Cloud o non cloud? Questo è il dilemma.

Almeno nella PA

C'era una volta l'etere. L'etere era una sostanza immaginaria, ipotizzata per la prima volta da Aristotele[1], il quale si chiedeva per quale ragione gli astri stessero appesi e non cadessero sulla terra. Dato che la legge sulla gravitazione universale non era ancora stata formulata, non era una domanda così peregrina ed egli ipotizzò una sostanza non visibile, l'etere appunto (o quintessenza, in aggiunta ad acqua, fuoco, terra ed aria), ovvero una specie di gelatina che avrebbe permeato il cosmo impedendo ai corpi celesti di caderci in testa.

L'idea dell'etere è stata poi ripresa in seguito, ad esempio quando si era ormai capito il meccanismo di trasmissione del suono attraverso l'aria, ma non si riuscivano a spiegare i meccanismi di trasmissione dei fenomeni elettrici o magnetici: prima che Maxwell scrivesse le sue equazioni a fondamento scientifico dell'elettromagnetismo, si pensò all'etere, una sostanza diffusa come l'aria nella quale le onde elettriche e magnetiche avrebbero riverberato come i suoni nell'aria. D'altra parte le attuali materia oscura ed energia oscura sono una forma di etere, nel senso che si capisce che qualcosa non torna nei modelli matematici e si cerca di riempire i vuoti con materiali immaginari, in attesa di comprendere a fondo i fenomeni o di trovare nuove teorie che non comportino sostanze ipotetiche[2].

Per molti, oggi, il cyberspazio, il cloud ed altri oggetti misteriosi sono una forma di etere, nel senso che si sa che esistono determinate applicazioni, non si capisce bene cosa siano in realtà e come operino e le si usa quindi con un atteggiamento fra il distaccato ed il mistico, senza approfondire più di tanto le implicazioni.

In realtà il cyberspazio non esiste: esistono data center, ben localizzati sulla superficie terrestre (o poco sotto di essa), fatti di cemento, acciaio, vetro e quant'altro. Esattamente come non esistono le macchine virtuali: esistono server remoti, fatti di metallo, plastica, silicio, che qualcuno ha costruito, pagato ed installato. E non esiste neppure il cloud: esistono hard disk pagati ed installati da qualcun altro.

Anche quei beni apparentemente immateriali, per usare la definizione dell'on. Quintarelli[3], in realtà sono riconducibili ad una dimensione fisica: se mi accreditano lo stipendio o un bonifico, è vero che non ho in mano dei dobloni da conservare in un forziere, ma è altrettanto vero che, da qualche parte sulla Terra, alcuni atomi di ferrite o altro materiale si orientano in modo da attestare che il mio conto bancario ha un saldo che da X è diventato Y, quindi, per quanto microscopico ed intangibile, comunque un oggetto fisico nello spazio reale.

Soprattutto occorre tenere ben presente che raramente qualcuno spende miliardi di dollari per installare macchine da mettere a disposizione gratuitamente al pubblico per puro amore del prossimo: un qualche ritorno deve averlo. Avendo chiare queste premesse, si può

[1] Breve storia dell'Etere, Gianfranco Verbana, Saggio pubblicato su Radio Rivista aprile-1995 in occasione del centenario della radio.

[2] Emergent Gravity and the Dark Universe, Erik Verlinde, Delta-Institute for Theoretical Physics Institute of Physics, University of Amsterdam - 2016

[3] Costruire il domani, Stefano Quintarelli, Il Sole 24 Ore

decidere di usare questi strumenti come si ritiene più opportuno, però con la piena consapevolezza delle conseguenze che le scelte fatte necessariamente comportano.

Anche per godere di altri beni ci sono opportunità diverse: case, auto o vacanze possono essere acquistate in contanti, pagate a rate con mutuo ipotecario o altra garanzia, affittate, prese in leasing. Almeno se i soldi ci sono, perché se la cifra necessaria per l'acquisto non è disponibile le opzioni si riducono.

Chiaramente in molti casi il cloud è comodissimo: poter condividere documenti con un gruppo, poter accumulare materiale per un libro o un articolo quando si opera su PC diversi, poter disporre in qualunque momento ed in qualunque parte del mondo dei propri corsi e dei propri scritti è utilissimo. Io, ad esempio, conservo in cloud tutti miei articoli e le mie relazioni, assieme a tutto il materiale raccolto per realizzarli; se anche dovesse essere rubato e diffuso, comunque, non me ne importerebbe nulla, trattandosi di articoli pubblicati e di informazioni raccolte principalmente dal WEB. Se poi qualcuno dovesse rubarmi un articolo ancora in fase di stesura, tutto sommato sarebbe una seccatura, ma non un dramma. Sull'economicità ho invece qualche riserva. Certo, un solo HD esterno, soprattutto se non si ha la possibilità di conservarlo in un luogo separato dal PC, non dà la stessa sicurezza e comodità, ma un HD da 1TB costa su Amazon sui 50 – 60 euro e dura diversi anni, 1TB su Dropbox o su GoogleDrive comportano una spesa di circa 120 euro anno, salvo sconti e promozioni, quindi un sistema di *private cloud*, tutto sommato, può essere quantomeno più economico, se non altrettanto affidabile.

Conosco un ingegnere specializzato in modelli strutturali e calcoli agli elementi finiti: le macchine virtuali gli hanno cambiato la vita! Mentre in passato doveva comprare i computer portatili più potenti in commercio, comunque sempre insufficienti, e doveva tenere in ufficio workstation potenti ed aggiornate, spesso ugualmente insufficienti, oggi può noleggiare una macchina virtuale, configurarla per bene, creare una copia in modo che se qualcosa va storto è sufficiente cancellare la copia e ricrearne un'altra per ripartire. Soprattutto può andare dai clienti con un portatile normale, sviluppare i suoi modelli sulla macchina virtuale, quindi, al momento dell'elaborazione, sfruttare il calcolo distribuito e noleggiare per un solo giorno due – tre – dieci macchine, a seconda delle necessità del momento. Quando però gli ho chiesto se non avesse paura di perdersi qualcosa o di vedersi copiare qualche modello, mi ha spiegato che i suoi modelli personali, le utility che ha sviluppato, i lavori fatti in passato stanno ben chiusi in ufficio, e sul cloud vengono usati limitatamente alle necessità del momento. Una persona consapevole e competente, che sfrutta a proprio favore le potenzialità degli strumenti, minimizzando i rischi conseguenti.

Le Pubbliche Amministrazioni non hanno però la stessa flessibilità, essendo sempre dibattute fra differenti problematiche, che vanno dalla necessità di garantire la conservazione di dati per tempi anche molto lunghi alla necessità di assicurare la continuità operativa, dai problemi di bilancio alla mancanza di personale qualificato, dai contrasti normativi ai problemi con gli organi politici.

Alla mancanza di una sistema centrale, ben strutturato e coordinato, si è trattato di supplire con indicazioni, linee guida, obblighi di legge non sempre chiari e rispettati.

Il problema sostanziale, in ogni caso, è che una PA deve assicurare che i dati che tratta siano accessibili soltanto a chi ne ha diritto e che siano conservati in modo sicuro e conforme alle norme vigenti, in un quadro normativo dove si intersecano regole europee, nazionali,

linee guida provenienti da diverse Agenzie. Per non parlare della competenza dei referenti interni, spesso scelti fra il meno peggio (senza offesa per i prescelti) e della preparazione dei tecnici esterni, il più delle volte scelti col criterio dell'offerta economicamente più vantaggiosa. Non dimentichiamo che il territorio italiano è diviso in circa 8000 Comuni, anche di piccole dimensioni, per cui le situazioni possono essere piuttosto variegate.

Vediamo allora qualche esempio di architettura di rete, gestione dei dati ed utilizzo del cloud. Si tratta naturalmente di un'analisi estemporanea fatta con la collaborazione di alcuni Enti amici, non di un'analisi scientifica del fenomeno.

Comune A

Server in doppio RAID 1, PC utenti con dischi dati in RAID 1 e SO su SSD, connessione di rete protetta da firewall fisico e software, NAS in RAID 1 con firewall software e diverso sistema operativo rispetto alla rete, situato in luogo nascosto. SO W10 aggiornato, antivirus, anti-malware e anti-ransonware su ogni PC, backup mattutino incrociato fra i dati del PC ed il server ed il data base dei programmi residenti sul server utilizzati della postazione ed il PC, backup notturno sul NAS e backup settimanale sulla seconda coppia di dischi del server. Immagine quindicinale automatica dei SO e dei programmi di ogni PC. Backup settimanale dei dati dei PC su HD esterni conservati in cassaforte, backup mensile completo, inclusivo delle immagini dei dischi, conservato in altro edificio in cassaforte a prova di acqua, fuoco e crollo.

Cloud usato solo temporaneamente per trasferire file di grandi dimensioni, conservazione sostituiva a norma[4].

Tutto è migliorabile, ma si tratta di un sistema abbastanza solido, che infatti ha resistito piuttosto bene all'involontario stress test in occasione del criptolocker: anche grazie alla formazione del personale, che ha immediatamente abbattuto la rete spegnendo lo switch, alla fine è andato perso un solo file, ovvero la registrazione dei buoni mensa della mattinata, facilmente ricostruibile.

Va detto però che per costruire questo sistema si sono verificate diverse condizioni favorevoli:

- Referente interno consapevole ed attento.
- Tecnico esterno disponibile e preparato.
- Amministrazione che dà fiducia e supporto.
- Bilancio sano, che consente ogni anno di effettuare aggiornamenti e migliorie.

E' particolarmente importante la possibilità e capacità di effettuare migliorie continue: se tutti gli anni si spendono cifre relativamente piccole si ha un sistema sempre aggiornato che non richiede interventi straordinari. Se invece si lascia degradare la dotazione, si finisce col dover spendere cifre importanti, con tutte le incertezze e le lungaggini che questo comporta.

Comune B

Server in RAID 5, connessione diretta alla rete senza protezioni hardware o software, NAS in backup continuo con stesso SO della rete, antivirus sul server e su ogni PC. Unico PC con backup giornaliero sul server è quello dei demografici (se non l'hanno tolto dall'ultima

[4] DPCM 13 dicembre 2013

volta che sono passato io). SO W7 prevalente, un PC con W10. Aggiornamenti manuali quando passa il tecnico (15gg in media).

Nessun anti-malware, nessuna protezione antivirus sul NAS, nessun HD scollegato dalla rete.

Cloud non utilizzato, conservazione sostitutiva a norma[5].

Comune C

Server in RAID 1, connessione diretta alla rete, SO WindowsXP e due PC con Seven, backup con Dropbox grazie alla cartella del server. I dati eventualmente salvati sui singoli PC restano unicamente sull'HD del singolo utente. Antivirus centralizzato sul server.

La ragioneria paga annualmente l'abbonamento per il backup, ma nessuno sa se esiste un contratto e quali siano le condizioni del servizio. Cloud non utilizzato, conservazione sostitutiva sconosciuta.

Comune D

"Non sappiamo, se ne occupa il tecnico". Il tecnico è entrato a gennaio e non ha ancora guardato com'è fatto il server, per cui non sa dire quanti dischi ci sono e come sono configurati. Sa però che ci sono 2TB di spazio disponibile e che il backup è assicurato da uno strimmer da 40GB su cui vengono salvati settimanalmente i dati principali del server. Quante cassette ci siano e quanto sovente vengano cambiate non si sa, sempre che vengano cambiate, come non si sa se dopo oltre 10 anni di onorato servizio siano ancora effettivamente funzionanti. Tutti i PC sono con Windows XP.

Cloud non utilizzato, conservazione sostitutiva sconosciuta. In generale non vedo molto bene l'idea di Dropbox, ma forse in questo Comune sarebbe da considerare.

Comune E

I dipendenti non sanno nulla ed i tecnici "per privacy" non rilasciano informazioni. La rete è peer-to-peer con Windows XP, ed apparentemente la connessione al WEB non ha protezioni. Il backup è incrociato: sono state individuate tre coppie di PC che fanno il backup una macchina sull'altra. Poiché i PC sono in numero dispari, il computer dei vigili non ha backup, infatti una volta si è perso tutto il data base delle multe e da allora fa la copia su chiavetta USB (sempre inserita). L'antivirus per XP non è aggiornato da maggio 2014.

Insomma, se la legge è uguale per tutti come ricordato dalla scritta qua sopra, la sicurezza informatica NON è invece uguale per tutti.

Anche i privati, tuttavia, non sempre brillano per consapevolezza e scelte oculate. Conosco una società che si occupa di brevettazione, quindi tratta dati che sono riservati ed appetibili: "per aumentare la sicurezza" (e sottolineo la motivazione, quindi non per comodità o risparmi, ma per la sicurezza) è passata a Google mail PRO, con incluso spazio su cloud e garanzia di conservazione per 10 anni.

[5] Anche la conservazione sostitutiva è ovviamente un cloud. In questo caso distinguo tra il gestore certificato ed un cloud generico e gratuito dei comuni servizi utilizzati anche dai privati.

In realtà il capo del CED non è né stupido né incompetente, ma guarda al suo stipendio: è consapevole della scarsa competenza tecnica del Consiglio di Amministrazione e del fatto che se si perdesse i dati si perderebbe anche il posto, mentre nessuno va ad indagare sulla qualità e sicurezza reale del sistema, finché tutto funziona. Certo affidare i dati a Google è molto più semplice – e, dal punto di vista del mero *disaster recovery*, forse anche effettivamente più sicuro – rispetto ad allestire un sistema di conservazione privato a prova di bomba. Anche inteso in senso letterale.

Ci sono però delle norme specifiche che obblighino all'utilizzo del cloud? In realtà, tranne la conservazione sostitutiva di cui vedremo meglio fra poco, non c'è né un obbligo ad usare servizi cloud né un divieto a conservare i dati in casa, fermi restando gli obblighi di sicurezza fisica ed informatica.

Sia il Governo italiano che l'Unione Europea, tuttavia, spingono sul cloud e vi è una pletora di indicazioni, raccomandazioni, linee guida orientate in questo senso. Viste le situazioni qui sopra descritte non mi sento neppure di dare tutti i torti, però ritengo che sia sbagliato portare le Pubbliche Amministrazioni su un cloud gestito da Società private più o meno serie, localizzato in luoghi non ben definiti, gestito in modo non pienamente trasparente e sul quale si può esercitare un controllo limitato. E' lo stesso problema di affidamento ai privati di servizi che dovrebbero – a mio parere - essere pubblici, come avevo già evidenziato nella relazione presentata un po' di tempo fa nell'edizione di Pisa[6]. Ritengo poi totalmente assurdo parlare di cloud in senso generico senza che questa spinta sia preceduta ed accompagnata da un percorso formativo che consenta di valutare gli aspetti tecnici e giuridici del fornitore scelto.

Al momento, gli unici obblighi sono quelli del menzionato DPCM 3 dicembre 2013 sulla conservazione, che è partito inizialmente obbligando a conservare l'elenco dei protocolli giornalieri su un server remoto, espressamente localizzato in Italia[7] (su questo punto ho qualche dubbio giuridico sulla legittimità della prescrizione alla luce delle norme europee, ma lascio la valutazione ai giuristi). In questo modo, in caso di perdita totale dell'archivio, si sarebbe potuto avere un elenco preciso di ciò che non era più recuperabile. Successivamente si sono aggiunti i contratti e le fatture elettroniche, i modelli 3D del sistema elettorale e via via si aggiungeranno altre categorie di documenti, con l'obiettivo finale (spero) di conservare in un luogo remoto e sicuro tutto l'archivio digitale dell'Ente.

Per questo lavoro si sono attivate le Società che già fornivano software agli Enti Pubblici, costruendo data center di conservazione sul territorio italiano e, in linea generale, conformi agli standard previsti dal decreto e dalle altre indicazioni AgID.

Eppure in molti documenti, raccomandazioni, linee guida, si continua a parlare di cloud in modo astratto e generico. Viene dunque spontaneo chiedersi: se già ci sono le norme e le strutture, perché non potenziarle ed estenderle ad un backup completo dei dati digitali dell'intero Ente? Perché lasciare questi data center ai privati e non realizzare dei data center statali o europei espressamente dedicati alle pubbliche amministrazioni, dove conservare i dati in tutta sicurezza? Sicurezza intesa a 360°, quindi sia nei confronti del *disaster recovery* che di una conservazione di dati pubblici esclusivamente presso strutture pubbliche sicure e riservate.

[6] http://urna.winstonsmith.org/materiali/2016/atti/ep2016se_17_giorio_Relazione_06.pdf
[7] Art. 9 DPCM 3 dic 2013

In ogni caso, non si può prescindere dalla formazione e dalla competenza di responsabili e operatori. Fin quando l'insieme dei dati pubblici, soprattutto dei piccoli Enti, che, almeno in Italia, costituiscono l'ossatura portante dell'apparato burocratico statale, vengono affidati alla buona volontà dei singoli ed alla fortuna di incontrare persone preparate ed amministrazioni attente, temo che carta e biro restino l'unico modo per garantire un minimo di integrità dei dati.

Infine, sarò retrogrado per dato anagrafico e mentalità, ma un HD con i miei dati privati ed uno con quelli del mio ufficio sotto il mio controllo diretto preferisco ancora avercelo. O magari anche due.