ARTICOLO

Privacy e cloud: cosa manca per l'attuazione del nuovo Regolamento Ue

Filippo Trifiletti – Direttore Generale di ACCREDIA

Con la diffusione e pervasione delle tecnologie nella nostra vita e nelle attività quotidiane, emergono nuove importanti priorità e aspetti da tenere in debita cura. Fra questi, forse il più delicato, è quello relativo alla tutela delle informazioni personali, che finiscono sulla rete. Di qui, l'esigenza di intervenire dal punto di vista normativo nel settore del *cloud computing*, per la tutela dei dati archiviati su internet.

Spesso infatti noi stessi non siamo a conoscenza di quanti dati finiscono e restano immagazzinati online, dove vengono localizzati, e soprattutto come possiamo proteggere le informazioni, che uso potrebbe esserne fatto e cosa succede se passiamo da un fornitore a un altro.

A livello comunitario e nazionale è diventata pertanto sempre più necessaria la definizione di uno standard di norme comuni, per verificare la capacità dei fornitori di tali servizi a garantire la sicurezza e la protezione dei dati, specie quelli personali soggetti alle normative sulla privacy.

A livello europeo, nel maggio 2016, è stato approvato il Regolamento UE 2016/679 sulla protezione dei dati personali e sulla libera circolazione degli stessi, che entrerà definitivamente in vigore, in tutti i Paesi dell'Unione europea, il 25 maggio 2018.

Il Regolamento introduce regole più chiare in materia di informativa e consenso, limiti al trattamento automatico dei dati personali; prevede poi che le imprese con certe caratteristiche[1] si dotino della figura del *Data Protection Officer* (Responsabile della protezione dei dati), incaricato di assicurare una gestione corretta dei dati personali. Si prevede inoltre la responsabilità dei titolari del trattamento per la violazione delle norme sulla protezione dei dati personali e le eventuali lesioni di diritti e libertà degli interessati.

Viene poi incoraggiata l'istituzione di meccanismi per la certificazione della protezione dei dati personali, e di sigilli e marchi, con l'obiettivo di dimostrare la conformità dei trattamenti effettuati dai titolari e dai responsabili del trattamento. Secondo l'articolo 42 del citato Regolamento, i soggetti legittimati a rilasciare questa certificazione sono l'Autorità di controllo competente per lo Stato (in Italia, il Garante per la protezione dei dati personali) oppure gli organismi di certificazione. Questi, secondo l'articolo 43, devono essere accreditati dall'Autorità di controllo competente oppure dall'Ente nazionale di accreditamento, che in Italia è Accredia, oppure da entrambi.

[1] In base al Regolamento (art. 37), la nomina del DPO è obbligatoria:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Ad oggi, non è stato ancora stabilito dal legislatore italiano, a chi spetti il ruolo di Ente di accreditamento, né sono stati definiti i criteri e alcuni requisiti per l'accreditamento degli organismi di certificazione, e neppure i criteri per la certificazione. Su questo, il Garante sta lavorando insieme alle altre Autorità dei Paesi UE per definire, entro l'anno, un quadro comune di criteri per accreditare gli organismi di certificazione e per la certificazione.

Accredia, dal canto suo, sta collaborando col Garante, per fornire tutta la sua esperienza in tema di accreditamento e certificazioni per garantire l'avvio delle attività entro l'entrata in vigore del Regolamento, nel maggio 2018.

Proprio per l'assenza di una disciplina definita sull'accreditamento, Accredia e Garante hanno ritenuto importante precisare che, al momento, le certificazioni di persone e tutte quelle emesse in materia di privacy e *data protection* rilasciate in Italia, sebbene possano rappresentare una garanzia o un atto di diligenza verso le parti interessate, non possono però definirsi conformi al Regolamento europeo.

Uno standard presente è l'ISO/IEC 27018, elaborato nel 2014. Su spinta della Commissione europea, delle Autorità nazionali e delle Commissioni per la protezione dei dati, ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) hanno, infatti, sviluppato e pubblicato l'ISO/IEC 27018 - *Information technology-Security techniques – Code of practice for protection of personally identifiable information in public clouds action as PII processors*.

E' il primo standard a livello internazionale che contribuisce a garantire il rispetto dei principi e norme in materia di privacy, da parte dei *provider* di *public cloud*. Questa norma infatti è indirizzata ai *service provider* di *public cloud* che elaborano dati personali (*PII-Personally Identifiable Information*) e che agiscono in qualità di *Data Processor*.

Si tratta però di Linee guida, riferite al Sistema di gestione dell'organizzazione, accreditabili in base alla norma ISO/IEC 17021 (la precisazione è importante, perché si ricorda che invece il Regolamento privacy si riferisce a certificazioni di prodotto ISO/IEC 17065) che prendono in considerazione i requisiti normativi per la protezione dei dati personali per definire i possibili rischi per la sicurezza informatica di un fornitore di servizi *cloud*. Non è quindi una norma certificabile se presa come riferimento unico, ma è possibile ottenere una integrazione del proprio certificato ISO/IEC 27001, rilasciato da un organismo di certificazione riconosciuto, per dimostrare la capacità del *provider* di assicurare la protezione dei dati personali.

Siamo quindi in attesa che a livello europeo il cosiddetto Gruppo di lavoro articolo 29 (l'Organismo consultivo composto da rappresentanti delle varie autorità nazionali che si occupano di privacy) definisca le regole per l'accreditamento, l'Italia potrebbe essere l'apripista in questo settore.

A livello comunitario, al momento, nessun Ente di normazione ha pubblicato norme o documenti para-normativi validi ai fini del Regolamento europeo sulla privacy. Il BSI (Ente di normazione inglese) ha però aggiornato la norma per la certificazione del Sistemi di gestione di una organizzazione in tema di privacy BS 10012:2017 - *Data protection. Specification for a personal information management system*. Inoltre, la Spagna si è contraddistinta con l'approvazione di un documento, non normativo, elaborato dal Garante spagnolo insieme all'Ente di accreditamento nazionale, che definisce le competenze per valutare questi organismi e i *Data Protection Officer*.

In Italia è allo studio una norma (UNI/UNINFO) per la definizione dei profili professionali relativi al trattamento e alla protezione dei dati personali, una professione intellettuale che esercitata a diversi livelli di complessità e in diversi contesti organizzativi, pubblici e privati. I profili identificati sono, oltre quello del Responsabile della protezione dei dati personali sopra richiamato, il Manager privacy, lo Specialista privacy e infine il Valutatore privacy. La norma farà riferimento alla Legge 14 gennaio 2013, n. 4, "Disposizioni in materia di professioni non organizzate".

Auspicando di far tesoro delle norme già previste in questo settore, Accredia pertanto si è messa a disposizione e fornirà al Garante e all'Ente di normazione nazionale tutto il supporto tecnico possibile, garantendo il suo *know-how* in materia di accreditamento.

Ogni giorno, infatti, verifichiamo la competenza, l'imparzialità e l'indipendenza degli organismi di certificazioni e dei laboratori che attestano la conformità di prodotti, servizi e professionisti agli standard di riferimento, facilitandone la circolazione a livello nazionale. L'accreditamento è sinonimo di garanzia e affidabilità per consumatori, mercato e Istituzioni. In più, grazie agli accordi di mutuo riconoscimento firmati a livello comunitario e internazionale coi rispettivi Enti di accreditamento, le prove di laboratorio e le certificazioni degli organismi accreditati sono riconosciute e accettate in Europa e nel mondo.

Ci sono quindi tutti gli elementi per garantire il cittadino e tutelare il suo diritto fondamentale alla sicurezza e alla protezione delle informazioni personali.

***ACCREDIA** è l'Ente unico nazionale di accreditamento designato dal Governo italiano. Il suo compito è attestare la competenza, l'imparzialità e l'indipendenza di chi deve garantire un grado elevato di protezione degli interessi pubblici, quali la salute, la sicurezza e l'ambiente.*

ACCREDIA è un'associazione privata senza scopo di lucro che opera sotto la vigilanza del Ministero dello Sviluppo Economico e svolge un'attività di interesse pubblico, a garanzia delle istituzioni, delle imprese e dei consumatori.

ACCREDIA ha 67 soci che rappresentano tutte le parti interessate alle attività di accreditamento e certificazione, tra cui 9 Ministeri (Sviluppo Economico, Ambiente, Difesa, Infrastrutture e Trasporti, Interno, Istruzione, Lavoro, Politiche Agricole, Salute), 7 Enti pubblici di rilievo nazionale, i 2 Enti di normazione nazionali, UNI e CEI, 13 organizzazioni imprenditoriali e del lavoro, le associazioni degli organismi di certificazione e ispezione e dei laboratori di prova e taratura accreditati, le associazioni dei consulenti e dei consumatori e le imprese fornitrici di servizi di pubblica utilità come Ferrovie dello Stato ed Enel.

L'Ente è membro dei network comunitari e internazionali di accreditamento ed è firmatario dei relativi Accordi di mutuo riconoscimento, in virtù dei quali le prove di laboratorio e le certificazioni degli organismi accreditati da ACCREDIA sono riconosciute e accettate in Europa e nel mondo.

Articolo pubblicato su www.agendadigitale.eu del 15 settembre 2017