Informatica

Quando il garante è in ritardo ...

di Nicola Bortolotti

Giunti ormai alle ultime battute della vicenda del Documento Programmatico sulla Sicurezza (che in realtà costituirà - per le ragioni ricordate nel numero scorso - solo l'inizio di un periodo-pilota molto delicato e pericoloso per l'informatica nazionale, una fase nella quale saranno Fiamme Gialle, Forze dell'ordine e giudici a monopolizzare la scena, si spera con maggiore senso della realtà rispetto agli ultimi due esecutivi e alle associazioni di categoria) occorre sottolineare come ci si avvicini al termine ultimo del 30 Giugno - more solito - *all'italiana*, tanto che da più parti già si ipotizza (e si auspica) un'ulteriore proroga dei termini (impossibile da prevedere alla data di chiusura della rivista).

Non a caso il primo ad essere in sostanziale ritardo è proprio il garante della privacy, il quale - data la pervasività dell'obbligo del DPS (ormai prevalgono considerazioni oltremodo prudenziali - anche se assai discutibili - secondo le quali la redazione del documento sarebbe in pratica consigliabile a chiunque utilizzi nella propria attività almeno un personal computer...) - aveva ufficialmente promesso con largo anticipo la pubblicazione di un modello, di uno scheletro di DPS al quale ci si potesse rifare nella preparazione del proprio.

Nel comunicato stampa del 23 Marzo 2004 si poteva infatti leggere: "Un modello base semplificato sarà disponibile a breve sul sito del Garante www.garanteprivacy.it". Uno *specimen* rivolto specificamente alle piccole e medie realtà (il che non sorprende, giacché la maggior parte delle grandi società ne erano già obbligate dal DPR 318 del 1999 - peraltro con risibili risultati visti i disastrosi effetti di alcune recenti diffusioni virali...).

L'"a breve" si è tuttavia risolto in un lasso di tempo consistente, visto che solo il 13 Maggio sono state pubblicate sul sito www.garanteprivacy.it le "Prime riflessioni sui criteri di redazione del Documento programmatico sulla sicurezza". Riflessioni nelle quali era contenuta un'ulteriore promessa - ora significativamente e frettolosamente scomparsa dal database del garante all'URL - ormai vuoto - www.garanteprivacy.it/garante/document?ID=1002164 ma ancora fedelmente consultabile nella memoria cache del motore di ricerca Google (www.google.it) o in copia conforme su altri siti, e di cui esistono comunque ulteriori testimonianze (ad esempio nell'ottima rivista telematica Interlex www.interlex.it). Una promessa che testualmente recitava: "L'Autorità ritiene opportuno pubblicare il contributo che ne è scaturito, per stimolare osservazioni, richieste di chiarimento e proposte che esaminerà al fine di pubblicare su questo sito, *entro il 1° giugno prossimo*, un documento rivisto che potrà essere liberamente utilizzato come guida operativa per redigere il Dps".

Purtroppo il lasso di tempo, già esile, tra la "guida operativa" definitiva e il termine perentorio del 30 Giugno si è risolto in un autentico battito d'ali, giacché *solo l'11 Giugno* sul sito è finalmente comparsa la "Guida operativa per redigere il Documento programmatico sulla sicurezza" all'URL www.garanteprivacy.it/garante/doc.jsp?ID=1007736; un vademecum in forma tabellare che - data l'importanza - viene parzialmente riprodotto in calce a questo articolo corredato da un esempio di compilazione.

Da notare altresì il fatto che altri esempi di compilazione di DPS, la maggior parte dei quali conformi ai suggerimenti del garante, vengono offerti del tutto gratuitamente in rete, ad esempio all'indirizzo www.infocare.it/dps.doc e www.vesema.it.

Schema tipo di regolamento per i comuni

Si è intanto chiusa il 15 Giugno la fase di consultazione rivolta agli Enti locali concernente lo "Schema tipo di Regolamento per il trattamento dei dati sensibili e giudiziari" sempre previsto - come il DPS - dal Testo Unico sulla Privacy (D.Lgs 196/2003).

Come viene ricordato sul sito del garante (all'indirizzo

www.garanteprivacy.it/garante/doc.jsp?ID=1003536) tale regolamento - una volta approvato dall'Autorità - costituirà lo schema tipo al quale Comuni e Comunità montane potranno convenientemente conformarsi al fine di assolvere automaticamente gli obblighi normativi senza essere costretti a sottoporre la propria particolare soluzione al parere del Garante.

Entro il 30 settembre i Comuni e gli altri Enti locali dovranno infatti approvare un Regolamento che individui i tipi di dati trattati e le operazioni con essi eseguibili (ai sensi degli art. 20 e 181). Per quanto riguarda la fattispecie funebre-cimiteriale, la scheda interessata dal modello - e visionabile, previa richiesta di una password, sul sito Ancitel all'URL www.ancitel.it/regolamentodatisensibili/indice_trattamenti.asp - salvo modifiche sarà la 27 (Settore polizia municipale - Denominazione del trattamento: Attività di vigilanza edilizia, in materia di ambiente e sanità nonché di polizia mortuaria).

Ancora ritardi e ripensamenti sulla CIE

Segna intanto il passo il cammino della Carta d'Identità Elettronica, tanto da meritare la copertina di giugno della già citata rivista telematica Interlex. Le più che giustificate obiezioni tecniche del Ministro dell'Innovazione Stanca, che lo avevano portato a sostenere parallelamente il progetto della CNS - Carta Nazionale dei Servizi, non hanno trovato ancora interlocutori disposti ad ascoltarle, in primis il Ministro dell'Interno Pisanu. Si va dunque

delineando una fase dialettica che probabilmente non gioverà né alla bontà tecnologica delle soluzioni adottate, né alla rapidità di attuazione, né ai costi. Lo scoglio sul quale ci si è arenati è la necessità di una onerosa banda laser - resa ormai di fatto obsoleta dai progressi della tecnologia microchip; un bisogno che appare viepiù superato grazie a considerazioni che hanno portato a un ridimensionamento delle funzionalità da inserire nella CIE, che sempre più appare come complementare e non sostitutiva della CNS.

APPENDICE - Il modello di DPS del Garante

Contrariamente alle scelte effettuate da molte delle società e organizzazioni già da anni obbligate a redigere un DPS sulla scorta del DPR del '99, il Garante ha privilegiato - pensando soprattutto alle medie e piccole realtà - un conciso modello a tabelle. Tale scheletro, nonostante il suo apprezzabile schematismo, può comunque ben applicarsi a qualsiasi situazione - anche abbastanza complessa - ed ha il grande pregio della leggibilità, risultando dunque di facilissima manutenzione.

Poiché il documento programmatico va aggiornato con cadenza annuale, una scelta siffatta è decisamente preferibile a quella verbosa, puramente testuale, in quanto rende assai semplice ogni modifica.

Nel seguito i pochi commenti sono riportati tra parentesi quadre. Nelle tabelle sono stati fatti alcuni banali esempi di utilizzo delle stesse, senza alcuna pretesa di fungere da riferimento.

[Intestazione] _____

Via _____, _____

Il titolare dei dati

Sig. _____

[facoltativamente - con Responsabile designato ai sensi dell'art. 4 lett. g) del codice

Sig. _____]

adotta il seguente Documento Programmatico sulla Sicurezza (redatto ai sensi del Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del D.Lgs. 30 giugno 2003, n. 196 e conforme alle indicazioni del Garante contenute nella Guida operativa dell'11 Giugno 2004)

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali

ID	Finalità perseguita Attività svolta	Categoria interessati	Natura dati S=Sensibile G=Giudiziario	Struttura di riferimento	Altre strutture concorrenti al trattamento	Descrizione strumenti utilizzati
DPCP	Dati personali di dominio pubblico	clienti	--	Segreteria	no	Server Linux-Samba
DPCF	Dati personali forniti	clienti	--	Segreteria	no	come sopra
DPD	Dati personali	dipendenti	--	Amministrazione	No	come sopra
...	...	...	...	...	...	...

Data di aggiornamento: _____ Compilata da: _____

Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti

ID	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
DPCP	---	HD File server (PC Server)	PC Desktop e Laptop Windows 9x/2000/XP	LAN Ethernet 100 Base TX
DPCF	---	come sopra	come sopra	come sopra
DPD	---	come sopra	come sopra	come sopra
...	...	...	...	...

Data di aggiornamento: _____ Compilata da: _____

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità
Segreteria	DPCP, DPCF	acquisizione e caricamento, consultazione, manutenzione
Amministrazione	DPD	come sopra
Amministrazione	DPCP, DPCF	consultazione
...	...	...

Data di aggiornamento: _____ Compilata da: _____

[su questa base saranno stilate specifiche lettere di incarico - a termine - per gli appartenenti a ciascuna struttura]

Tabella 3a – Analisi dei rischi - Comportamenti degli operatori

ID	Rischi	Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
1a	sottrazione di credenziali di autenticazione	Si	media
2a	carezza di consapevolezza, disattenzione o incuria	Si	alta
3a	comportamenti sleali o fraudolenti	Si	media
4a	errore materiale	Si	Alta
5a	altro evento	No	

Data di aggiornamento: _____ Compilata da: _____

Tabella 3b – Analisi dei rischi - Eventi relativi agli strumenti

ID	Rischi	Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
1b	azione di virus informatici o di programmi suscettibili di recare danno	Si	Media
2b	spamming o tecniche di sabotaggio	Si	Bassa
3b	malfunzionamento, indisponibilità o degrado degli strumenti	Si	Alta
4b	accessi esterni non autorizzati	Si	Alta
5b	intercettazione di informazioni in rete	Si	Bassa
6b	altro evento	No	

Data di aggiornamento: _____ Compilata da: _____

Tabella 3c – Analisi dei rischi - Eventi relativi al contesto

ID	Rischi	Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
1c	accessi non autorizzati a locali/reparti ad accesso ristretto	Si	media
2c	sottrazione di strumenti contenenti dati	Si	alta
3c	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Si	alta
4c	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Si	bassa
5c	errori umani nella gestione della sicurezza fisica	Si	media
6c	altro evento	No	

Data di aggiornamento: _____ Compilata da: _____

Tab. 4.1 – Le misure di sicurezza adottate o da adottare

ID	Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare (tempi)	Struttura o persone addette all'adozione
1	Mirroring (RAID 1)	3b 3c 4c 5c	tutti	Si		Titolare
2	Backup su CD/DVD	2a 3a 4a 1b 2b 3b 2c 3c 4c 5c	tutti	Si		Segreteria
3	Antivirus	1b	tutti	Si		Titolare
4	Firewall su server	1b 2b 4b 5b	tutti	Si		Titolare
5	Proxy	1b 2b 4b 5b	tutti	Si		Titolare
6	Serrature	1c 2c	tutti	Si		Titolare
7	Credenziali accesso	2a 3a 4b 5b 1c	tutti	Si		Titolare
8	UPS su server	4c	tutti	Si		Titolare
9	Modifica credenziali	1a 3a	tutti	Si		Titolare
10	Manutenzione	3b	tutti	Si		Titolare
11	Password accensione	1c	tutti	Si		Titolare
12	Password savescreeen	1c	tutti	Si		Titolare
13	Backup su HD	2a 3a 4a 1b 2b 3b 2c 3c 4c 5c	tutti	Si		Titolare
14	...	...	...	...		...

Data di aggiornamento: _____ Compilata da: _____

Tab. 5.1 - Criteri e procedure per il ripristino della disponibilità dei dati

Ripristino banca/DB/archivio	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
tutti	masterizzazione presidiata su CD/DVD riscrivibile. In caso di ripristino, semplice copia del contenuto del/dei CD/DVD sull'area condivisa dell'hard disk	al termine del backup verifica automatica
...	...	...

Data di aggiornamento: _____ Compilata da: _____

Tab. 5.2 - Criteri e procedure per il salvataggio dei dati

Salvataggio banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
tutte	al termine di ogni settimana lavorativa, masterizzazione su CD/DVD con verifica finale	cassaforte	Segreteria
tutte	alle ore 14 e alle ore 22 di ogni giorno copia automatica di tutti i files nuovi e aggiornati su hard disk addizionale del server	server	nessuno
...	...	...	...

Data di aggiornamento: _____ Compilata da: _____

Tab. 6 - Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Nessuno	---	---

Data di aggiornamento: _____ Compilata da: _____

Tab. 7 - Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Server di posta elettronica POP3	Conservazione temporanea dei messaggi email ricevuti	Provider XXX	a carico del soggetto esterno secondo le clausole di fornitura del servizio
...	...	...	...

Data di aggiornamento: _____ Compilata da: _____