CARLO SARZANA DI S. IPPOLITO

L'ACCESSO ILLECITO ALLE BANCHE DATI ED AI SISTEMI INFORMATICI PUBBLICI: PROFILI GIURIDICI

SOMMARIO: 1. La vulnerabilità della Società informatizzata e la sua dipendenza dall'ITC. — 2. Cenni sulla normativa relativa alla sicurezza nei sistemi informatici pubblici. — 3. Le banche dei dati in ambito pubblico: problemi definitori. — 4. Cenni sui problemi giuridici relativi all'uso delle apparecchiature informatiche e di telecomunicazione da parte dei pubblici dipendenti. — 5. Le Linee Guida del Garante per la protezione dei dati personali per quanto riguarda la navigazione in Internet e l'uso della posta elettronica. — 6. Accesso illecito ai sistemi informatici o telematici.

1. La vulnerabilità della Società informatizzata e la sua dipendenza dall'ITC.

Come ho già ho avuto occasione di dire in altre sedi e in varie occasioni[1] la tecnologia dell'informazione e delle comunicazioni ha creato nuove opportunità nel settore economico, aziendale, sanitario, dell'istruzione, ecc. Tuttavia, lo sviluppo tecnologico ha prodotto altre conseguenze: attualmente, l'economia dell'intera società è divenuta, lo si può affermare senza tema di smentita, completamente dipendente dalla ICT.

Ciò significa, tra l'altro, che incidenti, anche non molto gravi, nei sistemi dell'ICT ed, in particolare, nelle c.d. « infrastrutture critiche », possono danneggiare o addirittura interrompere servizi essenziali per la società e creare situazioni catastrofiche in aree importanti come quelle dell'energia, dell'approvvigionamento e dei consumi, delle telecomunicazioni, dell'erogazione di carburanti, dei servizi sanitari, dei servizi finanziari — inteso il termine in senso ampio — della difesa nazionale, dei trasporti ecc..

* L'articolo che segue riproduce, con qualche aggiunta e variante, la relazione svolta dall'autore alla Conferenza organizzata a Roma dall'Armed Forces Communications and Electronic Associations — AFCEA — capitolo di Roma — il 19 aprile 2007 sul tema La Sicurezza dei Sistemi Informativi Automatizzati nella P.A.

[1] Vedi da ultimo la mia introduzione al volume di Amore-Stanca-Staro dal titolo *I crimini informatici*, edizione Halley, 2006.

In effetti la risoluzione dello specifico problema della protezione delle infrastrutture critiche è da tempo all'attenzione di molti Paesi della comunità informatica mondiale.

Tuttavia alcune circostanze rendono tale problema altamente complesso. Vi è anzitutto il fattore relativo alla interconnessione ed alla interdipendenza tra le diverse infrastrutture per cui un incidente relativo ad una di esse può ripercuotersi a catena, amplificando i danni. Va inoltre tenuta presente la circostanza relativa al fatto che la quasi totalità di tali infrastrutture è in mano privata: ciò rende molto difficile il coordinamento ed il controllo da parte degli organi pubblici e perfino, a volte, l'intervento nei casi di emergenza.

Ed infine vi è l'alto rischio di attentati terroristici. A questo proposito va detto che vi è una certa unanimità di veduta, sia a livello nazionale che internazionale, in ordine alla possibilità di attentati nei confronti delle citate infrastrutture e alle conseguenze relative giacché la loro nota vulnerabilità delle infrastrutture le rendono un potenziale obiettivo.

Come ha rilevato la Commissione UE in una sua recente comunicazione dal titolo «*La protezione delle infrastrutture critiche nella lotta contro il terrorismo*« (COM (2004)702 final)... » un attentato informatico riuscito ad una rete telefonica pubblica priverebbe utenti pubblici e privati del servizio per periodi imprecisati e non conoscibili dagli interessati... con gravi possibili conseguenze collaterali di panico e di congestione, ad es., del traffico anche automobilistico. Un attentato ai sistemi di controllo di impianti chimici o di gas naturale liquido (o, aggiungo io, ad impianti nucleari) potrebbe comportare un numero elevato di vittime e gravi danni materiali... ».

In effetti la possibilità di attacchi ai sistemi informatizzati ha preoccupato particolarmente il settore militare, giacché i sistemi informatici, in questo settore, hanno finito per diventare parte importante del controllo di difesa. Inoltre, contrariamente al passato, l'attacco può essere condotto in modo potenzialmente devastante anche da civili, cioè da singoli individui.

La facilità dell'attacco rende più semplice, ed in certi casi addirittura più sicuro, nel raggiungimento degli obiettivi, l'opera di criminali o di organizzazioni.

Se poi il sistema informatico è collegato ad Internet, come accade sempre più frequentemente, anche in settori vitali, l'attacco può essere lanciato da chiunque in qualunque parte del mondo. Ecco perché Internet ha finito per diventare, in un certo senso, una piattaforma agevole per tutti coloro che vogliono danneggiare, non importa quale organizzazione o individuo che si avvale dei sistemi collegati alla Rete.

Proprio in relazione al problema della protezione delle infrastrutture critiche il Parlamento Europeo ha il 7 giugno 2005 ema-

nato un'apposita *Raccomandazione* [2005/2044 (INS)] rivolta al Consiglio Europeo.

Va rilevato infine che un richiamo alla protezione dell'infrastrutture critiche informatizzate si trova nell'articolo 7-*bis* della recente normativa antiterrorismo italiana e di cui alla legge 31 luglio 2005 n. 155.

La vulnerabilità della Information Society è stata di recente riaffermata in un importante rapporto del Consiglio d'Europa (2004) dal titolo: « *Organised crime in Europe: The threat of cybercrime* », nel quale si pongono in luce, tra l'altro, i preoccupanti legami tra il cybercrime, la criminalità organizzata ed il terrorismo. In particolare, si sostiene che Internet gioca un ruolo molto importante nelle attività terroristiche. Secondo il rapporto, infatti, i terroristi usano Internet per scopi di propaganda, per la distribuzione di messaggi, per raccogliere adesioni e fondi e per incitare all'odio razziale.

2. Cenni sulla normativa relativa alla sicurezza nei sistemi informatici pubblici.

Un'importante iniziativa adottata dal precedente governo fu quella della « *Direttiva relativa alla sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni* », di cui al D.P.C.M. del 16 gennaio 2002, nella quale veniva raccomandato, tra l'altro, alle Pubbliche Amministrazioni di avviare nell'immediato alcune azioni prioritarie, tali da consentire il conseguimento di un primo importante risultato e cioè l'allineamento ad una base minima di sicurezza attraverso varie iniziative.

La Direttiva venne seguita da un altro documento e cioè dalle « *Linee Guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura* » del giugno 2002.

Nella Direttiva sopraccitata si affermava, tra l'altro, « ...le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese e questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni del significato intrinseco delle informazioni stesse... ».

In attuazione della Direttiva di cui sopra, venne creato, con Decreto Interministeriale del 24 luglio 2002, il « *Comitato Tecnico Nazionale della Sicurezza Informatica e delle Telecomunicazioni delle Pubbliche Amministrazioni* » che esplicò i suoi compiti nell'arco della precedente legislatura.

Un documento che illustra l'opera svolta dallo stesso Comitato nel campo della sicurezza informatica è rappresentato dal volume dal titolo « *Proposte concernenti le strategie in materia di sicurezza informatica delle Telecomunicazioni per la Pubblica Amministrazione* », pubblicato nel marzo 2004.

Un'altra importante iniziativa che si ricollegava alla sopracitata Direttiva ed ai suggerimenti del Comitato Tecnico Nazionale fu quella relativa alla costituzione presso il CNIPA nel 2004 di un gruppo di lavoro misto con l'incarico di redigere uno schema di Linee Guida per la sicurezza dei sistemi pubblici.

Il risultato dell'opera del gruppo di lavoro, approvato dai vertici del CNIPA, venne pubblicato nel numero 23 dei Quaderni CNIPA del marzo 2006 con il titolo « *Linee Guida per il Piano Nazionale della Sicurezza ICT e per il Modello Organizzativo Nazionale di Sicurezza ICT per la Pubblica Amministrazione* ». Appare qui impossibile esporre compiutamente il contenuto delle citate Linee Guida data la loro complessità ed articolazione e mi limiterò, pertanto, a qualche flash.

Gli elementi più significativi del Piano Nazionale e del Modello Organizzativo scaturivano dall'analisi del panorama della sicurezza ICT delle Amministrazioni e dall'obiettivo di introdurre un nuovo e più efficace modo per conseguire la sicurezza nel settore pubblico. In effetti, il panorama dell'epoca vedeva il predominio di una sicurezza di tipo « tecnologico » che si accompagnava alla sostanziale inconsapevolezza dei fenomeni che la governavano. I fornitori di prodotti e metodologie giocavano — occorre dirlo — un ruolo chiave in questo panorama, promuovendo, spesso, soluzioni che non scaturivano da reali esigenze degli utenti, ma da inquietudini e timori debitamente fomentati ai fini commerciali.

I due settori del documento intendevano, in realtà, proporre un nuovo modo di affrontare il problema che si basava su due pilastri e cioè: la conoscenza delle problematiche e l'organizzazione.

Infatti, allorché l'informatica entra nelle attività comuni, è indispensabile sviluppare una capacità di governo di tali processi che comprenda gli aspetti di sicurezza, al pari di quanto avviene nelle attività tradizionali. Inoltre le organizzazioni, le cui strutture ed attività sono spesso fondate su modelli comportamentali desueti, devono adeguarsi ai nuovi strumenti informativi che stanno modificando gli abituali concetti di tempo e di spazio ... e perfino di norma giuridica.

In quest'ottica, senza osteggiare il mercato — che veniva anzi ritenuto indispensabile per il corretto sviluppo della sicurezza ICT — i due documenti ponevano in secondo piano le soluzioni tecniche e metodologiche, considerate strumentali rispetto ad un governo della sicurezza che si basava principalmente sulla conoscenza dei fenomeni e su una adeguata organizzazione. Il Piano era quindi incentrato sui temi della formazione, della sensibilizzazione e della circolazione delle informazioni, sia ai fini della prevenzione dei problemi, che di promozione e attestazione della sicurezza. Il tema dell'organizzazione era invece trattato in larga misura dal Modello Organizzativo che proponeva uno schema articolato che potesse adattarsi alle realtà eterogenee del comparto pubblico.

I due documenti sopra citati costituivano, tra l'altro, una prima azione di promozione della « cultura della sicurezza ». Essi erano, infatti, arricchiti da numerosi allegati che avevano l'obiettivo di sensibilizzare le amministrazioni sulle problematiche specifiche e di fornire alle stesse una guida concreta per l'attuazione degli interventi prioritari.

Passando ora ad altro argomento, va ricordato che accenni alla sicurezza informatica sono contenuti anche in altri testi normativi. Per quanto riguarda l'SPC (Sistema Pubblico di Connettività), regolato dal Decreto Legislativo del 28 febbraio 2005 n. 42, si rileva che esso, tra l'altro, richiama l'attenzione sulla necessità della sicurezza e riservatezza delle informazioni trattate e sulla necessità di salvaguardare il patrimonio informativo di ciascuna amministrazione. Altri riferimenti sono effettuati alle regole tecniche di sicurezza per il funzionamento del SPC, mentre, tra i compiti della Commissione di Coordinamento, prevista dal testo legislativo, vi sono anche quelli relativi alla verifica della qualità e della sicurezza dei servizi erogati dai fornitori qualificati del Sistema ed il promovimento del recepimento degli standard necessari a garantire, tra l'altro, la sicurezza del sistema. Riferimenti alla sicurezza informatica del SPC sono anche contenuti nei documenti collegati, redatti dai gruppi di lavoro « ad hoc » costituiti in seno al CNIPA ed approvati dalla Conferenza Stato-Regioni.

Un richiamo alla sicurezza delle reti pubbliche di comunicazione è contenuto, poi, nel decreto legislativo 1 agosto 2003 n. 259, concernente il « *Codice delle comunicazioni elettroniche* ». Altri riferimenti alla sicurezza informatica sono contenuti, anche, in vari articoli del decreto legislativo 7 marzo 2005 n. 82 relativo al « *Codice dell'Amministrazione Digitale (CAD)* », integrato dal successivo Decreto Legislativo 4 aprile 2006 n. 159[2].

Altri riferimenti alla sicurezza sono contenuti:
— nel D.P.C.M. 14 ottobre 2003;
— nel D.P.R. 11 febbraio 2005 n. 68;
— nel D.P.C.M. 13 gennaio 2004;
— nel D.P.C.M. 2 novembre 2005, ecc.

Il Codice è stato poi seguito da una Direttiva della Presidenza del Consiglio dei Ministri del 18 novembre 2005, avente come titolo « *Linee Guida per la Pubblica Amministrazione Digitale* », nel cui paragrafo 6 veniva anche trattato l'argomento relativo alla sicurezza informatica, affermandosi in proposito che « ... lo sviluppo della comunicazione telematica con cittadini e imprese e la conseguente necessità di operare sulla rete rendono essenziale l'adozione di adeguate misure di sicurezza informatica per rispon-

[2] Il Codice dell'Amministrazione Digitale, peraltro, è stato oggetto di penetranti critiche da parte del Consiglio di Stato, critiche contenute in due successivi pareri (7 febbraio 2005 n. 11995/04 e 30 gennaio 2006 n. 31/06) e da una parte della dottrina.

dere all'esigenza di garantire riservatezza e integrità dei contenuti, continuità e disponibilità dei servizi ».

In tema di sicurezza nel settore pubblico è opportuno accennare, per inciso, alle conseguente particolari in tema di responsabilità per omissione o negligenza nell'adozione e/o gestione delle misure di sicurezza, citando al riguardo l'orientamento della Corte dei Conti in tema di « danno patrimoniale di servizio » (a seguito di condotta omissiva o gravemente colposa che abbia prodotto effetti negativi nella gestione di un pubblico servizio) e di « danno all'immagine della P.a. » allorché sia intaccato il prestigio dell'amministrazione. Questo tipo di responsabilità, a mio avviso, ben potrebbe sussistere allorché si sia verificato un evento grave collegato ad omissioni o negligenze nella gestione dei sistemi di sicurezza, e se questi fatti, specie se in connessione con una rilevante diffusione mediatica, abbiano compromessa l'immagine di efficienza e di affidabilità dei sistemi informatici pubblici.

Sempre in tema di sicurezza informatica nel campo dell'Amministrazione della Difesa, va citato il recentissimo testo dal titolo « *Politica della sicurezza ICT nella difesa — Principi generali* » del 3 gennaio 2007 che in qualche parte riprende le indicazioni contenute nelle proposte formulate a suo tempo dal Comitato Tecnico Nazionale.

Scopo del documento, come detto in premessa, è quello di fornire una visione insieme degli obiettivi che lo Stato Maggiore della Difesa intende traguardare in materia di Politica di Sicurezza ICT per l'intero Comparto della Difesa.

Il documento in questione chiarisce che scopo della « Politica di sicurezza ICT » è quello di:

— promuovere ed individuare i criteri generali di sicurezza in modo indipendente dalla tecnologia in uso e in linea con la « missione istituzionale » della Difesa;

— definire ed assegnare in modo chiaro ruoli e responsabilità afferenti l'area della sicurezza;

— pianificare e provvedere le risorse necessarie per il raggiungimento degli obiettivi prefissati.

Particolarmente importanti sono i capitoli relativi al controllo degli accessi (7), alla gestione delle vulnerabilità tecniche (8-6) ed alla gestione degli incidenti di sicurezza informatica (9).

Passando ad altro argomento, va ora citata la recentissima *Direttiva n. 2* del 20 febbraio 2007 del Ministro per le Riforme e le Innovazioni nella pubblica amministrazione, relativa all'interscambio dei dati tra le Pubbliche Amministrazioni ed alla pubblicità dell'attività negoziale, il cui ruolo dichiarato è quello di guidare le amministrazioni nell'applicazione di alcune tra le più innovative tra le disposizioni del Codice dell'Amministrazione Digitale.

Va osservato al riguardo che il Codice in questione tratta il problema della sicurezza informatica in varie disposizioni (31-34-35-38-44-48-49-50-51 ecc.), mentre l'argomento sicurezza dei sistemi

informatici è particolarmente trattato nella Direttiva citata del 18 novembre 2005 (Linee Guida per la P.A. digitale) al paragrafo 6.

Date queste premesse, non può non destare perplessità il fatto che l'argomento della sicurezza, che è certamente molto importante allorché si tratta il problema dell'interscambio dei dati, sembra essere stato completamente trascurato nella Direttiva di cui sopra, a parte un generico e distaccato richiamo agli standard di interoperabilità e di sicurezza previsti nell'ambito del Sistema Pubblico di Connettività.

In argomento va ricordato, per incidens, che esistono precisi richiami alla sicurezza dei dati personali nel paragrafo 6/7 della Direttiva del Presidente del Consiglio dei Ministri — Dipartimento della funzione pubblica — del 18 febbraio 2005, relativa alle misure finalizzate all'attuazione nel settore pubblico delle disposizioni contenute nel D.L. 30 giugno 2003 n. 196 relativo al codice in materia di protezione dei dati personali.

Circa l'importanza della sicurezza informatica va ricordato quanto sostenuto anche dalla dottrina (vedi BELISARI, *Commento all'articolo 51 del C.A.D.* nel Commentario coordinato da Cassano-Giurdanella, Milano 2005, pp. 961 e segg.) e cioè che la sicurezza informatica costituisce una delle principali criticità per lo sviluppo dell'Amministrazione Digitale, la cui realizzazione diviene il presupposto indispensabile per l'erogazione dei servizi in rete.

In realtà la centralità del tema della sicurezza dei dati della pubblica amministrazione è dimostrata proprio dal citato articolo 51 del C.A.D. intitolato « Sicurezza dei dati » in cui si afferma, al primo comma, che « Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati », e al secondo comma che... « I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta ».

Va infine tenuto conto di una circostanza, già rilevata dal Comitato Tecnico Nazionale nel suo documento più innanzi citato, e cioè la eterogeneità delle fonti normative e regolamentari esistenti in tema di sicurezza informatica nel campo pubblico.

Questa situazione renderebbe quanto mai opportuno elaborare di una specie di Testo Unico della sicurezza che riordini l'intera materia.

Per concludere sull'argomento, appare opportuno indicare ora le possibili iniziative normative dirette a rendere effettiva la sicurezza informatica nel settore pubblico.

Al riguardo va rilevato che la effettività della sicurezza nel campo informatico pubblico richiede una forte attenzione politica e quindi una decisa volontà politica degli organi governativi diretta a creare gli strumenti normativi necessari perché la sicurezza

divenga uno degli obiettivi primari e concreti della pubblica amministrazione informatizzata.

A questo riguardo occorrerebbe, anzitutto, dare legittimità normativa al più innanzi citato documento del CNIPA relativo al Piano Nazionale di Sicurezza ed al Modello Organizzativo, sull'esempio dei paesi più importanti dell'Unione Europea, ed istituire, inoltre, valendosi eventualmente degli studi effettuati e dei modelli già delineati, una specie di Agenzia Nazionale per la Sicurezza Informatica Pubblica, collocata al massimo vertice governativo, che rappresenti il necessario organo di coordinamento delle iniziative delle varie amministrazioni in tema di sicurezza informatica.

3. Le banche dei dati in ambito pubblico: problemi definitori.

Secondo la dottrina[3] l'ordinamento vigente non sembra fornire definizioni in tema di banche dei dati pubblici. Tuttavia la dottrina si è sforzata di individuare le condizioni di base in presenza della quali si possa affermare che si è in presenza di tale banca dati e cioè:

1) la banca dati è realizzata e gestita da parte di una Pubblica Amministrazione (criterio soggettivo);

2) le informazioni contenute nella banca dati devono essere impiegate per il perseguimento di finalità pubbliche definite dalla legge o da regolamenti (criterio teleologico);

3) le informazioni devono essere rese accessibili agli utenti in base ai principi generali sull'accesso ai documenti amministrativi, fatti salvi i limiti legislativi afferenti alla tutela del segreto e dei dati personali.

In argomento va ricordato che il C.A.D. all'art. 60 si riferisce alle banche dei dati nazionali recitando al primo comma … « Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti ».

Secondo la dottrina citata la definizione si riferisce ad un livello di aggregazione di livello superiore rispetto a quello che caratterizza le banche dei dati tradizionalmente intesi.

L'opportunità di una precisa individuazione di tali banche dati e di una specifica disciplina ha fatto sì che le stesse, come affermato al terzo comma del citato articolo 60, devono essere, appunto, individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delegato per l'innovazione e

[3] Lettieri, *Il Codice della Pubblica Amministrazione Digitale*, citato, commento all'articolo 60, p. 271.

le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nelle materie di competenza e sentito il Garante per la protezione dei dati personali.

Allo stato, sia detto per inciso, non si hanno notizie in ordine all'attuazione della prescrizione di cui sopra, il che vuol dire che, a parte le disposizioni contenute nel codice per la protezione dei dati personali, le banche dati pubblici in generale e quelle che potrebbero essere definite come di interesse nazionale, non appaiono oggetto di particolari prescrizioni in tema di sicurezza, per cui di fatto potrebbero essere aperte all'accesso di *hackers* esterni ed interni.

Per inciso, e considerando il pericolo dell'attacco alle banche dati e dai sistemi informatici pubblici, va ricordato il fenomeno del « *netstrike* » (corteo telematico a scopi di protesta o sindacali) e del cosiddetto « *defacement* », ossia dello sfregio o comunque della modifica arbitraria, e spesso ingiuriosa, delle pagine web dei siti presi di mira, fenomeni che riguardano spesso il settore pubblico...

Il primo e cioè il *netstrike*, riguarda l'attività di una categoria particolare di hackers politicizzati denominati « *hacktivisti* ».

Si tratta di una nuova e, potenzialmente molto pericolosa forma di attacco, organizzata da parte dei sopraccitati « *hacktivisti* » con invito rivolto ad una massa indeterminata di utenti possessori di accesso Internet, affinché puntino il loro modem verso uno specifico URL ad una precisa ora e ripetutamente in modo tale che, saturando il sito web preso di mira, lo si renda di fatto inutilizzabile almeno per la durata della manifestazione.

Molti casi del genere si sono verificati anche in Italia e qui si omette di indicarli, ricordando solo, per il suo significato politico, l'attacco al principale sito governativo italiano (gov.it) effettuato per protesta nei confronti della c.d. legge Urbani in materia di proprietà intellettuale.

In ordine all'inquadramento giuridico del *netstrike*, alcuni P.M. (Procura della Repubblica di Bologna) a proposito di un « attacco del genere », effettuato nei confronti del sito del Ministero della Giustizia, hanno contestato agli organizzatori il delitto di cui all'art. 617-*quater* del codice penale. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche e telematiche). Secondo alcuni autori sarebbe applicabile alla fattispecie anche l'art. 340 del codice penale (interruzione di un ufficio o di un servizio di pubblica necessità), mentre secondo altri autori potrebbe anche farsi riferimento all'art. 414 del codice penale (istigazione a delinquere o apologia di reato).

In argomento non può non rilevarsi che si sta diffondendo un pericoloso atteggiamento cioè quello del blocco dei computer pubblici operato dagli stessi dipendenti. Mi riferisco al recente blocco effettuato in tutta Italia dai Comitati di Base dell'Agenzia delle

Entrate per protestare per l'atteggiamento del Governo in ordine al precariato.

4. Cenni sui problemi giuridici relativi all'uso delle apparecchiature informatiche e di telecomunicazione da parte dei pubblici dipendenti.

L'utilizzo sempre più diffuso delle nuove tecnologie nel settore della P.A. e particolarmente l'uso della posta elettronica (con l'obiettivo anche di attivare per ogni dipendente un'apposita casella) è stato considerato assolutamente prioritario nell'indirizzo programmatico del precedente Governo.

Tale obiettivo, già menzionato nel documento avente come titolo « *Linee guida per lo sviluppo della società dell'informazione nella legislatura* », approvato dal Consiglio dei Ministri del 31 maggio 2001 e richiamato dall'art. 24, comma 8 lettera *e*) della legge 16 gennaio 2003 n. 3, è stato poi ribadito nella Direttiva del Ministro delle tecnologie e dell'innovazione del 27 novembre 2003, avente come titolo « *Impiego della posta elettronica nelle pubbliche amministrazioni* ». L'iniziativa da ultimo citata ha però come corollario la risoluzione di una complessa problematica giuridica in ordine alla natura dei messaggi di posta elettronica (peraltro quest'ultima già in precedenza menzionata nella normativa in tema di documentazione amministrativa e di firma elettronica), ai diritti e doveri sia dei dirigenti che dei dipendenti, ai riflessi giuslavoristici e di protezione dei dati e della privacy dei dipendenti.

Con riguardo a quest'ultimo argomento, pure molto dibattuto in dottrina per quanto riguarda i poteri di controllo del datore di lavoro, va rilevato, per incidens, che il Codice per la protezione dei dati personali sembra ignorare, incredibilmente, la disposizione dell'art. 24 della legge quadro del 29 marzo 1983, n. 93, che ha sostanzialmente esteso al settore pubblico la normativa dell'art. 4 dello Statuto dei lavoratori in tema di uso di apparecchiature di controllo a distanza dell'attività dei dipendenti. In materia va tenuta presente la circostanza, confermata da varie ricerche effettuate in Italia ed all'estero, (soprattutto in Francia, Regno Unito e USA), secondo cui i dipendenti usano questa nuova tecnologia anche per scopi esclusivamente personali e ludici, partecipando in orario lavorativo a *chat line* e *hot line*, inviando messaggi privati di posta elettronica, accedendo a siti pornografici, ecc. ed, in generale, effettuando navigazioni non autorizzate in Internet. Tali ricerche hanno anche evidenziato che, sia nel campo pubblico che in quello privato, esiste da parte dei dirigenti un certo grado di tolleranza di fronte a simili comportamenti dei dipendenti che pure possono creare problemi, anche gravi, di sicurezza e di responsabilità per il datore di lavoro: non esiste tuttavia, in genere una normativa che legalizzi, per così dire, siffatta tolleranza.

Il problema, come già accennato, ha rilevanti profili giuslavoristici, costituzionali, di tutela della riservatezza, di responsabilità amministrativa e contabile nonché di carattere civilistico e penalistico. Qui di seguito si traccerà un breve profilo della situazione dal punto di vista strettamente normativo e giurisprudenziale.

A questo proposito va osservato che non esiste allo stato in Italia alcuna disposizione legislativa specifica che regoli l'uso della posta elettronica e la navigazione su Internet da parte sia dei dipendenti pubblici per quelli privati, mentre esiste qualche disposizione nel contratti collettivi e nelle Linee guida redatte dalla Confindustria.

Per quanto riguarda il campo pubblico, in realtà, esisteva una disposizione amministrativa relativa all'uso privato delle linee telefoniche d'ufficio, contenuta nel decreto del Ministro della funzione pubblica del 31 marzo 1994, con il quale fu adottato il « *Codice di comportamento dei dipendenti della P.A.* » ai sensi dell'art. 58-*bis* del D.Lgs. n. 29 del 1993. Si trattava dell'art. 10 che, nella prima parte del comma 5, prevedeva che … « salvo casi eccezionali dei quali informa il dirigente dell'ufficio, il dipendente non utilizza le linee telefoniche dell'ufficio per effettuare chiamate personali ».

La necessità di ampliare questa limitata facoltà di deroga collegata al requisito dell'eccezionalità indusse successivamente il Ministro della funzione pubblica a rivedere l'impostazione iniziale dell'art. 10 e, infatti, il nuovo Codice di comportamento dei dipendenti pubblici, di cui al decreto ministeriale del 28 novembre 2000, ha previsto al comma 3 dell'art. 10 che il dipendente… « salvo casi d'urgenza, non utilizza le linee telefoniche dell'ufficio per esigenze personali ».

Tale disposizione di carattere puramente amministrativo, a parte il riferimento alle sole apparecchiature telefoniche, non appare comunque tale da escludere, ad avviso dello scrivente, totalmente la responsabilità civile e penale nel caso di uso illecito delle linee telefoniche da parte del dipendente pubblico.

Per quanto riguarda ora l'orientamento dottrinale e giurisprudenziale in materia, va detto che la dottrina è divisa in ordine alla definizione della natura giuridica della posta elettronica ed alla possibilità dei dirigenti dell'ufficio di controllare l'uso che i dipendenti fanno, in genere, degli strumenti tecnologici posti a loro disposizione.

L'indirizzo dottrinario prevalente ritiene che, almeno sino a quando il dipendente non acceda alla sua casella ed apra il messaggio di posta elettronica, il messaggio stesso debba considerarsi come « corrispondenza chiusa » e come tale tutelata ai sensi dell'art. 616 c.p.. Questa tesi è stata sostenuta in giurisprudenza implicitamente da una decisione del T.A.R. Lazio, Sezione I-*ter*, n. 9425 del 15 novembre 2001, in relazione ad una *mailing-list* in ambiente pubblico secondo cui… « la corrispondenza trasmessa per via informatica o telematica, c.d. posta elettronica, deve es-

sere tutelata alla stregua della corrispondenza epistolare o telefonica ed è quindi caratterizzata dalla segretezza ».

La tesi in questione, sia detto per inciso, è stata anche sostenuta, sia pure senza adeguata motivazione, in passato dal Garante per la protezione dei dati personali (vedi parere del 12 luglio 1999), secondo cui, appunto, la posta elettronica sarebbe protetta ai sensi dell'art. 616, comma 4, del codice penale. Lo stesso Garante, peraltro, in altro parere del 1° marzo 2001 affermò, incidentalmente, la legittimità dell'accesso del titolare del trattamento alla casella del dipendente in casi di necessità o di urgenza, ad es. nel caso di assenza o impedimento dello stesso. Per quanto riguarda il punto di vista della giurisdizione contabile, è da citare una recente sentenza della Corte dei Conti, Sezione Giurisdizionale per la Regione Piemonte del 13 novembre 2003 che si è occupata del problema sotto il profilo del danno erariale. Con tale decisione è stata affermata, sia pure incidentalmente, la legittimità da parte dell'amministrazione pubblica della registrazione degli accessi dei dipendenti ai siti Internet ed il successivo controllo finalizzato, non solo alla repressione di comportamenti illeciti, ma anche ad esigenze statistiche e di controllo della spesa.

Nella specie si trattava di un dipendente di un ente pubblico che, nell'orario di lavoro, si era ripetutamente collegato a siti non istituzionali ed era stato per questo rinviato a giudizio dinanzi al Tribunale di Verbania per i delitti di cui agli artt. 314, 323 e 640, 2 comma, c.p., patteggiando poi la pena.

In ordine al potere del datore di lavoro di effettuare controlli per quanto riguarda l'uso della linea telefonica da parte del dipendente del settore privato, la sua legittimità è stata affermata, inoltre, dalla giurisprudenza, sia di legittimità che di merito, che si è occupata del problema, sia pure con differenti motivazioni (vedi Cass. Sez. Lavoro 3 aprile 2002, n. 4746, sulla quale si ritornerà tra poco, cui « adde » ordinanza del Tribunale Milano del 10 maggio 2002 che, in particolare, ha escluso la responsabilità del datore di lavoro *ex* art. 616 c.p.).

In realtà il tema della legittimità del monitoraggio da parte del datore di lavoro privato sull'uso di Internet e della posta elettronica nel luogo di lavoro è stato esaminato prevalentemente dalla dottrina giuslavoristica.

Tuttavia sulla possibilità dell'applicazione alla fattispecie della disposizione di cui all'art. 4 dello Statuto dei lavoratori (legge n. 300 del 1970) che vieta di utilizzo da parte del datore di lavoro di apparecchiature per il controllo a distanza delle attività lavorative, va citata la fondamentale decisione della Corte di Cassazione che, con la sopra citata decisione del 3 aprile 2002 n. 4746, ha affermato in modo netto che ai fini dell'operatività del divieto di utilizzo per il controllo a distanza dell'attività dei lavoratori privati previsto dal citato articolo 4 è necessario che il controllo riguardi

(direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito dell'applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi) quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate o di apparecchi di rilevazione di telefonate ingiustificate.

In argomento va ricordata anche una importante decisione della Corte dei Conti — Sezione Giurisdizionale Basilicata — del 22 marzo 2006 — che ha affermato la responsabilità contabile e l'obbligo di risarcire il danno, nei confronti di dipendente pubblico il quale, durante l'orario di lavoro e dalla sua postazione, si connetteva a siti in prevalenza pornografici dai quali erano stati poi contratti virus che avevano bloccato le reti informatiche dell'Ufficio ed inoltre aveva installato sul p.c. di ufficio giochi non autorizzati.

In tema di monitoraggio elettronico la più recente dottrina[4] riconosce peraltro, che il datore di lavoro ha indubbiamente un interesse legittimo ad effettuare forme di controllo circa l'esattezza della adempimento della prestazione lavorativa ed il corretto uso da parte del dipendente degli strumenti aziendali che gli sono posti a disposizione per l'espletamento delle mansioni lavorative.

Tale potere di controllo trova il suo fondamento nell'articolo 2104 del Codice Civile che impone al dipendente l'obbligo di diligenza nonché nelle disposizioni dell'ordinamento giuridico che stabiliscono la responsabilità civile, amministrativa e penale del datore di lavoro per gli abusi commessi dai dipendenti. Anche la dottrina[5] ha sostenuto che l'abuso della casella postale informatica assegnata al dipendente e gli accessi ad Internet per finalità extra lavorative possono provocare danni all'azienda non solo come perdita di risorse lavorative (tempo, occupazione di banda, ecc.), ma anche in termini di danni provocati dall'illecita attività svolta in rete dal lavoratore (virus informatici, trasmissione di notizie riservate, commissione di altri reati attribuibili all'azienda, ecc.).

In effetti l'abuso da parte dei dipendenti degli strumenti informatici affidati dall'azienda per lo svolgimento delle loro funzioni espone quest'ultima a rischio di un coinvolgimento civile e penale nel caso di illeciti commessi nei confronti di terzi.

Altra parte della dottrina[6] ha affermato, tuttavia, che è un diritto del datore di lavoro verificare la destinazione delle risorse aziendali, ma è altrettanto diritto del lavoratore non subire controlli subdoli ed occulti; pertanto il datore di lavoro, prima di in-

---

[4] Policella, *Il monitoraggio elettronico del dipendente per scopi difensivi*, in *Dir. internet* 2007, pp. 83 e segg.

[5] Così Secco, *Il controllo del traffico informatico in azienda* in *www.diritto.it* del dicembre 2003.

[6] Frediani, *Controllo di Log di connessione e privacy*, in *www.scint.it/print-app.php?id=166*.

stallare particolari software, deve dare comunicazione apposita ai dipendenti e, soprattutto, occorre che quella installazione sia supportata da obiettivi motivi, non determinati da intenti di controllo.

Un ulteriore delicato problema in materia è quello relativo ai cosiddetti messaggi sindacali.

I sindacati possono utilizzare liberamente la rete dell'ente per l'invio di messaggi elettronici ai loro membri? In questo caso si tratta o no di un messaggio strettamente personale, non suscettibile di conoscenza da parte del datore di lavoro?

In Italia, al contrario della Francia, vi sono scarsi precedenti giurisprudenziali e dottrinari in ordine ai problemi sopra enunciati[7].

Questa è comunque una interessante questione che il Garante avrebbe potuto esaminare, sia detto per inciso, nella sua « enciclica » di cui si dirà in appresso.

Sempre in tema di posta elettronica va citata la Direttiva dello Stato Maggiore Difesa dell'8 luglio 2004, avente come titolo « *La posta elettronica in ambito Difesa* » che detta regole univoche per l'impiego, appunto, della posta elettronica nel settore Difesa.

I concetti di carattere generale sono i seguenti:

a) i soggetti autorizzati all'uso della posta elettronica devono utilizzare il servizio per le attività istituzionali, compresi quelle discendenti da convenzioni o da accordi approvati, purché l'utilizzo sia lecito e non in contrasto con la normale attività lavorativa e,

---

[7] In realtà il problema relativo alle comunicazioni elettroniche tra sindacati ed aziende ed all'uso dei siti aziendali è stato oggetto di contrastanti decisioni dei giudici di merito. In generale il problema è stato affrontato basandosi sull'art. 25 dello Statuto dei lavoratori che prevede il diritto di affissione da parte delle rappresentanze sindacali in appositi spazi aziendali di comunicazioni e documenti informativi e l'obbligo del datore di lavoro di riservare appositi spazi aziendali... Alcune decisioni hanno ritenuto che il citato diritto di affissione doveva essere interpretato tenendo conto della realtà informatica... per cui costituiva condotta antisindacale il rifiuto del datore di lavoro di mettere a disposizione delle rappresentanze sindacali aziendali uno spazio « virtuale » all'interno del sistema informatico aziendale. Si vedano al riguardo la giurisprudenza e la dottrina citata nell'articolo di F. BUFFA di commento al decreto del Tribunale di Modena, in *Il Dir. Int.* n. 4/2005, p. 349. Quest'ultima decisione ha ritenuto che non costituiva condotta antisindacale quella del datore di lavoro di rifiuto del consenso alla diffusione nella rete aziendale di un comunicato di una singola organizzazione sindacale in risposta ad una precedente nota della rappresentanza sindacale unitaria, che pure era stata diffusa sulla stessa rete aziendale. Secondo l'estensore del decreto in questione non esisteva un diritto della singola organizzazione sindacale ad utilizzare l'indirizzario collettivo dell'azienda per diffondere comunicati di carattere sindacale, specie nel caso in cui appariva comunque garantita la facoltà di cui art. 25 dello Statuto. La dottrina (vedi il commento di Buffa alla decisione), afferma, incidentalmente, che deve essere escluso il controllo del datore di lavoro sul contenuto dei comunicati sindacali inviati ai lavoratori aziendali in quanto condotta antisindacale, dovendo lo stesso datore di lavoro limitarsi a controllare soltanto la formale provenienza del comunicato stesso dalle rappresentanze sindacali unitarie. Peraltro, a mio avviso, il problema è più vasto e comprende aspetti di tutela della privacy e di responsabilità accessoria del datore di lavoro per eventuali reati commessi proprio a mezzo dei comunicati inviati e diffusi sulla rete aziendale.

per il personale militare, nel rispetto del Regolamento di Disciplina;

b) tutti gli utenti dotati di servizi di posta elettronica devono essere riconoscibili ed identificati. È necessario perciò che siano posti in essere tutte le misure atte ad impedire l'uso del servizio ad utenti non identificati.

La tipologia delle caselle di posta elettronica previste sono due:

a) casella di posta elettronica funzionale;

b) casella di posta elettronica personale.

La prima è istituita per:

a) lo scambio di comunicazione ufficiale;

b) le esigenze specifiche della funzione collegata al servizio.

La seconda è istituita per tutti i dipendenti della Difesa, sia militari che civili (anche per i dipendenti per i quali non sia prevista la dotazione di un p.c.).

La casella di posta elettronica personale costituisce lo strumento di dialogo all'interno dell'Amministrazione della Difesa per le comunicazioni di carattere informale. Per le caselle di posta elettronica personale il titolare è direttamente e personalmente responsabile del suo uso e della custodia dei dati di accesso alla propria casella.

Il titolare della casella di posta elettronica funzionale deve inoltre porre in essere le procedure formali atte a garantire l'uso della posta elettronica in sua assenza secondo il principio generale della delega.

Passando ora ad esaminare rapidamente il profilo penalistico è da dire che la giurisprudenza della Suprema Corte è ormai consolidata in ordine all'inquadramento giuridico dell'illecito uso da parte del dipendente pubblico degli apparati telefonici d'ufficio, esso rientra, cioè, nell'ipotesi del peculato ordinario di cui all'art. 314, primo comma, del codice penale punito con la grave sanzione della reclusione da 3 a 10 anni (vedi da ultimo, Cassazione Penale Sezione VI, 10 febbraio 2006 n. 1535).

In tema di uso di illecito di fax d'ufficio esiste poi una recente sentenza della Suprema Corte (vedi Cassazione Sezione Penale VI, 26 ottobre 2005 n. 42248) che ha inquadrato il fatto nell'ipotesi di peculato ordinario.

A questo proposito va ricordato che il Consiglio dei Ministri del 22 dicembre 2006, su iniziativa del Ministro Nicolais, ha approvato un disegno di legge che prevede il licenziamento immediato dei dipendenti pubblici condannati per i delitti di corruzione, concussione e peculato, con pena da due anni in su, anche se abbiano patteggiato le pena.

Va subito detto che siffatto disegno di legge, se approvato come previsto, renderebbe molto difficile la posizione del dipendente pubblico incriminato per il tipo di illecito indicato (uso non autorizzato degli strumenti tecnologici in dotazione dell'ufficio) ed inciderebbe, comunque, sulla opportunità del ricorso ai riti alterna-

tivi motivato dalla necessità deflative del processo penale. La necessità di tale disposizione è motivata nella relazione al citato disegno di legge lì dove si afferma che … » è il fatto reato in sé a minare il carattere fiduciario del rapporto fra l'Amministrazione ed il dipendente mentre la circostanza che la pena possa essere diminuita per ragioni processuali non può attenuare l'impatto del fatto sul rapporto di lavoro.

Tutto ciò premesso, non c'è dubbio che l'intera problematica, nei suoi riflessi normativi ed amministrativi, andrebbe esaminata alla luce anche della evoluzione della coscienza sociale. Appare infatti « illusorie ed irrealistiche », come affermato in Francia dalla CNIL, organo di protezione della privacy, in un pregevole rapporto intitolato « *La cybersurveillance des salariés dans l'entreprise* » del marzo 2001, una proibizione assoluta dell'uso per scopi personali degli strumenti tecnologici in ambiente lavorativo.

Ciò che appare comunque urgente, di fronte alla diffusione del fenomeno, è di riesaminare l'inquadramento tradizionale dell'ipotesi di abuso nell'ambito penalistico per evitare soluzioni giurisprudenziali oggettivamente inique di fronte alla scarsa rilevanza della condotta, tenendo conto, da un lato delle esigenze di sicurezza e di correttezza amministrativa, dall'altro dalla necessità di evitare eccessive frustrazioni in ambiente lavorativo le cui conseguenze, sia detto per inciso, avrebbero come effetto una minore produttività.

In conclusione, andrebbe, ad avviso dello scrivente esaminata, in via prioritaria, la possibilità di « depenalizzare », per così dire, le ipotesi non gravi di uso privato degli strumenti tecnologici di ogni tipo da parte dei pubblici dipendenti, prevedendo per i fatti una semplice sanzione amministrativa, tenendo presenti le vigenti disposizioni in materia di depenalizzazione (cfr. legge 24 novembre 1981 n. 689 ed il D.Lgs. 30 dicembre 1999 n. 507).

5. Le Linee Guida del Garante per la protezione dei dati personali per quanto riguarda la navigazione in Internet e l'uso della posta elettronica.

In tema di utilizzo sul posto di lavoro di Internet e di posta elettronica è intervenuto il Garante per la protezione dei dati personali con un provvedimento dal titolo decisamente pretenzioso e cioè « *Linee Guida del Garante per Internet e posta elettronica* » iniziativa, sia detto per inciso, che ha fatto il paio con altre discusse iniziative dello stesso Garante (vedi il provvedimento del 23 novembre 2006 in tema di intercettazione e quello del 15 marzo 2007 relativo alla diffusione di notizie in ordine all'attività giudiziaria della Procura di Potenza).

In ordine al provvedimento relativo ad Internet e alla posta elettronica va osservato, preliminarmente, che il Garante non sembra

distinguere adeguatamente il settore pubblico da quello privato, tanto è vero che rivolge un invito a tutti i datori di lavoro, sia pubblici che privati, a dotare, eventualmente, il dipendente di una diversa casella destinata ad uso privato. Ora come è noto, le pubbliche amministrazioni sono vincolate dalla normativa anche penalistica e dalla interpretazione giurisprudenziale che considera comunque come peculato l'utilizzo di strumenti d'ufficio per fini privati.

Inoltre, in modo del tutto incongruo, nel dispositivo del provvedimento si vieta a tutti i datori di lavoro, sia pubblici che privati, di effettuare trattamenti di dati personali mediante sistemi di hardware e software che mirano al controllo a distanza dei dipendenti con riferimento implicito all'art. 4 dello Statuto dei lavoratori, fondando tale divieto su una disposizione del Codice neppure citata in premessa (articolo 154 comma 1° lettera *d*) che si riferisce invece ai casi di cui all'articolo 143 del codice concernente i reclami) ignorando sostanzialmente sia le citate decisioni interpretative della Suprema Corte sia il fatto che per i dipendenti pubblici non si applica in ogni caso l'articolo 4 dello Statuto dei lavoratori bensì l'articolo 24 della legge n. 93 del 1983.

Ciò che è decisivo comunque ai fini della vincolatività giuridica dei vari provvedimenti è che essi richiamano come base e presupposto della decisione le disposizioni degli articoli 24 e 154 primo comma lettera *b*) e *c*), disposizioni che non sembrano applicabili nella fattispecie.

Infatti l'articolo 24 riguarda i casi nei quali il trattamento può essere effettuato senza consenso, mentre l'articolo 154 primo comma, lettera *b*) riguarda l'ipotesi dei reclami, segnalazioni e ricorsi (mentre nella fattispecie non risulta che vi siano stati siffatti input) e la lettera *c*) riguarda la possibilità di prescrizioni rivolte, anche d'ufficio, ai titolari del trattamento, necessarie al fine di rendere il trattamento conforme alle disposizioni vigenti ma ciò con riferimento all'articolo 143 che si applica al procedimento previsto in tema di reclami.

Va osservato ancora che il divieto di cui nel dispositivo del provvedimento, indirizzato genericamente a tutti i datori di lavoro pubblici e privati e relativo all'uso di sistemi hardware e software che, secondo il punto di vista del Garante mirerebbero al controllo a distanza dei lavoratori, è basato sull'articolo 4 dello Statuto, disposizione che deve ritenersi non pertinente in tema di monitoraggio difensivo, come affermato della Suprema Corte.

Decisamente stravagante è la disposizione del provvedimento che prevede la possibilità della creazione del dipendente « fiduciario » che dovrebbe sostituire il dipendente assente o impedito: in caso di controllo da parte del datore di lavoro della casella di posta elettronica data in uso al dipendente... che cosa accade se il dipendente non ha fiducia nei suoi colleghi e non nomini il suo « alter ego »? Non sarebbe stato più sensato prevedere la tutela del-

l'interessato nominando un responsabile ad hoc nell'ambito dell'organizzazione che svolga, per così dire istituzionalmente, il compito che dovrebbe svolgere il fiduciario, designato eventualmente con l'accordo del sindacato.

In definitiva, si tratta di un provvedimento che dal punto di vista formale riveste il carattere di una specie di raccomandazione o segnalazione e che quindi non può in nessun caso giustificare l'applicazione, in caso di inosservanza, della grave sanzione penale di cui all'articolo 170 del cosiddetto Codice della privacy.

Può pertanto sostenersi che, come ritiene anche la dottrina[8], il datore di lavoro che si orientasse verso soluzioni operative diverse da quelle indicate o prescritte dal Garante non incapperebbe in ipotesi di trattamento illecito e quindi il suo comportamento non cadrebbe sotto il regime sanzionatorio[9].

6. Accesso illecito ai sistemi informatici o telematici.

Il fatto è previsto dall'articolo 615-*ter* del Codice Penale introdotto dalla legge n. 547 del 1993, intitolato «*Accesso abusivo ad un sistema informatico o telematico*» e che recita: 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'or-

---

[8] Ricchiuto, *Privacy e rapporto di lavoro: la vera portata delle Linee Guida* in *www.interlex.it* del 27 febbraio 2007.

[9] È interessante notare che lo stesso segretario generale del Garante, nel commentare la norma di cui all'articolo 31 1 comma, lettera *c*) della legge precedente n. 675/196, corrispondente all'attuale articolo 154, 1 comma, lettera *c*), affermava che il titolare ed il responsabile del trattamento non sono tenuti a rispettare le prescrizioni contenute nelle segnalazioni del Garante, vedi Buttarelli, *Banche dati e tutela della riservatezza*, Milano 1997, p. 503.

dine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, 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 ».

La norma trova la sua collocazione — come osserva la relazione alla legge — tra i reati contro l'inviolabilità del domicilio, perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelato nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 c.p..

La tutela è limitata ai sistemi informatici o telematici protetti da misure di sicurezza perché, dovendosi tutelare il diritto di uno specifico soggetto, è necessario, come sostenuto nella relazione citata, che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'accesso e le permanenza nel sistema alle sole persone da lui autorizzate.

Osservo, per inciso, a questo punto che, per quanto riguarda il termine « misure di sicurezza » usato in tema di accesso non autorizzato (art. 615-*ter*) e di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater*), tale termine è di uso corrente negli studi e nei documenti nazionali ed internazionali che si occupano dei problemi giuridici dell'informatica.

La disposizione in oggetto che mira, come già si è detto, a tutelare il cosiddetto domicilio informatico è stata oggetto di una importante sentenza della Corte Suprema e cioè quella del 4 ottobre 1999 n. 3067, secondo cui, con la previsione dell'articolo 615-*ter*, il legislatore ha assicurato la protezione del domicilio informatico quale spazio ideale (ma anche fisico) in cui sono contenuti dati informatici di pertinenza della sfera individuale, quale bene costituzionalmente protetto.

Tuttavia l'articolo citato — sempre secondo la Suprema Corte — non si limita a tutelare solamente i contenuti personalistici dei dati raccolti nei sistemi informatici protetti ma offre una tutela più ampia che si concreta nel « ius excludendi alios », quale che sia il contenuto dei dati racchiusi in esso purché attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente.

Ciò con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che il titolare sia persona fisica sia giuridica, pubblica o privata o di altro ente.

La condizione di punibilità del fatto è quella relativa alla esistenza di misure di sicurezza a protezione dei sistemi.

A questo riguardo, la Suprema Corte (vedi da ultimo Cass. Sezione VI Penale, 27 ottobre 2004 n. 46509) ha ripetutamente af-

fermato che non è ravvisabile il reato di accesso abusivo quando il sistema informatico nel quale l'imputato si sia abusivamente introdotto non risulti direttamente protetto da misure di sicurezza.

Incidentalmente va osservato che spesso la fattispecie di cui all'articolo 615-*ter* concorre con quella di cui all'articolo 615-*quater* relativo alla detenzione o impossessamento abusivi di codici di accesso.

Una decisione importante è quella recente del Tribunale di Viterbo (5 maggio-5 luglio 2005) relativo ad un dipendente bancario che, assegnato all'area controlli nell'estate del 2000 si era abusivamente inserito all'interno del sistema informatico dell'Istituto di credito, effettuando una serie di interrogazioni nell'area titoli e provvedendo poi alla stampa su carta di circa 1187 posizioni.

Il Tribunale di Viterbo ha mandato assolto l'imputato, osservando che non costituiva accesso abusivo ai sensi dell'articolo 615-*ter* la condotta del dipendente autorizzato all'uso del sistema informatico che abbia consultato dati relativi ad un settore diverso di quello di sua competenza, in assenza di un divieto espresso di accedere a quel determinato settore e in assenza di finalità personali o di terzi estranei all'ente di appartenenza.

Una recentissima sentenza della Suprema Corte (Sezione V 20 marzo 2007 n. 11689) ha affermato infine che « è ravvisabile il reato di accesso abusivo ad un sistema informatico (articolo 615-*ter* c.p.) nel caso di abusiva introduzione in una centrale telefonica per l'indebita effettuazione di telefonate sulle linee degli utenti privati, pur quando non ne sia derivata una violazione della riservatezza ».

Per concludere va ricordato che l'ipotesi di accesso illegale o illecito è previsto anche da due strumenti internazionali e cioè dalla Convenzione di Budapest di lotta alla cybercriminalità, redatta ad opera del Consiglio d'Europa, aperta alla firma nel novembre 2001 (art. 2) e dalla decisione Quadro dell'Unione Europea 2005/222/GAI del 24 febbraio 2005 (art. 2). Per quanto riguarda la Convenzione di Budapest non può non rilevarsi con vero rammarico, il fatto che l'Italia, nonostante abbia sottoscritto immediatamente la Convenzione al momento della sua apertura (nov. 2001), inspiegabilmente e nonostante che esista uno schema di provvedimento di ratifica redatto nel 2004 da un'apposita Commissione Interministeriale, non abbia provveduto sinora alla ratifica stessa[10].

[10] Nelle more della pubblicazione del presente articolo, si è avuta notizia che il Ministro della Giustizia aveva presentato al Consiglio dei Ministri dell'undici maggio c.a un disegno di legge di ratifica della Convenzione in oggetto, ottenendone l'approvazione per la successiva presentazione alle Camere. Il disegno in questione non è stato ancora stampato: sembra che il Ministro si sia servito, in gran parte, dello schema redatto dalla precedente Commissione Interministeriale. Come si dice? Meglio tardi che mai!!