Il cloud computing e l'internet of things ("IoT"): come minimizzare i rischi legali

Paolo Balboni: (Ph.D.) è un avvocato esperto di diritto europeo delle nuove tecnologie, della privacy e protezione dei dati personali, inoltre fornisce servizi di Data Protection Officer (DPO) per società multinazionali. Lead Auditor BS ISO/IEC 27001:2013 (IRCA Certified). Avvocato del Foro di Milano è Socio Fondatore dello studio legale di ICT Legal Consulting. Presidente dell'European Privacy Association, Cloud Computing Sector Director e Responsabile Affari Esteri dell'Istituto Italiano Privacy.
Theodora Dragan: Laureata in Giurisprudenza alla University College London e Associate specializzata in Privacy e protezione dei dati personali presso ICT Legal Consulting. Fellow della European Privacy Association.
Stefania Tonutti: Laureata in Giurisprudenza, Ph.D. in diritto nuove tecnologie, cultrice della materia presso l'Università di Bologna, bioeticista, specializzata in privacy sanitaria e genetica, master di I livello in diritto sanitario, master di II livello in Data Protection Officer, Associate presso ICT Legal Consulting, Fellow della European Privacy Association.

1. INTERAZIONE TRA CLOUD COMPUTING E IOT

Nell'agosto del 1991, la versione beta del servizio di cloud computing di Amazon è stata lanciata con il nome di EC2: "Elastic Compute Cloud". Oggi Amazon (Amazon Web Services) è diventato uno dei leader nel mercato del cloud: solo l'anno scorso, vantava un fatturato di oltre $ 11 miliardi e, secondo il settimanale *The Economist*, "*il suo progresso non mostra alcun segno di rallentamento nel suo percorso verso il dominio delle 'nuvole' del cloud computing*". In parallelo, anche l'Internet of Things ("IoT" o "internet delle cose") è in piena crescita. Gli esperti stimano che 50 miliardi di dispositivi intelligenti ne faranno parte entro il 2020.

Non solo: lo scorso luglio la società di ricerche di mercato Gartner ha pubblicato l'analisi "Market Insight: Cloud Shift – The Transition of IT Spending from Traditional Systems to Cloud".[1] Secondo Gartner, con più di $1 miliardo di spesa prevista, il cloud computing diventerà "*una delle forze più dirompenti della spesa IT fin dai primi giorni dell'era digitale*". Esempi di questa forza sono già visibili: il passaggio al sistema cloud fino al 2020 per quanto riguarda l'outsourcing dei processi di business è stimato a crescere del 40%, e nel mese di agosto 2016 Microsoft ha annunciato che la forte crescita della sua unità di cloud computing ha contribuito a incrementare i profitti trimestrali di $3,1 miliardi nel secondo quadrimestre del 2016. L'importanza dell'infrastruttura cloud non deriva solo dal fatto che sta sostenendo le operazioni di molte aziende (dalle start-up alle aziende top inserite in Fortune 500) ma anche dal fatto che sta creando allo stesso tempo le condizioni per una nuova generazione di start-up e fornitori di servizi innovativi, "born-in-the-cloud".

Il cloud computnig, attraverso le sue caratteristiche più tipiche quali elasticità, scalabilità, potenza ed economicità, sta sostanzialmente abilitando l'IoT. Uno dei motivi per il **collegamento stretto tra il cloud computing e l'IoT** resta nel fatto che la tecnologia dei dispositivi intelligenti è ancora nella sua fase pionieristica e largamente sviluppata da imprese innovative "born-in-the-cloud". L'aspetto principale che rende così interessante il connubio cloud-IoT è sicuramente la quantità di dati che l'IoT è in grado di generare, che possono essere analizzati al fine di trarre conclusioni rilevanti sugli utenti, le tendenze del mercato e così via (si nota un ulteriore collegamento con "Big Data & Analytics"). Ed è qui che l'IoT viene naturalmente sorretto dalla potenza e la flessibilità del cloud.[2]

> L'ASPETTO PRINCIPALE CHE RENDE COSÌ INTERESSANTE IL CONNUBIO CLOUD-IOT È SICURAMENTE LA QUANTITÀ DI DATI CHE L'IOT È IN GRADO DI GENERARE, CHE POSSONO ESSERE ANALIZZATI AL FINE DI TRARRE CONCLUSIONI RILEVANTI SUGLI UTENTI, LE TENDENZE DEL MERCATO E COSÌ VIA (SI NOTA UN ULTERIORE COLLEGAMENTO CON "BIG DATA & ANALYTICS"). ED È QUI CHE L'IOT VIENE NATURALMENTE SORRETTO DALLA POTENZA E LA FLESSIBILITÀ DEL CLOUD

2. LA SFIDA PER LA PROTEZIONE E LA SICUREZZA DEI DATI PERSONALI NELL'AMBITO DEL CLOUD E DELL'IOT

Cloud computing

Il Gruppo di Lavoro Articolo 29, nel suo "Parere 5/2012 sul *cloud computing*", ha identificato i principali rischi per la protezione dei dati in questo settore.[3] Il cd. WP29 cita, innanzitutto, la mancanza di controllo dei dati: affidando dati personali a sistemi gestiti da un fornitore di servizi *cloud*, i clienti rischiano di non poter prendere le misure tecniche e organizzative necessarie per garantire la disponibilità, l'integrità, la riservatezza, la trasparenza, l'isolamento, la portabilità dei dati e la possibilità di intervento sugli stessi. Ancora, i problemi legati al *lock-in*, l'interoperabilità e la man-

1 Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending. Gartnercom. 2016. Available at: http://www.gartner.com/newsroom/id/3384720. Accessed September 14, 2016.
2 Sul punto si veda anche Piano nazionale Industria 4.0, disponibile al seguente link: http://www.corrierecomunicazioni.it/upload/images/09_2016/160921192040.pdf.
3 Article 29 Working Party. Parere 5/2012 Sul Cloud Computing; 2012. Reperibile sul sito: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf. Ultimo accesso 14 settembre 2016.

PAOLO BALBONI
Founding Partner, ICT Legal Consulting

THEODORA DRAGAN
Associate, ICT Legal Consulting

STEFANIA TONUTTI
Associate, ICT Legal Consulting

canza di portabilità dei dati costituiscono delle sfide che possono essere superate solo tramite una ricerca approfondita ed una scelta accurata dei cloud provider (e delle relative offerte).[4] Nell'ambito dell'IoT, questi problemi possono essere molto gravi, dato che esso stesso si basa sull'interconnetività degli oggetti. Tuttavia, proprio questa innaturata condivisione di dati portata dai dispositivi IoT genera un traffico estremamente difficile da controllare (e tracciare). I dati raccolti sono inoltre spesso condivisi con terze parti, spesso all'insaputa della persona fisica cui si riferiscono i dati personali.
Un'altra problematica è costituita dalla mancanza di trasparenza: spesso, il cliente del cloud non è consapevole del fatto che, lungo la catena di trattamento dei dati, possono essere coinvolti sub-responsabili magari ubicati fuori dall'Unione Europea, in paesi che non offrono una protezione adeguata dei dati personali. Questo pertanto potrebbe portare a un trattamento illecito dei dati, se non vengono seguite le regole per il corretto trasferimento dei dati (ad esempio, tramite le Clausole Contrattuali Standard[5] o, nei casi di trasferimento verso gli Stati Uniti, il recentemente approvato Privacy Shield)[6]. La trasparenza è ancora più importante quando si parla dell'ambito IoT, poiché l'interconnettività degli oggetti può rendere la catena di trattamento dei dati ancora più difficile da mappare – occorre dunque prestare molta attenzione e ben mappare il cosiddetto "data flow" (flusso dei dati).
Un'ulteriore sfida identificata dal Gruppo di Lavoro Articolo 29 risulta dal fatto che i provider di servizi cloud sono perlopiù delle grande aziende che solitamente offrono contratti standard, lasciando poca margine di manovra alle aziende per negoziare i termini e le condizioni di utilizzo del servizio cloud. Il Gruppo di Lavoro aveva già identificato da tempo questo problema nel suo parere 1/2010, dove ha specificato che "lo squilibrio fra il potere contrattuale di un piccolo [cliente-Titolare] del trattamento rispetto a un grosso fornitore di servizi [tipicamente Responsabile del trattamento] non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati".[7]

IoT

Non è certamente possibile eliminare del tutto i rischi sopra descritti, è però possibile ridurre al minimo la possibilità che questi si materializzino.
Il Garante del Regno Unito ("Information Commissioner's Office" oppure "ICO") ha recentemente pubblicato un articolo sul suo blog, informando il pubblico su come "proteggersi" nell'utilizzo di oggetti intelligenti (testo completo qui).[8]
Anche se i dispositivi dell'IoT non sono propriamente "pericolosi", come il titolo dell'articolo suggerisce, vi è una reale necessità di essere consapevoli dei rischi di questa tecnologia e di adottare le misure necessarie al fine di evitare (o almeno ridurre al minimo) i rischi.
L'ICO ha identificato alcuni suggerimenti per coloro che si accingono ad utilizzare i dispositivi IoT:

1. operare una ricerca approfondita prima di iniziare a utilizzare i dispositivi intelligenti: non basta informarsi sulle caratteristiche del prodotto ma occorre estendere questa ricerca anche per quanto riguarda il produttore;
2. premurarsi che tutti i punti di accesso, siano essi fisici (router) o logici (log-in) ai dispositivi siano messi in sicurezza a mezzo di strati multipli di autenticazione, cifratura o altre specifiche caratteristiche di sicurezza;
3. verificare periodicamente la presenza di aggiornamenti di sicurezza e di assicurarsi che la nuova versione del software venga scaricata su tutti i dispositivi – le versioni precedenti sono più vulnerabili alle minacce.

3. CONCLUSIONI OPERATIVE

Concludiamo condividendo, per punti, alcune riflessioni operative al fine di ben gestire gli aspetti legali di scenari complessi che prevedono l'interazione dell'IoT con il cloud computing, minimizzando i rischi:

1. Occorre essere coinvolti sin dall'inizio per svolgere di regola un Data Protection Impact Assessment [9] e strutturare il trattamento secondo il principio di Data Protection by Design.[10]
2. Identificare precisamente: (i) flusso dei dati; (ii) tipologia di dati trattati (es., sensibili); (iii) i soggetti che svolgono il trattamento; (iv) i ruoli privacy di tali soggetti (i.e., titolare, responsabile, con-titolare)[11]; (v) le finalità del trattamento di ogni

LA TRASPARENZA È ANCORA PIÙ IMPORTANTE QUANDO SI PARLA DELL'AMBITO IOT, POICHÉ L'INTERCONNETTIVITÀ DEGLI OGGETTI PUÒ RENDERE LA CATENA DI TRATTAMENTO DEI DATI ANCORA PIÙ DIFFICILE DA MAPPARE – OCCORRE DUNQUE PRESTARE MOLTA ATTENZIONE E BEN MAPPARE IL COSIDDETTO "DATA FLOW" (FLUSSO DEI DATI)

4 Per approfondimenti: http://www.cloudwatchhub.eu/ e https://cloudsecurityalliance.org/group/privacy-level-agreement/.
5 Il trasferimento di dati personali da paesi appartenenti all'UE verso Paesi "terzi" (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il Paese in questione garantisca un livello di protezione "adeguato"; la Commissione ha il potere di stabilire tale adeguatezza attraverso una specifica decisione (articolo 25, comma 6, della Direttiva 95/46/CE).
In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall'articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46). La Commissione europea, ai sensi dell'articolo 26(4) della Direttiva 95/46/CE, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi (le cd. clausole contrattuali standard). Si tratta di una delle deroghe (stabilite nel comma 2 dell'articolo 26 della Direttiva 95/46/CE) al divieto di effettuare il trasferimento verso Paesi che non offrono garanzie "adeguate" ai sensi della Direttiva 95/46/CE.
In pratica, incorporando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione. Nel Nuovo Regolamento Europeo questa tematica è regolata dagli articoli 41 e ss.: la legittimità del trasferimento dei dati (sempre verso Paesi extra Ue) è subordinata ad una valutazione di adeguatezza da parte della Commissione Europea circa il livello di protezione assicurato in quel determinato Stato. In assenza di tale decisione, il trasferimento potrà avvenire solo in presenza di garanzie adeguate (clausole tipo, norme vincolanti d'impresa e clausole contrattuali), o al ricorrere di particolari situazioni specificate agli artt. 42 e 44.
La decisione della Commissione Ue relativa alle clausole contrattuali standard è reperibile al seguente link http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32010D0087
6Il 12 luglio 2016 la Commissione Europea ha adottato lo scudo UE-Usa per il trasferimento dei dati personali verso gli Stati Uniti, in seguito alla sentenza della Corte di Giustizia Europea C-362/14 che il 6 ottobre 2015 che ha annullato il precedente accordo cd. Safe Harbour (meccanismo che prevedeva un sistema di volontaria adesione ai principi concordati da Ue e U.s.a sotto la supervisione della Commissione Federale per il commercio degli Stati Uniti (Federal Trade Commission). La Corte aveva osservato come in realtà la Commissione non avesse proceduto ad una constatazione della adeguatezza della protezione dei dati personali garantita dagli Stati Uniti (come richiesto dalla Direttiva in materia di protezione dei dati personali), ma si fosse limitata ad esaminare e considerare sufficiente il regime del Safe Harbor. Per ulteriori approfondimenti si vedano i seguenti link: http://europa.eu/rapid/press-release_IP-16-216_en.htm ; http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (guida sintetica per le aziende
7 Gruppo di lavoro Articolo 29. Parere 1/2010 Sui Concetti Di "Responsabile Del Trattamento" E "Incaricato Del Trattamento".; 2010. Reperibile sul sito: http://ec.europa.eu/justice/policies/privacy/docshttps://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf /wpdocs/2010/wp169_it.pdf. Ultimo accesso 14 settembre 2016.
8 ICO- Guidance on the use of Cloud Computing, https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
9 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d'ora in poi Regolamento Generale sulla Protezione dei Dati) art. 35 Valutazione d'Impatto sulla protezione dei dati. "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. 2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno. 3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. 4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68. 5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. (...).
10 Regolamento Generale sulla Protezione dei Dati, art. 25 Protezione dei Dati fin dalla progettazione e protezione per impostazione predefinita. "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. 3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo."

OCCORRE ESSERE COINVOLTI SIN DALL'INIZIO PER SVOLGERE DI REGOLA UN DATA PROTECTION IMPACT ASSESSMENT E STRUTTURARE IL TRATTAMENTO SECONDO IL PRINCIPIO DI DATA PROTECTION BY DESIGN

(con-)titolare nel breve e medio/lungo termine
3. Redigere informative trasparenti e comprensibili[12]
4. Raccogliere i consensi necessari, o individuare il corretto presupposto di legittimità del trattamento[13]
5. Assicurare un effettivo esercizio dei diritti del soggetto interessato[14]
6. Notificare / Richiedere le Autorizzazioni se necessario alle Autorità competenti[15]
7. Identificare il corretto presupposto giuridico per porre in essere trasferimenti di dati fuori dallo Spazio Economico Europe (SEE) verso paesi che non offrono un "adeguato" livello di protezione dei dati (ad esempio, tramite le Clausole Contrattuali Standard o, nei casi di trasferimento verso gli Stati Uniti, il recentemente approvato Privacy Shield)[16];
8. Porre in essere adeguate misure di sicurezza tecniche ed organizzative per proteggere I dati (NB. Rigorosa gestione delle identità e controllo degli accessi)[17]
9. Identificare e porre in essere adeguate procedure di conservazione dei dati.[18]
10. Redigere solidi accordi di protezione dei dati personali (Data Processing agreements) tra le parti coinvolte che ben identifichino i rispettivi obblighi e le relative responsabilità ;
11. Non dimenticare di formazione il personale coinvolto nel trattamento dei dati, in modo che gli sia chiaro ciò che deve fare e la creazione di chiare procedure operative scritte a supporto.

La differenza fra una società che soccomberà sotto un'imponente mole di dati - obsoleta e disorganizzata - e quella che ne riuscirà ad estrarre il loro pieno valore - attraverso controlli i qualità sui dati e organizzazione sistematica dei medesimi - sta nella gestione dei **processi** di privacy e security compliance.
Un approccio strategico alla compliance privacy può generare un significativo ritorno sull'investimento (ROI). ■

LA DIFFERENZA FRA UNA SOCIETÀ CHE SOCCOMBERÀ SOTTO UN'IMPONENTE MOLE DI DATI - OBSOLETA E DISORGANIZZATA - E QUELLA CHE NE RIUSCIRÀ AD ESTRARRE IL LORO PIENO VALORE - ATTRAVERSO CONTROLLI I QUALITÀ SUI DATI E ORGANIZZAZIONE SISTEMATICA DEI MEDESIMI - STA NELLA GESTIONE DEI PROCESSI DI PRIVACY E SECURITY COMPLIANCE. UN APPROCCIO STRATEGICO ALLA COMPLIANCE PRIVACY PUÒ GENERARE UN SIGNIFICATIVO RITORNO SULL'INVESTIMENTO (ROI)

11 Regolamento Europeo Generale sulla Protezione dei Dati, art. 4 Definizioni "(...) 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
12 Principio di liceità, correttezza e trasparenza reperibili all'art. 5.1.a Regolamento Europeo Generale sulla Protezione dei Dati; cfr. anche artt. 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato e 14 Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.
13 Regolamento Generale sulla Protezione dei Dati, artt. 6-7ss.
14 Regolamento Generale sulla Protezione dei Dati, artt. 15ss.
15 D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" artt. 17 e 37.
16 Nuovo Regolamento Generale sulla protezione dei dati, artt. 44ss.
17 Nuovo Regolamento Generale sulla protezione dei dati, artt. 32ss.
18 Nuovo Regolamento Generale sulla protezione dei dati, artt. 5.1.e. Cfr. anche artt. 13, 14 e 25