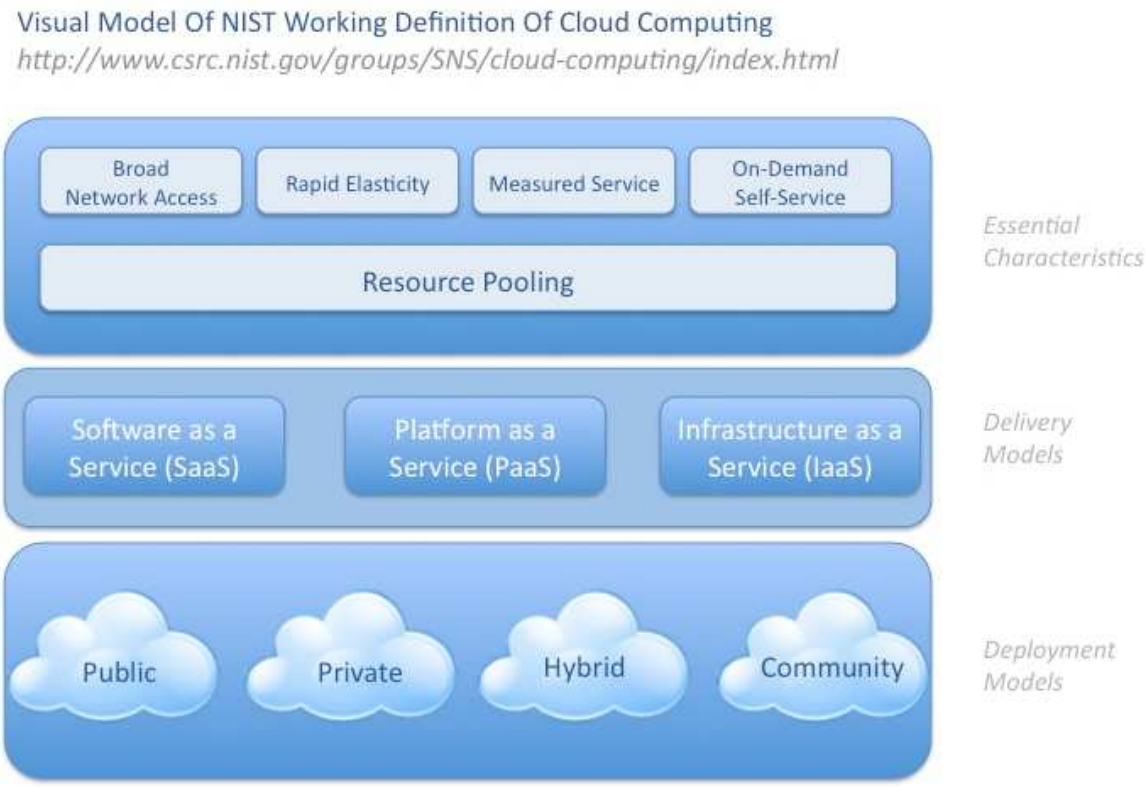
IL CLOUD COMPUTING: LA NUOVA SFIDA PER LEGISLATORI E FORENSER

La nuova tendenza dell'Internet degli ultimi anni ha portato alla nascita di numerose nuove applicazioni, spesso accompagnate dalla recente tendenza volta a una sorta di "dematerializzazione" degli oggetti informatici. Ci si riferisce in particolare al nuovo fenomeno del cloud computing, o più semplicemente cloud che vedrà sicuramente nei prossimi anni una vera e propria esplosione, imponendosi quale risposta agli ultimi anni di "dittatura" delle tecnologie della rete.

Un primo punto da considerare attiene alla sua definizione: al momento, la più autorevole può essere ricondotta alla formulazione del NIST[1] la quale lo definisce come «model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction»[2]. In sostanza quindi «il cloud computing è un paradigma distribuito che virtualizza dati, software, hardware e comunicazione dati in servizi»[3].



[1] National Institue of Standards and Technology; è un'agenzia federale governativa che si occupa della gestione delle tecnologie, si veda più in dettaglio http://www.nist.gov/index.html .

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST definition of cloud computing*, Special publication 800-145, 2011, pag. 2, disponibile all'indirizzo http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf .

[3] M. MATTIUCCI, *Cloud computing & digital forensics*, 2012, disponibile presso http://www.marcomattiucci.it/cloud.php .

Dalla definizione qui riportata è facile intuire come tale nuovo strumento appaia come una grande opportunità, soprattutto per le aziende che ormai basano gran parte delle loro attività su piattaforma ICT, spingendo le più grandi compagnie di servizi informatici internazionali a dotarsi e offrire servizi sempre maggiori[4]. Sempre secondo la definizione del NIST, l'architettura si basa essenzialmente su due livelli: fisico, in cui rileva la componente materiale ovvero i server, il network, lo storage e uno logico, dato dalla virtualizzazione delle risorse presentate all'utente. Cinque le caratteristiche essenziali:

- è un servizio on-demand self-service, in quanto non vi è interazione fra il CSP (Cloud Service Provider) e l'utente, il quale riceve automaticamente il contenuto afferente al servizio richiesto. È quindi un servizio customizzabile tipicamente legato alla forma del pay per use;

- si basa sul broad network access, sfruttando quindi non solo la rete client- server, ma anche le nuove forme d'accesso legate all'utilizzo di smartphone e tablet. Da ciò ne deriva un'ulteriore caratteristica legata alla scalabilità del servizio, nel senso che le risorse necessarie alla resa del servizio (ad esempio server) non sono stabilite ex ante, potendo essere ampliate o ristrette senza che ciò comporti compromissione del servizio, nel senso di caduta;

- è resource pooling, all'utente che richiede il servizio viene assegnato un certo numero di risorse del CSP, le quali tuttavia non restano fisse per ragioni essenzialmente di "fault tolerant": per questo motivo una volta che i dati vengono immessi sulla nuvola l'utente ne perde il controllo, nel senso che gli è preclusa la possibilità di conoscere precisamente dove fisicamente il dato richiesto si trova nell'istante preciso dell'ipotetica richiesta;

- è flessibile, o meglio dotato di rapid elasticity, in quanto a seconda delle esigenze del cliente o del runtime, gli strumenti che ne realizzano il servizio possono essere cambiati e ridotti senza che ciò comporti ricadute negative in termini di resa;

- è measured service, in cui il CSP può monitorare in ogni istante la qualità del servizio reso e in particolare il numero di risorse impiegate per far fronte alle esigenze di un dato cliente.

A livello di applicazione concreta, il cloud può manifestarsi come:

- Software as a service (SaaS), rappresenta la fetta più grande del mercato cloud, in quanto permette all'utente di utilizzare la piattaforma come fosse un servizio a cui sono connesse funzionalità tipiche ad esempio di un software. Il vantaggio risiede nel fatto che l'utente è dispensato da dover installare il programma, poiché tramite browser o applicazioni gli è permesso sostanzialmente lo stesso utilizzo. Si pensi ad esempio a Google Docs che permette la gestione ed elaborazione di documenti attraverso funzionalità tipiche di suite di programmi come ad esempio Office;

- Platform as a service (Paas), un framework di piattaforme di elaborazione virtualizzate che sono rese disponibili all'utente, spesso in combinazione al servizio precedente portandolo, di fatto, alla fruizione di un vero e proprio computer su

[4] Si vedano, solo per citarne alcuni, i servizi *cloud* di *Google, Microsoft, Amazon, IBM, Verizon, HP, Salesforce.com*.

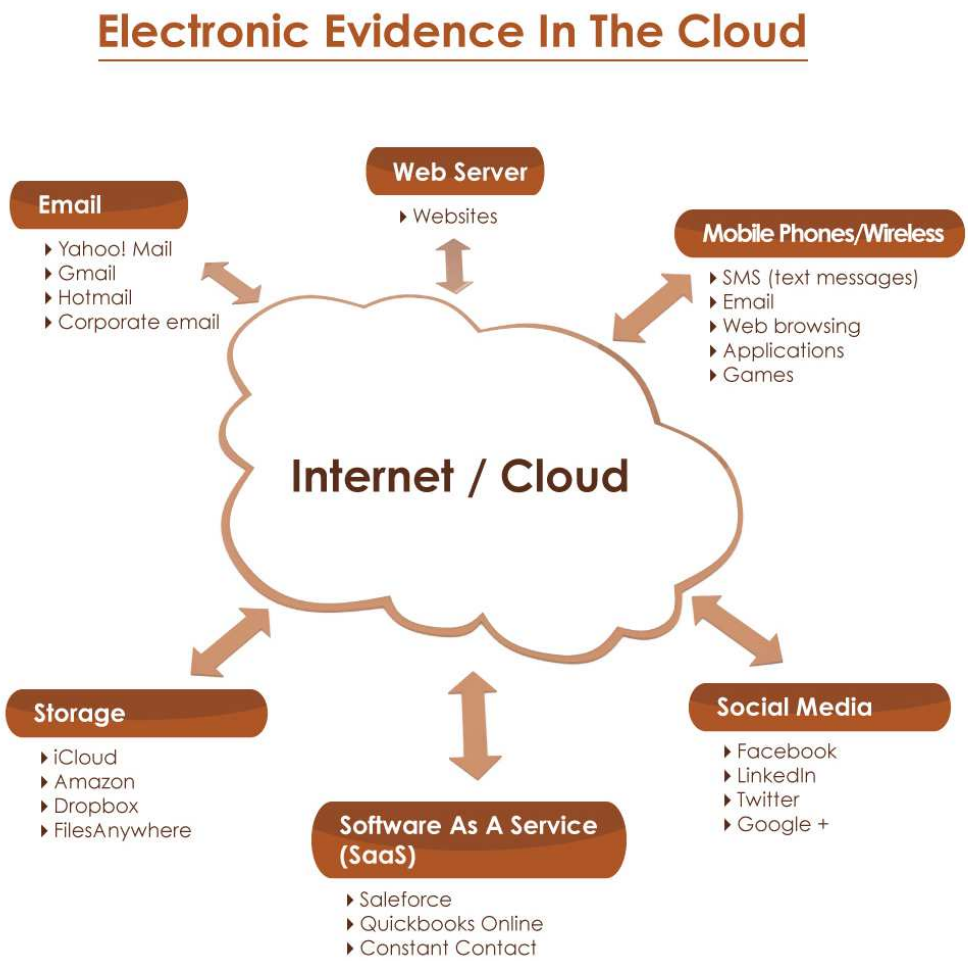
cloud;

• Infrastructure as a service (Iaas), si presenta come evoluzione delle due precedenti essendo il risultato di server, software, data center space e network: un utilizzo di questo tipo può essere sfruttato, ad esempio in grandi aziende con la creazione di complesse reti aziendali.

Questa piccola introduzione tecnica[5] consente, ai fini del nostro discorso, di delineare le difficoltà che l'informatica forense incontra allo stato dell'arte qualora sia necessario, far fronte all'acquisizione di dati contenuti all'interno di dette piattaforme. Non può sfuggire, infatti, come a oggi il cloud appaia un ottimo rifugio per soggetti mossi da intenzioni poco ortodosse: si pensi ad esempio ai "nobili reati" nel campo dei reati finanziari, del cyberlaundering, dell'evasione fiscale, o su un diverso fronte quelli legati ad esempio alla violazione del copyright o peggio ancora della pornografia infantile. Il fatto poi che allo stato attuale manchino linee legislative condivise a livello internazionale che in qualche modo consentano di porre alcuni limiti, sia in termini di controllo sia in termini di tutela della privacy, di certo non aiuta a venire a capo delle questioni emergenti. Su un fronte prettamente investigativo, le difficoltà che si registrano sono strettamente connesse alla caratteristica che abbiamo definito di resource pooling: l'acquisizione del dato postula in primis l'accesso allo stesso. Per quel che riguarda la normativa italiana, ad esempio, lo strumento processuale che potrebbe applicarsi è rappresentato dall'art. 254-bis c.p.p. in materia di sequestro di dati presso fornitori di servizi; bene ma a quale fornitore? E soprattutto dove? Tipicamente, poi, i servizi cloud possono poggiare su infrastrutture pubbliche che rendono il servizio al grande pubblico (ad esempio Amazon ASW), oppure su infrastrutture proprietarie, le quali rendono il servizio a una particolare categoria di soggetti, come ad esempio istituzioni o enti. Se dal lato proprietario i problemi d'accesso al dato possono essere "minori" nel senso che vi è una più alta possibilità di rintracciarli, nel caso d'infrastruttura pubblica la cosa si complica.

[5] Cfr più diffusamente M. TAYLOR, J. HAGGERTY, D. GRESTY, R. HEGARTY, Digital evidence in cloud computer systems, in *Computer law and security review*, n°26, 2010, pagg. 304-308; S. MANSON, E. GEORGE, Digital evidence and "cloud" computing, in *Computer law and security review*, n°27, 2011, pagg. 254-258; S. BIGGS, S. VIDALIS, Cloud computing: the impact on digital forensics investigations, in *Internet technology and secured transactions*, ICTST, 2009, pagg. 1-6.

Quand'anche ad esempio, si presentasse ad Amazon l'atto giudiziale che dispone il sequestro di dati, ulteriori difficoltà si aprirebbero agli occhi degli investigatori e in special modo dei forenser. In primis, i dati inseriti, una volta immessi nel circuito, vengono cifrati con algoritmi (per Amazon si veda l'algoritmo s3). In secondo luogo, qualora comunque si riuscisse ad ottenere i dati in chiaro, sorge il problema legato ai metadata dei file. Se, infatti, una corretta acquisizione di dati a seguito di beat stream image consente di ricostruire perfettamente l'allocazione e lo storico di tutte le informazioni contenute, nel cloud ciò non accade: perché sono gli stessi gestori del servizio a non conoscere quando e se l'utente carica contenuti (non vi è traccia quindi di uno storico), perché potenzialmente cambiano spesso allocazione spezzettandosi e quindi perdendone traccia. Da ultimo poi, gli ipotetici risultati ottenuti quali procedure hanno seguito? Può dirsi rispettata la formula della non alterazione e immodificabilità? Come può comprendersi sorge prima ancora che un problema di fattibilità, il problema dell'opportunità di perseguire detta via investigativa, in termini sia di tempo che di costi, umani e monetari, che rapportati al risultato, magari difforme rispetto ai criteri legali previsti, potrebbe portare a scoraggiarne l'utilizzo. Si auspica a che nel futuro, come sembra essere peraltro la tendenza attuale, possa arrivarsi a un'architettura normativa più stabile e concreta sulla quale porre le basi per una futura regolamentazione a livello internazionale in materia di "cloud derived evidence". Il percorso non sarà certo facile, in quanto gli interessi in gioco sono molteplici, interessando non solo gli utenti ma anche e soprattutto i fornitori di servizi cloud ai quali potrebbe necessariamente essere richiesto un onere di collaborazione, riaprendo l'acceso dibattito, o la "vecchia" ferita aperta, legata alla responsabilità e alla collaborazione degli ISP.



Su un diverso versante, si apre il problema legato ai termini di servizio impiegati, alla conseguente policy privacy, e alla sicurezza delle informazioni. Questo è uno dei punti più critici della nuvola, che è stata bersaglio di pesante critiche dal noto hacker Richard Stallman, definendolo come un ottimo esempio marketing 3.0 che esaltando le caratteristiche di hiding induce gli utenti a consegnare ai fornitori del servizio enormi quantità di dati. "In un'intervista al Guardian ha dichiarato che «il cloud computing è roba da stupidi e utilizzare applicazioni web come Gmail di Google è anche peggio della stupidità stessa. (…) Un motivo per cui non dovresti utilizzare applicazioni web per il tuo lavoro è che ne perdi il controllo»[6]. Al di là dell'intervento provocatorio inteso a far riflettere in maniera consapevole di quelli che sono i rischi legati all'utilizzo delle tecnologie, non può comunque tacersi come il problema della sicurezza e della tutela alla privacy[7] vivrà sicuramente nel futuro un nuovo acceso dibattito, alimentato dalle prospettive internazionali di regolamentazione del nuovo fenomeno.

[6] Da C. SARZANA, Considerazioni sull'*Internet* degli oggetti e sul *cloud computing*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica* (a cura di F. RUGGERI, L. PICOTTI), Giappichelli, Torino, 2011, pagg. 18-19.

[7] Si veda il caso statunitense delle istanze portate avanti dalla *Electon Privacy Information Center* cha ha chiesto alla FTC (*Federal Tecnological Commission)* di impedire a *Google* le procedure di *appliance* in quanto al momento la società non forniva sufficienti garanzie in ordine alla sicurezza delle pratiche connesse al *cloud* in termini di sicurezza e *privacy.*