MAGGIOLI EDITORE - La Pratica Forense

Privacy e DPS nella P.A.
S. Di Minco (Approfondimento 24/3/2011)

Brevi riflessioni in materia di Privacy e DPS nella PA (*)
Piccole esperienze di un consulente/docente & qualche consiglio operativo con "viaggio guidato" nel DPS del Comune di ADEMPIENZIA

1. Quale privacy ? A quale scopo? A cosa serve il DPS?

Cos'è davvero e in concreto la Privacy in Italia? Come viene percepita, vissuta e interpretata nel sistema pubblico ed in particolare negli Enti locali? Quali progressi sono stati compiuti in questi anni, sia sul piano culturale che su quello pratico? Qual è il grado complessivo di consapevolezza degli operatori che, a vario titolo, "maneggiano" quotidianamente una mole notevole di dati personali dei cittadini, rilevante sia per quantità che per qualità degli stessi (la PA tratta molti dati anche di natura sensibile e semi-sensibile)?
Gli Amministratori pubblici sono preparati a confrontarsi con la questione della sicurezza, affidabilità e disponibilità del patrimonio informativo degli Enti che sono chiamati a guidare? Quanto sono consapevoli - nel momento in cui pianificano priorità, investimenti e destinazioni di budget - del fatto che su quel patrimonio informativo si basa, sempre più in forma dematerializzata, ogni attività svolta dalla PA per perseguire rilevanti finalità di interesse pubblico?
Quanto è diffusa la convinzione che in fondo queste tematiche, come pure quelle legate alla sfida della digitalizzazione della PA, abbiano una valenza meramente tecnico-informatica? Che pertanto siano da delegare al Dirigente-informatico di turno, quando l'Ente ne è dotato, o al perito informatico (se c'è..) o al consulente-informatico o, ancora, specie nei piccoli Comuni, al dipendente, di qualsiasi categoria e profilo professionale, che abbia una cosiddetta sensibilità informatica? E' corretta questa impostazione alla luce di quanto previsto dalla normativa europea e nazionale vigente, ma anche solo sul piano del buon senso?
Sono questioni che mi pongo da anni, che mi lasciano tendenzialmente insoddisfatto e che talvolta mi provocano lo stesso senso di frustrazione che si prova quando non ci si rassegna ad accettare come ineluttabili alcune disfunzioni croniche del nostro Paese, per le quali non si riesce a trovare alcuna spiegazione apparentemente razionale (perché non si risolve il problema dei rifiuti a Napoli?....Perché non si riesce a terminare la Salerno-Reggio Calabria?..ecc...).
Per questo vorrei provare a condividere, in rete ma "senza rete", alcune di queste riflessioni, senza alcuna pretesa di esaustività e senza voler dispensare certezze, ma provando invece ad esprimere un punto di vista, dichiaratamente parziale e limitato, quale può essere quello di un professionista che vive lo sforzo continuo di far dialogare e mettere in connessione due facce della realtà che talvolta appaiono quasi contrapposte: da un lato, alcuni grandi principi, contenuti in norme internazionali, europee e nazionali quali il diritto fondamentale alla protezione dei dati personali, il diritto alla riservatezza, quello ad una buona amministrazione, il principio di non discriminazione ecc. (cui si sente di aderire anche intimamente e con una certa dose di passione, che si cerca poi di trasmettere nelle aule dell'Università ai giovani studenti, e nelle aule di formazione professionale, agli operatori); dall'altro, la crudezza del quotidiano e la logica dell'urgenza e dell'emergenza, che sembrano essere quelle prevalenti nel funzionamento della PA, con particolare riferimento a quella locale, con le quali ci si scontra inevitabilmente quando si viene interpellati per una qualche consulenza. In tale contesto si riceve spesso un messaggio di fondo, più o meno apertamente dichiarato: "caro avvocato, il nostro problema è quello di essere formalmente "a norma", e di ridurre i rischi di incorrere in sanzioni; quanto poi alla sua raccomandazione di invertire la prospettiva per conseguire i risultati sostanziali indicati dalla Legge...Eventualmente rivaluteremo in futuro... Al momento è troppo complicato e poi … abbiamo altre priorità".
Ecco allora che si scatenano le improvvisazioni e le soluzioni più fantasiose, pronte a cogliere questa esigenza così sentita e diffusa - in verità non solo nel settore pubblico - e capita anche di leggere in rete annunci che, approssimativamente, hanno questo tenore:
"**Devi redigere il tuo DPS della Privacy? Nessun problema! Te lo facciamo noi a 99 Euro in un giorno - Redatto, stampato e spedito a nostro carico con posta prioritaria**"

Chiunque abbia un minimo di cognizione di cosa sia un Documento Programmatico sulla Sicurezza (DPS) - di quale sia la sua funzione, sulla base di quali elementi di conoscenza ed analisi esso vada costruito ecc. - sa benissimo che quel tipo di annuncio propone una *patacca*!
E purtroppo, di patacche, ne sono state vendute e acquistate a migliaia in questa materia! Di vario formato, di vario colore, di varia consistenza e di vario prezzo, anche a soli 99 Euro!
A meno di doti medianiche e di chiaroveggenza, infatti, è evidente che nessuno può redigere un DPS "a distanza e in tempo reale", senza svolgere un'analisi concreta ed effettiva, sul campo, delle varie tipologie di rischio e dell'intensità con cui i rischi stessi si possono manifestare nel singolo e peculiare caso esaminato al fine di programmare ed esplicitare - appunto nel DPS - le relative modalità (misure) per neutralizzarli.
Il pensiero corre allora veloce a quelle straordinarie soluzioni che la italica fantasia adottò oltre venti anni fa, specie in alcune realtà territoriali, per "adempiere" all'obbligatorietà delle cinture di sicurezza nella circolazione stradale. Delle magnifiche magliette bianche con banda trasversale nera stampata sul davanti, che simulava perfettamente una cintura di sicurezza indossata,anche quando l'auto non era neppure dotata dell'apparato. Ovviamente, come sappiamo bene, l'obbligo della cintura aveva uno scopo nobile e importante: tutelare l'incolumità e la salute delle persone fisiche, o almeno ridurre i rischi di danno, in caso di collisione; evidentemente la maglietta non aveva alcuna chance di raggiungere lo scopo perseguito dalla norma, ma riduceva (o illudeva di di ridurre) un altro rischio: quello di incorrere nelle sanzioni che il Codice della strada prevedeva per il mancato uso della cintura. Esattamente come i DPS - *patacca* di cui sopra rispetto alle previsioni del Codice della Privacy.
D'altra parte questa cultura della soluzione fantasiosa, in funzione anti-sanzione, non placa mai la propria capacità di adeguarsi ai tempi. Infatti pare che una bella e pratica soluzione sia stata trovata anche per ovviare al fastidio dell'allarme sonoro che oramai tutti i modelli di auto in circolazione prevedono in caso di mancato allaccio della cintura di sicurezza: infatti è in vendita il solo "gancio" della cintura stessa, basta inserirlo nell'apposito alloggiamento e l'avviso sonoro sparisce...
Evviva l'Italia delle misure di sicurezza *PATACCA*!
Per fortuna la realtà è molto più complessa e articolata e vi sono molti comportamenti che denotano un senso civico esemplare, come pure autentiche punte di eccellenza e professionalità anche in materia di PA digitale e gestione dei dati personali nella PA locale.
Tuttavia, volendo proseguire con onestà intellettuale la stringata e parziale analisi sommariamente avviata, proverò di seguito - partendo da piccoli ma significativi episodi realmente verificatisi nella mia esperienza diretta - ad evidenziare alcuni profili di insufficienza che percepisco ancora troppo diffusi nell'applicazione concreta della disciplina vigente in materia di protezione dei dati nella PA. Successivamente proverò a riportare la riflessione su un piano più concreto, simulando di essere interpellato da una P.A locale - che immaginerò essere un Comune di circa 70/80.000 abitanti - alle prese con l'esigenza di adeguare obbligatoriamente il proprio DPS entro il prossimo 31 Marzo come in effetti tutti gli Enti devono fare. Simulerò che il Comune in questione, che chiamerò ADEMPIENZIA, abbia operato come mi è capitato molte volte di verificare nella realtà e cioè privilegiando l'esigenza di adempiere ad una formalità piuttosto che quella di conseguire una effettiva sicurezza nel trattamento dei dati; con un approccio non sistematico, poco integrato (ad esempio senza valorizzare le connessioni delle questioni di data protection con tutta la tematica dell'amministrazione digitale e di quest'ultima con l'esigenza della revisione dell'intero sistema procedurale e documentale) e poco attento a rendere partecipe e consapevole delle sfide e del contesto complessivo un attore determinante, ovvero tutto il personale e l'intera struttura organizzativa, senza la cui partecipazione collaborativa e consapevole sarà difficile, se non impossibile, raggiungere qualsiasi obiettivo ambizioso di riforma della PA che punti al miglioramento della qualità dei servizi ed alla realizzazione della Buona Amministrazione al servizio dei cittadini e dei loro diritti.

2. Piccola casistica, autentica, di interpretazione del diritto alla Privacy nella PA

Sono anni che, tra il serio e il faceto, prometto a me stesso di scrivere, prima o poi, un elenco dettagliato di tutte le "esperienze" più strane, fantasiose e talvolta incredibili, che ho raccolto in circa 15 anni di attività in qualità di consulente, formatore e docente universitario in materia di Diritto dell'informatica e di diritto alla privacy in particolare. Per una volta vorrei cominciare una riflessione proprio da qui - da casi veri un po' … strani - per poi cercare di ricondurre questi aneddoti ad una riflessione seria e, spero, anche un po' utile in tema di tutela dei dati personali nel sistema pubblico italiano, con particolare riferimento alla PA locale.

Caso 1: un Comune di circa 20.000 abitanti mi chiede di fornire una consulenza e alcune attività formative in materia di privacy. Non è ancora vigente il Codice della Privacy, ma c'è già da tempo la L. 675/96 e sono pienamente vigenti gli obblighi di sicurezza previsti dal DPR 318/99 e le relative sanzioni penali previste in caso di inadempimento. Al fine di avere una quadro della situazione di partenza, come faccio sempre, intervisto i responsabili di Settori e Servizi e compilo delle schede che ho predisposto allo scopo. Incontro dunque anche il Responsabile del servizio politiche sociali, la struttura che si occupa di tutte le varie situazioni di disagio presenti sul territorio (tossicodipendenze, problemi di salute mentale, indigenza e tutto quanto di più "sensibile" si possa immaginare); alla mia precisa domanda sulle specifiche misure adottate per il trattamento di dati prevalentemente sensibili, ecco la risposta: "non c'è alcun problema, sono una persona molto riservata". (Nota: dall'intervista è poi risultato che la struttura era priva delle "misure minime di sicurezza", a partire dalle più elementari.

Caso 2: uno studente non più giovanissimo, in una Università italiana, sta sostenendo l'esame nel cui programma vi è anche l'argomento privacy. L'esame sta andando malissimo e allora lo studente, per giustificare in parte lo scarso profitto, mi dice del suo status di studente/lavoratore che opererebbe, in qualità di perito informatico, nel Servizio sistemi informativi di una ASL; mi sembra doveroso allora - credendo anche di aiutarlo un po' - porgli una domanda di carattere molto generale in ordine ai principi generali del Codice della Privacy. La risposta, incerta e sintetica è : "c'è internet .... ci sono tutte queste informazioni....ci sono le reti informatiche..... tanti dati personali ...e quindi c'è la privacy..." Ogni tentativo di ottenere una risposta più precisa, ad esempio a proposito dei dati sensibili, del concetto di trattamento e degli obblighi di sicurezza risulta vano e infruttuoso. Chiunque abbia un minimo di esperienza di esami universitari, anche per il solo fatto di essere stato uno studente ed avervi assistito da spettatore, sa benissimo che i casi di totale impreparazione si verificano di frequente. Ma qui ciò che si intende evidenziare non è l'impreparazione dello studente, bensì quella di un "operatore di sistema" e di un "incaricato"(?) (auspicando che non avesse alcuna designazione di Responsabilità) nel trattamento di dati sensibili con strumenti informatici in una ASL... (ovviamente l'esame non è stato superato e, pur essendo trascorsi degli anni, lo studente non si mai più ripresentato.... ma c'è soprattutto da auspicarsi che non sia stato sincero a proposito del suo ruolo in una ASL).

Caso 3: durante una lezione, nell'ambito di un corso di formazione professionale dedicato al tema, destinato a personale di categoria C e D di un Ente pubblico locale (grande) - nella fase di transizione tra la L. 675 ed il Codice attuale - affronto la questione delle prescrizioni previste nell'allegato B del Codice stesso e mi soffermo per qualche istante sui requisiti previsti per la scelta e la custodia delle credenziali di autenticazione; in sintesi sto spiegando le caratteristiche di sicurezza minima che obbligatoriamente deve avere una password quando una delle persone partecipanti alza la mano e formula una osservazione di questa natura: "questa pretesa secondo la quale io dovrei essere l'unica che conosce la PW per accedere all'applicativo che utilizzo per la procedura X è assurda. Anzi se lo vuole sapere, io tengo ben in vista un post it, incollato allo schermo del PC, dove ho scritto in caratteri molto ben evidenti paola9 che è la mia PW; stamattina prima di venire qui mi sono accertata che fosse ben visibile in mia assenza e non ho alcuna intenzione di cambiare una prassi con la quale, in ufficio, ci troviamo benissimo. D'altra parte, nessuno dei miei superiori mi ha mai detto di fare diversamente"

Caso 4: un Comune di circa 25.000 abitanti ha da poco installato sul proprio territorio un sistema di videosorveglianza col quale vengono monitorati diversi spazi e luoghi pubblici.
Il Garante della Privacy ha da poco adottato il (primo) Provvedimento generale in materia di Videosorveglianza (del 29 aprile 2004) e chiedo dunque al Responsabile del servizio comunale che ha seguito tutta la procedura se ne ha tenuto conto. Mi guarda perplesso e poi mi dice: "cosa vuole che ci importi del Garante, ho parlato col Maresciallo dei Carabinieri!" (nota: ne ho poi parlato direttamente col Sindaco e, fortunatamente, la situazione è stata corretta).

Caso 5: Chiamo io stesso il distretto sanitario di base, unica struttura sanitaria presente in un territorio comunale di circa 25.000 abitanti, per conto di un'altra persona che deve rinnovare la patente di guida, e chiedo se ci sono moduli specifici per lo scopo indicato, se sono loro ad averli e se, eventualmente, c'è un modo per scaricarli on line. La persona che mi risponde è gentile, ma di poche parole e mi dice che devo recarmi personalmente perché non c'è la possibilità di scaricare ciò che occorre. Vado. Giunto sul posto mi si

dice che in realtà occorrono solo dei bollettini postali di CC che però loro non hanno (non tutti) ma che posso tranquillamente trovare in un qualsiasi Ufficio Postale. Allora io chiedo perché non me l'ha detto al telefono. La risposta: "non possiamo dare queste informazioni...c'è la privacy!"

Gli episodi anomali sarebbero ancora molti e alcuni di questi - formalmente immortalati in diversi DPS autentici che ho avuto modo di analizzare - sono stati da me utilizzati per costruire, in una specie di collage, il DPS dell'inesistente Comune di ADEMPIENZIA in merito al quale, di seguito, avanzerò alcune osservazioni critiche finalizzate ad individuare una possibile strategia operativa di superamento della logica dell'adempimento.

3. Il DPS del Comune di ADEMPIENZIA. Documento autentico al 90%, redatto ad uso di un bravo Dirigente che vorrebbe superare la logica dell'adempimento formale...

Il documento che segue è dunque solo parzialmente un documento di fantasia, in quanto si ispira a stralci di DPS autentici, da me arbitrariamente collezionati in unico ipotetico DPS, che ho immaginato fosse del Comune di Adempienzia. Ho poi ipotizzato che un bravo e serio Dirigente di codesto Ente, cogliendo il significato della normativa in materia di Privacy, mi avesse chiesto di esaminare il DPS esistente e fornire un parere sintetico in merito alla sua conformità alla normativa vigente. Ecco, grosso modo, cosa avrei potuto scrivere:

DOCUMENTO RISERVATO
ad uso esclusivo del Comune di ADEMPIENZIA

Valutazione di sintesi sulla conformità della situazione in atto presso il Comune di ADEMPIENZIA al quadro normativo vigente in materia di privacy e misure di sicurezza

***1. Premessa**: la presente nota è il risultato di una valutazione sintetica e schematica che scaturisce dall'esame dei documenti cui ho avuto accesso e dalle informazioni che ho acquisito attraverso i colloqui con il personale, a seguito della serie di incontri svoltisi presso il Comune di ADEMPIENZIA dal 21 al 25 gennaio 2011 ed ha la finalità esclusiva, senza alcuna pretesa di completezza, di offrire al Dr. Carlo Rossi - dirigente del Settore X - un quadro della situazione attuale ed alcuni suggerimenti su un possibile percorso per raggiungere un soddisfacente livello di adeguamento al quadro normativo vigente.*
La situazione che ho potuto verificare presenta diversi profili di problematicità che attualmente espongono l'intero Ente a possibili conseguenze negative di una certa gravità: innanzitutto sul piano concreto (in termini di effettiva sicurezza, disponibilità ed affidabilità del patrimonio informativo di cui dispone e su cui basa la propria attività istituzionale al servizio della cittadinanza e dell'utenza ADEMPIENZESE) ed inoltre sul piano giuridico, in termini di Responsabilità civile, Penale ed Amministrativa per la sostanziale mancata attuazione di alcune importanti misure di sicurezza previste dal Codice della Privacy (di seguito: Codice), principalmente ai sensi degli artt. 31, 33, 34 e 35 (ma anche con riferimento ad alcuni provvedimenti e prescrizioni del Garante, come ad esempio quello relativo agli Amministratori di sistema che avrebbe dovuto essere adottato entro e non oltre lo scorso 15 dicembre 2009).

***2. Responsabilità, compiti, profili e funzioni**. Il primo elemento di criticità è quello di una non sufficiente chiarezza nella individuazione (in concreto e non solo in teoria) delle diverse figure previste dal Codice, dei rispettivi ambiti di competenza e della conseguente ripartizione dei vari profili di Responsabilità. Nel caso concreto se, da un lato, sembra pacifico che tutti i Dirigenti di settore siano da considerarsi RESPONSABILI del trattamento ai sensi degli artt. 4 e 29 del CODICE (tale scelta risulta dal primo DPS adottato con determina del Direttore Generale nel 2004 ed è stata confermata nei successivi DPS), tuttavia, dall'altro, pone dei dubbi sul piano giuridico, in termini di legittimità ed efficacia, il fatto che da un certo momento in poi le determinazioni in ordine al profilo di responsabilità (poteri, funzioni, compiti, oneri, obblighi di vigilanza e di prescrizione sull'attività degli incaricati, ecc.) dei RESPONSABILI DEL TRATTAMENTO (i Dirigenti) siano delineate in un atto, sempre il DPS, adottato con Determina ma da un altro Dirigente þarimenti"RESPONSABILE del trattamento.*
Il Codice assegna esclusivamente al Titolare (l'ENTE nella sua interezza) la facoltà e la potestà di

designare il Responsabile del trattamento e definirne esattamente i compiti, infatti l'art. 29 afferma che ".I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.... il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni .. e delle proprie istruzioni ."

Direi che non è chiaro se e come ciò avvenga all'interno dell'Ente nonostante vi siano a carico del Titolare (Comune di ADEMPIENZIA) precise responsabilità "in eligendo"(in fase di designazione delle figure di RESPONSABILE del trattamento) ed altrettante precise responsabilità "in vigilando"(su tutta la successiva attività di tali figure).

***2.1 La specifica figura dell'ADS**. La situazione è poi altrettanto poco chiara con riferimento alle figure degli ADS (Amministratori di Sistema) rispetto alle quali c'è un Provvedimento generale del Garante del 2008 che non mi sembra correttamente attuato nella situazione concreta (l'individuazione di una "quota"di Responsabilità specifica, quale Amministratore di sistema, a carico del Dirigente del Settore Sistemi informativi, effettuata nel primo DPS dal Direttore generale non risponde affatto alla complessità dell'esigenza attuale). La prima conseguenza possibile, sul piano giuridico, per la mancata attuazione di tale Provvedimento (termine ultimo, perentorio, decorso lo scorso 15 dicembre 2009) è la sanzione del pagamento di una somma da trentamila a centottantamila euro (art. 161, comma 2 ter). Anche qui c'è una Responsabilità, riconducibile al titolare (Comune di ADEMPIENZIA) tanto "in eligendo" (in fase di designazione delle figure di ADS) che "in vigilando"(su tutta la successiva attività di tali figure).*

***Soluzione Consigliata**. Punto 2: Adozione di una delibera di Giunta che delinei un Piano strategico d'intervento che, oltre a individuare vari interventi necessari in materia, innanzitutto chiarisca la ripartizione dei profili di Responsabilità e assegni con precisione compiti, ruoli e funzioni in conformità alla normativa vigente (inclusa una modalità operativa di verifica sull'attività dei RESPONSABILI del trattamento). Punto 2.1 nella medesima delibera di Giunta va dato mandato ai Responsabili di adempiere al Provvedimento in materia di ADS sulla base di precisi indirizzi.*

***3. Adozione delle misure di sicurezza.** Si tratta di un punto delicatissimo in quanto si è avuta l'impressione della sostanziale mancata adozione di alcune importanti misure di sicurezza previste dal Codice. Sia con riferimento a quelle obbligatorie previste dall'art. 31, la cui mancata adozione (nel caso che si verifichi un danno) genera una sicura ed inevitabile Responsabilità civile di tipo oggettivo (ai sensi dell'art. 15 del codice e dunque nei modi previsti dall'art. 2050 del Codice civile), sia con riferimento a quelle previste dall'art. 33, la cui mancata adozione costituisce un'ipotesi di reato omissivo punito (anche se non si verifica alcun evento dannoso) con l'arresto sino a due anni ai sensi dell'art. 169 del Codice (oltre che con una sanzione amministrativa da 10.000 a 120.000 euro ex art. 162, comma 2 bis).*
Mi permetto di ricordare che le misure da adottare non sono solo di tipo "informatico"ma anche e, direi, soprattutto di tipo organizzativo e "comportamentale"(oltre che di tipo fisico).
Da questo punto di vista mi sembra opportuno sottolineare come, per quella che è stata la mia percezione in relazione al caso concreto, l'elemento più preoccupante sia la mancanza di una "cultura della sicurezza in tema di DATA PROTECTION che tende a generare comportamenti involontariamente "pericolosi"per la custodia e l'affidabilità del patrimonio informativo del Comune creando in tal modo "il vero problema"per l'Ente (ben aldilà dell'aspetto giuridico-formale). Per non parlare delle implicazioni che tutto ciò comporta in termini di effettiva realizzabilità degli obiettivi posti dalle strategie e dalle norme in materia di digitalizzazione della P.A.

***Soluzione Consigliata**: Programmazione nel Piano strategico d'intervento di cui al punto precedente di un "intervento operativo"finalizzato all'innalzamento del livello di sicurezza nella salvaguardia del patrimonio informativo dell'Ente (anche di quello che non ha una natura di dato personale) che preveda l'individuazione delle misure mancanti, ne definisca modalità (concrete) e tempi di adozione e sia accompagnato da un intervento di formazione/affiancamento che, graduato sui diversi profili omogenei di Responsabilità, contribuisca a creare quel livello minimo di consapevolezza senza il quale è impossibile raggiungere un livello adeguato di affidabilità. In effetti il Codice prevede che tale pianificazione, (comprensiva anche della formazione), sia obbligatoria e sia racchiusa nel "noto" DPS (Documento programmatico sulla sicurezza).*

Si dirà di seguito proprio del DPS del Comune di ADEMPIENZIA non prima però di aver evidenziato l'urgenza di iniziare tale attività a partire dalla sensibilizzazione della Dirigenza che è investita di rilevantissime responsabilità in tema di data protection, non sempre accompagnate da una adeguata consapevolezza.
Si ritiene fondamentale "collegare" tali interventi all'attuazione del Codice dell'Amministrazione digitale e non solo.
Risultano molto positivi gli interventi per la Sicurezza informatica già attuati (ad es. per la "sicurezza perimetrale)" e quelli programmati dal Settore sistemi informativi (ad es. per una gestione centralizzata e sicura delle credenziali di autenticazione che tenga conto dei diversi profili di autorizzazione o anche per la gestione centralizzata e sicura di tutti i "logfiles," per tutti i Sistemi) di cui si raccomanda la pronta attuazione. Tuttavia adottando una visione globale, considerando che la sostanza del problema non si riduce al solo approccio tecnico-informatico, tali interventi, benché necessari e opportuni, non possono essere considerati sufficienti, specie se non accompagnati da un sufficiente grado di consapevolezza diffusa che riguardi l'intero ENTE.

3.1 Misure inerenti tematiche specifiche.

Si è detto sopra sia delle misure previste dal Codice che della tematica specifica riguardante gli ADS (Amministratori di Sistema); ritengo di dover aggiungere una segnalazione specifica anche in relazione ad altre tematiche peculiari sulle quali ho avuto l'impressione di una problematicità nel Comune di ADEMPIENZIA:
1. disciplina sull'utilizzo della Posta elettronica ed Internet da parte dei dipendenti sul posto di lavoro;
2. Gestione dei RAAE (rifiuti di apparecchiature elettriche ed elettroniche) con riferimento alla problematica della presenza di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute per la dismissione o la vendita o a seguito di riparazioni e sostituzioni.
*Si tratta di due casi sui quali si è espressamente pronunciato il Garante, nel primo caso con **le linee guida del Garante per posta elettronica e internet**, (Gazzetta Ufficiale n. 58 del 10 gennaio 2007, Registro delle deliberazioni, Del. n. 13 del 1° gennaio 2007) è stata segnalata la necessità di "adottare un disciplinare interno" per affrontare la complessa problematica; nel secondo, con il Provvedimento **Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali** (13 ottobre 2008 G.U. n. 287 del 9 dicembre 2008) si sono prescritti specifici comportamenti da adottare a riguardo.*

***Soluzione Consigliata**: Nel quadro del Piano strategico d'intervento suggerito ed in fase di realizzazione dell'"intervento operativo" di cui al punto precedente, si suggerisce di prevedere specificamente le misure necessarie a conformarsi ai citati Provvedimenti del Garante. Si tenga presente che le soluzioni concrete sono di natura prevalentemente organizzativa e comportamentale; pertanto è fondamentale accompagnare l'adozione di un disciplinare con lo strumento della formazione (a partire dai Dirigenti).*

4. Il DPS del Comune di ADEMPIENZIA:

Prendendo come punto di riferimento il DPS adottato nel gennaio 2011 (che è poi, in linea di massima, il risultato di una sostanziale conferma dei DPS adottati negli anni precedenti) e dando per già espressi (si veda sopra, il punto 2) i dubbi e le perplessità circa la modalità formale di adozione del DPS e soprattutto l'efficacia delle prescrizioni in esso contenute (con riferimento alla parte in cui si individuano i profili di Responsabilità delle varie figure coinvolte nel trattamento), in relazione al suo contenuto, esso appare non completo sotto i seguenti profili:
1. non adeguata individuazione dei trattamenti;
2. non adeguato collegamento tra questi e le strutture dell'Ente ove gli stessi sono incardinati (specie le micro-strutture);
3. non sufficientemente valutabile il collegamento tra Trattamenti / Strutture / Responsabilità / Comportamenti standardizzati;
4. non adeguata analisi dei rischi in relazione né a singoli trattamenti, né a gruppi omogenei di trattamento, né a specifiche categorie di dati, né con riferimento alle singole Strutture (neppure quelle di massima dimensione), né con riferimento ai Trattamenti eseguiti in tutto o in parte all'esterno (outsourcing);

5. conseguentemente a quanto rilevato nel punto precedente, appare non adeguata l'individuazione delle misure in relazione agli specifici rischi; questo punto, insieme al precedente, ***è cruciale*** *poiché lo scopo fondamentale del DPS è quello di rilevare i* ***rischi concreti*** *al fine di neutralizzarli/ridurli al minimo e dunque deve necessariamente contenere, almeno in relazione a tipologie omogenee di rischio individuate, le relative "contromisure" (misure di sicurezza, appunto). Dunque se, ad esempio, in relazione al comportamento degli operatori si ritiene che vi sia un rischio ALTO di "sottrazione di credenziali di autenticazione" o uno MEDIO generato da una "carenza di consapevolezza, disattenzione o di incuria bisogna poi, necessariamente descrivere in che modo (con quali misure) si intende ridurre o neutralizzare tali rischi;*
6. mancata integrazione del DPS con documenti relativi a situazioni e tematiche di rischio specificamente individuate dal Garante (ad esempio con specifici Provvedimenti) sulle quali è opportuna e, talvolta, obbligatoria (ex art. 154 Codice) una adeguata valutazione del rischio e la relativa adozione di specifiche misure di sicurezza (anche solo di tipo organizzativo): ad es., come detto, Posta elettronica, Internet, ADS, RAAE (Rifiuti di apparecchiature elettriche ed elettroniche).

Soluzione Consigliata*: Nel quadro del Piano strategico d'intervento di cui sopra, si suggerisce di prevedere specificamente l'adozione di una procedura che conduca alla realizzazione di un DPS "concreto e non burocratico" che non sia necessariamente un documento "corposo" e "complicato" (l'attuale si compone di circa 90 pagine di cui una gran parte è molto "teorica" e poco significativa per la natura operativa che dovrebbe avere un DPS) ma che contenga necessariamente uno autentico sforzo di analisi e di valutazione di rischi concreti individuando le modalità operative, adottate o da adottare, per ridurre al minimo i suddetti rischi. Inevitabile il coinvolgimento, anche questo reale e non burocratico, di tutti i Settori (a partire dai Dirigenti). Fondamentale imparare come si fa, in maniera concreta. Necessario dunque programmare una attività di formazione/affiancamento semplice ed efficace che renda poi autonoma ogni struttura, fermo restando la necessità di avere poi un momento di sintesi finale. Da valutare insieme al Segretario generale la "tipologia" e la forma più opportune dell'atto con il quale adottare il DPS.*

5. Considerazioni conclusive

In conclusione e riassumendo quanto sopra esposto, a proposito della conformità della situazione in atto presso il Comune di ADEMPIENZIA al quadro normativo vigente in materia di privacy e misure di sicurezza, si ritiene che la situazione in atto sia caratterizzata da diversi elementi di criticità quali:
1. dubbi sulla correttezza della modalità "formale" di adozione del DPS e sull'efficacia delle prescrizioni in esso contenute con particolare riferimento alla parte in cui si individuano i profili di Responsabilità delle varie figure coinvolte nel trattamento;
2. non sufficiente chiarezza nella individuazione (in concreto e non solo in teoria) delle diverse figure previste dal Codice, dei rispettivi ambiti di competenza e della conseguente ripartizione dei vari profili di Responsabilità;
3. mancata adozione di alcune importanti misure di sicurezza previste dal Codice;
4. mancata adozione degli obblighi derivanti da altri Provvedimenti ed Atti del garante del Garante: ad es. in materia di ADS (Amministratori di Sistema) o di disciplina sull'utilizzo della Posta elettronica ed Internet da parte dei dipendenti sul posto di lavoro oppure della gestione dei RAAE (Rifiuti di apparecchiature elettriche ed elettroniche);
5. inadeguatezza del DPS esistente, specie per la sostanziale mancanza della sua parte fondamentale costituita da una concreta analisi dei rischi ed altrettanto concreta, e conseguente, adozione delle misure idonee a prevenire i rischi stessi;
6. carenza di una adeguato grado di "consapevolezza" da parte dei dipendenti e di una cultura diffusa della sicurezza in tema di data protection;
7. carenza di una visione strategica condivisa che colleghi il tema della sicurezza a fini di privacy, con il concetto più ampio di tutela del patrimonio informativo, a sua volta fondamentale per la realizzazione di una "solida" Amministrazione digitale.

Le suddette criticità possono avere per l'Ente una pluralità di ripercussioni negative: innanzitutto sul piano concreto (in termini di effettiva sicurezza, disponibilità integrità ed affidabilità del patrimonio informativo di cui dispone e su cui basa la propria attività istituzionale) ed inoltre sul piano giuridico, in

termini di Responsabilità civile, Penale ed Amministrativa.
Anche se nel corso degli ultimi anni, come detto sopra al punto 3, sono stati messi in campo interventi molto positivi per la sicurezza informatica dell'Ente (alcuni già attuati ed altri programmati dal Settore Sistemi informativi, che si raccomanda di portare a compimento), tuttavia adottando una visione globale, considerando che la sostanza del problema non si riduce al solo approccio tecnico-informatico, tali interventi, benché necessari e opportuni, non possono essere considerati sufficienti, specie se non accompagnati da un adeguato grado di consapevolezza diffusa che riguardi l'intero ENTE e da altre importantissime misure che spesso sono prevalentemente e/o esclusivamente di natura organizzativa e/o comportamentale.
Per queste ragioni si raccomanda l'adozione di un Piano strategico d'intervento che affronti la situazione nella sua complessità. Gli elementi fondamentali di tale strategia dovrebbero essere, in linea di massima, i seguenti:
1. adozione di una delibera di Giunta che, oltre a definire le linee d'azione del Piano, chiarisca la ripartizione dei profili di Responsabilità, assegni con precisione compiti, ruoli e funzioni in conformità alla normativa vigente (inclusa una modalità operativa di verifica sull'attività dei RESPONSABILI del trattamento) e dia mandato ai Responsabili di adempiere al Provvedimento in materia di ADS, Posta Elettronica ed Internet, Raee ecc., sulla base di precisi indirizzi;
2. realizzazione di un intervento di formazione (peraltro obbligatorio ai sensi del punto 19.6 dell'allegato B del Codice) che, graduato sui diversi profili omogenei di Responsabilità e di Incarico, contribuisca a creare quel livello minimo di consapevolezza (innanzitutto tra i Dirigenti) senza il quale è impossibile raggiungere un livello adeguato di affidabilità, oltretutto propedeutico ed imprescindibile per la realizzazione di una "solida" Amministrazione digitale;
3. programmazione di un intervento operativo (eventualmente con affiancamento di elevata competenza) volto ad innalzare il livello di sicurezza nella salvaguardia del patrimonio informativo dell'Ente (anche di quello che non ha una natura di dato personale) che preveda, a valle dell'attività formativa di cui al punto precedente (o in parallelo), l'individuazione delle misure mancanti, ne definisca modalità (concrete) e tempi di adozione;
4. adozione di una procedura per la realizzazione di un "autentico" DPS attraverso un'attività di formazione/affiancamento semplice ed efficace che renda poi ogni struttura in grado di operare in piena autonomia per una reale analisi e valutazione dei rischi concreti;
5. completamento, integrazione e revisione di tutta la documentazione, anche di natura regolamentare necessaria ai fini del corretto allineamento alla normativa in materia di data protection e sicurezza del patrimonio informativo.

Per quanto espressi in forma schematica, si ritiene che tali interventi siano fondamentali per consentire, non solo il riallineamento della situazione concreta del Comune di ADEMPIENZIA alla normativa vigente in materia di tutela dei dati personali, ma soprattutto per la creazione di una situazione di reale sicurezza, affidabilità, integrità e disponibilità del patrimonio informativo dell'Ente che è condizione indispensabile ed imprescindibile per la realizzazione di una "solida" Amministrazione digitale in linea con il Codice dell'Amministrazione digitale e, soprattutto, in grado di realizzare la missione oggi assegnata alla Pubblica Amministrazione locale nel contesto della Società dell'informazione e della conoscenza.

4. Riflessioni conclusive

La Pubblica Amministrazione italiana, di cui gli Enti locali costituiscono il sistema nervoso diffuso capillarmente sull'intero territorio nazionale, opera necessariamente su informazioni e dati, sempre più dematerializzati, che molto spesso hanno natura di dato personale e che talvolta sono anche di tipo sensibile e/o semi-sensibile.
Essa opera nel contesto della Società dell'informazione globale e nel quadro normativo europeo che, a seguito dell'entrata in vigore del Trattato di Lisbona, ha costituzionalizzato il diritto fondamentale alla protezione dei dati personali, espressamente riconosciuto nella Carta dei diritti fondamentali dell'UE (art. 8), nell'art. 39 TUE e nell'art. 16 TFUE. Sono trascorsi circa quindici anni dall'adozione della prima normativa organica italiana in materia di privacy e *data protection* (La L. 675/96, successivamente abrogata e sostituita dal cosiddetto Codice della Privacy) e oltre dieci anni dal primo regolamento - il DPR 318/99 (anche questo successivamente abrogato e sostituito da parte del Codice) - che ha specificato le misure minime di sicurezza

obbligatorie presidiate, peraltro, anche da sanzioni penali.
In tale quadro complessivo, alla luce della mia esperienza personale, pertanto limitata e parziale, cui ho fatto riferimento nelle pagine precedenti, ritengo che il grado di recepimento sostanziale della cultura della privacy nel sistema pubblico italiano, con particolare riferimento alla PA locale, non sia pienamente soddisfacente.
La situazione ha indubbiamente una sua complessità ed articolazione che non possono essere compiutamente rappresentate in poche righe; come pure, certamente, vi sono realtà organizzative che si sono strutturate in maniera eccellente per rispondere alle sfide della digitalizzazione e della protezione dei dati. Sono, però, altresì convinto che siano ampiamente diffuse realtà che, specie nel contesto complessivo sommariamente delineato, manifestano delle vere e proprie patologie da affrontare e rimuovere con assoluta urgenza.
Mi sembra, infatti, che troppo spesso la questione privacy e *data protection* venga vissuta nel concreto come un fastidio, un impaccio, un male necessario, un costo, un appesantimento, una seccatura ecc. Che molto spesso ciò sia causato dalla carenza di interventi appropriati di adeguamento culturale del personale della PA; che ciò determini un grado complessivo di consapevolezza non sufficiente da parte degli operatori, i quali, a vario titolo, trattano quotidianamente dati personali, anche di natura sensibile e semi-sensibile.
Quanto agli Amministratori pubblici locali, nella maggior parte dei casi essi sono del tutto impreparati a confrontarsi con la questione della sicurezza, affidabilità e disponibilità del patrimonio informativo degli Enti che sono chiamati a guidare, nonostante esso costituisca la base di qualsiasi attività svolta e servizio erogato dalla PA nel perseguimento di rilevanti finalità di interesse pubblico.
Continua poi ad essere troppo diffusa la convinzione che in fondo queste tematiche, come pure quelle legate alla sfida della digitalizzazione della PA, abbiano una valenza meramente tecnico-informatica, e che pertanto esse siano materia di cui si deve occupare il solo Dirigente -informatico, quando l'Ente ne è dotato, o il perito informatico (se c'è..) o il consulente-informatico o, ancora, il dipendente, di qualsiasi categoria e profilo professionale, che abbia una cosiddetta sensibilità informatica.
Questa impostazione costituisce un clamoroso errore che, oltre ad essere in sostanziale contrasto con la normativa europea e nazionale vigente, impedisce di fatto una presa in carico sostanziale della questione da parte dell'intera struttura del singolo Ente, con particolare riferimento alla PA locale. E anche se la situazione tende ad accentuarsi nelle organizzazioni di piccola e media dimensione prive di Dirigenza, anche in molti Enti più grandi, ove questa è presente, l'atteggiamento ed i risultati complessivi, al fondo, non sono poi così diversi proprio a causa della tendenza a collocare la questione nella casella tecnico-informatica.
La Pubblica amministrazione italiana nel suo complesso, e dunque anche il sistema della Pubblica Amministrazione locale, vive un passaggio decisivo nella transizione verso l'Amministrazione digitale e la sostanziale dematerializzazione delle attività amministrative. Ne consegue che il patrimonio informativo della PA, ed in primo luogo quello che ha natura di "dato personale" ma non solo, rappresenta più che mai un bene fondamentale e strategico dell'Ente che va dunque gestito e tutelato in maniera adeguata e sicura. In base alla normativa vigente in materia, tutti gli operatori - a partire dalle massime figure apicali sino ad arrivare ai dipendenti di categoria B - della struttura organizzativa di ogni Ente Pubblico, compresi i Gestori di pubblici servizi, sono coinvolti nelle attività di trattamento di dati in generale e di dati personali in particolare e, conseguentemente, sono destinatari di altrettanti doveri ed obblighi da cui discendono anche delle responsabilità, anche se graduate per funzioni differenziate. Nonostante ciò, la materia della sicurezza e protezione dei dati personali, continua erroneamente e troppo spesso ad essere ritenuta di stretta ed esclusiva competenza degli operatori con profilo tecnico-informatico presenti all'interno degli Enti. Al contrario essa ha invece una portata molto più ampia che coinvolge:
a) in primo luogo, i Dirigenti e funzionari dotati di responsabilità organizzative (prioritariamente interessati dalle rilevantissime responsabilità, anche penali, che il Codice della Privacy prevede in diversi casi di omessa o inidonea applicazione delle norme specifiche in materia) i quali nella maggior parte dei casi concreti riscontrabili sul campo sono individuati, oltretutto, quali "Responsabili del Trattamento" e talvolta anche quali "Amministratori di Sistema" all'interno delle strutture organizzative in questione;
b) così come riguarda, benché con implicazioni diverse, senz'altro anche tutti gli altri operatori, i quali, a seconda dei casi saranno quanto meno qualificabili come "incaricati del trattamento" e "operatori di sistema".
Risulta dunque evidente l'esigenza di operare in maniera decisa, accurata e costante, in primo luogo, per ribaltare radicalmente la prospettiva attuale e far sì che la questione della sicurezza ed affidabilità del patrimonio informativo della PA, sia assunta come una questione strategica e non settoriale, da inquadrare in

maniera sistematica e integrata in collegamento con la realizzazione dell'amministrazione digitale e con la conseguente necessità di revisionare l'intero sistema procedurale e documentale dell'Ente; in secondo luogo, e anche al fine di rendere realizzabile quanto appena enunciato, per innalzare il livello complessivo di consapevolezza in materia di sicurezza e protezione dei dati personali all'interno delle strutture organizzative della PA, affinché il passaggio dall'Amministrazione tradizionale a quella digitale possa avvenire, oltre che nel pieno rispetto della legalità e in maniera efficace, in un contesto di sicurezza sostanziale e di rispetto dei diritti fondamentali dei cittadini.

Prof. Avv. Sandro Di Minco (**)

(*) Benché le riflessioni sopra esposte siano state effettuate con esplicito riferimento al settore della Pubblica Amministrazione, e con prevalente attenzione alla PA locale, si ritiene che gran parte di esse abbiano una loro validità di fondo anche in riferimento al settore privato, con le dovute distinzioni relative alla differenza di contesto.

(**) Avvocato, esperto e consulente in Diritto dell'informatica, Amministrazione digitale e Privacy; Professore J. Monnet di Diritto dell'informatica nell'Unione europea Titolare del Modulo europeo GLOBALISATION AND THE COMMUNITY APPROACH FOR AN INFORMATION SOCIETY. CURRENT GENERAL LEGAL FRAMEWORK e docente di Diritto comunitario e delle nuove tecnologie nell'Università degli studi di Camerino; Docente nel Master di Diritto dell'informatica e teoria e tecnica della normazione dell'Università degli Studi "La Sapienza" di Roma. (sandro.diminco@tin.it)