La sfida è tra lasciare questi fenomeni inesplorati o emarginarli con normative costrittive, ovvero provare a ricostruire la loro disciplina, in modo da tutelare i vari interessi in gioco, sia pubblici che privati.
Il fenomeno *bitcoin,* una "moneta" in assenza di una Banca Centrale e di una regolamentazione, richiede, considerando i flussi di ricchezza che si trasferiscono con esso, un'attenta ricostruzione sistematica e, conseguentemente, uno studio delle criticità della sua circolazione. Indubbiamente, movimentazioni di *bitcoins*e, l'attività della loro creazione, il *mining*, sollevano questioni sotto il profilo fiscale nazionale, europeo (IVA) e internazionale.

Considerazioni simili si possono svolgere anche con riferimento al *crowdfunding*, con la differenza che in questo caso, l'Italia, al di là dei commenti positivi e negativi sul risultato ottenuto, ha agito tempestivamente –tra i primi interventi normativi registrati a livello mondiale-, legiferando in materia.

Con il termine *crowdfunding*, che letteralmente va tradotto con "finanziamento della folla", si intende la possibilità, per un soggetto, di trovare i finanziamenti necessari alla propria attività economica, direttamente sul web: i versamenti possono essere effettuati da chiunque sia, per qualunque ragione, interessato a quel dato progetto e intenda pertanto investirci. In altre parole, si può definire il *crowdfunding* come "un processo di raccolta dei fondi collettivo, realizzato tramite portali on line, attraverso il quale chiunque può elargire contribuzioni di diversa entità al fine di favorire lo sviluppo di un progetto, di una iniziativa che, per qualche ragione, ritengono opportuno sostenere, anche senza un ritorno economico.

Si pensi inoltre in questo fenomeno, alle numerose declinazioni dello stesso, nate dalla prassi, alla cui trattazione, anche per gli aspetti fiscali, si rimanda a quanto svolto nel Libro: *crowdfunding: donation based, renard based, lending crowdfunding, equity based* e *do it yourself.*

Per comprendere la portata del *crowdfunding* nell'era digitale può essere utile riflettere sulle efficacia di una prima forma di finanziamento da parte della "folla", che si può far risalire a un episodio storico, qui brevemente descritto. La Francia, per ricordare la dichiarazione di indipendenza americana del 1776 e in nome della vicinanza tra le due popolazioni, fece costruire una statua, progettata da Frédéric Auguste Bartholdi in collaborazione con Gustave Eiffel, da inviare a New York, la Statua della libertà. Verificando i fondi necessari per la costruzione del piedistallo che avrebbe dovuto sostenerla su Liberty island, vicina a Manhattan, si accorsero che le disponibilità economiche del neonato Stato federale non erano sufficienti e, il Congresso, non era disposto ad approvare lo stanziamento dei 100.000 dollari che ancora mancavano alla realizzazione del progetto. Così, Joseph Pulitzer, editore del giornale World, ebbe un'idea: si propose di indicare nel suo giornale i nomi di tutti i soggetti che avessero mostrato la loro disponibilità a effettuare un versamento in denaro in favore della costruzione del piedistallo, a prescindere dalla somma che fosse stata versata da ognuno di essi. Il risultato fu che, appena cinque mesi dopo, fu raccolta la somma di 102.000 dollari, stanziati da più di 120.000 persone: più dell'80% dei soggetti si era limitato a versare appena un dollaro, una cifra in sé insignificante, ma che, moltiplicata per migliaia di soggetti, è stata capace di sostituirsi a un finanziamento federale per un'opera pubblica.

In queste nuove frontiere del diritto, le materie del diritto tributario e del diritto commerciale trovano un terreno fertile da condividere, in quanto, citando nuovamente Uricchio, "internet, più che costituire un mero strumento o un'organizzazione dello strumento, si atteggia come luogo di

interazione sociale e, quindi, come ambiente giuridico all'interno del quale si creano e si manifestano forme di ricchezza di diversa natura, sia riconducibili alle categorie tradizionali, sia del tutto nuove".

Una riflessione su come nascono e come si evolvono queste recenti fattispecie, può essere svolta analizzando il percorso diacronico dei *bitcoins* e in particolare sulla figura del suo inventore/i; ancora oggi non si conosce la verità, se sia un singolo (Satoshi Nakamoto) e se questo sia una persona reale o meno, ovvero sia un team di professionisti o di studiosi o di "pirati" informatici.

La nascita convenzionale risale al giorno di Halloween del 2008; dalla genesi il valore è decisamente oscillato, mostrando elementi di elevata volatilità: per rendere l'idea, la prima ufficiale transazione è stata effettuata per compare una pizza per 10.000 *BTC* (sigla della criptovaluta), una cifra nel periodo esigua, ma che, in base al valore attuale dei *bitcoins* rispetto al dollaro equivarrebbe a circa 750.000 dollari.

Provando sinteticamente a definire il *bitcoin*, questo è un database distribuito tra i nodi della rete che tengono traccia delle transazioni, sfruttando la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione di proprietà dei *bitcoins*.

In sostanza, i *bitcoins* sono dei semplici files crittografati che contengono informazioni sul loro titolare; ogni *bitcoin* è infatti legato a una coppia di codici, dette "chiavi crittografiche": una chiave è privata, nel senso che la conosce solo il proprietario, l'altra invece è pubblica e permette la ricezione della moneta .

Per creare un *bitcoin* viene adottato un procedimento complicato, o meglio a complessità progressiva: vi sono algoritmi che provvedono alla loro creazione. Semplificando,all'avvio del programma *BitcoinMiner*, questo esegue un algoritmo e inizia a risolvere una serie di problemi matematici. Alla risoluzione di ogni problema il software genera un blocco di *bitcoins*, secondo un'operazione nota come *mining*(si consideri che secondo la complicazione progressiva degli algoritmi, il numero massimo di *bitcoins* generabili è già conosciuto –quindi sono a numero limitato- e si può stimare anche la relativa "produzione" nel tempo). Il *mining* può essere svolto in due forme: in solitaria o in *pool*. Il *mining* in solitaria consiste nella produzione di *bitcoins* per mezzo del proprio computer; nel *mining* in *pool*, invece, i problemi vengono condivisi da una rete di computer (ognuna delle quali è detta "nodo") che lavorano alla loro risoluzione. Il processo di generazione dei *bitcoins* sfrutta dunque la tecnologia *peer to peer*, nella quale gli utenti fruiscono in modo paritetico delle stesse risorse informative e condividono gli stessi dati a velocità di molto superiori a quelle di un sistema di tipo *client-server*, nel quale invece il computer che offre i propri servizi (il *server*), dovendo lavorare per soddisfare le richieste di più *client*, rischia di rallentare

notevolmente le operazioni. Nella logica *peer to peer*, invece, ogni computer è legato a tutti gli altri e comunica direttamente con ognuno di essi.

Tutte le informazioni relative alla creazione e alla circolazione dei *bitcoins* sono contenute in un database che è distribuito tra tutti i nodi della rete *bitcoin*. La completezza delle informazioni contenute nel database contribuisce anche a impedire che la stessa moneta possa essere spesa due volte: il database, infatti, memorizza non solo le creazioni di *bitcoins*, ma anche tutte le transazioni che vengono effettuate e le comunica a tutti i nodi della rete attraverso la "*blockchain*" o catena dei blocchi.

Quando un utente decide di operare una transazione in *bitcoins*e, in particolare, nel momento in cui si trasferisce la moneta elettronica a un altro indirizzo della rete, il software *bitcoin* invia un messaggio agli altri computer della rete *peer to peer,* informando tutti gli utenti che un certo valore in *bitcoins* sta per essere trasferito da un indirizzo a un altro. Gli stessi utenti possono anche verificare che per l'accettazione del pagamento sia stata usata la chiave privata corretta; avvenuta la transazione, il *cybercoin* trasferito non può più essere nuovamente utilizzato dall'utente che ha effettuato il pagamento (proprio perché dall'elenco delle transazioni risulta l'avvenuto "spossessamento" di quel gettone), mentre lo stesso entrerà nella materiale disponibilità dell'utente che lo ha ricevuto in pagamento (nel suo *wallet* o portafoglio elettronico).

In questa sede non si possono esaminare gli approfondimenti svolti nel Libro, a cui si rimanda, ma le analisi delle iniziative e dei dibattiti di Paesi come gli U.S.A., la Repubblica Federale di Germania, il Regno Unito, la Svizzera, la Repubblica Popolare Cinese, nonché l'Italia e l'U.E., mostrano un chiaro interesse per questo fenomeno, connotato a volte di negatività –in quanto privo di una banca centrale e per le sue dinamiche poco controllabili, nonché il quasi anonimato- ma a volte di positività, cogliendo le opportunità che uno strumento nuovo può portare o comunque della obiettiva considerazione che il fenomeno ormai è di vasta portata (in quanto le stime parlano di un controvalore, a marzo 2014, di oltre 6 miliardi di dollari).

Questo fenomeno, indubbiamente, pone diversi e cruciali problemi dal punto di vista fiscale: il problema della tassazione dei *bitcoins* può essere letto a seconda del diverso utilizzo che di esso può essere fatto: un primo aspetto è quello dell'attività di *mining*, il secondo è l'acquisto di merci o servizi e il terzo è la mera speculazione sul variare del valore della moneta elettronica.

Tralasciando per dovere di sintesi le diverse soluzioni -sia per quanto riguarda l'IVA che le imposte sui redditi - adottate nei vari Paesi, a cui si rimanda agli approfondimenti svolti nel Libro, si possono svolgere, brevemente le seguenti considerazioni, scindendo tra IVA e imposte sui redditi.

Per quanto riguarda l'attività di *mining* (e i proventi da essa derivanti) potrebbe non rientrare nella normativa IVA, poiché potrebbe esulare dal suo campo di applicazione: non vi sarebbe infatti un

legame sufficiente tra il servizio offerto e i corrispettivi eventualmente ricevuti. Le ulteriori entrate dei *miners*, non direttamente derivanti dalla generazione di *bitcoins*, potrebbero essere esenti da IVA, in quanto rientranti nella definizione *ex* art. 135, primo comma, lett. d), della Direttiva IVA.

Per quanto riguarda le imposte sui redditi, la generazione, gestione e cessione dei *bitcoins* potrebbero costituire operazioni in grado di creare reddito al soggetto che le pone in essere (in particolare, i proventi derivanti dal differenziale che si origina dall'impiego dei *bitcoins*, oppure da quelli che derivino dall'attività di generazione). Si potrebbe fare riferimento all'art. 67 TUIR e, quindi, a redditi diversi, in base alla possibilità di assimilare i *bitcoins* o a titoli non rappresentativi di merci, o a valute estere, o a crediti pecuniari o strumenti finanziari o, ancora, a rapporti attraverso cui possono essere conseguiti differenziali positivi e negativi in dipendenza di un evento incerto.

Nel caso invece di generazione di *bitcoins* tramite *mining*, l'eventuale reddito prodotto potrebbe essere ricondotto alla fattispecie disciplinata dalla lett. l) dell'art. 67 TUIR; è pur vero che, in realtà, simile riconduzione non appare molto corretta in riferimento al *mining* condotto in *pool*, dal momento che il progressivo complicarsi della risoluzione dell'algoritmo rende necessario svolgere questa attività in gruppo e con una certa abitualità (e con l'impiego di ingenti risorse economiche), il che varrebbe a far venir meno il requisito del "lavoro autonomo non esercitabile abitualmente" che caratterizza la norma il oggetto, ma inquadrerebbe profili di un'attività professionale.

Conclusioni

In un panorama, ormai, "digitalizzato", occorre che tutti gli i soggetti coinvolti maturino piena consapevolezza dei nuovi strumenti e delle conseguenze giuridiche da essi derivabili.

Il complessivo insieme delle categorie concettuali del diritto e del diritto tributario sono messe a dura prova da una rivoluzione informatica che non conosce confini di territorio.

L'avvento di Internet, il moltiplicarsi delle tecnologie dell'informatica e del loro rendimento operativo per il mondo del diritto presentano sempre più tutti i caratteri di una sfida a molte dimensioni.

La firma digitale e l'archiviazione digitale dei documenti sono soltanto alcuni dei grandi punti di emersione del fenomeno *net* e *new economy* al centro della obbligata attenzione del giurista, professionista o studioso, tributario.

Essa comporta anche un nuovo modo di pensare e giuridicamente regolare il rapporto tra privati e Stato (in tutte le sue accezioni).

Il processo di modernizzazione della società nel suo complesso, delle imprese e dei professionisti (italiani e stranieri) nonchè degli apparati pubblici attraverso le tecnologie ICT presuppone alcuni

requisiti fondamentali tra i quali sicuramente devono essere collocati un adeguato sistema normativo e la realizzazione delle infrastrutture tecnologiche.

Ma ciò non è sufficiente se si prescinde dal parallelo conseguimento di un altrettanto adeguato livello di alfabetizzazione informatica sia all'interno che all'esterno della struttura ordinamentale pubblica, ossia da una diffusione, *in primis* grazie ai contributi degli studiosi della materia, delle conoscenze informatiche tra dirigenti delle amministrazioni, gli operatori delle Forze dell'Ordine che dovranno porre in essere l'attività e i cittadini destinatari delle medesime.