3. Cenni sulla regolamentazione normativa ed amministrativa in tema di sicurezza informatica nei sistemi informatici pubblici

Carlo Sarzana di S. Ippolito*

1. Premessa

Appare opportuno, ai fini della comprensione degli aspetti giuridici della sicurezza informatica, ricostruire il quadro normativo ed amministrativo relativo, quadro che, allo stato, come rilevato dalla dottrina specialistica, presenta indubbi caratteri di frammentarietà e di scarsa coerenza sistematica. I paragrafi che seguono cercheranno quindi di ricostruire, in modo necessariamente sintetico, le linee del trend normativo sviluppatosi nel corso dei decenni precedenti in modo da offrire un panorama il più possibile completo, della situazione concernente la materia e di consentire ai "*decision makers*" di valutare la situazione stessa ed, eventualmente, di intervenire sul piano politico-normativo allo scopo di dettare le prescrizioni che apparissero necessarie per regolamentare la materia in modo esaustivo e coerente nell'ambito pubblico. Va ricordato in argomento che l'importanza della predisposizione di sistemi efficienti di sicurezza informatica relativamente al settore pubblico è stata ben sottolineata nella Direttiva del Ministro per l'Innovazione e le Tecnologie del 16 gennaio 2002 allorché è stato affermato che le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese e che questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse[1].

* Presidente aggiunto onorario della Corte di Cassazione, componente del Comitato Tecnico Nazionale Sicurezza Informatica nella Pubblica Amministrazione.

1. In tema di sicurezza informatica e di "stato dell'arte" in materia va citato, per inciso, un rapporto sulla sicurezza informatica negli Enti Locali, a seguito di una ricerca effettuata nel luglio 2002, dall'ANCITEL secondo cui "...solo il 12% dei Comuni intervistati ha adottato sistemi di difesa derivati da una valutazione complessiva dei rischi e di una vera applicazione delle *policy* di sicurezza, integrando le tecniche di *firewalling* con quelle di *intrusion detection* ed *antivirus* centralizzato. Di contro ... il 48% dichiara di utilizzare almeno una delle due tecniche sopraccitate, dimostrando un certo grado di attenzione al problema... Il restante 40% del campione indagato, conferma la preoccupante e diffusa tendenza a trattare operativamente le problematiche della sicurezza informatica con una poco chiara visione progettuale e, conseguentemente, si assemblano sistemi di sicurezza destrutturati".

2. Nel campo della sicurezza informatica pubblica va ricordata la figura dell'Autorità Nazionale della Sicurezza, posta alle dipendenze della Presidenza del Consiglio dei Ministri, che si serve per la sua attività di controllo e di omologazione dell'Ufficio Centrale per la Sicurezza. Il suo campo di attività riguarda la protezione delle informazioni coperte dal segreto di Stato, trattate in sistemi di elaborazione automatica e/o elettronica di dati, e delle notizie di cui è vietata la divulgazione previste dall'art.12 della Legge n. 801 del 24 ottobre 1977. Nell'ambito delle sue competenze l'ANS ha emanato varie direttive con DPCM, l'ultima è stata quella dell'11 aprile 2002.

2. Le prime iniziative normative

Come già accennato, la situazione normativa e regolamentare per quanto riguarda la sicurezza informatica nell'ambito pubblico presenta un aspetto non unitario essendo le varie prescrizioni, in generale, contenute in provvedimenti sparsi e non collegati tra di loro e non esistendo, almeno sino al 2001, un preciso indirizzo politico ed amministrativo al riguardo ed un centro politico-amministrativo di riferimento. Le stesse lodevoli iniziative in materia dell'AIPA, (soppressa con il D.lgs. n. 196 del 2003, art. 176) data la scarsa incidenza dell'azione della stessa sulle burocrazie ministeriali, restie tradizionalmente a recepire l'innovazione tecnologica, non sembrano aver avuto esiti concreti.

Un primo tentativo di mettere ordine nel settore dell'informatica pubblica è stato probabilmente quello compiuto dal Ministro per la Funzione Pubblica dell'epoca con la Circolare n. 51223 del 21 maggio 1990 avente come titolo "Indirizzi di normalizzazione delle tecnologie dell'informazione nella Pubblica Amministrazione" un paragrafo della quale era dedicato ai criteri generali per la sicurezza fisica delle installazioni e per la sicurezza logica delle applicazioni. Va ricordato anche il D.lgs. n. 39 del 12 febbraio 1993 con il quale, tra l'altro, venne creata l'AIPA che, secondo il testo dell'art. 7, c. 1, lett. a) aveva anche il compito di dettare i criteri tecnici riguardanti la sicurezza dei sistemi[2].

Vanno ricordati, tra gli altri, anche: il D.lgs. n. 212 del 12/7/1991 relativo alle modalità di accesso delle amministrazioni pubbliche al sistema informativo dell'anagrafe tributaria, art.1; il DPR 27/6/1992 n. 352c, art. 6; il c.d. Accordo Schengen (artt. 114 e 118) ratificato dall'Italia con Legge n. 388 del 30 settembre 1993; il DPCM del 5/5/1994, relativo alle modalità tecniche e ripartizione delle spese connesse alla realizzazione di collegamenti, ecc., artt.7 ed 8; il DPR 23/12/1997 n. 522, relativo ai compiti del Centro Tecnico per l'assistenza ai soggetti che utilizzano la RUPA, art. 2; il DPR 10/11/1997 n. 513, Regolamento recante criteri e modalità per l'archiviazione e la trasmissione di documenti con sistemi informatici e telematici, art. 3, comma 3; il DPCM del 20/11/1997, Principi e modalità di attuazione della rete G-net, pr. 2; il DPR n. 428 del 20/10/1998, Regolamento per la tenuta del protocollo amministrativo con procedura informatica, ecc., art. 3, comma 1, lett. a) e c); il DPCM 27/10/1999 n. 437, Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica,

ecc., art. 8, il DPCM del 31/10/2000, Regole tecniche per il protocollo informatico, ecc., art. 4, 1 comma lett. c); il DPCM del 30/5/2002, Direttiva per la conoscenza e l'uso del domicilio Internet "gov.it", ecc., pr. 26. Esistono infine vari decreti ministeriali relativi a specifici settori che qui non si elencano per brevità nonché varie circolari dell'AIPA in materia.

3. Sicurezza informatica e protezione dei dati personali

L'esame della normativa relativa alla sicurezza informatica fa emergere una particolare circostanza e cioè una prevalenza negli anni tra il 1996 ed il 2000 di prescrizioni dettagliate in tema di misure di sicurezza dirette alla protezione dei dati personali[3]. Il *trend* normativo ha inizio con l'art. 15 della Legge n. 675 del 23 dicembre 1996 (Tutela delle persone e di alti soggetti rispetto al trattamento dei dati personali) intitolato "Sicurezza dei dati" il cui comma 2 prevedeva la successiva emanazione di apposite "misure minime di sicurezza", poi effettivamente emanate con il DPR 28 luglio 1999 n. 318 (successivamente, insieme ad altri provvedimenti citati in questo scritto, vedi, ad es., D.lgs. 171/98, abrogato dal D.lgs. 30/6/2003 n. 196, su cui amplius)[4]. Va ricordato che con la Legge n. 675/96 venne introdotta la necessità del "documento programmatico per la sicurezza" (art.6) per quanto riguardava il trattamento dei dati di cui agli artt. 22 e 24 della Legge n. 675/96. Per inciso si rileva che il secondo comma del citato art. 6 stabiliva che l'efficacia delle misure di sicurezza indicate nel documento programmatico avrebbe dovuto essere oggetto di controllo periodico da eseguirsi almeno annualmente. Qualche innovazione in materia è stata introdotta con il D.lgs. n. 196/2003 agli artt. da 31 a 36 e con il disciplinare tecnico di cui allegato B relativo alle misure minime di sicurezza, estendendosi -tra l'altro- l'obbligo della redazione del documento programmatico, prima previsto soltanto in relazione al trattamento dei dati sensibili e giudiziari, a tutti i trattamenti di dati personali[5].

3. Motivi socio politici inerenti anche ad un forte *pressing* effettuato da vari interessati sui "*decision makers*" dell'epoca, sembrano fornire una plausibile spiegazione in ordine alla indubbia prevalenza dell'azione politico-legislativa in tema di protezione della *privacy* rispetto alle esigenze, pur estremamente importanti, relative all'adozione, in modo coerente ed unitario, di iniziative decise in tema di sicurezza informatica nei sistemi pubblici. È soltanto con la creazione della figura del Ministro per l'Innovazione e le Tecnologie che il problema della sicurezza informatica pubblica ha assunto carattere prioritario, rientrando tra gli obiettivi governativi.

4. Vari provvedimenti normativi emessi nel periodo 1996/2000, allorché accennano alla sicurezza informatica, richiamano espressamente l'art. 15 della Legge 675/96. Vedi, ad es., l'art. 2 del D.lgs. 13/5/1998 n. 171, l'art. 3, c. 4 del DPR 10/11/1997 n. 513, l'art. 11 del DM 31/7/1998, ecc.

5. Qualche perplessità tuttavia suscita il confronto tra il testo dell'art. 34 del D.lgs. n. 196/2003 ed il par. 19 dell'allegato B, intitolato "Documento programmatico sulla sicurezza" il quale, invece, prevede la redazione del citato documento soltanto nel caso dei dati sensibili e giudiziari, ripristinandosi in tal modo il testo dell'art. 6 dell'abrogato DPR n. 318/1999. Inoltre né l'art. 34 né il pr. 19 dell'allegato B contengono la prescrizione del secondo comma del citato art. 6 del DPR n. 318 circa l'obbligo del controllo periodico, ...*Quid iuris?*

4. Le linee guida in tema di sicurezza informatica

Una decisa azione governativa diretta a sviluppare l'informatizzazione delle strutture della P.A. ed a regolamentare anche la sicurezza dei sistemi informatici pubblici si è verificata, con la creazione della figura del Ministro per la Innovazione Tecnologica che già con il documento dal titolo "Linee Guida del Governo per lo sviluppo della società dell'informazione", al p. 1/21 aveva annunciato la redazione del Piano Nazionale per la sicurezza ICT e la privacy, seguito poi dalla fondamentale Direttiva del 16/01/2002, relativa alla sicurezza informatica e delle telecomunicazioni nelle P.A., elaborata di concerto con il Ministro delle Comunicazioni alla quale erano allegati due documenti di orientamento (Valutazione del livello di sicurezza e Base Minima di sicurezza). L'azione è stata completata nella prima fase con la creazione, mediante il Decreto Interministeriale del 24/7/2002 del Comitato Tecnico Nazionale della sicurezza informatica e delle telecomunicazioni nelle P.A[6].

Per completezza di esposizione vanno qui ricordate le prescrizioni in tema di sicurezza informatica a suo tempo elaborate a cura dell'AIPA e cioè le "Linee Guida in tema di sicurezza informatica" pubblicate nel periodico Quaderni dell'AIPA, n. 2, ottobre 1999, e soprattutto, la Raccomandazione n. 1/2000 avente come titolo "Norme provvisorie in materia di sicurezza dei siti Internet delle Amministrazioni Centrali e degli Enti Pubblici"[7].

5. Spunti per eventuali iniziative normative in materia di sicurezza informatica

Probabilmente, data la eterogeneità delle fonti normative e regolamentari relative alla materia, sarebbe opportuno, anche alla luce della Legge 29/7/2003 n. 229, (Interventi in materia di qualità della regolamentazione normativa e della codificazione-Legge di semplificazione 2001) e particolarmente dell'art. 10 (Riassetto in materia di società dell'informazione) comma 1, e comma 2, lett. d) ricorrere allo strumento del decreto legislativo da emanarsi su iniziativa del Ministro per

6. Vedi in materia anche il paragrafo relativo alla sicurezza nella Direttiva del Ministro per l'Innovazione, intitolata *Linee Guida in materia di digitalizzazione dell'Amministrazione*, del 20/12/2002. Dal canto suo il Ministro delle Comunicazioni con il Decreto del 14/1/2003, emesso di concerto con il Ministro della Giustizia, ha creato un Osservatorio per la sicurezza delle reti e la tutela delle telecomunicazioni.

7. Accenni alla materia sono contenuti in vari documenti dell'AIPA, vedi, ad es., Lo Studio di fattibilità relativo alla RUPA del gennaio 1996, la Relazione Annuale 2001, vol. II, e il Piano Triennale 2002-2005 relativo alla informatica nella P.A. Altro documento importante è lo studio dal titolo "La sicurezza dei servizi in rete", paper del 14.11.2001. Dal canto suo il Ministero della Giustizia ha commissionato al Politecnico di Torino uno studio dal titolo "Linee Guida per lo sviluppo di piani di sicurezza dei sistemi informatici del Ministero della Giustizia" consegnato il 12/11/2002. In argomento vedi anche i decreti dello stesso Ministro del 24/5/2001 e del 27/3/2002.

l'Innovazione, di concerto con quello delle Comunicazioni allo scopo di approntare un testo che coordini e regoli compiutamente la materia. L'opportunità di siffatta iniziativa appare chiara, ad avviso di chi scrive, ove si consideri la necessità di coordinare l'attività di svariate entità pubbliche, stabilendo prescrizioni di natura cogente, in modo da assicurate coerenza ed uniformità di indirizzo, pur facendo salve le particolari esigenze di alcuni soggetti pubblici. Passando ora ad altro argomento e tenendo presenti anche le dichiarazioni del Ministro per l'Innovazione relativamente allo sviluppo della posta elettronica, interna ed esterna, nell'ambito pubblico, appare opportuno disciplinare la materia, particolarmente per quanto riguarda la condotta degli operatori e degli utenti, e le conseguenze legali di eventuali abusi, servendosi dello strumento regolamentare previsto dalla Legge 10/1/2003 (Disposizioni ordinamentali in materia di Pubbliche Amministrazioni) con particolare riferimento all'art. 27, comma 8, lett. e) che prevede appunto l'estensione della posta elettronica nell'ambito delle P.A. e dei rapporti tra P.A. e privati.

Altra area di intervento potrebbe essere quella dell'*outsourcing* nel campo pubblico, strumento che è previsto in generale per il settore pubblico da alcune disposizioni normative (vedi, tra l'altro, l'art. 2 del D.lgs. 12/2/1993 n. 39, l'art. 3, comma 2 del DPR 28/10/1994 n. 478, e, da ultimo, i pr. 25 e 26 -allegato B- del D.lgs. 30/6/2003 n. 196) e la cui estensione è stata sottolineata dalle indagini effettuate dall'AIPA (vedi il Piano Triennale 2003-2005), anche se la dottrina -sia detto per inciso-, ha manifestato le sue perplessità in ordine al ricorso a tale istituto per quanto riguarda particolarmente la sicurezza informatica. La necessità, in ogni caso, di un controllo penetrante da parte dell'Ente committente e di correlativi particolari requisiti da parte del fornitore del servizio, in specie per quanto riguarda la serietà delle garanzie offerte, ed in particolare quanto all'affidabilità e professionalità del personale incaricato, postula che la "cabina di regia" in tema di sicurezza informatica resti saldamente nelle mani dell'Amministrazione. Al riguardo, e data la situazione di eterogeneità delle condotte da parte delle Amministrazioni pubbliche nella gestione della materia, sarebbe probabilmente opportuno un intervento normativo specifico.

Sempre nell'ambito di un auspicato intervento normativo in tema di sicurezza informatica andrebbe anche presa in considerazione la possibilità peraltro, largamente ammessa da alcune legislazioni estere (in particolare in USA) del ricorso,almeno in relazione a particolari sistemi informatici c.d. critici, all'opera delle *Tiger Teams o Red Teams* allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità del sistema informatico, evidenziando le eventuali "falle" delle reti e suggerendo, al bisogno, gli eventuali rimedi. Va da sé che le aziende alle quali dovesse essere affidato tale delicato incarico dovrebbero rispondere a criteri assoluti di affidabilità e per i componenti delle equipes dovrebbe essere previsto uno speciale NOS (Nulla Osta di Sicurezza)[8].

8. In tema di sicurezza informatica particolare attenzione occorrerebbe dedicare, ad avviso di chi scrive, ai problemi tecnici e giuridici delle reti Wireless.