Cybersecurity e P.A.: i principi, le norme ed i provvedimenti in materia

Prof. Avv. Michele Iaselli

Ministero della Difesa

Negli ultimi tempi si è assistito ad una rapida evoluzione delle minacce in campo informatico (v. anche minacce cibernetiche) ed in particolare per quelle incombenti sulla pubblica amministrazione, che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

Se da un lato la PA continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attività condotte da gruppi organizzati, non solo di stampo propriamente criminale.

Le pubbliche amministrazioni, dal punto di vista sicurezza, possono essere considerate come organizzazioni fortemente regolate, in considerazione del fatto che la loro attività si svolge nell'ambito e nei limiti di norme che hanno valore di legge. Il problema è che fino ad oggi sono state poche le norme giuridiche che si siano occupate di cyber security.

In effetti le norme di maggiore rilevanza sono quelle contenute nel Codice dell’Amministrazione Digitale (CAD - D.Lgs. 7 marzo 2005 s.m.i.), che all’art. 17 al fine di garantire l’attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell’amministrazione definite dal Governo, prevede che le pubbliche amministrazioni individuino mediante propri atti organizzativi, un unico ufficio dirigenziale generale responsabile del coordinamento funzionale.

Questo Ufficio sostituisce il Centro di competenza previsto dalla normativa previgente e il responsabile dei sistemi informativi automatizzati di cui all’articolo 10 del decreto legislativo 12 febbraio 1993, n. 39. Inoltre alla luce della recente riforma del CAD (d.lgs. n. 179/2016) lo stesso ufficio deve assicurare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Naturalmente anche l'Agenzia per l'Italia Digitale (AgID) deve assicurare il coordinamento delle iniziative nell’ambito delle attività di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica con particolare riferimento al Sistema Pubblico di Connettività.

Nei successivi articoli 50 e 51 del CAD si parla rispettivamente di disponibilità ed accessibilità dei dati al di fuori dei limiti di carattere normativo come nel caso della protezione dei dati personali, di sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, oggi regolamentati dalle misure minime di sicurezza previste dalla normativa sulla protezione dei dati personali.

In materia, difatti, occorrono ulteriori regole tecniche che in coerenza con la disciplina in materia di tutela della privacy introducano elementi utili per riconoscere l’esattezza, la disponibilità, l’integrità e per verificare l’accessibilità e la riservatezza dei dati.

Proprio per questi motivi è stata pubblicata sulla G.U. (Serie Generale n. 79 del 04/04/2017) la **Circolare AgID del 17 marzo 2017 n. 1/2017** contenente le "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

Le stesse misure sono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, emesso come previsto dalla **Direttiva 1 agosto 2015** del Presidente del Consiglio dei Ministri, che assegna all'Agenzia per l'Italia Digitale il compito di sviluppare gli standard di riferimento per le amministrazioni.

Tale Direttiva in considerazione dell’esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, sollecita tutte le Amministrazioni e gli Organi chiamati ad intervenire nell’ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici.

In tale ottica assume rilevanza anche **la nuova direttiva sulla protezione cibernetica e la sicurezza informatica nazionale** emanata con DPCM del 17 febbraio 2017 (pubblicato sulla GU n. 87 del 13-4-2017) che si pone l’obiettivo di aggiornare la precedente direttiva del 24 gennaio 2013 e di conseguenza anche la relativa architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche.

L’esigenza di un nuovo provvedimento nasce innanzitutto dall’emanazione della **direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS) nonché da quanto previsto dall'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla **legge n. 198 del 2015**, al fine di ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento.

Del resto lo stesso art. 51 del CAD specifica che l’AgID attui, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:

a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni.

La nuova dimensione della sicurezza e della privacy

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Le diverse questioni emerse nella materia in esame hanno confermato peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell’Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all’estero.

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso, quindi, necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale.

Tale processo è stato avviato, in Italia, già con il Codice per la protezione dei dati personali che ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, ha adottato un approccio “tecnologicamente neutro”, ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

Ma tale processo di adeguamento normativo ha compiuto un altro passo importante con il 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 (Regolamento generale sulla protezione dei dati) pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell’Unione Europea dei dati.

Come prevede l’art. 99 il Regolamento entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016), ma si applicherà a decorrere dal 25 maggio 2018.
L’iter di questo Regolamento, che entrerà direttamente in vigore nei singoli Stati membri dell'UE, è stato molto sofferto e sono passati ben quattro anni dalla prima proposta della Commissione Europea. Un testo inizialmente molto severo è stato reso più “digeribile” nel corso degli anni, anche se rimangono confermati i principi fondamentali del provvedimento europeo.

La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla proprio continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.

Originariamente la direttiva 95/46/CE, pietra angolare nell’impianto della vigente normativa dell’UE in materia di protezione dei dati personali, è stata adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri.
Successivamente incalzanti sviluppi tecnologici hanno allontanato le frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso.

La tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano. Le nuove tecnologie non hanno trasformato solo l’economia, ma anche le relazioni sociali.

È diventato, quindi, necessario instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche.

Nell’attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. *persona elettronica* (v. identità digitale) attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

Si deve precisare innanzitutto che l’obiettivo delle nuove tecnologie è quello di migliorare la qualità della vita dei cittadini nel rispetto della sicurezza e della privacy. Qualsiasi problematica inerente i rapporti tra nuove tecnologie e privacy va sempre risolta inquadrandola nell’ambito di una considerazione globale dei benefici socio-economici che scaturiscono dall’innovazione tecnologica. Ad esempio non possono trascurarsi i grandi vantaggi rappresentati dalle banche dati presenti in Rete oltre che nello svolgimento dell’attività amministrativa, anche nel migliorare in generale la qualità della vita dei cittadini e nel promuovere le attività produttive ed economiche.

Lo stesso discorso va necessariamente fatto con riferimento ad Internet ed in particolare al web 2.0.

L’avvento del web 2.0 (ma si parla già di web 3.0 e 4.0) inteso come evoluzione della rete e dei siti internet caratterizzata da una maggiore interattività che pone l’utente al centro della rete ha evidenziato ancora di più gli aspetti descritti in precedenza.

Difatti Internet non è più una semplice "rete di reti", né un agglomerato di siti Web isolati e indipendenti tra loro, bensì la summa delle capacità tecnologiche raggiunte dall’uomo nell’ambito della diffusione dell’informazione e della condivisione del sapere.

E’ naturale che in considerazione proprio di queste nuove potenzialità di Internet, è necessario un giusto ed equilibrato bilanciamento tra principi sacrosanti come la tutela della libertà di manifestazione e circolazione del pensiero e la tutela di altri interessi giuridicamente rilevanti, come la riservatezza, che assumono anch’essi un rango di carattere costituzionale e potrebbero essere lesi da un esercizio sconsiderato della libertà in questione.

E’ ovvio che la soluzione vada trovata caso per caso di fronte ad un potenziale conflitto, cercando di tutelare l’interesse ritenuto preminente.

I contenuti creati dagli utenti e resi pubblici attraverso il mezzo telematico, costituiscono un potenziale veicolo di violazioni degli interessi di terzi e in questo senso una minaccia per diritti quali l’immagine, l’onore e la reputazione, nonché la riservatezza.

Come messo in risalto da alcuni interpreti, la rete, che per sua natura tende a connettere individui, formazioni sociali e istituzioni di ogni genere, pone questioni “inquietanti” in quanto risolvibili solo con nuovi approcci, soluzioni mai adottate prima e in taluni casi non ancora individuate.

In considerazione delle caratteristiche di accesso di particolari strumenti del web 2.0 ma anche di banche dati presenti in rete, legati alle tradizionali credenziali di autenticazione (user id e password) assume particolare rilevanza la problematica della clonazione dei profili: attraverso semplici procedure, peraltro illustrate in rete, è possibile accedere al profilo di un determinato utente e agire per conto di questo.

Le ipotesi di reato collegate a simili forme di abuso possono essere le più varie ma si riconducono tutte senz’altro al furto di identità che negli ultimi tempi sta preoccupando particolarmente l’Autorità per la protezione dei dati personali.

Altra tipica rappresentazione del furto d’identità è il phishing che è un tipo di frode ideato proprio allo scopo di rubare l'identità di un utente. Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa.

Il Garante sta esaminando questo problema del furto d’identità con viva preoccupazione ponendo la sua attenzione in tutti quei settori particolarmente delicati collegati alle nuove tecnologie come le manipolazioni genetiche e l’utilizzo dei sistemi biometrici nel campo della sicurezza.

Come è noto le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare.

In tema di accessi informatici i sistemi biometrici rappresentano la ricerca più avanzata nel campo della sicurezza. Alcune caratteristiche fisiche dell’utente autorizzato all’accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Di fronte alla rapida ascesa di tali metodologie il Garante sta assumendo un atteggiamento particolarmente rigido in quanto spesso le finalità di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano resa possibile dall’innovazione tecnologica.

Vanno garantiti sempre il rispetto della dignità della persona, il rispetto dell’identità personale, il rispetto dei principi di finalità e di proporzionalità ed infine la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ma il phishing come si è detto in precedenza è innanzitutto una vera e propria frode di carattere informatico e si ricorda che l’art. 10 della Legge 547/93 ha inserito nel corpo delle norme penali in tema di truffa la specifica ipotesi di frode informatica.

Lo stesso non si può dire per altre tipologie di furti d’identità in rete che non vengono inquadrate in specifiche figure di reato riconosciute dal nostro ordinamento e solitamente si fanno rientrare nell’ambito del Capo IV del Titolo VII del Codice penale: Dei delitti contro la fede pubblica – falsità personali.

Solo di recente con il DL 14 agosto 2013, n. 93**,** convertito dalla L.15 ottobre 2013, n. 119 è stata introdotta, per la prima volta, nel codice penale, la nozione di "identità digitale", prevedendo un'aggravante per il delitto di frode informatica (art. 640 ter), "*se il fatto è commesso con furto o indebito utilizzo dell'identita' digitale in danno di uno o piu' soggetti*". Si tratta per di più di un'aggravante a effetto speciale, in quanto prevede la pena della reclusione da due a sei anni e della multa da euro 600 a euro 3.000.

Nuovi Principi Generali
del Regolamento Europeo

Il principio di Trasparenza

(art. 12)

Il principio di accountability (art. 24)

Il principio della privacy by design e by default (art. 25)