SERVIZI DI CLOUD COMPUTING E PROTEZIONE DEI DATI PERSONALI IN AMBITO BANCARIO

Avv. Luca Bolognini
Presidente Istituto Italiano per la Privacy e la Valorizzazione dei Dati
Founding Partner Studio ICT Legal Consulting

Avv. Enrico Pelino
Fellow Istituto Italiano per per la Privacy e la Valorizzazione dei Dati

19 gennaio 2015

I – PREMESSA

Il presente manualetto si prefigge un obiettivo pratico, quello di fornire una sintesi aggiornata e giuridicamente scrupolosa, in materia di protezione dei dati personali, sull'adozione di soluzioni cloud nel settore bancario, connotata da un taglio divulgativo, che permetta al lettore di avere un prospetto di sintesi sui profili di maggiore rilevanza.

Il presente contributo vuole porsi anche come un'agile guida che indichi un metodo per gestire in termini concreti la scelta di un fornitore cloud.
Al termine e dopo la parte dedicata alle conclusioni sarà presentato uno schema riepilogativo dei punti evidenziati, pensato per fungere da *checklist* ai fini di una verifica pratica in occasione dell'esame di offerte di fornitura cloud.

Quanto alla perimetrazione dell'area giuridica, la rassegna ragionata che sarà presentata in queste pagine è focalizzata, come già indicato, su questioni relative alla tutela dei dati personali, il che non esclude ulteriori cenni a profili giuridici di portata più generale che siano connessi con qualcuna delle tematiche privacy.

Il lettore a cui il contributo si rivolge ricopre un ruolo decisionale o consulenziale, è cioè chiamato ad effettuare scelte operative di acquisto/valutazione di soluzioni cloud e/o ad analizzare gli aspetti giuridici connessi con quelle soluzioni, ma non ha una competenza o formazione specifica sugli aspetti di diritto che interessano questa tecnologia. Il lettore ideale di questo manualetto ha in ogni caso familiarità con concetti base del diritto alla protezione dei dati personali, quali appunto la nozione di "dato personale", di "interessato di trattamento", di "trattamento", di "responsabile" e "titolare", di "misure di sicurezza", concetti che non verranno

perciò qui ripetuti. Ha inoltre una conoscenza tecnica minima di termini informatici di utilizzo corrente, quali “storage”, “infrastruttura”, “piattaforma”, “ridondanza”, “data center”.

Il cloud nel settore bancario

Nello specifico dell'ambito bancario, vanno menzionate innanzitutto le integrazioni effettuate dalla Banca d'Italia con l'intervento di aggiornamento n. 15 del 24 luglio 2013 al Titolo V della circolare n. 263 del 27 dicembre 2006, soprattutto per quanto concerne l'inserimento nella detta circolare dei Capitoli VIII e IX. Si tornerà comunque sull'intera questione più avanti in queste pagine.

Sul piano degli interventi di studio e di sensibilizzazione in ambito bancario, si registrano in Italia occasioni di riflessione dedicate alla tecnologia cloud nel settore bancario, già a partire dal seminario organizzato il 28 settembre 2012 dalla Banca d'Italia, sul tema *“Il cloud computing nel sistema finanziario - standard, regolamentazione e controlli”* al quale ha partecipato anche l'Ufficio del Garante per la protezione dei dati personali.

Al di là della circolare già citata e degli approfondimenti svolti in momenti di studio e di incontro come quello menzionato, mancano tuttavia lavori di sintesi in forma di specifiche linee guida nel settore bancario che possano raccogliere e sintetizzare l'esperienza che sulla tecnologia cloud si è andata accumulando e organizzando nel tempo, anche in settori diversi da quello specifico di riferimento. Il presente contributo non ambisce a, né può per evidenti ragioni di spazio e di formato, colmare questo vuoto, può tuttavia fornire qualche utile indicazione che

funga, questo è l'augurio, da traccia per un sviluppare un più ampio lavoro di settore.

A livello internazionale, è possibile reperire in risorse web dedicate al settore bancario spunti anche molto recenti che rivelano un interesse crescente per la tecnologia cloud, ancorché essi mostrino in molti casi un atteggiamento non solo di attenzione ma anche di attesa, che fotografa una fase nella quale le reali possibilità di applicazione della tecnologia cloud nel settore bancario non appaiono ancora del tutto messe a fuoco, specialmente per ciò che attiene alla gestione dei processi critici. È comunque una fase caratterizzata da una forte mobilità, da uno sviluppo che può preludere a un'adozione più generalizzata di soluzioni cloud. In particolare, si ha notizia di istituti di credito che hanno cominciato a sperimentare e ad adottare soluzioni cloud e di altri che sarebbero in procinto di farlo[1].

Su un piano diverso e più generale, un dato notevole e di grande stimolo è rappresentato dalla vasta iniziativa alla quale la Commissione UE ha impresso l'avvio ufficiale nel 2012, volta a promuovere e a supportare una sempre più vasta adozione della tecnologia cloud in Europa, attraverso una strategia di semplificazioni e armonizzazioni.

Considerato perciò il particolare momento storico, che vede oggettivamente la convergenza di varie tendenze favorevoli al fenomeno cloud, il presente

1 Cfr. FLINDERS, *Is cloud computing almost too good to be true for banks?*, in *Computerweekly.com*, 6 gennaio 2014 url: computerweekly.com/news/2240212022/Is-cloud-computing-almost-too-good-to-be-true-for-banks; CROSMAN, *Banks Pushed Toward Cloud Computing by Cost Pressures*, in *Americanbanker.com*, 10 marzo 2014, url: http://www.americanbanker.com/issues/179_47/banks-pushed-toward-cloud-computing-by-cost-pressures-1066124-1.html; GROENFELDT, *Some Banks Are Heading To The Cloud -- More Are Planning To*, in *Forbes on-line*, 26 giugno 2014, url: *forbes.com/fdc/welcome_mjx.shtml*; BROWN, *Six reasons why cloud computing will transform the way banks serve clients – and the five hurdles to* overcome, in *Banking Technology on-line*, 28 luglio 2014, url: http://www.bankingtech.com/236322/six-reasons-why-cloud-computing-will-transform-the-way-banks-serve-clients-and-the-five-hurdles-to-overcome/

manualetto vuole porsi anche come strumento tempestivo di ausilio pratico nella fase di approccio a questa tecnologia e alla valutazione dei servizi da acquisire.

Scelte di inquadramento giuridico ed espositive di questo manualetto

Si può anticipare da subito che, per esigenze di semplificazione dell'analisi, ci si muoverà nell'ottica di servizi cloud rivolti a soggetti privati (quali sono appunto le banche, mentre per ragioni di spazio e di formato non si prenderanno in considerazione le specifiche questioni che attengono all'adozione di soluzioni cloud nella Banca d'Italia, che è soggetto di diritto pubblico), che operano prevalentemente su dati comuni, ancorché spesso caratterizzati da tratti specifici, quali l'idoneità a fotografare in maniera pervasiva e minuziosa l'attività relazionale degli interessati di trattamento e abbastanza numerosi e pervasivi da combinarsi in composti aggregati caratterizzati da un particolare valore informativo aggiunto.

Circa, infine, la modalità espositiva scelta, si è optato per organizzare il discorso in modo da riflettere i passaggi operativi tipicamente affrontati quando si individua e si sceglie una soluzione cloud, che possono schematizzarsi nei due seguenti:
- una prima fase "preparatoria" riguarderà appunto le attività che di regola è necessario compiere in vista dell'adozione di soluzioni cloud, sostanzialmente attività di individuazione dei trattamenti di dati personali da migrare su tale tecnologia e valutazione delle ragioni economiche e di opportunità connesse;
- una seconda fase "operativa" sarà volta all'individuazione delle principali questioni contrattuali da tenere presenti per minimizzare il rischio giuridico e allinearsi con le migliori pratiche suggerite a livello nazionale e comunitario.

Si presenteranno infine delle conclusioni e la già indicata scheda pratica in forma di

checklist.

Quadro sintetico delle principali fonti giuridiche di documentazione/disciplina

Mancano in materia di cloud specifici atti normativi nel settore privacy, per cui gli indirizzi seguiti e normalmente applicati trovano la loro base in posizioni autorevoli di natura interpretativa. Prescindendo in questa sede dalla considerazione di lavori dottrinari, anche in sintonia con il taglio immediato e pratico di questo lavoro, vale la pena limitarsi a quelli realizzati da soggetti istituzionali, comunitari e italiani, anche in considerazione dell'ampio consenso di cui tali lavori di inquadramento godono.

Lo stesso Garante italiano si è limitato tenere un approccio di tipo informativo e di consiglio, mettendo a punto dapprima una scheda informativa sul cloud computing e quindi una breve guida ragionata alle questioni più rilevanti da tenere presenti nella scelta di un fornitore di servizi cloud. Ciò che più si avvicina a un inquadramento di tipo precettivo, pur senza esserlo in stretti termini giuridici, è l'opinione 5/2012 dei Garanti europei (cd. "Gruppo di lavoro *ex* art. 29 dir. 95/46/CE"), considerata una vera e propria "*landmark opinion*" in materia sia per la soluzione di questioni chiave sia per il grado di dettaglio e la ricchezza dell'analisi. Va segnalato, senza che il passaggio possa essere ulteriormente esplorato, che il Supervisore europeo in materia di trattamento dei dati personali, o EDPS, a qualche mese di distanza dall'opinione citata ha a sua volta affrontato alcuni profili giuridici in materia di cloud computing e protezione dei dati personali, pervenendo a conclusioni che appaiono meno nette e più dubitative in merito all'allocazione dei ruoli privacy. In termini pratici, comunque, la posizione del Gruppo di lavoro è

quella seguita anche dal Garante italiano e quella generalmente osservata, anche per la facilitazione che introduce.

Sempre in ambito europeo, una rassegna di indicazioni che hanno raccolto l'interesse dei giuristi e dei pratici, soprattutto nel momento iniziale di affermazione del fenomeno cloud, ma che restano tuttora valide e di orientamento, sono le linee guida emanate dall'ENISA (*European Network and Information Security Agency*), l'Agenzia europea per la sicurezza delle reti e dell'informazione.

In ambito nazionale si registra una produzione di studi e lavori soprattutto nel settore amministrativo. Tuttavia, le indicazioni contenute appaiono in larga misura, una volta scremate delle precisazioni specifiche rivolte alla pubblica amministrazione, applicabili anche in un contesto imprenditoriale privato. Si segnalano i proposito il documento dell'*Agenzia per l'Italia Digitale,* dal titolo *"Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione"*, vers. 1.0, del 24 maggio 2013[2], e inoltre le linee guida Consip e le raccomandazioni dell'agenzia Digit PA, dirette evidentemente a soggetti pubblici, ma ugualmente applicabili alle esigenze di soggetti privati, prescindendo dalla parte più strettamente amministrativistica e dai riferimenti al codice dell'amministrazione digitale applicabili alla PA.

Occorre infine tenere presente che nell'Unione europea sono in corso, come già anticipato, iniziative di promozione e radicamento della tecnologia cloud, che per impegno e ampiezza trovano pochi altri precedenti. In particolare, nel settembre 2012, la Commissione ha adottato l'iniziativa dal titolo *"Unleashing the Potential of*

2 Disponibile all'url: www.agid.gov.it/sites/default/files/documentazione/cloud_pa_consultazione_pubblica_v1.0_bozza.pdf.

Cloud Computing in Europe"[3], diretta anche a un'armonizzazione degli standard e all'elaborazione di modelli contrattuali, nel contesto della quale sono stati creati una European Cloud Partnership (ECP), attiva nell'attività di diffusione della conoscenza della tecnologia in esame e di riduzione degli ostacoli che possono presentarsi alla sua adozione in Europa e uno Steering Board all'interno dell'ECP. Proprio lo Steering Board ha assai di recente reso disponibile uno studio, che si segnala per l'ampiezza della ricerca di cui rappresenta la sintesi, pubblicato con il titolo di *"Trusted Cloud Europe Survey - Assessment of Survey Responses"*[4]. Si tratta dell'analisi dei risultati di un ampio lavoro di consultazione relativo alle idee e alle proposte contenute in un precedente lavoro del Board, di carattere programmatico, dal titolo *"Trusted Cloud Europe Survey"*[5].

In definitiva, come emerge da questa rapidissima rassegna, il cloud è ben più di una tecnologia di recente affermazione, rappresenta un preciso obiettivo politico-giuridico sul quale la Commissione europea ha basato una serie di iniziative strategiche nel contesto della *Digital agenda for Europe*.
Qui di seguito si propone una rapida classificazione di questo materiale in ordine strettamente cronologico:

Autorità emanante	Anno e titolo	Sintesi dei contenuti
Steering Board ECP	2014, *"Trusted Cloud Europe Survey - Assessment of Survey Responses"*	Lavoro statistico su questionari basato sulle proposte contenute nello studio dal titolo "Trusted Cloud Europe" (ved. *infra*)
Steering Board ECP	2014, "Trusted Cloud Europe"	Lavoro contenente proposte in materia di cloud computing
AGenzia per l'Italia Digitale	Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione, vers.	Lavoro tecnico in materia di scenari per possibili soluzioni cloud, discussione di standard di interoperabilità

3 Cfr. ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.
4 Disponibile all'url: ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe-survey-assessment-survey-responses
5 Disponibile all'url: ec.europa.eu/digital-agenda/en/european-cloud-partnership.

	1.0, del 24 maggio 2013	
EDPS (European Data Protection Supervisor)	2012, *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*	Si tratta di un'opinione che propone un quadro interpretativo non in tutto e per tutto combaciante con quello dello del Gruppo di lavoro. Esamina varie tematiche. Le principali: Scelte strategiche della Commissione in materia di cloud computing Allocazione dei ruoli privacy Inquadramento di profili alla luce dell'emanando regolamento europeo (GDPR)
Commissione UE	2012, *Communication on "Unleashing the potential of Cloud Computing in Europe"*	L'iniziativa si propone tre obiettivi principali: - semplificazione degli standard - sviluppo di adeguati termini contrattuali - costituzione della European Cloud Partnership (ECP)
Gruppo di lavoro ex art. 29	2012, Opinione 5/2012	Opinione *landmark*. Ampia e dettagliata analisi. Temi principali: Allocazione ruoli privacy Legge applicabile Circolazione dati extra UE/SEE Subfornitori del cloud provider Poteri di controllo del titolare Accorgimenti contrattuali. Taglio tecnico. Per giuristi esperti della materia.
Garante italiano prot. dat. pers.	2012, *"Cloud computing - proteggere i dati per non cadere dalle nuvole - La guida del Garante della Privacy per imprese e pubblica amministrazione"*, suggerimenti di *best practice* contrattuali[6]	Esame per punti di una serie di questioni contrattuali di interesse. Non affronta questioni specifiche relative all'allocazione dei ruoli, alla legge applicabile e alla generale disciplina del cloud in ambito privacy. Taglio non tecnico e non strettamente giuridico. In larga misura sovrapponibile al precedente
Garante italiano prot. dat. pers.	2011, *"Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, Schede di documentazione[7]	Esame per punti di una serie di questioni contrattuali di interesse. Non affronta questioni specifiche relative all'allocazione dei ruoli, alla legge applicabile e alla generale disciplina del cloud in ambito privacy. Taglio non tecnico e non strettamente giuridico.

6 http://www.garanteprivacy.it/documents/10160/2052659/CLOUD+COMPUTING+-+Proteggere+i+dati+per+non+cadere+dalle+nuvole+-+sing.pdf

7 http://www.garanteprivacy.it/documents/10160/10704/1819933

Digit PA	DigitPA, Linee guida per il disaster recovery delle Pubbliche amministrazioni. Ai sensi del comma 3, lettera b) dell'articolo 50-bis del DLgs. n. 82/2005 e s.m.	Linee guida in materia di CO e DR, con indicazioni che appaiono d'interesse anche per il settore privato, una volta operati i dovuti adattamenti
Consip	2011, *"Cloud Security: una sfida per il futuro"*, in *Quaderni Consip*, n. II/2011	Esame per punti di una serie di questioni contrattuali di interesse. Non affronta questioni specifiche relative all'allocazione dei ruoli, alla legge applicabile e alla generale disciplina del cloud in ambito privacy. Taglio non tecnico e non strettamente giuridico. In larga misura sovrapponibile al precedente
ENISA (European Network and Information Security Agency)	2009, *Cloud Computing Security Risk Assessment*[8]	Esame per punti di una serie di questioni contrattuali di interesse. Non affronta questioni specifiche relative all'allocazione dei ruoli, alla legge applicabile e alla generale disciplina del cloud in ambito privacy. Taglio non tecnico, rivolto a non giuristi

*

8 Cfr. url: enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

II - FASE "PREPARATORIA" ALL'ADOZIONE DI SERVIZI CLOUD

La fase preparatoria è una **fase di scelta**. Scelta dei settori di attività da trasferire sul cloud (e quindi, dal punto di vista privacy, dei gruppi di dati personali generati e utilizzati in quei settori), scelta del tipo di cloud o di eventuale combinazione di tipi diversi di cloud.

La scelta implica da un lato il **censimento** dei flussi di dati oggetto di trattamento e dall'altro implica la **consapevolezza** di: a) quali siano le caratteristiche e la convenienza economica delle soluzioni cloud che si vogliono scegliere rispetto a soluzioni ICT standard quelle già operative; b) quali siano le conseguenze giuridiche di tali scelte.

Censimento dei trattamenti e dei dati

Dal punto di vista del metodo, si pone sempre la necessità di effettuare innanzitutto un censimento dei trattamenti di dati personali svolti tipicamente da un istituto di credito. La mappa che ne risulterà permetterà di valutare in maniera critica le effettive esigenze di approvvigionamento cloud e le specifiche garanzie da richiedere per ogni tipologia di trattamenti.

Un censimento di questo genere, in un settore complesso come quello bancario, richiede evidentemente una necessaria opera di astrazione e semplificazione, dal momento che le tipologie di trattamenti sono varie e differenziate. Va subito premesso che una meticolosa opera di catalogazione esulerebbe dagli scopi di questo contributo. Si individueranno perciò, a titolo di esempio e senza alcuna pretesa di esaustività, alcuni gruppi omogenei di trattamento in ambito bancario. Volendo ridurli entro uno schema pratico, una prima ripartizione può essere fatta tra trattamenti svolti per finalità amministrative interne relative alla gestione del

funzionamento della struttura (gestione del personale e attività di relazione con altri soggetti privati e pubblici) e trattamenti svolti per finalità di offerta di servizi tipici alla clientela. Tale ultima macro-categoria si presta ad essere ulteriormente suddivisa, senza pretesa di esaustività, entro le seguenti tipologie di trattamento:

- trattamento di schede anagrafiche e dati di contatto dei clienti;
- trattamento di dati di contenuto prevalentemente economico relativi a operazioni di gestione patrimoniale dei clienti, includendo in questa espressione una vasta gamma di attività, che vanno dalla registrazione di movimenti in entrata/uscita su conto-corrente, a concessioni di affidamenti, a operazioni su strumenti finanziari, quali azioni, obbligazioni, fondi di investimento, ecc.;
- trattamento di dati di profilazione in senso lato[9] della clientela, incluse, a seconda dei casi, informazioni relative alla propensione al rischio, informazioni sul reddito e sulla composizione del nucleo familiare;
- trattamento di dati aggregati in istruttorie relative a specifici clienti, che includono informazioni relative alla solvibilità e affidabilità economica, elementi significativi relativi a operazioni pregresse anche nei confronti di soggetti terzi, informazioni sul nucleo familiare, livello reddituale, garanzie, perizie patrimoniali, risultanze di procedimenti processuali, iscrizioni e trascrizioni, ecc.;
- trattamento di dati richiesti dall'assolvimento delle obbligazioni antiriciclaggio[10], quali l'identificazione del cliente e del titolare effettivo del rapporto, la raccolta di informazioni sulla natura e scopo del rapporto e il controllo costante del medesimo, il popolamento dell'archivio unico

9 Il termine "profilazione" è qui inteso nel senso ampio di classificazione degli interessati secondo alcuni indici cui sono attributi determinati valori per ciascun interessato, in associazione a criteri di elaborazione delle informazioni basati su quei valori, e non nel senso più ristretto e tecnico di profilazione per attività di marketing.

10 Cfr. d.gls. 21 novembre 2007, n. 231 e ss.mm. e direttive 2005/60/CE e 2006/70/CE.

informatico previsto dalla normativa di settore;

- trattamento di dati relativi a rapporti civilistici che riguardano clienti o terzi, quali ad esempio procedure esecutive, concorsuali, successioni.

Si tratta di tipologie che possono peraltro integrarsi vicendevolmente. Va da sé che le categorie di massima appena ricordate costituiscano una forte semplificazione dei complessivi trattamenti. Tuttavia aiutano a fornire un primo quadro di orientamento a cui riferirsi, sufficiente per gli scopi di questa analisi. Va evidenziato che lo schema di cui sopra costituisce una sintesi e una rielaborazione della tabella assai dettagliata di trattamenti in ambito bancario contenuta nel provvedimento del Garante per la protezione dei dati personali del 17 aprile 2012, doc. web n. 1886775 (§ B.1) in materia di anagrafe tributaria.

Occorre naturalmente evidenziare da ultimo che un censimento dei trattamenti e una mappatura del relativo livello di rischio dovrebbe già essere disponibile all'interno dell'istituto di credito, in quanto:

a) precisi obblighi di vigilanza su particolari dati economici e finanziari volti a rafforzare i controlli interni, soprattutto in seguito all'ultima crisi finanziaria, sono espressamente previsti nel settore bancario. Essi sono sintetizzati e specificati nella già citata circolare n. 263/2006, come integrata con il 15° aggiornamento del 2013. D'interesse soprattutto le parti relative al sistema informativo, all'esternalizzazione delle soluzioni ICT, alla predisposizione e all'aggiornamento del piano di continuità operativa (Titolo V, Capitoli VIII e IX).

b) una mappatura dei flussi dati, limitatamente a quelli personali, è in via generale fortemente opportuna, se non proprio implicita, nell'adeguamento alla corrente normativa in materia di protezione dei dati personali, specialmente tenuto conto delle caratteristiche di un istituto di credito e dello svolgimento di processi critici al

suo interno.

Analisi giuridica della tipologia di dati: nella specie dati "comuni" e di aggregati di dati comuni

Com'è noto, nella sistemazione del codice privacy, i dati personali possono essere sussunti entro tre categorie, una di carattere generale, quella dei dati cd. "comuni", e due specifiche, quelle dei dati sensibili e dei dati giudiziari. Ebbene, elemento che emerge subito dalla sommaria rassegna sopra proposta è che i dati oggetto di trattamento nelle macroaree sopra individuate sono tutti definibili, di regola e in via generale, alla categoria dei dati "comuni"[11]. Ciò ha una certa rilevanza nel contesto dell'analisi che si sta conducendo in materia di cloud computing e comporta un alleggerimento degli obblighi di sicurezza[12]. Sul punto è comunque necessario evidenziare che la legislazione applicabile alle misure di sicurezza potrebbe non essere quella italiana, per cui quanto appena notato va collocato nel contesto concreto normativa nazionale che effettivamente governa l'ambito della sicurezza. Fare in ogni caso riferimento a quanto si preciserà più avanti sulle specifiche misure di sicurezza prescritte dal Garante in ambito bancario.

Risultano invece sempre e comunque applicabili, quale che sia la normativa che regola, lato responsabile di trattamento, il profilo della sicurezza, le prescrizioni di

11 Cfr. anche Garante prot. dat. pers., *Linee guida per i trattamenti relativi al rapporto banca-clientela, provv. 25 ottobre 2007, doc. web n. 1457247, § 3.6*, nel quale l'Autorità ha ritenuto applicabile l'ipotesi di esonero dal consenso di cui all'art. 24, co. 1, lett. g) (legittimo interesse del titolare del trattamento) in occasione della cessione di sportelli bancari, e conseguentemente dei dati personali ivi raccolti e trattati, verso altra banca cessionaria, in considerazione della natura appunto comune dei dati in questione.

12 Per scrupolo, va notato che non può escludersi che qualcuno dei trattamenti sopra elencati possa implicare anche dati sensibili, o perfino dati giudiziari (qualora per qualche ragione vengano in considerazioni procedimenti penali), tuttavia si tratta di ipotesi da considerarsi accidentali rispetto alla natura e alle caratteristiche dei trattamenti identificati.

cui alla citata circolare n. 263/2006 e ss. mm. in tema di continuità operativa e disaster recovery, che richiedono uno specifico coordinamento tra la banca e il fornitore di servizi ICT.

Si è accennato al fatto che l'aggregazione di dati comuni può essere di per se stessa fonte di informazioni aggiuntive, che superano le singole componenti di cui sono formate. Ciò appare particolarmente rilevante nell'ambito bancario, nel quale si registrano rapporti anche di lunga durata con i clienti, che riflettono in maniera capillare non solo il complesso delle operazioni economiche ma anche, sia pure su un piano più sfumato, quello delle relazioni di vita. In definitiva, si tratta di un patrimonio informativo assai penetrante, che deve essere presidiato da particolari attenzioni, potendo avere l'effetto di "mettere a nudo", per così dire, l'esistenza dell'interessato e perfino di determinare esclusioni da occasioni di vita e professionali. Ciò potrebbe indicare, in termini tecnici, la presenza di un "trattamento che presenta rischi specifici" (art. 17 codice privacy).

Non consta tuttavia una prassi interpretativa in questo senso da parte dell'Autorità di protezione dei dati personali, almeno non in ambito bancario, con l'eccezione del provvedimento relativamente recente in materia di anagrafe tributaria e lotta all'evasione dall'Agenzia delle entrate (doc. web n. 1886775), che però esamina ipotesi nelle quali i dati conferiti dalle banche all'Agenzia delle entrate risultano sottoposti a particolari procedure di elaborazione e analisi.

Vanno evidentemente rimarcate, allora, le differenze rispetto al trattamento in ambito cloud: prima e più evidente tra tutte il fatto che nessuna analisi e nessuna elaborazione sui dati è consentita, né deve esserlo, al cloud provider. In definitiva perciò il complesso di dati aggregati gestiti in ambito bancario ed, in ipotesi,

esternalizzati su una soluzione cloud non dovrebbe richiedere attenzioni diverse da quelle che sarebbero dovute per l'esternalizzazione di dati comuni.

Fatta questa premessa generale, pare opportuna qualche precisazione più specifica, pur nei limiti pratici di questo manualetto. In particolare, va segnalato che nel già citato provvedimento, il Garante ha tenuto a evidenziare comunque le caratteristiche invero particolari dei dati bancari, quali complessi di informazioni di natura granulare, idonei a determinare interconnessioni reciproche, capaci di fotografare in maniera capillare le relazioni interpersonali. Appare utile riportare un passaggio significativo di quel provvedimento: "*Va rilevato, quindi, che la previsione di un'ingente concentrazione di tali categorie di dati presso un unico titolare genera un incremento esponenziale dei rischi insiti nel trattamento di dati personali rispetto alla quantità di informazioni raccolte, anche laddove il trattamento avvenga nel più rigoroso rispetto delle misure di sicurezza. Ciò, soprattutto, in relazione all'interesse che il valore strategico di una simile banca dati può suscitare sia con riferimento ad accessi abusivi ed a utilizzi impropri, che alla proliferazione di interconnessioni e raffronti*".

Ancorché il cloud provider vada considerato, nella generalità dei casi e salvo diversi inquadramenti specifici, come un responsabile del trattamento e nonostante non si registri una duplicazione del complesso di informazioni (altro profilo sul quale il Garante insiste), quanto piuttosto una loro allocazione presso il cloud provider (sia pure in termini ridondanti per mere ragioni di sicurezza) e benché quest'ultimo, come già notato, non effettui in alcun modo operazioni autonome di elaborazione dei dati conferiti, le preoccupazioni evidenziate dal Garante rappresentano comunque un elemento di cui tenere debito conto, in ambito di esternalizzazione cloud di processi bancari, anche in vista di possibili orientamenti futuri dell'Autorità. Di qui per esempio l'attenzione a selezionare fornitori di cloud

che presentino livelli qualitativi certificati e garanzie stringenti in tema di sicurezza.

Valutazione delle ragioni per l'adozione di una tecnologia cloud

Nelle aree di trattamenti bancari sopra indicate, la migrazione da soluzioni informatiche per così dire "tradizionali" a soluzioni cloud può rispondere a una serie di esigenze, che appaiono, con una certa semplificazione, sintetizzabili nelle seguenti: risparmio in termini economici e scalabilità. Quest'ultima indica la possibilità di contrarre o espandere, con ragionevole fluidità, la richiesta di fornitura di servizi informatici a seconda delle effettive esigenze aziendali.
La scalabilità va altresì considerata in rapporto all'integrazione (che dovrebbe essere garantita e non problematica) con l'infrastruttura informatica esistente[13].

Il risparmio, da intendere sia come risparmio di denaro sia come risparmio di tempo e limitazione nella dispersione di risorse, dipende essenzialmente dall'adozione di schemi di pagamento basati su formule del tipo "pay-per-use", che riconducono l'utenza informatica ai modelli tradizionali normalmente utilizzati per l'approvvigionamento di servizi, ad es. quelli energetici o telefonici.

L'utilità economica del cloud si apprezza sia in termini di abbattimento di spese correnti complessive (che includono cioè anche i costi di mantenimento / rottamazione hardware, sicurezza e guardiania, rinnovo e aggiornamento delle licenze, ecc.) sia in termini di allocazione efficiente dei costi, dal momento che il

1. 13 La Banca d'Italia ad esempio, nell'ultima relazione annuale, evidenzia proprio l'esigenza di scalabilità come una delle ragioni alla base della propria acquisizione di servizi cloud. Cfr. la Relazione sulla gestione e sulle attività per l'anno 2013, del 30 maggio 2014, p. 20: *"Le architetture elaborative. – Nell'ottica di rafforzare la flessibilità e la scalabilità della capacità elaborativa, è stata rivista l'architettura dei sistemi intermedi avvalendosi in particolare di tecniche di virtualizzazione (cloud computing)..."*, disponibile all'url: bancaditalia.it/pubblicazioni/relapago/rela-gest-att-bi-14/rel_gest%20_BI_13.pdf.

pagamento riguarda solo la parte del servizio effettivamente utilizzata sia infine in termini di liberazione di risorse tecniche da collocare nello sviluppo di attività strategiche (es. sviluppo di applicativi su piattaforma PaaS).

Vantaggi ancora più evidenti si presentano poi quando vengono create nuove realtà imprenditoriali o nuovi rami di attività, perché il ricorso a servizi cloud evita il pagamento *"up front"*, ossia immediato dei costi di creazione / attivazione / personalizzazione di un data center e premette peraltro, per le stesse ragioni, una più rapida implementazione dei processi.

Il ricorso a servizi informatici cloud modifica la relazione con le risorse informatiche, e di questo occorre avere consapevolezza. Le modifica in due sensi principali:

1. i servizi offerti sono diversi, cumulabili secondo le esigenze del cliente o acquistabili separatamente, il che presenta vantaggi in termini di flessibilità e di completezza;
2. i programmi che vengono sottoscritti in abbonamento non rimangono al cliente in maniera permanente al termine del contratto.

Per quanto riguarda il primo punto, e nell'ottica di semplificare al massimo, l'offerta può riguardare sia servizi infrastrutturali, sia interi sistemi operativi (che in questo modo diventano sistemi operativi online), sia singoli gruppi di processi. Il mercato propone peraltro una serie di soluzioni più articolata e più ricca.

Per quanto riguarda il secondo punto, deve essere chiaro che mentre, per fare un esempio relativo al cloud SaaS, si è tradizionalmente abituati ad acquistare la licenza per un prodotto e poi a mantenere quel prodotto installato sul proprio

terminale per tutto il tempo in cui sarà ancora utile rispetto alle proprie necessità di elaborazione, con l'offerta cloud quel prodotto al termine del contratto non sarà più disponibile (resteranno naturalmente in essere gli "output" dell'applicazione, ossia i prodotti realizzati con essa).

Il cloud, in altri termini, implica un modo di ragionare e di rapportarsi alle soluzioni tecnologiche completamente nuovo rispetto al passato. A mero titolo di chiosa rispetto all'ultimo punto accennato, sotto il profilo economico il mantenimento dell'installazione *on premise* di applicazioni obsolete non presenta invero particolari vantaggi, quantomeno per un utilizzo di tipo imprenditoriale: il valore economico di mercato delle stesse si riduce costantemente; esse possono, almeno in via tendenziale, presentare crescenti vulnerabilità; nell'uso di prodotti obsoleti è insita una perdita di efficienza produttiva.

Altre ragioni per l'adozione di soluzioni cloud sono la disponibilità dei dati tendenzialmente 24 ore su 24 e 7 giorni su 7 (fare comunque riferimento alle SLA) e la loro accessibilità indipendentemente dal sistema operativo utilizzato e dal tipo di terminale (fisso, mobile) e di modello. Si tratta naturalmente di funzionalità disponibili anche con altre tecnologie, ma certamente esse trovano nel cloud una naturale espressione, per la sua stessa struttura di sistema distribuito e virtualizzato.

Occorre in ogni caso sempre valutare attentamente il rapporto costi / benefici rispetto a soluzioni tradizionali già collaudate, valutazione da effettuare anche in termini di ROI, ossia di *return of investment* atteso dalla migrazione verso soluzioni cloud. Nella valutazione dei costi occorre dare espressione numerica anche ai costi legali. Le pagine che seguono vogliono essere un *vademecum* per identificare quale è

il "rischio" legale e quali sono i percorsi per ridurlo al minimo già a partire dalla fase contrattuale.

Conclusivamente si segnala che un'interessante sintesi estremamente condensata e di pronta consultazione dei pro e dei contro dell'adozione di tecnologia cloud in ambito bancario, nella prospettiva anglosassone, si può leggere nel già citato articolo di BROWN, "*Six reasons why cloud computing will transform the way banks serve clients – and the five hurdles to overcome*", cfr. nota 1 di questo manualetto.

Valutazione dei fattori percepiti come d'ostacolo all'adozione di una tecnologia cloud

Specifici passaggi sui quali porre attenzione saranno meglio indicati più avanti, tuttavia in questa sede preparatoria va evidenziato che il principale elemento che, nella percezione comune (e non sempre esatta), rappresenta il vero aspetto di freno nei confronti dell'adozione della tecnologia in esame è probabilmente rappresentato dal timore di una perdita di controllo di gruppi di informazioni o di interi processi.

In linea di principio, si tratta di un rischio comune a qualsiasi tipo trasmissione di segnali su reti che attraversino più paesi. Esistono vari modi per perimetrare il rischio: dalla trasmissione di porzioni di informazioni in partenza difficilmente ricostruibili e criptate alla limitazione fisica dell'ambito territoriale di circolazione dei dati e ciò fino ad arrivare alla soluzione radicale di una concentrazione dei processi più critici presso il titolare del trattamento, ricorrendo (se la soluzione scelta è comunque quella del cloud) a un cloud privato. La differenziazione dei trattamenti in base alla loro criticità, e dunque delle soluzioni tecnologiche scelte

per gestirli, è in generale sempre un buon criterio da seguire.

La perdita di controllo, va precisato, costituisce un fenomeno non solo giuridico ma anche di fatto, e dunque, in una certa misura, è insensibile alla prestazione di garanzie giuridiche. Ossia, indipendentemente dal fatto che un ambito di circolazione di dati risponda ai requisiti di legge e sia assistito da impegni contrattuali dei soggetti coinvolti, la perdita di controllo può verificarsi in seguito a un incidente di sicurezza o essere determinata da ordine dell'Autorità (si pensi non solo a esigenze di prevenzione o di repressione di reati, ma anche a ragioni di stato o interessi nazionali e a crisi politiche). In un certo qual modo è cioè inevitabile. Del resto, rappresenta un problema trasversale a buona parte delle scelte di esternalizzazione, anche a quelle tradizionali, dunque va affrontata tenendo conto di categorie generali.

Verifica preliminare dell'affidabilità del fornitore cloud

La prima forse delle attività da svolgere, pare perfino superfluo evidenziarlo, è di procedere a verifica dell'affidabilità e della serietà del cloud provider. Affidabilità e serietà devono essere declinate non solo in termini di capacità comprovata di rispetto dei livelli di servizio garantiti e di rispetto degli impegni contrattuali, ma anche in termini di esperienza e presenza sul mercato e stabilità economica e finanziaria. Un elemento per misurare la capacità di rispettare effettivamente termini e condizioni può essere il riferimento a rapporti di *audit* sviluppati da terzi soggetti indipendenti e alla presenza di certificazioni. Elementi ulteriori che rafforzano l'affidabilità economica possono essere costituiti da adeguate polizze assicurative del fornitore cloud.

L'importanza dell'affidabilità giuridica ed economica del cloud provider è stata del resto evidenziata anche dal Garante per la protezione dei dati personali in più occasioni[14].

Quali soluzioni cloud per i trattamenti individuati

Rispetto alle tipologie di dati comuni sopra individuate, occorre comprendere quali servizi di cloud computing potrebbero tipicamente essere sottoscritti da un istituto di credito. Qui di seguito alcune possibilità:

- gestione o acquisizione di *business process*, ossia di routine ammnistrative interne ottimizzate per la fornitura di beni e servizi, attraverso servizio cloud, ossia "Business Process as a Service" (BpaaS). Può trattarsi *business process* che intervengono su trattamenti critici, occorre perciò valutarne attentamente le implicazioni;
- applicazioni cloud che permettono di gestire la corrente attività amministrativa e contabile "da ufficio", di tipo *all-purpose*, eventualmente arricchite da funzioni o da ulteriori applicativi diretti a svolgere attività più specifiche, quali ad esempio software per l'elaborazione di buste paga. Si tratta di soluzioni che a livello di cloud computing sono soddisfatte da prodotti di tipo SaaS (Software as a Service). In scenari più complessi, nei quali sia ipotizzabile anche lo sviluppo di applicazioni e un ambiente di test, il modello verso cui è preferibile orientarsi è una soluzione di tipo PaaS (Platform as a service).

14 Cfr. le pubblicazioni divulgative dal titolo *"Cloud computing - proteggere i dati per non cadere dalle nuvole - La guida del Garante della Privacy per imprese e pubblica amministrazione"*, 24 maggio 2012, p. 25 e *"Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, Schede di documentazione, 23 giugno 2011, pp. 14-15.

- soluzioni che permettono di effettuare lo *storage* di grandi quantità di dati, ad esempio il complesso delle attività di gestione e movimentazione finanziaria dei clienti. Può trattarsi dell'archiviazione di fascicoli relativi a istruttorie su specifici clienti. Può trattarsi di spazi per la gestione virtuale dei fascicoli di procedimenti giudiziari di cui sia parte la banca.

Queste e altre attività richiedono essenzialmente la disponibilità di notevoli spazi di archiviazione che potrebbero essere gestiti attraverso soluzioni di tipo IaaS (Infrastructure as a Service) o come qualcuno preferisce indicare "STaaS" (Storage as a Service), inteso in ogni caso come una subpartizione dello IaaS;

- soluzioni sofisticate che permettono la gestione informatica delle operazioni effettuate sul patrimonio del cliente, incluse applicazioni di home banking. Vengono qui in considerazione i modelli SaaS e PaaS e BPaaS;
- allo stesso modo applicazioni specificamente disegnate per l'assolvimento degli adempimenti antiriciclaggio o particolari strumenti di analisti della clientela possono essere efficacemente trasportati su soluzioni cloud di tipo SaaS, PaaS e BPaaS.

Verosimilmente comunque la tipologia dominante di servizi cloud verso i quali un istituto di credito tendenzialmente potrà orientarsi è quella del modello SaaS e/o quella del modello PaaS.

Qui di seguito un breve schema riassuntivo:

Tipologia di dati personali	Tipologia di cloud
attività amministrativa e contabile cd. "da ufficio" (inclusa	SaaS, PaaS, BPaaS

gestione del personale)	
Storage generico di dati	IaaS
Applicazioni sofisticate per la gestione dei rapporti attivi e passivi nel settore bancario	SaaS, PaaS, BPaaS
Adempimento normativa antiriciclaggio ed estrazione di particolari profili clienti	SaaS, PaaS, BPaaS

Coordinamento e integrazione con processi e progetti esistenti

Un punto da tenere presente nella valutazione preliminare di soluzioni cloud è quello dell'integrazione con processi e progetti già in essere. Può trattarsi da un lato dell'adesione ad attività che importano necessariamente la gestione telematica di flussi di dati e che impegnano come tali sistemi e applicazioni, rispetto ai quali vanno valutati costi, possibilità e opportunità di una migrazione sul cloud, anche in considerazione dell'eventualità che tali processi coinvolgano altri soggetti, ad esempio altri istituti di credito o la Banca d'Italia.

È opportuno in tal senso comprendere in anticipo se le soluzioni cloud che si intende sottoscrivere presentino interferenze negative con l'organizzazione corrente delle attività e dei processi o se possano, anche attraverso l'utilizzo di specifiche condivise, integrarsi senza difficoltà con esse.
Infine occorre premurarsi di verificare che la migrazione sul cloud avvenga nel rispetto delle policy ICT vigenti[15], per cui è necessario verificare che le misure di sicurezza ivi previste sia compatibili con quelle garantite dal cloud provider.

15 Cfr. Circolare n. 263/06 cit., Titolo V, Capitolo VIII, Sezione II.2.

Ulteriori indicazioni

La banca titolare del trattamento dovrebbe valutare la strategia di adesione alla tecnologia cloud più adatta a mantenimento del controllo sui dati personali. In particolare, si presentano alcune linee strategiche di fondo da tenere presenti nella scelta di soluzioni cloud:

- ***Cloud pubblico, cloud privato, community, cloud ibrido –*** È sempre opportuno preliminarmente valutare se rispetto all'adesione a un cloud pubblico non risulti maggiormente adeguata per le proprie esigenze l'adozione di una struttura cloud cd. "privata", ossia di titolarità della stessa banca o al limite di tipo "community", ossia al servizio di un numero limitato di soggetti che condividono gli stessi obiettivi di business, oppure una struttura "ibrida", ossia dotata di caratteristiche sia di un cloud privato sia di un cloud pubblico. Considerazioni in questo senso sono state espresse anche dai Garanti europei nell'opinione 5/2012, i quali hanno rilevato che, quantomeno nel breve termine, una transizione verso un sistema di cloud pubblico appare realisticamente complessa per società di grandi dimensioni, come appunto gli istituti di credito, per svariate ragioni, che vanno dalla particolare criticità dei trattamenti effettuati, a valutazioni di efficienza/costi rispetto a soluzioni private o ibride[16]. Probabilmente la soluzione migliore è allora quella di ragionare per criticità dei processi, ripartendoli per grado di rilevanza strategica e decidendo di consenguenza il riparto in termini di soluzioni tecnologiche per la loro gestione. In definitiva, non tutte le soluzioni cloud sono necessariamente adatte a tutti i trattamenti di dati.
- ***Modificare nel tempo il coinvolgimento in soluzioni cloud –*** L'approccio con

16 Gruppo ex art. 29, *cit.*, p. 26.

qualsiasi tecnologia dovrebbe essere dinamico e non statico e lasciare aperta la possibilità di rimodulare nel tempo i volumi e le modalità. Per riprendere lo spunto precedente, si può realisticamente pervenire all'adozione di soluzioni cloud anche come esito di una sperimentazione a crescita progressiva, che permetta di familiarizzare con la tecnologia, e testarne l'utilità in termini di ritorno di investimento e di sicurezza di gestione e controllo.

La scelta di esternalizzare processi bancari in ambiente cloud è considerata dalla Banca d'Italia un'alternativa valida a soluzioni più datate di *outsourcing* e perfettamente percorribile nel contesto in esame. Si trova infatti espressamente contemplata, sia pure brevemente, al Titolo V, Capitolo VIII, Sezione VI.3 della circolare 263/06 e ss.mm.. Per comodità di lettura si riporta qui il passaggio: *"L'intermediario pone particolare cautela nella valutazione di offerte di servizi in outsourcing erogati secondo modelli innovativi che prevedono la fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile dall'utente (cloud computing).*

Il cloud computing può essere implementato secondo diverse tipologie:

- cloud privato: ambienti interni alla società o al gruppo che permettono la condivisione di risorse ICT tra più aree e realtà aziendali; questo caso non rientra nella definizione di servizio esternalizzato;

- community: i servizi sono utilizzati da un ristretto numero di organizzazioni, tipicamente operanti nello stesso settore economico, che condividono analoghe necessità e obiettivi. La condivisione delle risorse informatiche è ristretta a dette organizzazioni;

- cloud pubblico: i servizi sono erogati a un vasto numero di utenti con funzionalità offerte in maniera aperta e condivisa. I fornitori in genere sfruttano la possibilità di condividere in modo flessibile le proprie risorse tra i diversi utenti e applicano di norma tariffe proporzionali all'utilizzo (pay-per-use).

Nel caso dell'acquisizione di servizi in community o in cloud pubblici i maggiori rischi potenziali possono richiedere una più elevata complessità dei controlli da predisporre, in particolare in caso di esternalizzazione di componenti critiche".

Non si condivide peraltro l'invito a una particolare cautela, che avrebbe ragione di essere solo ad esito di un ragionato confronto con altre soluzioni in termini di sicurezza informatica e di rispetto di parametri accettabili di continuità operativa. L'invito per chi si trova a dover confrontare le caratteristiche di soluzioni alternative è di utilizzare solo e soltanto dati oggettivi, quali:

- la presenza di certificazioni internazionali in materia di sicurezza e qualità dei processi, es. certificazioni ISO, in particolare la recentissima ISO 27018, specifica in materia di cloud computing;
- i valori degli SLA e la tipologia di misure di sicurezza logiche, fisiche e organizzative dichiarate;
- la presenza di *audit* di terze parti indipendenti e la possibilità di accedere a tali *audit;*
- la possibilità per il cliente di disporre di "cruscotti" software di controllo per un monitoraggio continuo dei dati conferiti nel cloud;
- la conoscenza delle procedura in essere nel caso di incidenti di sicurezza;
- l'adozione di strumenti che rendano lecito il trasferimento di dati anche in area extra UE/SEE;
- la solidità finanziaria del cloud provider

*

III - SINTESI DELLE REGOLE GIURIDICHE IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Si ritiene opportuno proporre una sintesi delle principali regole giuridiche privacy applicabili in materia di cloud computing, come utile quadro di riferimento giuridico nella fase di preparazione alla scelta della soluzione cloud così come in quella più propriamente negoziale. Ove i lineamenti della disciplina giuridica applicabile fossero già noti sarà invece possibile saltare agilmente questa sezione e pervenire direttamente alla successiva.

Allocazione dei ruoli privacy

Una prima fondamentale operazione dell'interprete è quella di allocare i ruoli attivi del trattamento, ossia individuare nella coppia di soggetti banca – cloud provider chi sia titolare del trattamento e chi responsabile del trattamento. L'analisi, che per lungo tempo ha creato perplessità e spaccature in dottrina, appare ormai del tutto consolidata per effetto di una scelta precisa operta dai Garanti europei, cosiddetto "Gruppo di lavoro ex art. 29", con la storica opinione 5/2012. Sugli specifici profili della legge applicabile, l'opinione va letta in collegamento con la precedente opinione 8/2010.

Forse il maggior pregio dell'opinione 5/2012 è proprio quello di avere deciso che, nella generalità dei casi e salvo eccezioni specifiche, il fornitore di servizi cloud deve considerarsi responsabile del trattamento, mentre il cliente, in questo caso l'istituto di credito, assume il ruolo di titolare del trattamento.

Naturalmente, ciò impone alcuni oneri al titolare. Per indicarne soltanto alcuni: quello di designare per iscritto il cloud provider; quello di vigilare ed effettuare controlli; quello di sostituire il responsabile per il quale sia venuto meno il rapporto di fiducia. La mancata designazione del responsabile, ciò va evidenziato, non è priva di conseguenze giuridiche, perché potrebbe determinare la configurazione del diverso schema della titolarità autonoma o congiunta tra banca e cloud provider, con un completo scardinamento degli assetti che rendono lecito il trattamento.

Benché l'atto di nomina sia atto unilaterale recettizio del titolare del trattamento, resta il fatto che la concreta disciplina del rapporto, così come modulata nell'atto di designazione, è suscettibile di articolarsi secondo formulazioni ben diverse tra loro, pur nel rispetto dei poteri che spettano al titolare del trattamento, ed è pertanto materia autenticamente negoziale. Ne segue che è sempre buona regola quella di verificare fin da subito l'adesione del responsabile al testo di nomina che il titolare del trattamento intende predisporre o viceversa, da parte del titolare, sincerarsi che il modello di nomina eventualmente già predisposto dal responsabile (come spesso avviene nella pratica) sia in linea con le proprie aspettative sulla gestione del rapporto.

Ambito territoriale di circolazione dei dati e liceità del trattamento

L'impostazione data dai Garanti europei ha precise conseguenze giuridiche. Innanzitutto, il trasferimento dei dati personali al cloud provider non va considerato autonoma operazione di trattamento, nella specie “comunicazione”, ma semplice circolazione interna alla struttura del titolare e non richiede un

consenso espresso dell'interessato.

Tuttavia, secondo le regole generali, la circolazione interna non necessita di ulteriori condizioni di liceità quando si svolge entro la UE/SEE o coinvolge quel limitatissimo numero di paesi, vere e proprie oasi, la cui normativa in materia di tutela dei dati personali è stata giudicata come adeguata a quella europea dalla Commissione[17]. Diversamente, occorre che il trasferimento dei dati sia presidiato da adeguati elementi che lo rendono lecito, ossia alternativamente:

- l'espressione di consenso da parte dell'interessato, soluzione pressoché impraticabile, considerati i volumi di trattamento e la possibilità di determinazioni diverse da parte degli interessati
- l'adozione dei modelli contrattuali standard approvati dalla Commissione europea (*standard clause*);
- l'adozione di *binding corporate rules* (BCR) che abbiano positivamente superato la procedura di approvazione attualmente prevista;
- il trasferimento a soggetti che aderiscano all'accordo cd. "Safe harbor" stipulato nel 2000 tra la Commissione europea e il Dipartimento di commercio statunitense[18], sebbene non possa tacersi che tale strumento, che spesso si risolve in un'autocertificazione e che comunque poggia su un nucleo di regole di trattamento molto limitate, appaia disallineato rispetto agli sviluppi più maturi e recenti della normativa europea[19]. Inoltre, va notato che lo strumento non consente una circolazione realmente globale dei dati;
- contratti *ad hoc*, che rappresentano uno strumento estremamente farraginoso e poco funzionale.

17 Si tratta dei seguenti: Andorra, Argentina, Australia, Canada, Guernsey, Isole Faeroe, Israele, Isola di Man, Jersey, Monaco, Nuova Zelanda, Quebec, Svizzera, Uruguay.
18 Cfr. Commissione UE, decione 520/2000/CE.
19 Gruppo ex art. 29, *cit.*, p. 18.

In termini pratici, le due modalità attraverso le quali un cloud provider può imprimere una circolazione veramente globale ai dati personali, pur mantenendo livelli di tutela considerati tra i più avanzati si riducono al ricorso alle *standard clause* e alle BCR.

Fondamentale pertanto la verifica che il cloud provider si sia effettivamente dotato degli strumenti giuridici che rendono lecita la circolazione dei dati personali extra UE/SEE. L'alternativa può essere soltanto quella di servirsi di cloud provider che garantiscano, anche rispetto alla filiera dei propri subfornitori, che la circolazione dei dati resti confinata nell'esclusivo spazio UE/SEE o in paesi ritenuti adeguati e che tale rimarrà per tutta la durata del rapporto.

Legge applicabile e giurisdizione

Altro punto che ha trovato una sua precisa collocazione in seguito all'opinione 5/2012 dei Garanti europei è la determinazione della legge applicabile. Infatti, le regole di riparto previste nella direttiva 95/46/CE sono venute a saldarsi con l'allocazione del ruolo di responsabile del trattamento sul cloud provider. Per l'effetto, la legge applicabile è quella del titolare del trattamento (assumendo che questi sia stabilito in uno stato membro UE). Se, ad esempio, un istituto di credito italiano affida la gestione di dati personali di terzi a un cloud provider nel contesto di una fornitura di servizi cloud PaaS, la normativa applicabile sarà quella di cui al d.lgs. 30 giugno 2003, n. 196, cd. "codice privacy", con tutte le relative conseguenze in materia di obblighi di vigilanza del titolare del trattamento, di sua responsabilità giuridica quale soggetto decisionale di vertice, comprese le eventuali sanzioni.

Diverso regime per le misure di sicurezza applicabili al responsabile del trattamento stabilito in uno Stato membro, che in base all'art. 17(3) dir. 95/46/CE, sono quelle dello Stato di stabilimento. La determinazione della legge applicabile deve tuttavia avvenire contrattualmente tra titolare del trattamento e responsabile[20]. Incerte le conseguenze, nel caso di mancata individuazione contrattuale.

Sul piano operativo, può già anticiparsi che nella fase di studio dei contratti si suggerisce sempre di verificare che la legge applicabile non sia determinata dalle parti in difformità delle previsioni di cui sopra. Ad avviso di chi scrive deroghe pattizie appaiono invalide ove tendano ad escludere la legge europea a favore di legge nazionale extraeuropea, in quanto il complesso articolato normativo europeo si collega a un particolare riconoscimento dei diritti fondamentali dell'interessato, entro uno schema giuridico fatto di richiami tra norme e criteri di bilanciamento rispetto ad altri diritti fondamentali, che non può essere pattiziamente accantonato dalle parti a detrimento dei terzi interessati.

La questione della giurisdizione è più complessa e non facile da comprimere nello spazio di questo paragrafo. Per semplificare e tenere presenti i soli rapporti tra titolare del trattamento e cloud provider, si farà applicazione delle generali disposizioni civilistiche di applicazione internazionale. Un punto chiave da tenere presente infatti è che la direttiva 95/46/CE non indica criteri di individuazione della giurisdizione[21], dunque in ambito di tutela dei dati personali sono previste

20 Si riportano l'articolo in questione, per la parte che qui interessa:
"1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration...
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:... the obligations set out in paragraph 1, ***as defined*** *by the law of the Member State in which the processor is established,* ***shall also be incumbent on the processor****".*

21 Cfr. anche posizione conforme del Gruppo ex art. 29 nell'opinione 8/2010, pag. 10.

regole specifiche che deroghino ai principi generali, quantomeno tra titolare e responsabile.
Si segnala infine che, ove la legge applicabile sia quella italiana, il giudice competente è determinato in via funzionale in base alla "residenza" del titolare del trattamento, ai sensi dell'art. 10, co. 2 d.lgs. 1° settembre 2011, n. 150.

Misure di sicurezza specifiche in ambito bancario

Il Garante per la protezione dei dati personali ha individuato specifiche misure di sicurezza alle quali le banche devono adeguarsi, nel provv. 12 maggio 2011 n. 192 (in G.U. n. 127 del 3 giugno 2011), con decorrenza variamente prorogata e definitivamente fissata a partire dal 30 settembre 2014 (cfr. provv. 22 maggio 2014).

Occorre subito sgombrare il campo da perplessità applicative. Come si è indicato infatti, in via generale, la disciplina delle misure di sicurezza dovrebbe seguire la normativa applicabile nello Stato membro in cui il responsabile del trattamento è stabilito, ai sensi dell'art. 17(3) dir. 95/47/CE. Nella specie, tuttavia, le misure trovano applicazione soggettiva al titolare del trattamento: esse cioè riguardano l'attività di tracciamento delle operazioni svolte da incaricati delle banche stabilite in Italia e, come tali, sono soggettivamente applicabili agli istituti di credito italiani anche quando questi esternalizzino attività su responsabile stabilito in un diverso paese della UE. Il passaggio si trova peraltro chiarito espressamente dal Garante nel provvedimento 18 luglio 2013: *"Le misure in questione, inoltre, debbono essere osservate pure dalle società che operano in outsourcing –anche quando non appartengono al gruppo bancario- allorché l'attività esternalizzata sia connessa all'esecuzione di rapporti contrattuali (intercorrenti tra banca e cliente) e richieda l'utilizzo di funzioni applicative a*

supporto dell'operatività bancaria". Ricorrendo le condizioni applicative di cui sopra, le misure potrebbero interessare anche il cloud provider nominato quale responsabile del trattamento, nella misura in cui questi (*rectius*: i suoi incaricati) sia coinvolto nelle operazioni relative all'esecuzione dei rapporti contrattuali banca-cliente. Come chiarito dal Garante per la protezione dei dati personali nel Provvedimento del 18 luglio 2013, infatti, tali obblighi di tracciamento riguardano il fornitore esterno solo "*allorché l'attività esternalizzata sia connessa all'esecuzione di rapporti contrattuali (intercorrenti tra banca e cliente) e richieda l'utilizzo di funzioni applicative a supporto dell'operatività bancaria*", ed inoltre "*gli obblighi di tracciamento devono essere riferiti ai soli addetti a funzioni applicative* [non alle funzioni di system admin, tipicamente nella competenza del fornitore tecnologico cloud, ndr] *dei sistemi informativi.*"

Schematicamente, le misure sono ripartite in due gruppi:

<u>Misure necessarie</u>

- *Designazione dell'outsourcer quale responsabile del trattamento*. Si tratta di una modalità corrente in ambito di trattamento dei dati personali e non presenta particolari criticità
- *Tracciamento delle operazioni*. Si tratta di dati di *log* delle operazioni effettuate dagli incaricati (non per funzioni di amministrazione di sistema) su dati bancari riconducibili al singolo cliente individuato, utilizzando sistemi interattivi. I *log* riportano: codice identificativo dell'incaricato, data e ora dell'operazione, codice della postazione di lavoro utilizzata, codice del cliente, tipologia di rapporto contrattuale.
- *Conservazione dei log (anche relativi alle operazioni di inquiry)*. Deve essere garantita per almeno 24 mesi.
- *Implementazione di alert*. Si tratta di sistemi di individuazione di

comportamenti anomali e rischi relativi a operazioni di inquiry.

- *Periodico audit interno di controllo e rapporti.* Si tratta di un'attività da compiere con cadenza annuale. Particolare importanza va data ai profili di *accountability.* Non è richiesto che il controllo sia svolto da terze parti indipendenti, ma che quantomeno non vi sia coincidenza tra controllati e controllanti. I rapporti vanno sottoposti agli organi decisionali della banca e tenuti a disposizione del Garante.

Misure opportune

- *Informativa*. Nel determinare l'ambito di circolazione dei dati è opportuno precisare che essi potranno circolare tra agenzie e filiali di ciascuna banca.
- *Data breach – informazione all'interessato.* Nel caso di trattamenti illegittimi sui dati dell'interessato, questi deve essere prontamente informato. Non è previsto un termine specifico
- *Data breach – comunicazione al Garante*. Nel caso di violazioni nella protezione dei dati personali, il Garante deve essere tempestivamente informato. Non è previsto un termine specifico. Deve trattarsi di violazioni rilevanti, ma non è fornita una parametrazione di questo concetto

Si richiede evidentemente un controllo preliminare della banca circa l'effettiva necessità del cloud provider di gestire le operazioni di tracciamento richieste, cosa che non pare probabile perché di norma il cloud provider non interviene, a mezzo di propri incaricati, in operatività applicative relative ai rapporti bancari istituto/cliente.

Va evidenziato comunque che dal punto di vista tecnico il tracciamento richiesto non presenta, rispetto ai comuni standard di mercato, particolari complessità.

*

IV - FASE CONTRATTUALE: PUNTI SUI QUALI PORRE SPECIALE ATTENZIONE

Qui di seguito si riporta un breve prontuario delle questioni contrattuali che costituiscono tipicamente punti da tenere in considerazione (alcuni, come la continuità operativa, in particolare considerazione) nella fase contrattuale. Non si ripeteranno invece le considerazioni già fatte su altri aspetti: verifica della presenza di requisiti di compatibilità rispetto alle misure di sicurezza prescritte dal Garante per la protezione dei dati personali alle banche, verifica dell'atto di nomina del responsabile (sia che provenga dal titolare del trattamento sia che si utilizzi un modello fornito dal cloud provider), verifica della scelta della legge applicabile e della giurisdizione, verifica della presenza di condizioni di legittimità nel caso di eventuale circolazione dei dati personali in area extra UE/SEE, controlli sulle garanzie e sull'affidabilità generale del fornitore, verifica di compatibilità e di integrazione delle soluzioni cloud con i sistemi già esistenti, ossia in definitiva interoperabilità piena. Appare utile evidenziare che i temi di cui sopra e quelli che si esamineranno qui di seguito non riguardano esclusivamente un fornitore di tecnologia cloud ma qualsiasi *outsourcer* della banca, sono cioè applicabili anche a schemi tradizionali di esternalizzazione.

Continuità operativa e disaster recovery

Si tratta di punti chiave, strettamente connessi con il profilo dela sicurezza, validi

nel pubblico quanto nel privato. Per quanto riguarda poi lo specifico settore bancario, l'intera materia è puntualmente disciplinata al Titolo V, Capitolo IX circ. 263/2006 e ss.mm. Banca d'Italia. Da una corretta predisposizione dei piani di continuità operativa, nei quali è necessariamente coinvolto anche il cloud provider, in base e nei limiti dei processi esternalizzati, derivano conseguenze ragguardevoli, sia di tipo patrimoniale sia di immagine e reputazione per l'istituto di credito. Assicurare la continuità operativa in processi critici di particolare rilevanza può avere inoltre riflessi sistemici sull'intero settore finanziario. Controlli e verifiche sui processi che sono parte del piano di continuità operativa, che naturalmente deve includere anche la fase del ripristino di dati e processi, ossia il momento del *recovery*, sono richiesti dalla circolare citata con una tempistica adeguata (controllare gli SLA del fornitore, ved. anche oltre), che per l'intero piano deve avere cadenza almeno annuale. È inoltre necessario il coinvolgimento dei ruoli decisionali della banca. La continuità operativa è perciò, sia per l'indubbia rilevanza sia per l'espressa previsione della Banca d'Italia, cui gli istituti di credito non possono sottrarsi, un tema essenziale di discussione e di negoziazione con il fornitore di tecnologia cloud e va condotta in maniera necessariamente granulare, ossia confrontando per punti le esigenze della banca con l'offerta del fornitore cloud.

Si suggerisce anche di verificare in quale modo sia gestita la ridondanza necessaria per il disaster recovery, la sincronizzazione tra le varie copie, e come ciò impatti in termini di protezione dei dati personali, soprattutto nel senso di garantire che siano implementate procedure efficienti per la separazione dei dati da quelli di altri titolari, in maniera da evitare promiscuità e accessi illegittimi[22] e sia possibile la cancellazione sicura di tutte le copie quando questa si renda necessaria per

22 Il punto, oltre a discendere dalla diretta applicazione della normativa in materia di protezione dei dati personali, è direttamente richiamato nella circolare n. 263/06 della Banca d'Italia al Titolo V, Capitolo VIII, Sezione VI.3.

decisione del titolare del trattamento. È cioè necessario che il titolare del trattamento non si limiti a recepire le indicazioni che il cloud provider fornisce in tema di *disaster recovery* ma che pretenda, senza scendere in oscuri tecnicismi, di conoscere come la gestione delle copie dei dati si inserisce nel complessivo quadro di rispetto della privacy.

In via di ulteriore misura di sicurezza può essere consigliabile in ogni caso provvedere a un autonomo *back-up* delle informazioni maggiormente rilevanti, per consentire un ripristino di funzionalità qualora eventi imprevedibili possano rallentare o impedire le normali procedure di *disaster recovery*. Potrebbe in tal senso essere oggetto di verifica se il cloud provider fornisca strumenti adeguati e pratici anche per il *back-up* in locale.

Occorre infine notare che elemento di non secondaria importanza nella complessiva procedura di garanzia e ripristino della continuità operativa è rappresentato dalla tempestiva diffusione di allerte che possano permettere di dichiarare lo stato di crisi del sistema informativo in tempi rapidi. Si tratta di un passaggio correttamente evidenziato anche nella citata circolare e va definito con il fornitore di servizi cloud.

Audit

La procedura di *audit* è oggetto di specifica attenzione nella citata circolare 263/2006. Si tratta di audit non solo interni, ma necessariamente estesi ai processi e ai dati affidati in gestione informatica al fornitore cloud, nei limiti di tale esternalizzazione. Deve evidenziarsi che in materia di sistemi distribuiti, come appunto quelli di cloud computing, le modalità di svolgimento di un *audit* tendono

a differire da quelle tipicamente applicate a un *outsourcing* tradizionale. In particolare, l'accesso *in loco* a una singola struttura, ancorché centrale, pare avere un'utilità limitata e non essere la scelta più efficiente. Senza alcuna pretesa di suggerire le modalità ritenute più opportune per l'*audit*, ci si limita a segnalare l'opportunità di richiedere rapporti effettuati da soggetti terzi e basati su criteri di valutazione che tengano conto appunto della struttura distribuita del cloud e siano perciò ottimizzati rispetto a tale soluzione tecnologica. Diventa in tal senso particolarmente rilevante precisare quali siano i criteri e le metodologie applicati da tali terzi indipendenti.

Si evidenzia infine la connessione tra il tema dell'*audit* e quello dell'*accountability* e in definitiva il collegamento con la necessaria predisposizione di un sistema di tracciatura. Tutto ciò è anche oggetto di espressa raccomandazione da parte della Banca d'Italia nella citata circolare n. 263/06, che evidenzia altresì la necessità di richiedere un tracciamento sulle operazioni compiute sui dati conferiti nel cloud. Vale la pena riportare il passaggio: *"Il fornitore... assicura la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive. Sono concordate con il fornitore di servizi modalità di audit adeguate alla criticità delle risorse esternalizzate e in considerazione dell'architettura del fornitore"*. Anche in tal senso è necessaria una verifica puntuale dell'offerta del fornitore cloud. Del resto, va notato, la tracciatura si integra anche con le già notate prescrizioni in materia di sicurezza degli istituti di crediti individuate dal Garante.

SLA e PLA

Gli SLA, *Service Level Agreement*, sono una componente essenziale dell'offerta cloud,

perché introducono in essa:

- criteri di misurazione trasversali a tutte le prestazioni garantite dal cloud provider, da confrontare con le esigenze specifiche dell'istituto di credito. La continuità operativa e il disaster recovery richiedono il rispetto di specifici parametri temporali per il ripristino (cfr. circolare citata n. 263/2006), che vanno verificati rispetto all'offerta del cloud provider;
- uno strumento di comparazione fra varie offerte cloud;
- un parametro per valutare in maniera precisa l'eventuale inadempimento da parte del cloud provider;
- un parametro di riferimento per i clienti dell'istituto di credito.

Si desidera evidenziare che nella valutazione degli SLA è fondamentale comprendere quali sono gli effettivi elementi presi in considerazione, in maniera da comprendere il reale significato delle percentuali di servizio garantite dal fornitore di tecnologia cloud.

Per PLA, *Privacy Level Agreement*, si intendono SLA focalizzati su parametri rilevanti in materia di protezione dei dati personali, soprattutto per ciò che attiene alle modalità di attuazione delle misure di sicurezza, incluse le garanzie relative alla continuità dei servizi, ai tempi di risposta nei confronti di eventi pregiudizievoli, alla percentuale di successo da attendersi nelle risposte, ecc.
Ove i PLA non siano menzionati espressamente come tali, essi vanno ricercati all'interno degli SLA.

Nella più volte menzionata circolare n. 263/06 della Banca d'Italia si raccomanda di specificare che i livelli garantiti di servizio devono essere tali anche nel caso di

"emergenza o di contesa delle risorse da parte di altri suoi clienti"[23]. Non è chiaro dalla formulazione se la contesa in questione faccia riferimento soltanto all'impegno di risorse computazionali o faccia riferimento anche a controversia giudiziale dalla quale risulti ad esempio un provvedimento di sequestro dei server, in ogni caso la verifica della disponibilità effettiva dei livelli garantiti indipendentemente dal numero di altri clienti che impegnano le risorse del cloud provider deve essere elemento oggetto di verifica.

Questioni attinenti ai subfornitori del cloud provider

Un passaggio, denso di conseguenze pratiche, sul quale i Garanti europei si sono particolarmente soffermati nella citata opinione 5/2012 è quello relativo alla disciplina applicabile ai subfornitori del cloud provider. Infatti, se questo elemento non riceve adeguato chiarimento contrattuale, l'intero schema di tutele rischia di essere posto nel nulla. Il tema si connette a quanto già osservato circa la necessità di assicurare che il trasferimento dei dati extra area UE/SEE sia effettuato lecitamente.

Ci sono in proposito i seguenti passaggi essenziali da osservare[24]:

- i subfornitori devono essere direttamente conoscibili dal titolare del trattamento, come devono essere conoscibili il tipo e i servizi oggetto del subappalto, quindi nel caso che ci occupa da parte dell'istituto bancario, che deve poter determinare in quale stato sono stabiliti e deve essere in grado di identificarli;
- i subfornitori devono essere contrattualmente vincolati (dal cloud provider) al rispetto della normativa europea in materia di protezione dei dati

23 Cfr. Titolo V, Capitolo VIII, Sezione VI.3.
24 Cfr. Gruppo ex art. 29, op. 5/2012 (versione inglese), soprattutto pp. 9 e 20.

personali;

- i subfornitori devono essere contrattualmente vincolati (dal cloud provider) in modo da riflettere le obbligazioni del contratto principale, ossia quello tra il cloud provider e il titolare, ossia nel nostro caso l'istituto di credito;
- deve permanere la responsabilità giuridica del cloud provider per eventuale trattamento illegittimo dei dati da parte dei propri subfornitori;
- il titolare deve poter approvare i subfornitori da parte del cloud provider (in genere lo fa nella fase iniziale del rapporto) e deve successivamente potersi opporre alla loro sostituzione con altri soggetti, se questi non siano di suo gradimento.

Detto altrimenti, il titolare deve poter estendere il potere decisionale che è conforme al suo ruolo anche rispetto ai subfornitori del cloud provider, pur nel rispetto di un ragionevole criterio di bilanciamento rispetto alle esigenze di funzionamento dell'organizzazione complessiva del cloud provider. Ciò è tuttavia possibile soltanto se nel contratto che stipula con il cloud provider siano fornite specifiche garanzie in tal senso[25]. In termini concreti, perciò, questo implica un preciso onere dell'istituto di credito di verificare come è gestito nel contratto di fornitura cloud il tema dei subfornitori, pretendendo il rispetto di quanto stabilito nell'opinione 5/2012 dei Garanti europei.

Localizzazione dei data center

Tema in parte contiguo a quello appena esaminato è quello della possibilità del

25 Id., *cit.*, p. 21.

titolare del trattamento di conoscere dove si trovino in un certo momento i dati conferiti nel cloud, da intendersi propriamente come pretesa di conoscere dove siano collocati i server sui quali *possono* essere processati i dati forniti dal cliente, dunque in definitiva dove si trovano i data center. Questa pretesa conoscitiva, articolabile in senso più o meno concreto / astratto secondo valutazione di ragionevolezza e buona fede, discende direttamente dal ruolo apicale e decisorio del titolare del trattamento e in particolare dall'onere di vigilanza sulla circolazione dei dati all'interno della propria struttura.

In senso pratico, ciò si traduce nel verificare da parte dell'istituto bancario che il cloud provider metta a disposizione effettivi strumenti di monitoraggio sulla circolazione dei dati all'interno del cloud. Nell'esperienza concreta, molti fornitori di servizi cloud offrono programmi applicativi che permettono di svolgere tali attività conoscitive.

Deve notarsi che la conoscenza della locazione fisica dei data center è espressamente richiesta all'intermediario finanziario dalla citata circolare n. 263/06 della Banca d'Italia. In particolare, viene specificato: *"A causa della possibilità tecnica per il fornitore di spostare rapidamente e in modo trasparente all'utente le risorse dedicate ai vari clienti, è importante che le locazioni dei data center utilizzabili siano preventivamente comunicate"*[26].

Portabilità dei dati personali e libertà di migrazione ad altro provider

Un aspetto particolarmente sottolineato dai Garanti europei nell'opinione citata[27] e

26 Cfr. Titolo V, Capitolo VIII, Sezione VI.3.
27 Id., *cit.*, p. 16.

dal Garante italiano nei due documenti sopra menzionati contenenti linee guida in materia di cloud computing riguarda la portabilità dei dati. La portabilità, a ben vedere, è strettamente connessa al concetto del mantenimento del controllo da parte del titolare sui dati personali che conferisce nel cloud, dal momento che solo attraverso la garanzia della portabilità il titolare può essere veramente libero di gestire le vicende del proprio rapporto contrattuale con il cloud provider senza condizionamenti e limitazioni e dunque mantenendo un pieno potere decisionale rispetto ai dati conferiti nel cloud. Gli aspetti relativi alla portabilità dei dati, compresi quelli che riguardano il formato aperto o proprietario della loro codifica vanno chiariti in sede contrattuale. Occorre notare che la messa a disposizione da parte di alcuni cloud provider di strumenti gratuiti e di libero accesso per la conversione di dati in formato proprietario in dati in formati liberi costituisce un'oggettiva garanzia di portabilità, salve ulteriori limitazioni da esaminare nel caso di specie.

Il tema della portabilità dei dati è strettamente legato a quello della possibilità di migrare verso diverso fornitore di tecnologia cloud in tempi rapidi e senza eccessive difficoltà: ciò riguarda sia l'assenza di vincoli tecnici di *vendor lock-in* sia l'assenza di vicoli giuridici. Su quest'ultimo punto va considerata l'eventuale disciplina del recesso contenuta nel contratto con il cloud provider. Si evidenzia che la già citata circolare della Banca d'Italia sottolinea l'importanza di evitare situazioni di *lock-in* e l'opportunità di disporre di adeguate *exit strategy*.

Corollario privacy della libertà di migrazione è la garanzia che i dati conferiti al cloud provider che viene abbandonato siano effettivamente cancellati da questi, con una tempistica certa e con metodi sicuri e che tale tempistica non impatti negativamente nella migrazione ad altro fornitore.

Elemento aggiuntivo di valutazione è altresì rappresentato dalla facilitazione o meno della migrazione verso e dal cloud provider attraverso specifiche procedure o applicazioni messe a disposizione dal provider stesso.

Notificazione nel caso di data breach

In considerazione del ruolo altamente strategico dei dati personali trattati dagli istituti di credito, appare rilevante affrontare la tematica della notificazione di episodi di *data breach*, ossia di violazioni di sicurezza idonee a compromettere la riservatezza dei dati o della loro integrità. Il tema è connesso, ma anche distinto, da quello della funzione di allerta interna nel caso di violazioni della sicurezza, e coinvolge i rapporti dell'istituto di credito con soggetti esterni: la Banca d'Italia, il Garante per la protezione dei dati personali (nel caso in cui siano coinvolti dati personali ovviamente), gli interessati di trattamento (nella stessa circostanza). Non è possibile in questa sede fare approfondimenti. Ci si limita perciò a osservare che la gestione degli obblighi di comunicazioni di violazioni della sicurezza deve necessariamente considerare anche il rapporto con il fornitore di servizi esternalizzati e va coordinato con le esigenze interne dell'istituto, con le sue policy e con gli obblighi normativi. Una verifica in tal senso con il fornitore deve consentire di individuare le modalità e il protocollo seguito nel caso di violazione.

Accesso da parte di autorità di polizia

Un profilo rilevante e spesso trascurato riguarda l'accesso da parte di autorità di

polizia / servizi segreti (indicate anche con il nome collettivo e ampio di "*law enforcement agencies*" o "LEA") al patrimonio di informazioni gestito dal cloud provider.

Uno dei punti evidenziati dai Garanti europei nell'opinione 5/2012 riguarda proprio l'informazione circa eventuali richieste di accesso ai dati personali da parte di LEA, informazione da declinare come vero e proprio impegno contrattuale del cloud provider nei confronti del titolare del trattamento, nel nostro caso la banca che sottoscrive il servizio cloud[28].

Le richieste di accesso ai dati personali da parte delle LEA devono naturalmente rispettare le specifiche norme procedurali previste nelle rispettive legislazioni nazionali, punto che occorre verificare con attenzione caso per caso.

Evidentemente, affidare dati personali a un cloud provider stabilito in un determinato paese può determinare il coinvolgimento diretto in richieste di accesso ai dati personali da parte delle autorità locali di polizia, determinando con ciò un potenziale ampliamento dell'esposizione dei dati personali a questo genere di ispezioni, con una conseguente riduzione dell'attesa di riservatezza degli interessati rispetto ai propri dati personali. Il ragionamento si applica evidentemente anche all'intera filiera dei subfornitori.

D'altro canto, va pure osservato che, in termini realistici, il detto ampliamento potenziale appare in molti casi privo di reale fondamento, dal momento che sono in essere numerosi accordi bilaterali e multilaterali internazionali di collaborazione in materia penale, che determinano una sostanziale armonizzazione a livello

28 Id., ibidem.

pressoché globale delle possibilità di accesso ai dati personali per ragioni penali o di sicurezza.

Si segnala, per scrupolo d'aggiornamento, che sono recentemente intervenute sul tema dei trattamenti svolti da autorità di polizia o da servizi segreti due ulteriori precisazioni ragionate da parte dei Garanti europei, a sottolineare la rilevanza dell'argomento, l'opinione 01/2014 *"on the application of necessity and proportionality concepts and data protection within the law enforcement sector"* e l'opinione 04/2014 *"on surveillance of electronic communications for intelligence and national security purposes"*.

Dal punto di vista concreto, occorre accertarsi che gli accordi con il fornitore cloud prevedano una gestione delle richieste effettuate dalle attività di polizia, con garanzia di informazione preventiva alle banche nel caso di richieste delle autorità, ovviamente nei casi in cui ciò sia consentito giuridicamente.

Comprensione della struttura contrattuale

Sia permesso un cenno finale a questioni relative a questioni pratiche di gestione della struttura contrattuale. La struttura contrattuale adottata da un fornitore di servizi cloud potrebbe essere complessa e distante dalle tipologie alle quali si è abituati, ciò anche per la ragione che essa deve trovare applicazione in paesi diversi ed è dunque difficilmente configurabile su misura del singolo cliente. Del resto, la complessità di un contratto va parametrata anche con la complessità di un servizio offerto, che nella specie è connotata da un elevato livello tecnologico. In termini di buona prassi, ci si limita a suggerire alla parte che sottoscrive l'accordo contrattuale con il fornitore di servizi cloud di prendere tutto il tempo necessario alla

comprensione della struttura contrattuale e di richiedere tutti i necessari chiarimenti per metterla a fuoco.

Considerazioni di chiusura e riepilogo

Si riporta, per utile riepilogo e sguardo d'insieme, quanto indicato dalla Banca d'Italia nella più volte citata circolare n. 263/2006 e ss.mm. a proposito delle valutazioni da effettuare in occasione di esternalizzazioni, Titolo V, Capitolo VIII, Sezione VI, n. 1: *"Con particolare riferimento all'esternalizzazione di parte o tutto il sistema presso fornitori al di fuori del gruppo di appartenenza, la scelta è basata su* ***un'analisi del rischio****, che considera in primo luogo la stima dei rischi delle risorse e servizi da esternalizzare (ad es., tiene conto della* ***classificazione dei dati*** *e della criticità dell'operatività interessata, valutando in particolare i rischi derivanti dalla* ***perdita del controllo diretto*** *su componenti del sistema informativo e personale critici, nonché dei volumi delle operazioni) e quindi valuta i rischi dei* ***possibili fornitori*** *(ad es., condizioni finanziarie, posizionamento sul mercato, qualità e turnover del management e del personale,* ***capacità di gestire*** *la* ***continuità operativa*** *e di fornire accurati e tempestivi* ***report*** *direzionali sull'attività svolta, competenza ed esperienza, qualità e sicurezza nonché economicità e maturità, in un adeguato orizzonte temporale, della fornitura), la qualità dei* ***sub-fornitori****, la* ***ridondanza*** *delle linee di comunicazione utilizzate nonché l'affidabilità, la sicurezza e la scalabilità delle tecnologie adottate.*

Nell'elaborazione del modello architetturale e delle strategie di esternalizzazione vanno considerati approcci tesi a contenere, per quanto possibile, il grado di dipendenza da specifici fornitori e partner tecnologici esterni al gruppo bancario (c.d. vendor lock-in), salvaguardando la possibilità di sostituire la fornitura con un'altra funzionalmente equivalente (ad es., privilegiando il ricorso a ***standard aperti*** *per le connessioni, la*

memorizzazione e lo scambio di dati, la cooperazione applicativa) e prevedendo opportune ***exit strategies****.*

Tali valutazioni tengono conto del principio di proporzionalità e dell'opportunità, per le banche di maggiore dimensione, di ***mantenere all'interno della banca o del gruppo competenze professionali*** *per gestire una transizione tra modelli di sourcing in caso di grave necessità.*

Il mantenimento nel tempo da parte del fornitore delle condizioni necessarie a fornire un servizio rispondente alle esigenze e conforme alle norme è assicurato attraverso ***idonei strumenti contrattuali*** *e procedure di controllo".*

IV - CONCLUSIONI

Non constano ancora nel settore bancario italiano, fatte salve le dettagliate prescrizioni individuate dalla Banca d'Italia nella circolare n. 263/2006 e ss. mm., specifici atti normativi che regolano le soluzioni cloud o anche solo linee guida ufficiali di orientamento o *best practice*, che siano espressamente orientate al settore bancario in tema di cloud computing. Soprattutto si rileva l'assenza di una normazione delle questioni che interessano l'applicazione delle disposizioni in materia di protezione dei dati personali rispetto alle soluzioni cloud in ambito bancario.

Ciò non costituisce necessariamente una lacuna, perché comporta semplicemente il richiamo di schemi di ragionamento giuridico già in essere a un livello più generale. Del resto non è da escludersi che in un prossimo futuro non si registrino interventi normativi più specifici nel settore esaminato o più in generale in tema di cloud computing e dati personali. C'è da notare che le condizioni concrete esistono: il contesto fattuale registra, sul piano del *business*, una rapida e crescente affermazione della tecnologia in esame e, sul piano delle azioni di strategia politico-economica, c'è il convinto supporto e l'appoggio espresso da parte della Commissione europea. Dunque la direzione è quella di un'espansione, e l'espansione molte volte richiede una precisazione del quadro normativo applicabile. Nel settore bancario, non stupisce che, nonostante alcune titubanze o resistenze, si cominci ad avere notizia delle prime adesioni a servizi cloud da parte di istituti di credito esteri. In definitiva, la migrazione anche nel settore bancario verso tale tecnologia, in una misura e per comparti ancora tutti da definire, va precisando i suoi contorni e si preannuncia, verosimilmente, come prossima.

A fronte di un certo ritardo nella riflessione giuridica sul cloud nel contesto del settore bancario italiano, non resta che applicare come si è detto, *per relationem* e *mutatis mutandis*, quanto già emerso in altri ambiti.

In particolare, appaiono utile e opportuno cogliere gli spunti che provengono dai corposi lavori di inquadramento effettuati nel settore pubblico, soprattutto ad opera della Consip e di DigitPA e quindi dell'AGID e, in ambito privacy, dalla riflessione e dalle linee di orientamento del Garante, mentre a livello europeo il riferimento chiave resta quello della puntuale e ampia opera di inquadramento del Gruppo ex art. 29.

Sul piano strettamente normativo, deve ripetersi che vengono in applicazione innanzitutto le disposizioni le disposizioni di comune applicazione contenute nel Codice privacy e quelle specifiche prescritte dal Garante per il settore bancario, in particolare sotto il profilo delle misure di sicurezza.

Occorre notare, a conclusione dell'esame condotto, che la scelta di soluzioni cloud in ambito bancario non presenta, almeno ad una prima generale analisi, macroquestioni applicative. Né certo il Testo unico bancario, né il Testo unico della finanza contengono disposizioni che si pongono come incompatibili o comunque d'ostacolo rispetto a tale scelta tecnologica.

Gli aspetti su cui porre maggiore attenzione nel processo di migrazione verso soluzioni cloud appaiono in definitiva comuni a quelli che si prospettano in altri settori imprenditoriali, sia pure con declinazioni talvolta specifiche. Particolare attenzione va attribuita ai temi della continuità operativa e del disaster recovery e dell'*audit*, da coordinare con le disposizioni della più volte citata circolare della

Banca d'Italia, e prestando particolare cura alla garanzia della portabilità dei dati personali, dell'interoperabilità piena con i sistemi ICT in essere nella banca e con l'esigenza di libertà da situazioni di *vendor lock-in*. Sulle specificità alle quali prestare attenzione si rimanda comunque alle osservazioni già svolte più sopra, per non tediare il lettore con inutili ripetizioni.

Estremamente raccomandabile appare poi la scelta di fonitori cloud dotati di certificazioni ampiamente riconosciute a livello internazionale. Si evidenzia anche che nell'estate 2014 è stato rilasciato un nuovo specifico standard per il settore cloud, l'ISO 27018, che rappresenterà inevitabilmente un fattore di grande significato nella scelta del fornitore cloud.

Sullo specifico versante privacy, ci si permette di ricordare che uno degli elementi cui prestare maggiore attenzione è la garanzia della liceità nei trasferimenti di dati personali in area extra UE/SEE, operando i fornitori cloud in un contesto tendenzialmente globale. Sul punto esistono vari schemi giuridici che rendono lecito il trasferimento, tuttavia, come si è notato, quelli più funzionali e più in linea con il livello di maturazione della normativa sono rappresentati dall'adozione di *model clause*, ossia di contratti standard e immodificabili definiti dalla Commissione europea, o delle *binding corporate rule*, ossia corpi di regole adottati spontaneamente da gruppi di imprese e sottoposti a uno specifico procedimento di verifica e approvazione da parte delle Autorità garanti.

Dal punto di vista metodologico, si ribadisce di dare spazio alle attività di tipo preparatorio prima di concentrarsi su aspetti più concretamente operativi e contrattuali. Si tratta soprattutto dell'esigenza di monitorare con precisione i flussi dati da esternalizzare e di attribuire loro un coefficiente di criticità all'interno dei complessivi processi bancari. Tali attività che vanno coordinate con quelle già in essere per esigenze di controllo interno e tornano di grande utilità sia nella fase

negoziale (es. verifica delle singole operazioni di continuità operativa e recovery e loro congruenza con la garanzia di ripristino dei processi critici) sia nella fase di *audit*.

Al termine di questo manualetto è fornita come si è anticipato una scheda riepilogativa pratica, sul modello di una *checklist*, ossia di una lista di controllo, che elenca singolarmente punti di attenzione ritenuti significativi, proponendo anche una qualificazione in termini di importanza per ciascuno di essi.

SCHEDA PRATICA DI VALUTAZIONE (CHECKLIST)

La presente checklist vuole essere uno strumento pratico-riepilogativo di massima per il titolare del trattamento nel valutare la scelta di soluzioni cloud

Punto da esaminare	Importanza	Sì	No	Note del compilatore
Questioni di metodo				
Si è effettuato un censimento preliminare dei trattamenti di dati personali che si intende migrare su tecnologia cloud?	3			
Si sono distinti i vari trattamenti censiti in base al livello di criticità?	3			
Si è valutato se adottare una soluzione cloud pubblica, privata o ibrida o eventualmente una soluzione community?	1			
Si dispone delle SLA relative ai servizi resi e si è effettuato già su questa base un confronto tra varie offerte di servizi cloud?	1			
Il fornitore dei servizi cloud è un soggetto economico affidabile, con esperienza nel settore?	2			
Il fornitore dei servizi cloud è un intermediario o gestisce direttamente i servizi offerti?	1			
Si dispone di tutti i testi contrattuali che costituiscono l'offerta di servizi cloud?	2			
Si è compresa la struttura di tali documenti?	2			
Questioni giuridico/informatiche				
Il trattamento dei dati avviene integralmente all'interno della UE/SEE oppure può avvenire all'esterno di essa? In tal caso sono state adottate soluzioni giuridiche che rendono lecito il trattamento? (es. standard clause, binding corporate rule)	3			
È possibile conoscere dove si trovano i data center che trattano i dati conferiti nel cloud? Sono per esempio forniti “cruscotti” di controllo al cliente?	2			
È prevista l'applicazione della giurisdizione italiana ai trattamenti di dati personali?	3			
È prevista quale legge applicabile al trattamento dei dati personali la legge italiana?	3			
È assicurata la continuità operativa? Con quali specifiche garanzie? Secondo quali parametri di erogazione (ved. SLA)?	3			

È assicurato il disaster recovery? Con quali specifiche garanzie? Secondo quali parametri di erogazione (ved. SLA)?	3			
Si è provveduto a determinare se vi è conformità tra le prescrizioni in tema di esternalizzazione e di continuità operativa contenute ai Capitoli VIII e IX del Titolo V della circ. n. 263/2006 e ss. mm. della Banca d'Italia e le garanzie fornite dal cloud provider?	3			
È assicurata la portabilità dei dati? Sono state in particolare controllate le specifiche utilizzate?	2			
Sono previste possibilità adeguate di uscita dal contratto? (da coordinare con il precedente)	2			
Può essere assicurata un'efficiente interoperabilità rispetto alla struttura ICT esistente? (da coordinare con la portabilità dei dati)	2			
Sono garantite procedure di *audit* da parte di terze parti indipendenti? E i risultati dell'*audit* sono accessibili?	2			
È assicurato l'isolamento dei dati conferiti rispetto a dati conferiti da terzi?	3			
Il cloud provider dispone di certificazioni internazionali adeguate? È certificato o in corso di certificazione rispetto allo standard specifico per il cloud, ISO 27018?	2			
È assicurata l'adozione delle misure di sicurezza minime previste dall'allegato B al codice privacy? (Ove la legge applicabile alle misure di sicurezza sia quella italiana)	3			
Sono state adottate le misure di sicurezza individuate dal Garante con specifico riferimento al settore bancario?	3			
È assicurata l'adozione di misure di sicurezza idonee che riflettano lo stato dell'arte tecnologica? Quali? (Passaggio da valutare insieme a quello sulla legge applicabile alle misure di sicurezza)	3			
Il cloud provider ha espresso la propria adesione al modello di atto di nomina a responsabile del trattamento che gli è stato sottoposto?	1			
È previsto un diritto di recesso delle parti? I termini di questo diritto sono compatibili con le esigenze imprenditoriali della banca?	2			
I dati sono effettivamente cancellati in maniera definitiva dai server del cloud provider al termine del rapporto?	3			

Il contratto disciplina i profili relativi ai subfornitori? (Conoscibilità degli stessi, diritto di opposizione dell'istituto di credito)	3			
Il cloud provider dà informazione al titolare nel caso di data breach e nel rispetto di quali parametri (cfr. SLA)?	2			
Il cloud provider prevede una policy, una procedura o comunque uno schema operativo tipico applicabile nel caso di richieste di accesso da parte delle LEA? Questo schema prevede anche le ipotesi nelle quali dell'accesso è data notizia all'istituto di credito?	1			

Tavola sul grado di importanza delle questioni

1 punto il cui esame è opportuno dal punto di vista giuridico e pratico. L'eventuale risposta negativa non condiziona tuttavia il processo decisionale

2 punto il cui esame è fortemente opportuno dal punto di vista giuridico e pratico, perché può generare disallineamenti tra le parti e perfino a contenzioso e in ogni caso può tradursi in procedure macchinose, esporre a rischi e, nella migliore delle ipotesi, aggravare il carico di lavoro. L'eventuale risposta negativa dovrebbe essere ponderata con la massima attenzione e, se possibile, superata in seguito all'adozione di opportuni accorgimenti

3 punto la cui presenza è necessaria per non incorrere in attività illegittime o in responsabilità giuridiche o in nullità di clausole. L'eventuale risposta negativa dovrebbe rappresentare un rilevante ostacolo nel processo decisionale, da superare imprescindibilmente con opportuni accorgimenti