PUBBLICA AMMINISTRAZIONE 24

The endless paper

Nonostante tutto il digitale avanza

Ottobre 2015

GRUPPO 24 ORE

Sommario

L'Agenda digitale ha bisogno di nuove leggi o di professionisti capaci?

Andrea Lisi *

** Presidente Anorc*

L'Italia galoppa verso **orizzonti sempre più digitali**, almeno dal punto di vista della produzione normativa. Gli ultimi mesi (come del resto gli ultimi anni) sono stati caratterizzati da un impetuoso e costante flusso di normative, primarie e secondarie, che in un modo o nell'altro toccano il mondo digitale, senz'altro in voga in questi ultimi anni. Ormai non c'è Finanziaria o normazione d'urgenza che non abbia al suo interno un articolo che infiammi gli animi con nuove proposte dal punto di vista dell'**innovazione digitale**.

Questa alluvione normativa non sempre si è tradotta in reale innovazione, purtroppo. Anzi, l'**assenza di sanzioni specifiche in capo alla PA** in caso di inadempimento, la previsione costante che la digitalizzazione per l'ente pubblico debba essere a costo zero (anzi perseguire logiche di risparmio) e l'inevitabile contraddittorietà di un sistema normativo in costante evoluzione, contribuiscono ad **alimentare il caos piuttosto che a favorire una reale informatizzazione** amministrativa che guardi davvero verso servizi digitali in favore di cittadini e imprese. In verità, l'attuale, avvilente situazione non costituisce una novità se solo si ricorda la locuzione latina di Tacito *Corruptissima re publica plurimae leges*.

Le norme da tempo si accavallano con eccessiva fretta, spesso smembrando la sistematicità che dovrebbe animare un Codice. Faccio riferimento ovviamente al Codice dell'amministrazione digitale che ormai somiglia sempre più a un **campo minato** piuttosto che a un rigoglioso giardino dove raccogliere i frutti dell'innovazione. Si pensi, ad esempio, alla legge 6 agosto 2015 n. 125 (recante disposizioni urgenti in materia di enti territoriali) che per l'ennesima volta ha messo mano alle ormai infinite questioni dell'Anagrafe nazionale della popolazione residente e della Carta d'identità elettronica, che erano state recentemente oggetto di ennesimi interventi normativi di – presunto - riordino.

Si ha la **sensazione** sempre più spiacevole **che i nostri Governi procedano alla cieca**, mossi da esigenze di comunicazione piuttosto che da una reale analisi strategica di fabbisogni concreti e scenari futuri.

Le modifiche al Cad

Un barlume di speranza può ancora essere alimentato nel momento in cui si legge - con un pò di ottimismo che speriamo di non dover ritenere folle – l'**articolo 1** (rubricato Carta della cittadinanza digitale) contenuto nella **legge delega 7 agosto 2015, n. 124**, in materia di riorganizzazione delle amministrazioni pubbliche.

In questo importante articolo, il Governo si impegna "*ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, con invarianza delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, uno o più decreti legislativi volti a* ***modificare e integrare****, anche disponendone la delegificazione,* ***il codice dell'amministrazione digitale****, di cui al decreto legislativo 7 marzo 2005, n. 82, di seguito… Cad, nel rispetto dei seguenti principi e criteri direttivi"*. Senz'altro l'ennesima specificazione circa "*l'invarianza delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente*" può far storcere il naso all'attento lettore, ma confidiamo nel fatto che questo sia un *modus operandi* necessario per una legge delega di tale portata. In ogni caso, la lett. *m)* dell'articolo 1 è profondamente corretta nel momento in cui specifica che occorre necessariamente "***semplificare*** *le modalità di adozione delle regole tecniche e assicurare la neutralità tecnologica delle disposizioni del Cad, semplificando allo stesso tempo il Cad medesimo in modo che contenga esclusivamente principi di carattere generale"*.

Il decreto legislativo n. 82/2005 va reso davvero un Codice perché ad oggi non lo è mai stato realmente. E in questa stessa direzione va la lett. *o)* del predetto articolo 1, col quale si vuole garantire con questo o questi ennesimi e futuri decreti legislativi una **maggiore coerenza e** un **migliore coordinamento con il dettato europeo** (decreti resisi urgenti in seguito alla pubblicazione il 28 agosto 2014 nella Gazzetta Ufficiale dell'Unione europea del Regolamento (Ue) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno - che abroga la direttiva 1999/93/Ce - noto con l'acronimo di eIDAS - *electronic IDentification Authentication and Signature*) e con le tante, troppe norme italiane che trattano la materia del digitale.

Osservazioni finali

Sostanzialmente favorevoli si può essere, in verità, a tutti gli altri punti contenuti nell'art. 1, laddove nella loro inevitabile genericità mirano a fare ordine nel caos, cercando anche di affidare al Governo la definizione più precisa di **strumenti di controllo e valutazione** (trasparenti e appunto digitalizzati) delle performance. Forse ci si sarebbe aspettati un maggior coraggio nel preannunciare finalmente un **reale sistema sanzionatorio** per chi in materia di digitale procede ostinatamente a passo di gambero ormai dagli anni '90. Insomma, se si vuole essere positivi occorre sperare che il legislatore si sia finalmente reso conto del fatto che non si può andare avanti sommando algebricamente norme su norme e che **occorra invece fare ordine** e, anche attraverso le norme, semplificare. Ma le sole leggi non bastano per fare innovazione.

Infatti, ciò che può far ben sperare (o risultare pericolosissimo) è la lett. *n)* dell'articolo 1, laddove finalmente si inizia a parlare in Italia di **competenze professionali necessarie per la PA** che voglia davvero digitalizzarsi come la normativa da tempo richiede. Il Governo si impegna, infatti, a "*ridefinire le competenze dell'ufficio dirigenziale di cui all'articolo 17, comma 1, del Cad, con la previsione della possibilità di collocazione alle dirette dipendenze dell'organo politico di vertice di un responsabile individuato nell'ambito dell'attuale dotazione organica di fatto del medesimo ufficio, dotato di adeguate competenze tecnologiche e manageriali, per la transizione alla modalità operativa digitale e dei 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*".

La direzione intrapresa sembra essere quella di prevedere per ogni pubblica amministrazione un **Manager dell'innovazione digitale**, un professionista, cioè, della digitalizzazione documentale al servizio dei processi digitali, che non sia - ed è qui che si può vincere o perdere la battaglia - al servizio della politica, e non funga solo da specchietto per le allodole contribuendo a determinare l'ennesimo, completo fallimento nel campo dell'innovazione di cui l'Italia non ha assolutamente bisogno.

Costruiamo allora questa **nuova professionalità**, impegniamoci tutti a farlo in maniera corretta, multidisciplinare, superando gli steccati ordinistici e le barriere già erette dalle professioni più tradizionali. Il nostro Paese ha bisogno di professioni nuove, che poggino senz'altro sulle fondamenta di quelle precedenti, ma superandole e cercando di guardare molto più lontano. Anorc Professioni, ad esempio, ha sviluppato una sua proposta, presentata agli organi competenti anche in materia di normativa tecnica alla luce della legge n. 4/2013 ("Disposizioni in materia di professioni non organizzate"), illustrata e giudicata in modo positivo dal Comitato tecnico-scientifico della Coalizione nazionale delle competenze digitali durante la presentazione del progetto effettuata in data 17 settembre 2015.

C'è **ancora molta strada da fare**, ma bisogna intraprenderla con coraggio e senza se e senza ma, perché mai come oggi vale il monito che ci ha consegnato Aldo Moro: "*Siate indipendenti. Non guardate al domani, ma al dopodomani*".

L'AGENDA DIGITALE HA BISOGNO DI NUOVE LEGGI O DI PROFESSIONISTI CAPACI?
(Andrea Lisi)

Al DIG.Eat 2015 si parlerà di Agenda digitale e normativa di riferimento nella tavola rotonda
Stairway to heaven: i gradini normativi verso l'Italia digitale

Sala Auditorium, ore 10.00-13.00

Le competenze digitali della PA: quelle che sono e quelle che dovrebbero essere

Luca Attias * e Fabio Cristofari **

** Cio Dgsia Corte dei conti*
*** Funzionario informatico Dgsia Corte dei conti*

In Italia viviamo, ormai, in un **contesto di "emergenza digitale"**: si tratta, di fatto, dell'unica emergenza trasversale che, se non verrà affrontata una volta per tutte in modo serio e risolutivo, non consentirà neppure in parte di combattere le numerose altre emergenze di questo Paese che, anche per questo motivo, resteranno irrimediabilmente tali.

Vogliamo soffermarci più specificatamente su uno degli aspetti dell'emergenza digitale: l'**emergenza occupazionale nel settore digitale**, con riferimento ai *digital skills*.

Il numero di occupati nel digitale negli ultimi anni è diminuito soprattutto in Italia rispetto a quanto è avvenuto negli altri paesi della Ue. Sebbene in valore assoluto non siano pochi gli impiegati nell'IT nel nostro Paese, è un dato di fatto che molti di essi siano male impiegati.

Il caso della pubblica amministrazione

Analizziamo, in particolare, il caso della PA, partendo dall'ormai folle numero di **data center** pubblici (anche se, a fatica, la maggior parte di essi si può definire tale). Questo numero, tra censiti e non, è notoriamente maggiore di 10mila ed in questi Ced sono impiegate almeno 30mila persone per l'infrastruttura di base e molte di più sono quelle che si occupano delle relative applicazioni infrastrutturali e trasversali; sono quasi introvabili in questo ambito, invece, gli **esperti di cloud**.

Ma, se la **situazione** infrastrutturale è decisamente complessa, quella **applicativa** appare tragica e forse irrisolvibile.

Nella nostra PA sono state sviluppate un numero spaventoso di applicazioni non interoperabili, che fanno le stesse cose, sulle stesse norme ed in modo completamente diverso. In Italia abbiamo migliaia di esperti di protocollo, di sistemi *custom* di gestione documentale, di gestione del trattamento giuridico, di controllo di gestione; abbiamo ancora qualcuno che pensa di poter fare da sé sulla contabilità finanziaria ed analitica e sul trattamento economico; e abbiamo **pochissime persone**, invece, che **si occupano di open data e di Big Data**, di sistemi conoscitivi, di *Internet delle cose* (Iot), di *Data Driven Decision*, di *Programmatic Buying Management*, di *e-Commerce Management*, di *Web Marketing Management*, di *Seo/Sem Management*, e quasi non esistono *Chief Technology Officer*, *digital architec, cloud integrator* e così via.

La frammentazione, unita all'individualismo degli enti, ha creato una **situazione caotica** nel digitale che non ha altri corrispettivi nel mondo; abbiamo degli ordini di grandezza che farebbero tremare anche Paesi come la Cina, l'India e gli Stati Uniti, ma a tutto ciò rimaniamo incredibilmente indifferenti!

Paradossalmente, sarebbe meglio non aver proprio nulla e poter partire da zero, come hanno fatto alcuni paesi che hanno copiato i sistemi più efficienti sul mercato senza il peso di normative preesistenti. Un pò come ha fatto l'Estonia, che, dal nulla, è diventato uno dei paesi digitali più avanzati al mondo sul fronte pubblico. **Capovolgere il sistema italiano è un'impresa dura**: abbiamo troppe normative, troppe applicazioni, troppe infrastrutture, troppi addetti e nessuna *governance*.

Abbiamo creato una quantità enorme di occupazione non sana (parliamo di diverse centinaia di migliaia di individui che operano nel pubblico e nel privato) che in molti casi risulta essere dannosa e per la quale si spendono somme ingenti.

Allora, avendo sviluppato *software* sbagliato (**"digitale sbagliato"** rende ancora più l'idea…) non si sono sviluppati i mercati informatici sani ed è anche per questo che si è persa competitività e, inevitabilmente, occupazione.

Non è più possibile giustificare l'occupazione sbagliata con la necessità di dare lavoro, perché è una politica perdente. L'assistenzialismo occupazionale, in genere clientelare, è un suicidio tutto italiano che conduce a risultati tragici nelle classifiche internazionali. Dobbiamo assolutamente e con urgenza **riqualificare con progettualità il lavoro** improduttivo e dannoso.

Il gap tra esperti IT e non-IT

Nel campo delle "competenze digitali" abbiamo però anche un altro problema di fondo da affrontare e gestire in modo

strutturale, per acquisire la consapevolezza di vivere l'emergenza digitale e, forse, risolverla: è il **gap culturale** esistente tra il mondo degli esperti IT e non-IT.

Questo *gap* è generato essenzialmente da **fattori di ordine culturale** che, se sommati alle cronicità storiche del nostro Paese - raccomandazioni, qualità della classe dirigente, corruzione di varia natura e a vari livelli – diventano drammaticamente dirompenti e causa dello sprofondamento dell'Italia nei diversi *rating* di settore.

A chiarimento di quanto affermato, riportiamo un piccolo elenco (che può essere allargato a piacere) esemplificativo delle aberranti, ma divertenti, **affermazioni e considerazioni**, totalmente confutabili in letteratura, espresse in assoluta buona fede da personale interno ed esterno ad una delle amministrazioni pubbliche riconosciute tra le più avanzate del settore informatico pubblico:

- "Perché non internalizziamo i servizi informatici"?
- "I soldi che spendete in questo settore sono troppi!"
- "Perché non assumiamo dei laureati in informatica e poi li mettiamo a fare "*data entry*" sui sistemi informativi?"
- "Le mie informazioni sono al sicuro solo sulla mia *pen-drive*!"
- "Il nostro Ced deve essere posizionato all'interno del nostro edificio per motivi di sicurezza"
- "Quest'anno non ci sono i soldi: dobbiamo spegnere quel sistema o quel servizio"
- "Gli oneri informatici sono tutti rimodulabili"
- "Pretendo il sistema informativo entro quindici giorni!"

Il filosofo digitale

È in questo contesto che nasce, con la giusta dose d'ironia, l'inedita teoria del cosiddetto filosofo digitale: "*come tutti sono in grado di capire, da quando esiste l'Uomo, concetti fondamentali legati all'alimentazione, alla salute (la medicina), ai trasporti e a ciò che si muove intorno a queste scienze umane, oggi come oggi deve essere così anche per l'informatica, anche senza necessariamente essere degli addetti ai lavori*".

È triste constatare, invece, come molti manager pubblici sostengano con convinzione le **palesi assurdità riportate nell'elenco** di cui sopra. Tali atteggiamenti non sono più ammissibili poiché alcune scelte nel campo dell'informatizzazione sono scelte oramai strategiche e di competenza del *business* e non solo degli organismi e delle strutture tecniche che devono solo fornire il supporto alle decisioni. Non è un caso infatti che la maggior parte del *budget* discrezionale delle amministrazioni è allocato, da diversi anni, proprio sul settore informatico.

La teoria del "filosofo digitale" porta a sostenere che, ormai, un manager di una qualsiasi organizzazione, dovrà necessariamente **confrontarsi**, nello svolgimento del proprio lavoro, **con l'informatica e con l'utilizzo di uno più sistemi informativi**, indipendentemente dalla propria formazione culturale e professionale. Egli dovrà aver chiara una serie di elementi, culturali e metodologici, riguardanti questa complessa materia, che diano supporto e maggiore consapevolezza per la risoluzione di alcune delle problematiche connesse alla gestione del proprio lavoro in rapporto con *l'Information Technology*.

Non servirà allora una sovrapproduzione di norme e regolamenti informatici, anche importanti - perlopiù disattesi nella loro *execution* – senza questa **"acquisizione di consapevolezza manageriale informatica da parte della classe dirigente del paese"**: tutto ciò diverrebbe paradossalmente ed inevitabilmente dannoso.

In conclusione, se non si avrà coscienza pubblica del fatto che, ormai, la civiltà di un Paese deve misurarsi anche dal **grado di digitalizzazione raggiunto**, allora vivremo sempre in un drammatico contesto di emergenza digitale, purtroppo ancora inconsapevole.

LE COMPETENZE DIGITALI DELLA PA: QUELLE CHE SONO E QUELLE CHE DOVREBBERO ESSERE (Luca Attias e Fabio Cristofari)

Al DIG.Eat 2015 le competenze digitali saranno al centro del dibattito dell'incontro
This must be the place: diamo alle competenze digitali il posto che meritano

Sala Auditorium, ore 14.00-15.00

Il procedimento amministrativo tra digitale e gestione documentale

Gianni Penzo Doria *

** Vice Presidente Anorc, Direttore generale dell'Università degli Studi dell'Insubria*

Cinque lustri: la **legge** 7 agosto 1990, **n. 241**, "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" *(in GU n. 192 del 18 agosto 1990)* ha da poco compiuto 25 anni e non li dimostra.

Un quarto di secolo di riforme: 7 agosto 1990-2015

Abbiamo di fronte, infatti, un articolato di norme che ha rivoluzionato – e che continua a rivoluzionare – i rapporti tra cittadini e imprese da una parte e amministrazioni pubbliche dall'altra, estirpando sempre più il sentimento di sudditanza verso quest'ultime. Si tratta, in concreto, di un'infrastruttura giuridica che ha subito un'evoluzione costante con il mutare della dottrina e della giurisprudenza, al passo con il cambiamento sociale e tecnologico. Ciò che oggi qualifica particolarmente l'istituto della **trasparenza amministrativa**, tuttavia, è la concentrazione del *focus* della **nuova "disclosure" sul procedimento amministrativo**, che deve risultare permeabile e percepito dalla collettività.

È in questa direzione che si comprendono le impegnative previsioni contenute negli **articoli 23 e 35 del Dlgs n. 33/2013**, a mente delle quali le amministrazioni sono obbligate a pubblicare gli elementi essenziali dei procedimenti, quali i termini, i responsabili, gli atti e i documenti da allegare all'istanza, per fare solo alcuni esempi, in un'ottica di trasparenza e, al contempo, di controllo diffuso sull'utilizzo delle risorse.

Dunque, l'impianto di una delle leggi cardine dell'ordinamento italiano regge ancora, pur con periodiche integrazioni, considerato che la modifica più recente ai rapporti tra trasparenza e procedimenti è rinvenibile nella **legge 7 agosto 2015, n. 124**, contenente le *Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*.

Infatti, la novella prescrive di *"ridefinire e semplificare i procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio 'innanzitutto digitale'"* (**digital first**), nonché l'organizzazione e le procedure interne a ciascuna amministrazione» (articolo 1, comma 1, lett. *b*).

Si vuole ribadire, pertanto, l'**intima connessione con il digitale**, al punto che la parola *procedimento* registra nella stessa legge una trentina di ricorrenze. Ciò comporta l'impossibile dissociazione di un'amministrazione moderna dalla mappatura, dalla semplificazione e dalla digitalizzazione dei procedimenti amministrativi.

E, come se non bastasse, molti sono i rinvii a provvedimenti legislativi di competenza dell'Esecutivo che entro un paio di anni dovrebbero aver consentito il riordino, la semplificazione e l'accelerazione di alcuni procedimenti critici (articolo 4). Da ultimo, non si può non notare l'**abbinamento delle tematiche digitali a quelle inerenti corruzione**, **pubblicità e trasparenza**, attive in un pensiero centrale anche attraverso la modifica dello stesso Dlgs n. 33/2013 (articolo 7), che tra poco esamineremo.

Il digitale e la riforma della PA

Ora, a che punto siamo? Può il digitale concorrere alla crescita del Paese **partendo**, ad esempio, **dai procedimenti** come punto centrale della riforma, oggi come ieri?

La risposta è certamente positiva, ma a **due condizioni**. In primo luogo, serve il **consapevole utilizzo del digitale nativo**, posto che gli adempimenti previsti possono essere portati a termine soltanto attraverso l'informatica; in seconda istanza, gli scienziati dell'organizzazione devono poter incidere in un campo solo apparentemente appannaggio del diritto amministrativo e intersecarsi, in una **visione trasversale**, con giuristi, archivisti, diplomatisti e informatici.

In poche parole, è **impensabile il lavoro** a silos, **a compartimenti stagni**, a segmenti autistici autoreferenziali all'interno delle amministrazioni pubbliche.

Il contesto normativo

In tema procedimentale la legge n. 241/1990 rappresenta la pietra angolare, ma non è l'unica fonte. Serve, quindi, una

consapevolezza sui numerosi adempimenti richiesti, in una logica di processo trasversale indipendente da uffici o ruoli cristallizzati.

Ci sono, infatti, almeno **altre tre normative regolatrici**. Il primo riferimento ineludibile è il **Dpr 28 dicembre 2000, n. 445**, in tema di sistema documentale e di protocollo informatico: qui emerge chiaro il concetto del *records management,* con un impatto imprescindibile non soltanto sui modelli organizzativi, ma anche sulla efficacia e sull'affidabilità dell'azione amministrativa.

Ulteriormente, non possono mancare i rinvii al **Dlgs 7 marzo 2005, n. 82** e, nello specifico, all'articolo 41, sui rapporti tra procedimento amministrativo e fascicolo informatico. Con l'avvento del digitale, infatti, i rapporti tra cittadini e amministrazioni pubbliche hanno subito un'accelerazione costante, all'interno di un minore formalismo nelle comunicazioni, anche se non del tutto scevro da ambiguità giuridiche, soprattutto dal lato dell'evidenza probatoria.

Infine, è indispensabile la padronanza di un tassello imprescindibile della riforma, contenuto nel **Dlgs n. 33/2013**, con particolare riferimento agli adempimenti inerenti alla tabella dei procedimenti amministrativi.

È bene sgombrare il campo da eventuali fraintendimenti: le normative richiamate sono solo la **base del sistema procedimentale digitale**, il quale convive con il nostro complessivo sistema ordinamentale e con le esigenze emerse ed emergenti; due esempi tra tutti: il Codice privacy contenuto nel Dlgs n. 196/2003 e le disposizioni anti-corruzione contenute nella legge n. 190/2012.

Il Dpr 28 dicembre 2000, n. 445

Figlia della Riforma Bassanini e inizialmente contenuta nell'abrogato Dpr n. 428/1998, la normativa in materia di **gestione documentale e di protocollo informatico** è confluita - tuttora senza alcuna modifica o integrazione - nel Titolo IV del Dpr n. 445/2000.

Il sistema documentale serve ad attribuire certezza giuridica riguardo alla data (topica e cronica) e alla provenienza di un documento. Questo non si risolve in una semplice segnatura da apporre o da associare al documento, ma - in un sistema di misurazione delle performance (Dlgs n. 150/2009) o di verifica dei tempi di avvio o di esecuzione dello stesso procedimento (articolo 2 della legge n. 241/1990) - costituisce una **garanzia** come terza parte fidata. Del resto, che senso ha produrre e conservare documenti per i quali sussistono dubbi in merito alla loro affidabilità?

Inoltre, la **tempestività** con la quale il sistema documentale comunica con il responsabile del procedimento (articoli 5 e 6 della legge n. 241/1990) è di fondamentale ausilio nei casi in cui il fattore tempo è essenziale (si pensi ai termini per una costituzione in giudizio) o in quelli in cui anche un solo giorno di ritardo potrebbe determinare negativamente l'efficacia di un provvedimento adottato; ciò senza considerare i problemi risarcitori o di indennizzo del danno da ritardo. In concreto, la **gestione affidabile dei documenti** è il **fulcro giuridico-amministrativo delle amministrazioni pubbliche**.

Il Dlgs 7 marzo 2005, n. 82

Il Codice dell'amministrazione digitale rappresenta il caso limpido dell'importanza di una corretta gestione del procedimento amministrativo. Esso, infatti, risulta rappresentato e formalizzato in maniera autentica nel rispettivo fascicolo informatico.

Infatti, il Cad ha evidenziato uno stretto legame tra i documenti, il fascicolo e il procedimento, rimarcando le interrelazioni su fronte dell'agire pubblico: *"La pubblica amministrazione titolare del procedimento raccoglie in un **fascicolo informatico** gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241"* (Dlgs n. 82/2015, articolo 41, comma 2). Inequivocabile.

Il Dlgs 14 marzo 2013, n. 33

Anche il Dlgs n. 33/2013, meglio noto come decreto Trasparenza, esplicita diffusamente i legami appena descritti, soprattutto alla luce degli articoli 23 e 35.

Infatti, *"Per ciascuno dei provvedimenti compresi negli elenchi di cui al comma 1 sono pubblicati il contenuto, l'oggetto, la eventuale spesa prevista e gli estremi relativi ai principali documenti contenuti nel fascicolo relativo al procedimento"* (Dlgs n. 33/2013, articolo 23, comma 2).

Di conseguenza, documenti, fascicolo e procedimento rappresentano una *triade perfetta* per la trasparenza amministrativa e la loro mappatura, unita a un aggiornamento costante, rappresentano un binomio di efficienza.

Conclusioni

Nonostante qualche incertezza tecnica, siamo di fronte a un **assetto normativo coerente**, indirizzato all'applicazione della trasparenza attraverso documenti, procedimenti e fascicoli. L'**attuazione** piena, tuttavia, non può prescindere dalla **digitalizzazione completa delle procedure**, in quanto tassello indefettibile.

Del resto, gli adempimenti previsti sono realizzabili esclusivamente se le amministrazioni divengono *digital by default*. Assurdo sarebbe il ritenere di continuare a proclamare efficacia e trasparenza senza **mettere mano al sistema documentale e procedimentale**.

Infatti, in base al *principio di documentalità*, le amministrazioni pubbliche si estrinsecano *per tabulas*, cioè attraverso la **formalizzazione** dei loro **atti in documenti conservati ordinatamente in fascicoli e serie**. Come può un'amministrazione pubblica dirsi al passo con i tempi se non ha piena contezza della mappatura, della tempistica e delle criticità delle azioni che svolge? Tutto il resto è accozzaglia di idee priva di concretezza, perché la trasparenza passa per documenti, fascicoli e procedimenti in ambiente digitale.

IL PROCEDIMENTO AMMINISTRATIVO TRA DIGITALE E GESTIONE DOCUMENTALE
(Gianni Penzo Doria)

Al DIG.Eat 2015 la digitalizzazione dei processi della PA sarà argomento di dibattito nella tavola rotonda Stairway to heaven: i gradini normativi verso l'Italia digitale

Sala Auditorium, ore 10.00-13.00

Condivisione e riutilizzo delle informazioni pubbliche: nuove norme per un impulso all'economia digitale

Sarah Ungaro *

* *Digital&LawDepartment*

La **normativa** sul riutilizzo di dati, informazioni e documenti nel settore pubblico **cambia**. Forse solo dal momento che, come spesso accade, dobbiamo adeguarci a una **direttiva** europea (nello specifico, la **2013/37/Ue**), o forse anche perché qualcosa davvero sta cambiando grazie alla consapevolezza delle possibilità che la digitalizzazione ci offre di ripensare e rendere più efficienti i processi gestionali delle nostre amministrazioni pubbliche, ampliando e migliorando al contempo la qualità dei servizi resi a cittadini e imprese.

La condivisione

Al di là delle considerazioni retoriche, **un elemento** su tutti **sembra connotare questo cambio di passo**: la condivisione.

In effetti, le norme su trasparenza amministrativa (Dlgs n. 33/2013)[1] [1], accesso alle basi di dati tra amministrazioni (articolo 58 del Cad, di cui al Dlgs n. 82/2005, modificato dal Dl n. 90/2014)[2] [2] e riutilizzo dell'informazione nel settore pubblico (Dlgs n. 36/2006, così come modificato dal Dlgs n. 102/2015) valorizzano la condivisione, da un lato, delle **informazioni circa le scelte discrezionali dell'amministrazione** e i dati relativi all'andamento generale della gestione **e**, dall'altro, del **patrimonio informativo pubblico** allo scopo di favorirne la fruizione da parte di altri enti pubblici, cittadini e imprese.

Tale condivisione è dunque volta a perseguire **non solo finalità di trasparenza e pubblicità dell'agire amministrativo** (e in definitiva, un controllo sull'impiego di risorse pubbliche), **ma anche** una maggiore efficienza nella gestione di dati, informazioni e documenti delle amministrazioni, favorendone il riutilizzo anche per **finalità commerciali**.

L'attenzione al potenziale economico del riutilizzo dei dati del settore pubblico, infatti, non è un tratto caratteristico solo della recente disciplina sugli open data, ma connota anche le norme sulla trasparenza amministrativa, le quali sanciscono il diritto a utilizzare e riutilizzare (fatte salve le norme sul trattamento dei dati personali del Dlgs n. 196/2003) i dati oggetto di pubblicazione obbligatoria (pubblicati in formato di dati di tipo aperto, ai sensi dell'articolo 68 del Cad), nelle modalità previste dal Dlgs n. 36/2006, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte di provenienza e di rispettarne l'integrità. Tale **modalità di pubblicazione**, dunque, escludendo ovviamente le ipotesi in cui siano pubblicati dati personali, presenta di fatto implicazioni **simili alle** cosiddette **licenze con richiesta di attribuzione e di condivisione**, allo stesso modo utilizzate anche per gli open data.

Proprio il Dlgs n. 36/2006 è stato oggetto di importanti modifiche introdotte dal recente Dlgs n. 102/2015 e apportate per recepire le disposizioni della Direttiva 2013/37/Ue, con lo scopo di stimolare il mercato di servizi e prodotti a contenuto digitale a sfruttare e riutilizzare il patrimonio informativo pubblico.

Innanzitutto, è stata rivoluzionata l'impostazione letterale dell'articolo 1 che, se nella formulazione precedente stabiliva che non sussisteva alcun obbligo in capo alle pubbliche amministrazioni e agli organismi di diritto pubblico di consentire il riutilizzo dei documenti nella loro disponibilità, ora prevede che **gli** stessi **enti si adoperino** attivamente **affinché i documenti pubblici siano riutilizzabili** anche a fini commerciali.

In questa prospettiva, sono state rafforzate le disposizioni che pongono l'attenzione sul **riutilizzo** dei dati pubblici **per finalità commerciali**, anche riformulando le norme dedicate alla tariffazione (i cui dettagli, che avrebbero dovuto essere

---

[1] *A questo si aggiunga la legge 7 agosto 2015, n. 124, articolo. 7, comma 1, lett. h), circa il riconoscimento della libertà di informazione attraverso il diritto di accesso, anche per via telematica, di chiunque, indipendentemente dalla titolarità di situazioni giuridicamente rilevanti, ai dati e ai documenti detenuti dalle pubbliche amministrazioni, al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.*

[2] *Convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114.*

adottati entro il 15 settembre 2015, dovranno essere disciplinati con decreto dai ministri competenti, di concerto con il ministro dell'Economia e delle finanze e sentita l'Agenzia per l'Italia digitale).

Totalmente rinnovate risultano anche le disposizioni dedicate alle **modalità di richiesta di riutilizzo di documenti**, le quali ora prevedono esplicitamente che gli enti titolari dei dati pubblici adottino prioritariamente **licenze aperte standard**, oppure predispongano licenze personalizzate standard, richiamando l'articolo 52 del Cad e la necessità che le amministrazioni pubblichino il catalogo di dati, di metadati e delle banche dati in loro possesso, nonché i regolamenti che ne disciplinano la facoltà di accesso telematico e riutilizzo. Nello specifico, si dispone anche che gli enti titolari debbano comunicare i motivi di un eventuale rifiuto al soggetto che richiede dati pubblici non ancora resi disponibili, sulla base delle cause di esclusione elencate all'articolo 3 dello stesso Dlgs n. 36/2006. Tuttavia, in proposito, non si può non rilevare che il nostro legislatore abbia omesso di recepire correttamente il **termine di** 20 giorni previsto dalle disposizioni della direttiva 2013/37/Ue, lasciando invece quello di **30 giorni** già contemplato nella versione previgente, entro cui le pubbliche amministrazioni e gli organismi di diritto pubblico sono tenuti a esaminare le richieste e a rendere disponibili i documenti al richiedente.

Inoltre, in linea con quanto già disposto dalle Regole tecniche sul documento informatico (Dpcm 13 novembre 2014), le nuove norme impongono che i **documenti** siano resi **disponibili insieme ai relativi metadati**, rispetto ai quali le citate regole tecniche già prevedono che ai documenti siano associati i metadati minimi obbligatori (articolo 3, comma 9, del decreto). Tali documenti, ove possibile, dovranno essere pubblicati in formati leggibili meccanicamente e inseriti nel portale www.dati.gov.it gestito da AgID per la ricerca dei dati in formato aperto rilasciati dalle pubbliche amministrazioni.

Di grande impatto innovativo sono poi le disposizioni che estendono la disciplina sul riutilizzo dei documenti nel settore pubblico anche a quelli i cui diritti di proprietà intellettuale sono detenuti da **biblioteche (comprese quelle universitarie), musei e archivi**, sempre che questi non ricadano nei casi di esclusione previsti all'articolo 3 dello stesso decreto e, in ogni caso, qualora il loro riutilizzo sia autorizzato in conformità alle disposizioni del Codice in materia di protezione dei dati personali (Dlgs n. 196/2003) e del Codice dei beni culturali (Dlgs n. 42/2004).

Anche queste norme risultano sintomatiche dell'**importanza**, anche economica, **attribuita alla valorizzazione del patrimonio informativo pubblico**, e chiaramente emanate nella prospettiva di ampliarne le possibilità di fruizione per i cittadini e le imprese. Ciò non solo attraverso la condivisione e il riutilizzo, anche a fini commerciali, di dati, informazioni e documenti degli enti pubblici e originariamente formati e detenuti da questi per finalità amministrative e istituzionali, ma anche mediante la digitalizzazione delle risorse culturali, elemento che nel nostro Paese costituisce un potenziale economico di primissimo rilievo.

CONDIVISIONE E RIUTILIZZO DELLE INFORMAZIONI PUBBLICHE: NUOVE NORME PER UN IMPULSO ALL'ECONOMIA DIGITALE
(Sarah Ungaro)

Al DIG.Eat 2015 si discuterà di condivisione e riutilizzo del patrimonio informativo pubblico all'evento With a little help from my friend: open data e Trasparenza in aiuto di cittadini e aziende

Sala Manzoni, ore 15.15-17.30

e-Health e protezione dei dati personali

Franco Cardin *

** Consiglio direttivo Anorc*

La **sostenibilità dei servizi sanitari dei paesi europei**[3] è oggetto di sempre maggiore attenzione, oltre che per le conseguenze della grave crisi economica, che ha determinato un'inevitabile contrazione delle risorse finanziarie disponibili, anche e soprattutto per le **forti tensioni** che diversi fattori esercitano sulla spesa sanitaria complessiva e, in particolare:

- il **progressivo invecchiamento della popolazione**[4], con il conseguente inevitabile aumento delle patologie cronico-degenerative che si caratterizzano per l'elevata onerosità di gestione, sia in fase di ricovero che di assistenza territoriale;
- gli **elevati costi** relativi all'utilizzo di tecnologie sempre più sofisticate e ai nuovi farmaci salvavita.

A queste tensioni devono aggiungersi le **pressioni esercitate dai cittadini-utenti** che, sempre più informati e maggiormente attenti alla propria salute e al proprio benessere (patient empowerment), chiedono servizi sanitari migliori e una maggiore personalizzazione delle cure.

Questa **progressiva evoluzione del contesto** economico, socio-demografico e culturale ha costretto i paesi europei ad adottare **diverse iniziative** finalizzate a garantire una maggiore efficienza ed efficacia dei propri sistemi sanitari, **tra le quali l'e-Health** assume un ruolo strategico di fondamentale importanza.

L'e-Health in Europa

L'Agenda digitale europea che, come è noto, definisce le **strategie e** le **linee guida per la promozione delle tecnologie digitali**, suggerisce di attivare iniziative rivolte alla sanità, indirizzate rispettivamente a:

- garantire l'**accesso on line sicuro ai dati sanitari** sia da parte dei professionisti sanitari che dei cittadini/utenti;
- diffondere maggiormente l'uso della **telemedicina**;
- definire un **Minimum Data Set** per i dati del paziente (Patient Summary);
- garantire l'**interoperabilità** dei sistemi di eHealth;
- supportare l'**Ambient Assisted Living** (la domotica a supporto della disabilità e della fragilità).

Nello specifico documento della Commissione europea *"eHealth Action Plan 2012-2020: Innovative Healthcare in the 21th century*" viene evidenziato che l'**utilizzo di soluzioni e strumenti di e-Health**, comprese le applicazioni per dispositivi mobili (m-Health), accompagnato da adeguati cambiamenti di ordine organizzativo nei sistemi sanitari, può comportare:

- un **miglioramento della salute e della qualità della vita** dei cittadini/utenti, dovuta alla maggiore efficacia dei processi di cura e di riabilitazione;
- una **maggiore efficienza** e produttività dei sistemi sanitari e, conseguentemente, la possibilità di preservarne la sostenibilità economica;
- un'**opportunità di crescita del mercato** delle tecnologie informatiche e telematiche dedicate alla sanità.

Lo stesso documento però evidenzia che, nonostante queste opportunità e questi vantaggi, la **diffusione su vasta scala** dell'e-Health - e, in particolare, dell'mHealth - è **intralciata dai seguenti ostacol**i:

- **carente sensibilizzazione e scarsa fiducia** nelle soluzioni di e-Health da parte di cittadini/pazienti e professionisti

---

[3] *La spesa pubblica in ambito sanitario nei 27 Stati membri dell'Ue è passata da una media del 5,9% del Pil nel 1990 al 7,2% del Pil nel 2010 e secondo le proiezioni il dato potrebbe crescere ulteriormente fino all'8,5% del Pil nel 2060.*

[4] *Questa tendenza è confermata anche dall'Istat, le cui elaborazioni, relative all'evoluzione della struttura demografica della popolazione residente in Italia, evidenziano che il fenomeno dell'invecchiamento della popolazione nei prossimi decenni assumerà una dimensione particolarmente significativa. Tra il 2015 e il 2050 la percentuale della popolazione over 65 e over 85, rispetto al totale dei residenti, passerà rispettivamente dal 21,5 al 33,1 e dal 3,2 al 7,6. Tale fenomeno è confermato dall'indice di vecchiaia, dato dal rapporto tra popolazione con età pari o superiore a 65 anni e la popolazione al di sotto dei 15 anni, che dal 154% del 2015, passerà al 262% nel 2050.*

sanitari;
- **mancanza di interoperabilità** tra le diverse soluzioni di e-Health;
- **assenza di chiarezza giuridica** sulle applicazioni mobili nel settore sanitario e del benessere e mancanza di trasparenza sull'uso dei dati personali rilevati con tali applicazioni;

L'e-Health in Italia

In attuazione delle azioni previste dall'Agenda digitale europea per lo sviluppo dell'e-Health e considerata l'importanza che l'innovazione digitale in sanità assume nell'ambito del processo di miglioramento del rapporto costo-qualità dei servizi offerti ai cittadini/utenti, il **documento della presidenza del Consiglio dei ministri del 3 marzo 2015**, "Strategia per la crescita digitale 2014-2020 in Italia", prevede, per il comparto sanità, le seguenti **linee di intervento** [5]:
- **ePrescription**: ricetta medica elettronica;
- **dematerializzazione** dei referti medici e delle cartelle cliniche;
- **referti on line**;
- **fascicolo sanitario elettronico** e dossier sanitario.

La protezione dei dati personali nell'ambito delle iniziative di e-Health

A fronte delle molteplici opportunità offerte dallo sviluppo dell'e-Health che, come abbiamo visto, rappresenta un **obiettivo strategico fondamentale e irrinunciabile** per poter garantire non solo una migliore efficienza ed efficacia dei sistemi sanitari, ma anche la loro sostenibilità, vi sono però **elevate criticità - e conseguenti particolari rischi -** dovuti all'impatto che l'utilizzo delle tecnologie informatiche e telematiche in ambito sanitario inevitabilmente hanno sulla protezione e sulla sicurezza dei dati personali dei cittadini/utenti[6]

Non va dimenticato, infatti, che **per la particolare natura dei dati personali contenuti** - si tratta di dati idonei a rivelare lo stato di salute e, in alcuni casi, di dati genetici - l'accesso ai sistemi informativi sanitari da parte di soggetti non autorizzati o di criminali informatici può comportare per i cittadini/utenti **diverse tipologie di danni** [7].

Per queste ragioni, gli aspetti legati alla **necessità di garantire**, nell'ambito delle iniziative di e-Health, **il corretto trattamento dei dati personali e la loro sicurezza**, sono stati oggetto negli ultimi anni di particolare analisi da parte del Gruppo di lavoro ex articolo 29 della direttiva 95/46/Ce [8], nonché di specifica regolamentazione da parte dell'Autorità garante del nostro paese.

A fronte delle prime iniziative di condivisione informatica - da parte di distinti organismi o professionisti - di dati e documenti sanitari formati nel tempo da più soggetti e riguardanti gli eventi sanitari occorsi a uno stesso cittadino/paziente, avente lo scopo di garantirgli un migliore processo di cura, il Garante per la protezione dei dati personali ha adottato le **"Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario"** del 16 luglio 2009.

Pochi mesi dopo, a fronte di un'ulteriore iniziativa messa in atto da alcune aziende sanitarie pubbliche e private, consistente nell'offrire al cittadino/paziente la possibilità di accedere ai referti relativi alle prestazioni diagnostiche ricevute con modalità informatiche o telematiche, l'Autorità garante ha adottato le **"Linee guida in tema di referti on line"** del 19 novembre 2009.

Con entrambe queste linee guida l'Autorità garante - tenuto conto della mancanza di specifiche norme di carattere primario o regolamentare in materia e valutate sia l'utilità che le elevate criticità insite in queste nuove iniziative - ha ritenuto necessario individuare un **primo quadro di regole, accorgimenti e cautele**, finalizzate non solo a rispettare l'obbligo di fornire un'adeguata informativa e ad acquisire il consenso dell'interessato, ma anche e soprattutto a garantire

---

[5] *È opportuno ricordare che nel nuovo "Patto per la salute per gli anni 2014-2016" viene dedicata al tema dello sviluppo dell'e-Health una particolare attenzione, tanto da prevedere la definizione di uno specifico "Patto per la sanità digitale", ossia un piano strategico teso a rimuovere gli ostacoli che rallentano l'impiego sistematico dell'innovazione digitale in sanità.*

[6] *Per una panoramica sulle criticità e sui rischi insiti nell'utilizzo delle tecnologie informatiche e telematiche in sanità si veda "La sicurezza nei sistemi informativi sanitari", a cura di Fabio Di Resta e Barbara Ferraris di Celle", Edisef, 2010.*

[7] *Si veda a questo proposito "La sicurezza dei dati personali sanitari" Claudia Ciampi, in Rivista di Diritto, Economia, Management, n. 3 – 2014, pagg. 27-51.*

[8] *Sulle problematiche relative all'e-Health, si vedano in particolare i seguenti pareri adottati dal Gruppo di lavoro ex articolo 29: WP 131 del 15 febbraio 2007 sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche; WP 202 del 27 febbraio 2013 sulle applicazioni per dispositivi intelligenti; WP 223 del 16 settembre 2014 on the recent devolopments on the Internet of Things.*

la massima sicurezza possibile dei dati. Tutte queste misure di sicurezza sono state poi recepite e inserite nello schema di **Dpcm in materia di Fascicolo sanitario elettronico** e nel Dpcm 8 agosto 2013 in materia di referti on line.

Conclusioni

La protezione dei dati personali in ambito sanitario rappresenta non solo un obbligo di legge finalizzato a garantire il rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei cittadini/utenti, con particolare riferimento alla riservatezza e all'identità personale – il cui non rispetto può comportare rilevanti responsabilità amministrative, penali e civili -, ma anche un'**opportunità di creare la necessaria fiducia verso le soluzioni di e-Health** e, quindi, un fattore abilitante per un maggiore ed effettivo sviluppo delle stesse.

Per questo i produttori di soluzioni di e-Health, nonché le aziende sanitarie che intendono adottarle, devono prestare una **sempre maggiore attenzione agli aspetti relativi alla protezione dei dati personali** dei cittadini/utenti, con particolare riferimento alle idonee e preventive misure di sicurezza in grado di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per cui essi erano stati raccolti.

Per concludere, **è auspicabile** non solo che i produttori di soluzioni di e-Health applichino, già in fase di progettazione delle stesse, i principi della *privacy by design* e *privacy by default*, ma anche e soprattutto **che nelle aziende sanitarie la protezione dei dati personali dei pazienti diventi un obiettivo primario**, sostenuto dal management, per il cui raggiungimento siano previsti specifici percorsi formativi che consentano la sensibilizzazione di tutto il personale e la crescita di adeguate professionalità in materia di sicurezza dei dati.

E-HEALTH E PROTEZIONE DEI DATI PERSONALI
(Franco Cardin)

Al DIG.Eat 2015 l'e-Health sarà tra gli argomenti principali della tavola rotonda
You can't always get what you want: i limiti privacy di mobile, app, e-commerce e cookie

Sala Manzoni, ore 10.00-13.00

Le nuove sfide di sicurezza e privacy nello scambio di dati personali tra amministrazioni pubbliche

Graziano Garrisi *

* *Consiglio direttivo Anorc*

Un **provvedimento del Garante privacy del 2 luglio 2015** ha indicato una serie di misure di sicurezza da adottare per le banche dati pubbliche e le modalità relative allo scambio dei dati personali tra amministrazioni.

In attesa di standard e linee guida…

Il riformulato articolo 58, comma 2, del Codice dell'amministrazione digitale (Dlgs 82/2005)[9] impone infatti alle amministrazioni pubbliche di comunicare tra loro non più mediante la predisposizione di apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate, ma attraverso la messa a disposizione - a titolo gratuito - di accessi alle proprie basi di dati, mediante la cosiddetta **cooperazione applicativa** (disciplinata all'articolo 72 dello stesso Cad).

Pertanto, in attesa che l'Agenzia per l'Italia digitale (AgID) definisca gli standard di comunicazione e le regole tecniche, l'Autorità garante ha prescritto **specifiche misure tecniche e organizzative** da adottare (anche in conformità a quanto già espresso in un precedente parere del 4 luglio 2013) per "*ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti o non conformi alla finalità di raccolta dei dati personali, alla natura degli stessi e alle specifiche caratteristiche del trattamento*".

Di particolare interesse l'**Allegato 2** al provvedimento che contiene un **elenco di tutte le misure necessarie** che disciplinano: "Modalità d'accesso", "Presupposti per la comunicazione di dati personali" (la convenzione era lo strumento con cui le amministrazioni potevano stabilire le garanzie a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi, attualmente da definirsi in appositi regolamenti dell'ente), "Soggetti incaricati del trattamento" (fornendo una regolamentazione dei ruoli da attribuire in ambito privacy, nel rispetto di idonee procedure di autenticazione e autorizzazione degli utenti da implementare), "Dati sensibili e giudiziari" (che ovviamente dovranno essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati), "Misure di sicurezza" e "Controlli" da attivare.

Le misure di sicurezza e organizzative da mettere in campo

Con specifico riferimento alle misure di sicurezza prescritte dal Garante, accanto a quelle minime previste dagli articoli 33 e seguenti del Codice privacy e dal relativo Allegato B, le amministrazioni pubbliche che erogano o fruiscono dei servizi di accesso alle banche dati devono assicurare anche una serie di misure idonee che - nel provvedimento in esame – sono state **tassativamente indicate**:

a) gli **accessi alle banche dati** devono avvenire soltanto tramite l'uso di postazioni di lavoro connesse alla rete IP dell'ente autorizzato o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali);

b) laddove l'accesso alla banca dati dell'erogatore avvenga in forma di *web application* esposta su rete pubblica (Internet), l'applicazione deve essere realizzata con **protocolli di sicurezza**, provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014, emessi da una Certification Authority e riconosciuti dai più diffusi browser e sistemi operativi;

c) le procedure di **registrazione** devono avvenire con il riconoscimento diretto e l'identificazione certa dell'utente;

d) le regole di **gestione delle credenziali di autenticazione** devono prevedere:

i. l'identificazione univoca di una persona fisica;

---

[9] *Disposizioni modificate dall'articolo 24-quinquies, comma 1, del Dl n. 90/2014, convertito, con modificazioni, dalla legge n. 114/2014.*

ii. processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura, seguendo una **procedura operativa prestabilita** o di accettazione di forme di autenticazione forte quali quelle che prevedono l'uso di *one time password* o di certificati di autenticazione (Cns o analoghi);

iii. credenziali costituite da un dispositivo in possesso e uso esclusivo dell'incaricato provvisto di pin o una coppia username/password, ovvero credenziali che garantiscano analoghe **condizioni di robustezza**;

e) nel caso le credenziali siano costituite da una coppia username/password, l'adozione di **politiche di gestione delle password**:

i. la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), deve essere **modificata** dallo stesso al primo utilizzo e, successivamente, **almeno ogni tre mesi**; le ultime tre password non possono essere riutilizzate;

ii. le password devono avere **determinati requisiti di complessità** (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);

iii. quando l'utente si allontana dal terminale, la **sessione deve essere bloccata**, anche attraverso eventuali meccanismi di time-out;

iv. le **credenziali devono essere bloccate** a fronte di reiterati tentativi falliti di autenticazione;

f) devono essere sempre presenti **misure di protezione perimetrali logico-fisiche**, quali ad esempio firewall e reti private virtuali (Vpn);

g) i **sistemi** software, i programmi utilizzati e la protezione antivirus devono essere **costantemente aggiornati**, sia sui server che sulle postazioni di lavoro;

h) le **misure di sicurezza** devono periodicamente essere riconsiderate e adeguate ai progressi tecnici e all'evoluzione dei rischi;

i) la **procedura di autenticazione** dell'utente deve essere protetta, attraverso meccanismi crittografici di robustezza adeguata, dal rischio di intercettazione delle credenziali;

j) introduzione di meccanismi volti a permettere il **controllo degli accessi**, al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;

k) in caso di **accessi via web** deve essere di regola esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;

l) **comunicazione tempestiva** su:

i. **incidenti sulla sicurezza** occorsi al proprio sistema di autenticazione, qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti alla fruibilità di dati oggetto di convenzione;

ii. ogni eventuale **esigenza di aggiornamento di stato** degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

iii. **ogni modificazione tecnica o organizzativa** del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole sopra riportate o la loro perdita di efficacia;

m) tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. A tal fine:

i. il fruitore deve fornire all'erogatore, contestualmente a ogni transazione effettuata, il **codice identificativo dell'utenza** che ha posto in essere l'operazione;

ii. il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque **riferito univocamente** al singolo utente incaricato del trattamento che ha dato origine alla transazione;

iii. il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilità, su richiesta, di **identificare l'utente** nei casi in cui ciò si renda necessario.

Osservazioni finali

Si tratta, a ben vedere, di misure di sicurezza e organizzative di non poco conto che impegneranno severamente le pubbliche amministrazioni, soprattutto in considerazione delle **pesanti sanzioni previste in caso di inadempimento**. Preme ricordare, infatti, che molte delle prescrizioni ivi indicate rientrano tra le cosiddette misure di sicurezza "necessarie", perché emanate ai sensi dell'**articolo 154, comma 1, lett. *c*** [10]; un esempio, in tal senso, è tutto quanto contemplato nel

[10] *Il mancato adempimento delle misure di sicurezza necessarie ivi indicate comporta sanzioni amministrative che variano da un minimo di 30mila a un massimo di 180mila euro.*

sopra citato Allegato 2 al provvedimento e riguarda l'introduzione di una **nuova ipotesi di comunicazione all'Autorità garante nei casi "data breach"** (da farsi entro 48 ore dalla conoscenza del fatto) ovvero di tutte quelle violazioni dei dati o incidenti informatici che possano avere un impatto significativo sui dati personali detenuti nelle banche dati pubbliche, da effettuarsi nelle modalità e nelle forme descritte nell'Allegato 1 del provvedimento.

La **sfida in questo settore si preannunzia ardua**, soprattutto perché nel caso specifico è proprio l'Autorità garante per la protezione dei dati personali a intervenire, richiamando l'attenzione delle PA e del legislatore su queste tematiche, sopperendo così alla temporanea mancanza dei sopra indicati standard di comunicazione e delle regole tecniche di AgID (che avrebbero dovuto essere definite entro 90 giorni dall'entrata in vigore delle nuove disposizioni).

Tutto, quindi, viene rimesso ancora una volta alla solerzia delle pubbliche amministrazioni più avvedute, che magari in questi anni hanno già puntato e investito molto in sicurezza per **tutelare l'importante e delicato patrimonio informativo costituito dai dati dei cittadini**, mentre per molte altre amministrazioni che meno si sono adoperate in questa direzione – in quella costante alterità tutta italiana tra pochi e sparsi casi di eccellenza e numerose zone d'ombra - ancora più complesso (ma non impossibile!) sarà adeguarsi a queste nuove disposizioni.

LE NUOVE SFIDE DI SICUREZZA E PRIVACY NELLO SCAMBIO DI DATI PERSONALI TRA PA (Graziano Garrisi)

Al DIG.Eat 2015 si parlerà di sicurezza dei dati della PA nella tavola rotonda
You can't always get what you want: i limiti privacy di mobile, app, e-commerce e cookie

Sala Manzoni, ore 10.00-13.00