CHIOMENTI

Seminari Bordoni

Cloud distribuito, supercalcolo e web 3.0

Decentralized cloud. Opportunità e sfide

Gilberto Nava

Roma, 23 Maggio 2019

Cloud storage services

- Sfruttando un modello di «*cloud computing*» il servizio consente di memorizzare una significativa quantità di dati in uno spazio virtuale ospitato su milioni di server remoti cui si può accedere istantaneamente.

- Questi servizi consentono di usufruire di uno spazio di archiviazione maggiore rispetto a quello disponibile mediante strumenti *hardware*, senza dover sostenere costi ingenti per la realizzazione di infrastrutture in *cloud*.

- I servizi di *cloud storage* sono – ad oggi – generalmente gestiti, manutenuti e forniti da un numero limitato di operatori strutturati e con una significativa presenza sul mercato («*cloud storage providers*»).

Il modello decentralizzato applicato alla *cloud storage industry*

- Con i servizi di «cloud distribuito» i dati vengono registrati in modalità criptata su milioni di server ma sono accessibili unicamente al proprietario dei dati.

- Le *server farm* vengono sostituite dall'utilizzo di capacità di archiviazione diffusa sui numerosi server.

- Non ci sono più singoli «*point of failures*» che possono essere soggetti a «*data breach*» e attacchi ostili.

Le opportunità | I

- La capacità di archiviazione è maggiore e i costi sono sostanzialmente ridotti.

- Sfruttando la tecnologia sottostante è possibile raggiungere maggiori livelli di efficienza nell'incontro tra domanda e offerta di servizi di archiviazione dei dati.

- Sulla base della costante fluttuazione delle esigenze di capacità di archiviazione si possono innescare scambi di «spazio» inutilizzato (mediante *marketplace* distribuiti).

Le opportunità | II

- La decentralizzazione del servizio consente di offrire una soluzione alternativa al problema della concentrazione, in capo ai *providers*, della possibilità di controllare un'enorme quantità di dati.

- Un modello di *cloud storage* distribuito avrebbe effetti benefici sulle dinamiche competitive del mercato dei *cloud storage services,* che conta al momento un numero molto limitato di *players*. Con un allargamento dei soggetti che offrono questi servizi si mitigherebbe il rischio che l'interruzione dei servizi prestati anche da uno solo di tali fornitori possa determinare conseguenze pregiudizievoli su larga scala.

I casi più interessanti

Le sfide
Uno sguardo alle principali tematiche di *data protection* | I

- La decentralizzazione dei servizi di *cloud storage* deve al contempo conciliarsi con le previsioni in materia di protezione dei dati personali individuate dal Regolamento (UE) 2016/679 (c.d. «**GDPR**»), quali:

- L'identificazione della catena dei responsabili del trattamento (art. 4, n. 7). Ogni soggetto partecipante al cloud diffuso potrebbe essere individuato come responsabile esterno del trattamento, con le conseguenti problematicità a livello di controllo e autorizzazioni al trattamento dei dati in capo al titolare dei dati personali.

- Il trasferimento dei dati verso paesi terzi (Capo V, art. 44 e ss.). Il modello decentralizzato e i problemi nell'individuazione della ubicazione dei server che ospitano il cloud rende complessa, ad esempio, (i) la verifica dell'adeguatezza della protezione del dato nel Paese terzo, (ii) la fornitura di garanzie adeguate sulla base di clausole contrattuali standard come previste dalla Commissione europea e (iii) la presenza di diritti azionabili e mezzi di ricorso effettivi.

Le sfide
Uno sguardo alle principali tematiche di *data protection* | II

- L'obbligo di minimizzazione dei dati, ossia l'obbligo di trattare i dati in modo adeguato, pertinente e limitatamente a quanto necessario rispetto alle finalità per le quali sono gestiti. Con il cloud distribuito l'archiviazione è potenzialmente senza limiti di estensione temporale e di diffusione dei dati.

- Il diritto all'accesso (art. 15), che consente all'interessato di ottenere dal titolare del trattamento la conferma, tra l'altro, circa (i) lo svolgimento di trattamenti, (ii) le finalità del trattamento, (iii) le categorie di dati personali trattati e i destinatari a cui i dati sono comunicati. Anche in questo caso il *decentralized cloud* implica delle difficoltà per l'interessato nell'individuare chi sia il responsabile del trattamento e chi debba quindi consentire l'esercizio del diritto all'accesso.

- Il diritto all'oblio, ossia il diritto dell'interessato a ottenere la cancellazione dei dati ove ne ricorrano le condizioni normativamente previste. Nel caso in cui l'informazione sia stata registrata su un numero significativo di *device*, una cancellazione definitiva sarebbe difficilmente verificabile.

Le sfide

I vincoli imposti dalla regolazione finanziaria e assicurativa | I

i. L'impiego di servizi in *outsourcing* nelle forme del *cloud computing* da parte di banche, imprese di investimento e compagnie assicurative è oggetto di particolare attenzione da parte delle Autorità di vigilanza di settore.

ii. La Banca d'Italia ha disciplinato specificamente nel 2013 l'utilizzo di servizi *in community* e *in cloud* da parte delle banche italiane, imponendo alle stesse requisiti aggiuntivi rispetto a quelli previsti dalla disciplina generale in materia di esternalizzazione di funzioni aziendali;

iii. La *European Banking Authority* (EBA) nel dicembre 2017 ha pubblicato delle Linee Guida specificamente dedicate all'esternalizzazione *in cloud* di funzioni aziendali da parte delle banche europee;

iv. Nel febbraio 2019, l'EBA ha pubblicato nuove Linee Guida in materia di esternalizzazione, che contengono specifiche previsioni dedicate all'impiego di servizi *in cloud*. Le nuove Linee Guida si applicheranno a banche, istituti di pagamento, IMEL e talune categorie di imprese di investimento europee, a partire dal 30 settembre 2019, sostituendo – tra l'altro – le Raccomandazioni EBA di cui al punto precedente;

v. La *European Insurance and Occupational Pensions Authority* (EIOPA) ha recentemente pubblicato un *paper* dedicato all'impiego di servizi *in cloud* da parte delle imprese di assicurazione, annunciando l'intenzione di pubblicare delle Linee Guida specifiche, analoghe a quelle già adottate dall'EBA, entro la fine del 2019.

Le sfide
I vincoli imposti dalla regolazione finanziaria e assicurativa | II

Come illustrato dall'EBA nelle nuove Linee Guida in materia di *outsourcing*, la necessità di prevedere regole specifiche per l'esternalizzazione di servizi *in cloud* nei settori vigilati poggia sulle seguenti considerazioni:

- le prestazioni e la qualità dei servizi *in cloud* e il livello di rischi operativi cui è esposto l'intermediario che utilizza i medesimi servizi dipendono significativamente dalla capacità del fornitore di garantire in modo appropriato la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi, nonché dei processi utilizzati per elaborare, trasferire o memorizzare tali dati. Una appropriata tracciabilità dei meccanismi finalizzati alla registrazione delle operazioni svolte dall'intermediario è inoltre fondamentale per individuare eventuali *data breach*;
- i fornitori di servizi *in cloud* gestiscono spesso un'infrastruttura informatica geograficamente distribuita, che impone una particolare attenzione alla gestione, anche contrattuale, della sicurezza e del trattamento dei dati dell'intermediario;
- la sub-esternalizzazione dei servizi *in cloud* ha natura più dinamica rispetto alle forme di esternalizzazione tradizionali. È necessaria quindi una maggiore certezza circa le condizioni e i limiti entro cui il fornitore può delegare la propria attività a terzi.

Le sfide
I vincoli imposti dalla regolazione finanziaria e assicurativa | III

- In considerazione dei profili di attenzione richiamati nella slide precedente, le Autorità di vigilanza richiedono agli intermediari di predisporre controlli rafforzati in relazione all'affidamento di servizi *in cloud*, soprattutto in caso di esternalizzazione di componenti critiche. Le Autorità di vigilanza richiedono in particolare che:

  a. le locazioni dei *data center* utilizzabili siano preventivamente comunicate all'intermediario;

  b. siano previsti adeguati meccanismi di isolamento dei dati di un intermediario rispetto agli altri clienti, a garanzia della loro riservatezza e integrità;

  c. il fornitore garantisca contrattualmente il rispetto dei livelli di servizio stabiliti, anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti, e assicuri la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive;

  d. siano concordate tra le parti modalità di *audit* adeguate alla criticità delle risorse esternalizzate e in considerazione dell'architettura del fornitore;

  e. l'intermediario debba dotarsi di un registro dei rapporti di *outsourcing* che, con riferimento ai servizi *in cloud*, descriva chiaramente le modalità di erogazione del servizio (*public*, *private*, *hybrid*, *community*), i dati trattati e le locazioni dei *data center* impiegati;

  f. le risorse che svolgono le attività di *audit* sui fornitori di servizi *in cloud* siano dotate di professionalità adeguata al livello di complessità dei servizi oggetto di verifica.

Le sfide
I vincoli imposti dalla regolazione finanziaria e assicurativa | IV

- L'impiego di modelli di servizio «distribuiti» da parte dei soggetti vigilati deve essere coordinato con gli oneri di gestione dei rapporti con i fornitori imposti ai medesimi soggetti dalla disciplina di vigilanza in materia di esternalizzazione di servizi *in cloud*.
- In particolare, gli obblighi rafforzati di controllo sui fornitori, sulla loro operatività e sulle modalità di conservazione e trattamento dei dati imposti agli intermediari dalle linee guida di settore in materia di *cloud computing* potrebbe astrattamente limitare la diffusione di modelli di servizio effettivamente decentralizzati.
- D'altra parte, il mercato dei servizi *in cloud* è esposto a rilevanti rischi di concentrazione, poiché tali servizi sono ordinariamente prestati da un numero ristretto di grandi *player* internazionali. Di conseguenza, l'interruzione dei servizi prestati anche uno solo di tali fornitori potrebbe determinare conseguenze sull'operatività degli intermediari a livello sistemico.
- L'introduzione di modelli decentralizzati potrebbe in questo senso contribuire ad ampliare la platea dei potenziali fornitori di servizi *in cloud* e contribuire di conseguenza alla riduzione dei richiamati rischi di concentrazione.

Grazie

Gilberto Nava

gilberto.nava@chiomenti.net