Informatica

Innovazione tecnologica: buoni propositi e discutibili realtà

di Nicola Bortolotti

Nell'ultimo SMAU, un salone decisamente in tono minore - a testimonianza del difficile momento che sta vivendo il settore informatico, uno spazio di rilievo era occupato dagli espositori istituzionali, in primis dal governo italiano che, con i suoi progetti di "e-government" e di "e-democracy" orientati alla "società dell'informazione", sta tentando - su una linea già profondamente marcata dal precedente esecutivo - di colmare un innegabile e profondo "gap" sintetizzato dalle parole del ministro Lucio Stanca, così come appaiono nella presentazione del recente "Rapporto innovazione e tecnologie digitali in Italia": "L'Italia, negli anni, ha investito poco in queste tecnologie ed in particolare in quelle informatiche in cui non è andata oltre il 65% della media dell'Unione Europea e il 40% degli Stati Uniti. Ed anche per questo il nostro Paese, malgrado i suoi valori di imprenditoria e di lavoro, ha accumulato un serio differenziale di produttività e quindi di competitività, un differenziale irrecuperabile senza un grande ed urgente impegno innovativo".

Finanziamenti poco mirati

In realtà il punto della situazione dovrebbe essere non solo sul "quanto" si investe ma assai di più sul "come". Che - sul fronte tecnologico - vi siano già stati "grandi e urgenti impegni innovativi" da parte sia dell'attuale che del precedente governo nell'arco di quasi un decennio, è fuori di dubbio. Ciò non ostante, i risultati duraturi sostanzialmente modesti (fatta eccezione per i portali governativi e poco altro) dovrebbero fare riflettere, in quanto diretta conseguenza di errori, sovrapposizioni, finanziamenti poco mirati, misure tampone, leggi discutibili o premature, miopia complessiva a livello europeo.
Gli esempi, al proposito, sono numerosi e pervasivi. Si pensi, per iniziare, agli investimenti in beni e servizi informatici. Esistono numerose agevolazioni e finanziamenti - anche a fondo perduto - tuttavia temporanei ed erogati "a pioggia" o senza nessun disegno strategico sotteso, della cui esistenza i legittimi destinatari sono spesso ignari. Che trasformazione strutturale possono indurre misure siffatte?

Ammortamenti accelerati

Assai meglio sarebbe affrontare alla radice il problema fondamentale, ossia il fatto che imporre ammortamenti pluriennali su beni e servizi avanzati - la cui obsolescenza accelerata spesso limita a dodici, massimo ventiquattro mesi la vita utile - è semplicemente grottesco. In sostanza sarebbe da considerare, per beni e servizi informatici, una sorta di "legge Tremonti" permanente, cercando di destreggiarsi tra le burocratiche e spesso anacronistiche insidie a cui costringono le "armonizzazioni" comunitarie e gli inevitabili abusi ed elusioni che una tale misura potrebbe suo malgrado incentivare. Non è certo un compito facile ma, nel caso in cui si volesse ancora procrastinare il problema, non si potrà che prendere atto anche in futuro della scarsa (ma giustificata) propensione delle aziende all'innovazione tecnologica: innovazione che - oltre ad investimenti ingenti e ripetuti - impone anche un cambiamento di mentalità, di procedure, di protocolli - con i conseguenti obblighi e costi formativi - tutt'altro che lievi.

Informatica, figlia di un dio minore

Che l'informatica sia sempre (e spesso a sproposito) utilizzata come specchietto per le allodole o facile espediente pubblicitario o giornalistico, lo si può facilmente desumere anche in ambito legale. Mentre la legislazione sempre più spesso si occupa del "mondo digitale" anche sul versante penale prevedendo da almeno dieci anni aggravanti tutt'altro che

lievi ed evocate non di rado a sproposito (in primis l'"Accesso abusivo ad un sistema informatico o telematico" introdotto dall'ormai famoso articolo "615ter" della Legge 23 dicembre 1993, n. 547 e il "640ter" sulla "Frode informatica" - si veda la nota 1), malgrado il concetto di virus sia stato esplicitamente introdotto con il "615quinquies", ciò non ostante la figura dell'informatico in ambito legale è incredibilmente e vergognosamente considerata - ancora oggi - inesistente.
Le CTU (Consulenze Tecniche d'Ufficio) in ambito informatico, infatti, di fatto non esistono nelle tabelle ufficiali dei compensi, per cui i giudici possono retribuire i periti solo "a vacazione", ossia in modo poco più che risibile.
La gravità di una siffatta situazione - non adeguatamente segnalata e denunciata - è riscontrabile nella maggior parte delle motivazioni di sentenza che riguardino l'ambito informatico/telematico: da una parte CTU - la cui importanza sarebbe invece fondamentale - spesso inadeguate, in quanto lacunose e approssimative, redatte senza la necessaria accuratezza ed esperienza; dall'altra CTP (Consulenze Tecniche di Parte) mediamente di adeguata caratura, in quanto commissionate "a libero mercato" dagli imputati ad esperti del settore.
È difficile comprendere perché nessuno degli esecutivi abbia ancora corretto questa evidente anomalia.

Il "digital divide"

È un altro termine citato frequentemente dal mondo politico e imprenditoriale, e rappresenta un problema mondiale concernente il sempre più profondo solco che divide chi può avere accesso alle moderne tecnologie e chi invece ne rimane ai margini. Calato nella realtà dell'Italia, il "digital divide" si traduce principalmente in due problematiche: disporre di risorse hardware e software a basso costo e la possibilità di accedere alle reti "a banda larga" (più semplicemente - anche se non esattamente - ad una connessione ADSL).
Per quanto riguarda l'hardware, nei paragrafi precedenti è stata già evidenziata la assoluta necessità di venire incontro, sotto il profilo fiscale, alla rapida obsolescenza degli investimenti tecnologici. Sarebbe anche opportuno incentivare con forza - più di quanto non avvenga oggi - la strategia delle "donazioni". Ma sul fronte software la questione è assai più complicata, con grosse responsabilità anche a livello europeo.

La politica bifronte sull'Open Source

Il grande movimento dell'"Open Source", il termine con il quale si identificano software i cui sorgenti sono accessibili e modificabili, rappresenta una composita comunità mondiale dal peso rilevante e vieppiù crescente, con la quale non è ormai possibile non fare i conti a livello sovrannazionale.
Anche limitandosi ad un solo aspetto - per molti versi riduttivo - questo significa, dal punto di vista dell'utente - sia esso un privato o la pubblica amministrazione, un'impresa familiare o una multinazionale - poter contare su programmi e formati "aperti", controllabili (soprattutto dal punto di vista dell'affidabilità e della sicurezza) e gratuiti. Se si pensa che il costo di un sistema operativo e di un software di office automation "tradizionali" può incidere anche per il 45% sul costo complessivo di un Personal Computer completo nuovo, è facile immaginare quanto una scelta - soprattutto politica - sul fronte dell'Open Source possa influire a colmare la voragine del "digital divide".
A tale proposito, tuttavia, visti gli enormi interessi in gioco, le risposte fornite a livello non solo italiano ma europeo (e non solo) sono state a dir poco ambigue ed è sufficiente un minimo esempio al proposito.
Risale al 1998 la creazione da parte della Comunità Europea di una commissione di lavoro sul software libero che produsse un "white paper" al quale seguirono specifici finanziamenti nell'ambito del programma IST scarsamente utilizzati e che - spesso - non avevano nulla a che vedere con l'Open Source.
Nel frattempo è stata anche parzialmente finanziata con fondi comunitari l'ECDL foundation (www.ecdl.com, a cui si deve la cosiddetta "Patente Europea del Computer" il cui referente in Italia - www.ecdl.it - è AICA - www.aicanet.it) i cui "syllabus", ossia i programmi d'esame, nonostante le dichiarazioni d'intenti sono pedissequamente ricalcati sulla suite Microsoft Office e sul sistema operativo Microsoft Windows e - solo tardivamente e malamente - sono stati aperti a un prodotto non Microsoft come Linux (in una specifica distribuzione) e l'obsoleto Sun StarOffice 5.2 (si veda al proposito il link
linfe.it/OpenLab/NoteFormazione/openECDL).
Da una parte - dunque - si "flirta" con la comunità open source, dall'altra si fa formazione e si certificano competenze basandosi su prodotti commerciali chiusi e onerosi (è bene sottolineare questi ultimi attributi, in quanto l'essere open source non impedisce affatto la commercializzazione).

E il software libero in Italia?

Nel belpaese non si sfugge alla "regola" europea. Da un lato aperture e commissioni di lavoro sull'open source; dall'altro accordi strategici di molti ministeri con i "grandi" del software, convenzioni con Consip, imponenti acquisti di licenze (malgrado le raccomandazioni della defunta AIPA) da parte della Pubblica Amministrazione, nonostante in più punti non ottemperino alle indicazioni contenute nel DPCM 6 agosto 1997, n. 452 "Capitolato (...) relativo (...) alla licenza d'uso dei programmi" (si veda in proposito la nota 2).

E dire che - allo stato attuale - un prodotto come Open Office (www.openoffice.org) ha raggiunto una piena maturità anche nella versione italiana: è un completo pacchetto di office automation multipiattaforma, sostanzialmente immune ai virus, in grado di importare ed esportare files in formati "proprietari" e consente - con immediatezza e a costo zero - di creare di ogni documento la versione PDF (perfettamente "portabile" e leggibile su ogni computer con gli Adobe reader gratuiti reperibile all'indirizzo www.adobe.it).

La "banda larga"

La diffusione delle connessioni veloci a Internet (ADSL, ma non solo) rappresenta un altro punto dolente. La strada degli incentivi governativi fin qui seguita non è stata solo inefficace ma addirittura dannosa: con la Finanziaria 2003 si è voluta malamente "premiare" (in maniera ben poco trasparente - una sorta di lotteria "a tempo" e fino ad esaurimento fondi gestita dai fornitori di accesso stessi) la stipula di nuovi contratti dimenticando che in molte località economicamente poco appetibili l'ADSL non arriva ancora. In prospettiva storica si ricorderà che anche le comunicazioni telefoniche "interurbane" venivano considerate poco redditizie, e non a caso furono gli stati a doversene sobbarcare l'onere. Con i gestori privati, invece, questo contributo ADSL (se erogato) è andato proprio nel senso contrario: una roulette sbagliata e comunque di corto respiro, che non ha incentivato nessun provider ad estendere o migliorare la propria rete aggravando - anziché mitigando - il "digital divide" italiano.

In aggiunta a questo c'è da rilevare come un'altra questione rimanga sostanzialmente irrisolta, mentre l'authority sta a guardare: oggi, infatti, può essere particolarmente difficile cambiare gestore ADSL, in quanto la linea può rimanere anche per mesi associata al fornitore precedente bloccando ogni nuova attivazione. Da rilevare che - tecnicamente - una operazione simile richiede al massimo una trentina di secondi; si dovrebbe dunque agire con decisione per stroncare questo apparente disservizio che costituisce in realtà un autentico abuso nei confronti degli utenti nonché un atto di concorrenza sleale.

Sul fronte normativo - tuttavia - non sono tutte spine: la recente azione governativa è stata infatti sostanzialmente positiva per quanto riguarda le reti via radio, come rilevato nel numero precedente e in quello corrispondente dell'anno scorso.

Il "caso" Consip

Ritornando al difficile rapporto tra informatica e pubblica amministrazione, emblematico è il "caso Consip", risoltosi solo da pochi mesi. Consip S.p.A. nasce da un ambizioso e condivisibile progetto previsto all'articolo 26 della Legge Finanziaria 2000 (legge n.488 del 23 dicembre 1999): razionalizzare gli acquisti della P.A. consentendo ingenti risparmi complessivi.

Nonostante i buoni propositi e i notevoli risultati conseguiti in altri settori, in campo informatico il sito di riferimento www.acquistinretepa.it è diventato ben presto un incubo, in quanto il meccanismo delle convenzioni (peraltro giocoforza ristrette ad alcuni grossi fornitori, il che ha suscitato l'interesse dell'antitrust), in un mondo così rapidamente mutevole come quello dell'informatica, di fatto "ingessavano" o addirittura impedivano buona parte degli investimenti. A ciò andava di frequente aggiunta una inaccettabile incertezza nei tempi di fornitura.

In molti casi, poi, non vi era neppure contenimento della spesa, in quanto i prezzi del "negozio sotto casa" non di rado erano inferiori a quelli delle convenzioni. Singolare - a questo proposito - la posizione di alcune avvocature che giustificavano l'acquisto a prezzi superiori a quelli di mercato. Ma - nello stesso parere del 3 marzo 2003 - si forniva una agevole via di fuga, specifica per il mondo dell'informatica, qualora nelle convenzioni Consip non fosse compreso quanto richiesto (si veda la nota 3).

I crescenti malumori generali hanno poi trovato una espressione ufficiale nel luglio quando (fonte ADNKronos) vi è stata una "dura denuncia della Corte dei Conti sul progetto degli acquisti centralizzati, gestiti oggi dalla Consip: il sistema potrebbe favorire i cartelli tra le grandi aziende estromettendo di fatto le piccole imprese dalle gare, mentre non vi sarebbero prove certe sui risparmi conseguiti. Anzi, in alcuni casi le amministrazioni stesse avrebbero denunciato un aggravio delle spese e un peggioramento della qualità di beni e servizi ricevuti".

L'imbarazzante "affaire" ha poi trovato una ormai improcrastinabile e razionale soluzione con l'allegato alla Legge 1 Agosto 2003 n. 212, che ha convertito, con modificazioni, il Decreto Legge 24 giugno 2003, n. 143: scompare, in particolare, l'obbligo di servirsi di Consip qualora si contrattino con altri soggetti costi uguali o inferiori (si veda la nota 4).

Leggi vessatorie

L'innovazione tecnologica avrebbe assoluta necessità di leggi e regolamenti chiari e applicabili. Purtroppo la materia complessa e la casistica sostanzialmente "nuova" non aiutano il legislatore, che da circa dieci anni per un passo avanti ne fa uno indietro.

La normativa sul diritto d'autore, più volte modificata, con le sue incomprensibili regalie alla Siae (l'obbligo di apposizione del "bollino" introdotto dalla Legge 248/2000 che ha avuto bisogno di due chiarificazioni e delimitazioni, la prima con il DPCM 338/2001 e la seconda con il DPCM 296/2002) è uno dei tanti esempi della sostanziale incomprensione di chi legifera nei confronti del mondo digitale.

Sulla "guerra" dei "nomi a dominio" Internet è ormai la giurisprudenza a tenere banco (un recente caso da manuale, la storia di armani.it, è ben riassunto sulla rivista on-line Punto Informatico all'indirizzo punto-informatico.it/p.asp?i=44815).

Del lungo e difficile iter della firma digitale si tratta e si continuerà a trattare con regolarità su questa rivista, almeno sino a che gli sforzi non sortiranno un risultato chiaro e duraturo a livello europeo.

Ma la notizia di stretta attualità - anche questa a suo modo paradigmatica - è la pubblicazione sulla Gazzetta Ufficiale n. 174 dello scorso luglio del Decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" (si veda la nota 5).

Un "testo unico" è sempre un evento positivo ed in effetti questo codice, in vigore dal primo gennaio del prossimo anno, è un notevole compendio che prende l'avvio dalla nota Legge 675/96 "sulla privacy" passando per il tardivamente emesso regolamento di attuazione DPR 318/99 "sulle misure minime".

L'accoglienza riservata agli addetti ai lavori a questo decreto è fin troppo - e per certi versi inspiegabilmente - generoso. Forse perché - a detta di molti - di fatto istituzionalizza la figura dell'"esperto" in sicurezza dati.

La creazione o il consolidamento di alcune figure professionali qualificate, pur in una difficile contingenza di mercato, non può tuttavia far dimenticare che alcuni aspetti, decisamente vessatori nei confronti di tutti gli operatori informatici e caratterizzanti in negativo il DPR 318, sono stati in toto confermati, così come alcune ingenuità tecniche. Non essendovi state applicazioni concrete delle pesanti fattispecie contemplate nel precedente regolamento (e già criticate nel numero 2/2000 della rivista), esse sono state integralmente riproposte nel DL 196/2003: ad esempio il rovesciamento dell'onere della prova nel caso di danno cagionato a terzi, per cui - ad evitare un pesantissimo risarcimento in sede civile - si dovrà dimostrare l'indimostrabile in campo informatico, ossia provare "di avere adottato *tutte* le misure idonee a evitare il danno". Viene da sorridere, pensando alle CTU retribuite a vacazione... Rimangono altresì le severe conseguenze penali e resta anche il risibile richiamo ad aggiornare gli antivirus almeno ogni sei mesi (anche se - in realtà - il punto 16 dell'allegato parla ora di "idonei strumenti elettronici" e non più semplicemente di "programmi", il che potrebbe sottintendere anche firewall e altre soluzioni hardware). Sei mesi, come se la fulminea diffusione di virus su macchine dotate di software Microsoft in agosto e settembre, non avesse insegnato proprio nulla...

NOTE:

Nota 1 - Estratto dalla Legge 23 Dicembre 1993, n. 547

Art. 615ter - (Accesso abusivo ad un sistema informatico o telematico) - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubbli-

co, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
Art. 615quinquies - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) - Chiunque diffonde, comunica o consegna un programma da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a venti milioni".
Art. 640ter - (Frode informatica) - Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.
La pena è della reclusione da uno a cinque anni se e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con l'abuso della qualità di operatore del sistema.
Il delitto è punito a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Nota 2 - Estratto dal DPCM 6 agosto 1997, n. 452

Art. 38 - Modifiche ai programmi
(...)
4. Nel caso in cui l'amministrazione ritenga di continuare ad operare con la versione originaria dei programmi, deve darne comunicazione all'impresa, la quale rimane impegnata a continuare a prestare, su tale versione, i servizi e la collaborazione di supporto in atto.
5. L'amministrazione, per proprie esigenze operative, ha facoltà di effettuare autonomamente modifiche ai programmi in uso ed alla relativa documentazione. In tal caso il diritto d'uso delle modifiche appartiene all'amministrazione.
Art. 39 - Garanzia dei programmi
1. Fatto salvo quanto previsto dall'articolo 6, l'impresa garantisce per un anno l'amministrazione per i difetti e i vizi originari o sopravvenuti dei programmi non imputabili a fatto dell'amministrazione.
(...)
3. Salvo che l'amministrazione non chieda la risoluzione del contratto, l'impresa deve ripristinare la piena funzionalità dei programmi entro ventiquattro ore dalla richiesta dell'amministrazione o nel diverso termine indicato nel contratto.
Art.42 - Penalità per difetti di funzionamento
1. Per ogni giorno o frazione di giorno di non corretto funzionamento dei programmi, per cause, non imputabili all'amministrazione ovvero a forza maggiore o a caso fortuito, inerenti ai programmi stessi o ad altri funzionalmente connessi ovvero alle prestazioni connesse di cui all'articolo 33, comma 4, è applicata una penale pari, nei contratti che consentono l'utilizzazione dei programmi per un tempo determinato, ad un ventesimo de corrispettivo, ragguagliato ad un mese, e, negli altri contratti, al due per mille del corrispettivo dei programmi non utilizzabili. Sono fatti salvi le diverse misure previste nel contratto, nonché il risarcimento dell'eventuale maggior danno subito dall'amministrazione.

Nota 3 - Estratto dal parere prot. n° 03046 del 3 marzo 2003 dell'Avvocatura Distrettuale dello Stato di Firenze

"(...) Con tale ratio, che vede dunque il ricorso alle Convenzioni CONSIP come un beneficio per gli acquirenti pubblici globalmente considerati, contrasta, ad avviso della Scrivente, la possibilità di acquistare altrove, anche a condizioni singolarmente migliori, gli stessi beni oggetto di convenzione. L'episodico vantaggio di un singolo soggetto pubblico andrebbe infatti a detrimento degli altri. Si deve pertanto escludere, secondo questa Avvocatura, la possibilità di acquistare altrove anche a condizioni migliori, beni o servizi di cui alle Convenzioni.
Va da sé, naturalmente, che, affinché l'obbligo sussista, vi deve essere corrispondenza fra il bene o servizio di cui la singola Amministrazione necessita e quanto offerto dalle Convenzioni.
Così (e si veda il comma V dell'art. 24) è possibile 'svincolarsi' dalle Convenzioni quando, motivatamente si individuino le caratteristiche del bene o servizio di cui l'istituto necessita, e, altrettanto motivatamente, si riscontri che dette caratteristiche non sono comprese in quanto offerto dalle Convenzioni.
Un motivazione del genere può essere più agevole, ad esempio, per quanto attiene a prodotti informatici, per i quali la rapida obsolescenza e le quasi infinite possibilità di diversa configurazione consentono, per il migliore andamento della Amministrazione, di individuare un 'tipo di prodotto' ad hoc per ogni utilizzazione, quando si evidenzino esigenze particolari tali da far ritenere non sufficiente ricorrere ad apparecchiature standard, mentre ben più ardua si presenterebbe per prodotti - sostanzialmente fungibili come gli articoli di cancelleria e i carburanti."

Nota 4 - Estratto dall'allegato alla Legge 1 agosto 2003, n.212 - Modificazioni apportate in sede di conversione al DL 24 giugno 2003, n. 143

(...)
d) dopo il comma 4, è inserito il seguente:
"4-bis. Gli enti pubblici, le società pubbliche, i concessionari di pubblici servizi, nonché tutte le amministrazioni pubbliche, individuate nell'articolo 1 del testo unico di cui al decreto legislativo 24 luglio 1992, n. 358, e successive modificazioni, e nell'articolo 2 del decreto legislativo 17 marzo 1995, n. 157, e successive modificazioni, escluse quelle statali per i soli uffici centrali, possono stipulare ogni tipo di contratto senza utilizzare le convenzioni quadro definite dalla Consip S.p.a., qualora il valore dei costi e delle prestazioni dedotte in contratto sia uguale o inferiore a quello previsto dalle stesse convenzioni definite dalla Consip S.p.a. I contratti così conclusi sono validi e non sono causa di responsabilità personale, contabile e amministrativa, a carico del dipendente che li ha sottoscritti, previste al comma 4"

(...)

Nota 5 - Estratto dal Decreto legislativo 30 giugno 2003, n. 196

(...)
Art. 15 (Danni cagionati per effetto del trattamento)
1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
(...)
Nota all'art. 15:
- Si riporta il testo dell'art. 2050 del codice civile:
"Art. 2050 (Responsabilità per l'esercizio di attività pericolose).
- Chiunque cagiona danno ad altri nello svolgimento di una attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno."
(...)
Art. 169 (Misure di sicurezza)
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
(...)
Allegato B
Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del codice)
Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:
Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.