Servizi UC&C in ambito cloud: sicurezza dei dati e garanzie sulla loro riservatezza.
Garantire la sicurezza dei dati e garantire la riservatezza nell'ambito di servizi UC&C attivati su soluzioni cloud vuole dire, in prima battuta, porsi seriamente il problema e poi, di conseguenza, affrontare le questioni sotto diversi profili sulla base delle diverse competenze ed ambiti professionali interessati.
A tale proposito pare utile ricordare che i risultati migliori si raggiungono solo attraverso una stretta collaborazione tra le diverse figure professionali quali, ad esempio, il fornitore del servizio UC&C, il fornitore del servizio cloud, il legale, il responsabile ITC ed il risk manager: considerazione magari banale ma che spesso viene dimenticata anche, ma non solo, per ragioni di contenimento dei costi.
Un primo aiuto ai professionisti ed alle aziende anche, o forse soprattutto, medio piccole, tipiche del panorama italiano, caratterizzate da una minore disponibilità di risorse economiche ma, proprio per questo, maggiormente interessate ad avvalersi di servizi professionali cloud, può essere fornito, in un'ottica di informazione e formazione, da Cloud Security Alliance Italy Chapter (https://chapters.cloudsecurityalliance.org/italy/); questa è, infatti, un'associazione non riconosciuta non profit di diritto italiano, rappresentante la divisione nazionale dell'ente no profit denominato "Cloud Security Alliance" (https://cloudsecurityalliance.org /) che ha come uno degli scopi precipui quello di promuovere le best practice di sicurezza nell'ambito del Cloud Computing e contribuire alla sicurezza di tutte le altre forme di computing attraverso l'educazione agli usi del Cloud Computing.
Il primo aiuto per i soggetti sopraindicati può quindi, nel concreto, essere fornito dalla traduzione in italiano della Guidance (attualmente giunta alla versione 2.1 ed incorso di stesura la versione 3.0) ovvero una guida dal taglio pratico-generalista che dovrebbe essere d'aiuto per meglio comprendere quali domande porre, quali sono le prassi correntemente raccomandate, e le potenziali insidie da evitare nell'ambito del cloud computing.
Il passo successivo è, come detto, affidarsi alle competenze dei singoli professionisti.

Da un punto di vista giuridico le questioni poste nel titolo di questo contributo trovano soluzioni - o meglio punti di attenzione - principalmente sotto due aspetti normativi: quello attinente le questioni civilistico contrattuali e quello attinente ai principi dettati dal codice in materia di protezione dei dati personali. Fare in queste poche righe una disamina completa dei vari aspetti risulterebbe del tutto impossibile nonché foriera di omissioni o eccessive semplificazioni. Pare quindi più opportuno, in questa sede, fare dei cenni alle questioni giuridicamente più interessanti, lasciando ad un'analisi approfondita il singolo caso specifico.

Con "**aspetto civilistico-contrattuale**" si intendono tutte quelle questioni, per altro importantissime, inerenti gli accordi che regolano o dovrebbero regolare l'azienda fruitrice di un servizio UC&C con il fornitore o i fornitori di piattaforme o servizi cloud. Assume quindi una grande rilevanza, proprio ai fini della sicurezza dei dati o delle garanzie sulla loro riservatezza,

la fase precontrattuale in cui si cerca di formalizzare in un contratto il tipo di servizio fornito, gli impegni e le garanzie del fornitore del servizio, l'indicazione di dove vanno i dati trattati e di come vengono trattati (si pensi ad esempio al caso dei dati condivisi durante una web collaboration), la durata ed il rinnovo del contratto. Sotto questo profilo altri aspetti contrattuali da considerare sono la legge e la giurisdizione applicabile (spesso il fornitore di servizi risiede ed opera al di fuori dei confini nazionali o, addirittura dei confini UE), l'assistenza fornita ed i livelli di servizio garantiti (c.s. SLA) ed, infine l'importanza delle clausole c.d. di way-out ovvero la garanzia di poter cambiare fornitore cloud, per i motivi più svariati, senza eccessivi traumi per l'azienda o il professionista cliente che devono poter rientrare nella piena e totale disponibilità dei dati in formato elettronico standard, in tempi rapidi e con modalità precise e chiare, in modo da evitare di essere di fatto nell'impossibilità tecnica od economica di migrare su altre piattaforme o verso altri fornitori di servizi.

Alcune problematiche devono poi essere prese in considerazione anche tra aziende che usufruiscono tra di loro di servizi UC&C attivati su soluzioni cloud quali ad esempio questioni relative alla proprietà intellettuale dei dati, delle idee, dei documenti ecc.

Le questioni concernenti le disposizioni del codice in materia di **protezione dei dati personali** sono di diversa natura: si pensi, ad esempio, a quelle norme poste a tutela del trattamento sicuro dei dati, riassunte da un lato nel Disciplinare Tecnico e dall'altro nella norma di portata più ampia di cui all'art. 31 dove il criterio di adeguatezza non è quello dell'ormai temporalmente e tecnologicamente superato citato Disciplinare Tecnico bensì quello delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.
Altre importanti questioni attengono poi le norme da tenere presente in materia di esportazione dei dati, che avviene quasi sempre in ambito cloud, dall'Italia verso paesi UE o extraUE: ovvero quelle degli artt. 43, 44 e 45 del codice in materia di trattamento dei dati. Il principio generale dell'art. 45 chiarisce che: "Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza." Da qui il consiglio pragmatico, ove applicabile, di avvalersi di servizi di cloud che crittografano in automatico i dati sul pc/server dell'utente e quindi "escano da casa propria" già crittografati indipendentemente dall'utilizzo di protocolli di rete protetti (https...) proprio al fine di aggirare "elegantemente" le problematiche in diritto, sottese e sopra evidenziate, senza però violare le norme le legge attualmente vigenti.

Non deve peraltro trarre in inganno o dare un falso senso di sicurezza la modifica apportata al

codice in materia di protezione dei dati personali dal recente decreto legge 6 dicembre 2011, n. 201, convertito con modificazioni dalla L. 22 dicembre 2011, n. 214; la materia è infatti molto più scivolosa di quella forse un pochino superficialmente presentata dalla stampa e richiede una attenta analisi caso per caso. A tale proposito non va dimenticato che a livello europeo si sta ultimando la predisposizione di norme e di direttive specifiche proprio inerenti l'universo cloud tese tra l'altro a considerare in maniera giuridicamente più precisa tale tecnologia che per sua definizione precipua è del tutto sovranazionale, con le conseguenti questioni afferenti norme del tutto diverse tra nazione e nazione.

L'importanza di un'analisi giuridica da parte di un legale trova, infine, conferma anche nella necessità di evitare i rischi conseguenti a scelte disinformate; le questioni che il professionista o l'azienda potrebbero dover affrontare sono, infatti, di varia natura e vanno da problematiche civilistico-contrattuali all'incorrere in sanzioni civili, amministrative ma anche penali, tutte previste dal codice in materia di protezione dei dati personali, oppure nelle norme sulla

responsabilità amministrativa degli enti di cui alla legge 231/2001.

avv. **Valerio Edoardo Vertua**
Perfezionato in Computer Forensics ed Investigazioni Digitali
Co-fondatore di Cloud Security Alliance Italy Chapter