ASSOCIAZIONE CULTURALE
PER LO STUDIO DEL DIRITTO

techne

Vicolo Chiuso, 5 - 33170 Pordenone
tel. 0434 522866 - fax 0434 246429
associazione@e-curia.it
www.rivistatechne.it

Realizzazione editoriale
Forum, Editrice Universitaria Udinese srl
Via Palladio, 8 - 33100 Udine
www.forumeditrice.it

Stampa
Lithostampa, Pasian di Prato (UD)

Reg. Trib. di Pordenone n. 514 del 27.07.2004

SOMMARIO

EDITORIALE

Glauco Riem

«Techne» dedica questo numero alla cosiddetta semplificazione delle norme in tema di tutela del trattamento dei dati personali espressamente voluto dal legislatore a favore delle imprese.
Detta nuova norma riguarda in particolare il Documento Programmatico sulla Sicurezza e le 'nuove' misure minime di sicurezza cui l'impresa è tenuta; si tratta decreto del 25 giugno 2008, n. 133s, e del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato in G.U. del 9 dicembre denominato *Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali*.

In apertura, una breve nota del Presidente degli Industriali di Pordenone Maurizio Cini illustra i motivi che hanno determinato l'intenzione di pubblicare questo numero speciale della rivista «Techne», onde informare i propri associati delle novità legislative in merito alla semplificazione privacy ed organizzare il convegno del 6 marzo 2009 con la collaborazione dell'Associazione culturale per lo studio del diritto e dell'informatica di Pordenone e lo Studio Legale Riem.

Glauco Riem illustra invece i temi generali sull'attuale assetto normativo in tema di trattamento e protezione dei dati personali così come delineato dal decreto legislativo 196 e del suo Allegato B e la filosofia legislativa dell'apparato normativo sulla tutela della riservatezza.

Andrea Sirotti Gaudenzi analizza gli aspetti problematici dei rapporti fra datore di lavoro e dipendente, inquadrando detti rapporti fra il dettato normativo vigente, la ponderosa serie di provvedimenti del Garante e la semplificazione proposta dalla legge n. 133 /2008 e la novella dell'art. 34 del D.Lgs. 196/03.

Stefano Corsini descrive nel merito ed in dettaglio le novità introdotte dal su citato decreto in tema di semplificazione privacy previsto per le piccole e medie imprese.

Paolo Vicenzotto delinea le problematiche legate all'autocertificazione quale documento sostitutivo del Documento Programmatico sulla Sicurezza ed individua le semplificazioni previste in relazione all'adozione delle misure minime sulla sicurezza nel trattamento dei dati personali.

Luca Zenarolla, dopo un breve *excursus* sul succedersi nel tempo delle norme in punto privacy, analizza i due più recenti provvedimenti del Garante in tema di sicurezza nel trattamento dei dati personali e segnatamente sulle misure tecniche preventive alla memorizzazione elettronica, alla cifratura delle informazioni ed ai compiti e mansioni assegnati all'amministratore di sistema.

Infine la vignetta di Federico Cecchin sinteticamente interpreta la semplificazione nella 'giungla' del tessuto normativo vigente.

Chi desiderasse avere ulteriori delucidazioni sulla semplificazione privacy per le piccole medie imprese, potrà consultare direttamente la documentazione inserita nei sotto indicati link. In particolare segnaliamo il link ove effettuare il *down load,* in formato elettronico, di una bozza di autocertificazione quale documento sostitutivo del Documento Programmatico sulla Sicurezza nelle piccole e medie imprese.

- http://www.unindustria.pn.it
- http://www.e-curia.it

SEMPLIFICAZIONE PRIVACY PER L'IMPRESA

Maurizio Cini
Presidente Unindustria di Pordenone

La normativa riguardante la tutela dei dati personali è un argomento con il quale ci confrontiamo ormai dal 1996, anno in cui è stata approvata la L. n. 675/1996 (c.d. legge sulla privacy).
Nel corso degli anni il legislatore ha introdotto varie modifiche alla norma (poi divenuta Testo Unico in materia di trattamento dei dati personali con il D.Lgs. 196/03), alla quale si sono poi affiancati numerosi Provvedimenti dell'Autorità Garante della Privacy, che prescrivono misure e comportamenti da adottare per proteggere i dati personali degli interessati (intesi sia come singoli cittadini, sia come imprese o enti).
Negli ultimi mesi sono state apportate alcune novità alla disciplina con l'obiettivo – a dire il vero non sempre raggiunto – di semplificare gli adempimenti delle aziende.
Nel mondo delle imprese infatti la tutela dei dati personali viene avvertita come un onere, una fonte di adempimenti burocratici e di costi.
In parte questo atteggiamento trova giustificazione nella natura stessa di una normativa effettivamente complessa, che solo di recente ha cercato di cogliere le distinzioni esistenti tra realtà produttive operanti in ambiti differenti o tra imprese di dimensioni diverse, prescrivendo regole più semplici per alcune tipologie di trattamenti.
La protezione dei dati personali non deve però essere considerata un 'lusso' a cui un'azienda può rinunciare, ma è una necessità in una realtà in cui l'uso dei dati è condizione indispensabile per la quotidiana operatività, la sopravvivenza e lo sviluppo dell'impresa.
Gli obblighi imposti dalla normativa sulla privacy vanno perciò affrontati con

un approccio positivo, e la loro attuazione in azienda può essere l'occasione per verificare la corretta impostazione delle procedure connesse all'utilizzo delle informazioni.
L'azienda potrà, ad esempio, verificare se i dati presenti nei propri archivi sono stati acquisiti in modo lecito; se sono stati definiti correttamente i compiti e le responsabilità dei soggetti che – in virtù delle loro mansioni in azienda – trattano dati personali; se le misure di sicurezza informatica sono adeguate ad assicurare alla rete aziendale ed alle banche dati una buona protezione da virus informatici, dalle intrusioni di *hackers*, da azioni di spionaggio industriale; se vengono effettuate copie di sicurezza affidabili dei dati; se la posta elettronica e internet vengono utilizzati in modo corretto dai dipendenti; se i sistemi di video-sorveglianza non sono troppo invasivi.
L'obiettivo di questa pubblicazione è pertanto quello di fornire agli associati una guida alle recenti semplificazioni ed alle novità della legge in materia di trattamento dei dati personali, la cui adozione in azienda deve comunque essere valutata con estrema attenzione.
Non va infatti trascurato l'aspetto sanzionatorio legato alla non corretta applicazione della normativa privacy: il recente decreto 'mille proroghe' ha particolarmente inasprito le sanzioni per diverse fattispecie di condotte non conformi al dettato del Codice Privacy.

LE COMPLESSE MODALITÀ DI TUTELA DEL TRATTAMENTO DEI DATI PERSONALI E L'ESIGENZA DI UNA REALE SEMPLIFICAZIONE

Glauco Riem

La semplificazione si scontra con l'inevitabile complessità delle problematiche che riguardano la tutela nel trattamento dei dati sensibili (cioè quelli di cui alla previsione dell'art. 4, comma 1, lettera d) del D.Lgs. 196/03, sulla salute, sulla vita sessuale, sulle opinioni politiche, sull'adesione a partiti, sindacati, sull'origine razziale, sulle convinzioni religiose).
Il fulcro del problema relativo alla predetta tutela era già stato precisamente delineato ed individuato nel 1981 dalla Convenzione di Strasburgo in materia e riguardava il diritto alla riservatezza nei confronti delle informazioni sulla «vita privata, relativa all'elaborazione automatizzata dei dati di carattere personale (protezione dei dati)», di ogni singolo individuo.
L'accento era posto dunque sulla possibile indiscriminata conoscenza dei dati che se ne sarebbe potuta ricavare semplicemente digitando un nome e cognome in una banca dati in cui tali informazioni erano state inserite ed elaborate. Tale problema di difficile soluzione, attesa la complessità della gestione della sicurezza informatica relativa all'accesso ai dati, è stato portato ad una estrema complessità da una normativa nazionale ipertrofica che, come una sorta di linea Maginot, ha apparecchiato all'operatore ignaro una innumerabile e minuziosa serie di adempimenti che ancora oggi spaventano gli stessi addetti ai lavori.
Ed allora ecco l'odierna pretesa necessità di semplificare la tutela della riservatezza nel trattamento dei dati personali con provvedimenti che non appaiono di mera facciata.
Bene il legislatore avrebbe fatto a dettare sin da subito delle norme più semplici: bastava mediare il dettato normativo di cui alla Convenzione 108 di

Strasburgo, del 28 gennaio 1981, che, in soli 21 articoli, aveva – anche in dettaglio – regolato la materia ed aveva dettato una serie di linee guida generali sul comportamento che gli operatori avrebbero dovuto osservare nelle attività di trattamento dei dati personali dei singoli soggetti.
La minuziosità dei dettagli espressi nel testo del Codice in materia di protezione dei dati personali (D.Lgs. 196/03) si sostanzia invece in 186 articoli oltre, naturalmente, a quelli contenuti negli allegati al predetto codice. Ogni articolo è irto di adempimenti che rinviano ad altri articoli ed ad altri adempimenti: la lettura comparativa del tessuto normativo che così si crea risulta allora difficile anche agli addetti ai lavori, che devono tener conto anche dei provvedimenti e delle pronunce di uno dei Garanti privacy più prolifico e facondo dell'Unione Europea.
Il problema della semplificazione non è problema solo italiano, ma è avvertito negli altri stati dell'Unione. In proposito Brigitte Zypries (Spd), ministro della giustizia tedesco, ha affermato che bisognerebbe «valutare seriamente una possibile semplificazione delle leggi sulla protezione dati dando seguito però a maggiori controlli sull'attività degli operatori».
Stando infatti alla lettura del tessuto normativo sulle tutele accordate ai cittadini tedeschi dalla normativa privacy, il dibattito sull'inasprimento delle pene sembrerebbe superfluo: gli strumenti di 'repressione' normativa del fenomeno infatti non mancano e permettono, anche attraverso l'applicazione di sanzioni penali, una forte tutela del cittadino.
La normativa comunque – come del resto anche in Italia e negli altri paesi dell'Unione Europea –dovrebbe essere rivisitata in vista di una profonda, ma reale semplificazione. Le norme privacy infatti sono a suo tempo 'cresciute' in modo disomogeneo ed è diffusamente sentita l'esigenza di una disciplina non più spinta verso una regolamentazione minuziosa e pedante della materia, che rende poi difficili i controlli di merito, ma appunto semplificata e ciò anche perché, come spesso accade, il legislatore costruisce una normativa ipertrofica che poi fa 'cilecca' per l'insufficienza di organico di coloro a cui sono demandati i controlli e le ispezioni.
La tutela dovrebbe poter poi essere rivolta ad attività atte a prevenire gli illeciti più che a sanzionare gli abusi.

Ed allora, riteniamo che, ancora una volta, il legislatore italiano sembra abbia perduto un'occasione propizia: nel cosiddetto decreto 'milleproroghe' infatti, a proposito di semplificazione e alleggerimento degli adempimenti privacy, leggiamo le *Nuove disposizioni in materia di tutela della riservatezza* (Decreto Legislativo 30 giugno 2003, n. 196):
«la sanzione amministrativa per violazione delle disposizioni di cui all'articolo 13 in materia di informativa di interessati è raddoppiata passando dalla forchetta *tremila euro-diciottomila euro* a quella *seimila euro-trentaseimila euro* (articolo 161);
è raddoppiata la sanzione amministrativa per violazione della disciplina sulla cessione dei dati, che ora va da diecimila euro a *sessantamila euro* (articolo 162);
la sanzione per omessa o incompleta notificazione va *ventimila euro* a *centoventimila euro* (articolo 163);
più che raddoppiata invece è la sanzione per omessa informazione o esibizione: da diecimila euro a sessantamila euro (articolo 164)».
All'articolo 162 sono aggiunti poi due commi che recitano:
«2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da *ventimila euro a centoventimila euro*. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta.
2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da *trentamila euro a centottantamila euro*».
L'aggiunto l'articolo 164-bis (Casi di minore gravità e ipotesi aggravate), prevede invece:
«1. Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.
2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e

164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da *cinquantamila euro a trecentomila euro*. Non è ammesso il pagamento in misura ridotta.
3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo *sono applicati in misura pari al doppio*.
4. *Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo* (es.: *un milione e duecento mila euro*) quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore».
Tutto ciò riteniamo non abbia bisogno di molti commenti, se non quello che esprime il disagio che le diverse categorie economiche provano nel gestire gli adempimenti di un apparato normativo complesso, rigido e veramente severo.

QUALCHE RIFLESSIONE ALLA LUCE DELLA 'SEMPLIFICAZIONE' PRIVACY

Andrea Sirotti Gaudenzi

La legge 6 agosto 2008 n. 133 ha convertito in legge il D.Lgs. 25 giugno 2008, n. 112, che prevedeva, tra le altre cose, una serie di semplificazioni (vere o presunte) in tema di adempimenti sulle questioni attinenti la protezione dei dati personali. Innanzitutto, l'art. 29 della novella ha inserito un nuovo comma all'interno dell'art. 34 del D.Lgs. 196/03, nel tentativo dichiarato di semplificare quelli che con una espressione impropria vengono definiti 'adempimenti *privacy*'. In particolare, la nuovo norma ha introdotto il principio in virtù del quale «i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale»[1] non siano più tenuti a redigere il Documento Programmatico sulla Sicurezza (DPS). Tale adempimento, infatti, viene sostituito dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. Si deve osservare che la legge di conversione, rispetto al precedente decreto legge, ha esteso l'applicazione della esenzione, dato che il decreto esonerava dall'obbligo di compilazione del Documento Programmatico solo i datori di lavoro che avessero trattato, come unici dati sensibili, quelli «costituiti dallo stato di salute o di malattia dei dipendenti». In questo senso, la modifica appare opportuna, anche se la formulazione della norma sembra coprire un contesto assai esteso, essendosi fatto riferimento non solo ai lavoratori dipendenti, ma a tutti (o, almeno, così ci sembra di poter leggere) i collabo-

ratori, soprattutto in considerazione dell'espressione «e collaboratori anche a progetto».
La riforma consente di ritornare sul tema dei rapporti tra datore di lavoro e dipendente, in relazione all'utilizzo di strumenti informatici quali l'*e-mail* aziendale.

Lavoratore dipendente e diritto alla riservatezza della corrispondenza telematica

Come noto, l'art. 4 dello Statuto dei lavoratori pone il divieto di usare «impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori»[2]. Peraltro, «gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati solo previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti»[3]. La Suprema Corte ha rilevato che «ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della legge n. 300/70, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate»[4].
Inoltre, l'art. 8 dello Statuto stabilisce il divieto in capo «al datore di lavoro, ai fini della assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoro»[5].
Ciò significa che nessuno strumento informatico o telematico che consenta di raccogliere informazioni in ordine ai dati sensibili indicati dall'art. 4 dello Statuto o a dati non attinenti a valutazione strettamente personali è da ritenersi illecito[6].

Con riferimento alla possibilità di effettuare un controllo da parte del datore di lavoro sulla posta elettronica del lavoratore dipendente, in dottrina sono state espresse numerose opinioni[7], anche se la giurisprudenza ha assunto un orientamento teso al riconoscimento di una tutela minore rispetto ai messaggi di posta elettronica 'aziendali'[8].
In particolare, nel 2001, in ordine alla possibilità di configurare la violazione dell'art. 616 c.p., il GIP del Tribunale di Milano[9] ha ritenuto che non potesse ravvisarsi alcun illecito penale nel comportamento del legale rappresentante di una società che operasse un controllo sui messaggi di posta elettronica dei dipendenti. In particolare, ha rilevato che, in attesa di una codificazione dei comportamenti ai fini dell'omologazione e dell'accettazione di un uso standardizzato dello strumento, molte sono le problematiche che si sono affacciate con la nascita della 'buca delle lettere elettronica'; tra queste, dividendole per aree tematiche e con specifico riferimento all'utilizzo di tale strumento da parte del lavoratore, si possono elencare le seguenti:

a) utilizzo anche per fine privato dell'indirizzo di posta elettronica da parte del lavoratore con eventuale esposizione dello stesso sulla carta da visita intestata a proprio nome;
b) possesso di un indirizzo 'generalista' per cui la posta ivi indirizzata può avere come destinatario un qualunque altro dipendente con conseguente incertezza sulla 'consegna';
c) mancata individuazione del mittente (in possesso di un indirizzo in codice o con sigla) che non provvede a sottoscrivere il messaggio ovvero che non si preoccupa di farsi riconoscere rendendosi di fatto anonimo.

Limitando sostanzialmente la nostra analisi alla prima problematica, va detto innanzitutto come non possa mettersi in dubbio il fatto che l'indirizzo di posta elettronica affidato in uso al lavoratore, di solito accompagnato da un qualche identificativo più o meno esplicito, abbia carattere personale, nel senso cioè che lo stesso viene attribuito al singolo lavoratore per lo svolgimento delle proprie mansioni.
L'Autorità Giudiziaria ha posto il proprio ragionamento sul fatto che uno strumento personale non sia qualificabile *tout court* come 'privato' e, pertanto, 'riservato'. Tuttavia, lo stesso tribunale del capoluogo lombardo ha rilevato che 'personalità' dell'indirizzo non significa necessariamente 'privatezza' del medesimo «dal momento che, salve le ipotesi in cui la qualifica del

lavoratore lo consenta o addirittura lo imponga in considerazione dell'impossibilità o del divieto di compiere qualsiasi tipo di controllo/intromissioni da parte di altri lavoratori che rivestano funzioni o qualifiche sovraordinate (fattispecie che potrebbe effettivamente indurre a qualche dubbio), l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario (ma sempre appartenenti all'azienda) a prescindere dalla identità o diversità di qualifica o funzione: ipotesi, frequentissima, è quella del lavoratore che 'sostituisce' il collega per qualunque causa (ferie, malattia, gravidanza) e che va ad operare, per consentire la continuità aziendale, sul personal-computer di questo ultimo anche per periodi di tempo non limitati»[10].
Pertanto, secondo l'Autorità giudiziaria milanese, il lavoratore che utilizza – per qualunque fine – la casella di posta elettronica, aziendale, si espone al 'rischio' che anche altri lavoratori della medesima azienda – che, unica, deve considerarsi titolare dell'indirizzo – possano lecitamente entrare nella sua casella (ossia in suo uso sebbene non esclusivo) e leggere i messaggi (in entrata e in uscita) ivi contenuti, previa consentita acquisizione della relativa *password*, la cui finalità non è certo quella di 'proteggere' la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore, bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società.
Ad ogni modo, questo tipo di impostazione è stato considerato valido anche da un recente *dictum*[11], nel quale è stato affermato che l'*e-mail* aziendale appartiene al datore di lavoro e, quindi, quando il superiore gerarchico acceda alla posta elettronica professionale del dipendente, non può essere configurato il reato di violazione di corrispondenza.

L'orientamento del Garante e una riflessione finale

Il Garante, con un provvedimento del marzo 2007[12], ha affermato il principio in virtù del quale i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali. Tuttavia, spetta al datore di lavoro definire le *modalità d'uso* di tali strumenti, dovendo adeguatamente considerare i diritti dei lavoratori e la disciplina vigente in tema di relazioni sindacali. Infatti, il prov-

vedimento del Garante dispone che debba gravare «sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli»[13]. Peraltro, quanto sopra deve essere effettuato «tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali»[14].
A questo punto, ci si deve chiedere cosa ne sarà di quei datori di lavoro che prevedono di poter accedere agli strumenti elettronici 'assegnati' ai dipendenti, con facoltà di poter accedere (anche solo occasionalmente) a dati qualificabili come sensibili degli stessi (come *e-mail* del coniuge o del partito politico di appartenenza trasmessa all'indirizzo di posta elettronica aziendale del lavoratore). In particolare, è possibile – a questo punto – che il datore di lavoro possa ritenersi esentato dall'obbligo di redigere il documento programmatico?

NOTE
[1] Art. 34, comma 1 bis, D.Lgs. 196/03.
[2] Art. 4, legge n. 300/1970.
[3] *Ibidem.*
[4] Cass. Civ., sez. lav., 3 aprile 2002, n. 4746, in *Rass. Foro it.,* voce 'lavoro (rapporto)', n. 854.
[5] Art. 8, legge n. 300/1970.
[6] P. Colella, *I controlli informatici sul posto di lavoro*, in *Jei*, www.jei.it.
[7] In particolare, si veda: A. Stracuzzi, *Il commercio elettronico e l'impresa*, Il Sole-24 Ore, Milano, 2002[2], pp. 185 e ss.
[8] Trib. Milano, 14 giugno 2001, in *Foro it.,* 2002, II, col. 385.
[9] Trib. Milano, 10 maggio 2002, in *Dir. informatica,* 2002, p. 1063, con nota di A. Stracuzzi e in *Giur. merito,* 2002, p. 1303, con nota di G. Rognetta.
[10] *Ibidem.*
[11] *Ibidem.*
[12] Trib. Chivasso, 20 giugno 2006, in *Foro it.,* 2007, II, col. 132.
[13] Garante prot. dati pers., I marzo 2007, in *Gazzetta Ufficiale* n. 58 del 10 marzo 2007.
[14] *Ibidem.*

LE SEMPLIFICAZIONI DEGLI ADEMPIMENTI PRIVACY PER LE PICCOLE E MEDIE IMPRESE

Stefano Corsini

In data 19 giugno 2008 l'Autorità Garante per la protezione dei dati personali ha individuato ulteriori soluzioni per agevolare, pur sempre nel rispetto dei principi fondamentali in materia di trattamento di dati, le attività di ordinaria gestione amministrativo-contabile.
Innanzitutto va fatta chiarezza sul significato di questi due termini.
Analizzando nell'insieme i provvedimenti di semplificazione del Garante, possono intendersi quali attività svolte per finalità amministrative e contabili tutte quelle operazioni effettuate in ragione dell'ordinaria gestione dell'impresa. Possono perciò riguardare i trattamenti di dati personali relativi ad altre imprese, ai fornitori, ai dipendenti e collaboratori, utilizzati per scopi afferenti a:

- l'organizzazione aziendale;
- la gestione dei contratti dell'azienda;
- la gestione giuslavoristica del personale;
- la gestione degli adempimenti verso le Pubbliche Amministrazioni;
- la gestione economico-contabile dell'azienda.

Il provvedimento riguarda in particolare l'informativa e il consenso, istituti basilari della disciplina sulla protezione dei dati personali.
Per quanto attiene all''informativa' da rendere ai sensi dell'art. 13 D.Lgs. 196/03, il Garante ha rilevato come spesso tale onere possa essere assolto con formule da rendere oralmente invece che per iscritto, specie se il trattamento riguarda dati personali non sensibili né giudiziari (ad esempio nelle ipotesi di gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, dipendenti, realtà esterne di supporto anche in *out-*

sourcing), ed ha sottolineato altresì la diffusa abitudine di utilizzare espressioni tecnico-giuridiche che di fatto ostacolano la comprensibilità dell'informativa stessa.
Secondo il Garante è possibile fornire, anche oralmente, una prima serie di informazioni essenziali per rimandare poi i dettagli ad un testo completo ed esaustivo contenuto altrove (ad es. il sito internet del titolare, oppure bacheche, messaggi vocali preregistrati, ecc.), oppure si può utilizzare uno spazio all'interno dell'ordinario materiale cartaceo e della corrispondenza (ad esempio nei documenti di conferma degli ordini commerciali).
Nel rapporto con fornitori, clienti, dipendenti e collaboratori non è necessario ripeterla in occasione di ogni contatto: è sufficiente fornirla con una formula generale *una tantum*, all'inizio delle operazioni di trattamento (che potranno anche protrarsi nel tempo).
L'informativa, quindi, potrà essere fornita secondo le modalità sin qui indicate, anche attraverso dei modelli uniformi predisposti dalle associazioni rappresentative di categoria, a meno che essa non riguardi trattamenti 'delicati' (dati genetici o biometrici) che contemplano informazioni di natura sensibile ed anche giudiziaria, nel qual caso tutte le informazioni relative alle modalità di trattamento dovranno essere obbligatoriamente rese in modo dettagliato.
Con particolare riferimento ai trattamenti di dati personali (non sensibili) nell'ordinaria attività d'impresa, non è necessario il *consenso* nei casi in cui:

- i dati vengono trattati nell'esecuzione di un contratto o in fase pre-contrattuale per adempiere a specifiche richieste del cliente (effettivo o potenziale);
- il trattamento viene posto in essere per dare esecuzione ad un obbligo di legge;
- i dati provengono da albi, registri ed elenchi pubblici;
- i dati sono relativi allo svolgimento di attività economiche da parte dell'interessato.

Oltre a queste ipotesi, che abbracciano una cospicua area dei trattamenti effettuati ordinariamente da un'impresa, il Garante ha definito un'ulteriore possibilità per non richiedere il consenso. Predetta ulteriore ipotesi riguarda il titolare del trattamento che abbia già venduto un prodotto o prestato un

servizio ad un interessato nell'ambito dello svolgimento di ordinarie finalità amministrative e contabili, il quale potrà utilizzare i recapiti di posta elettronica e cartacea forniti dall'interessato medesimo, *per inviare ulteriore suo materiale pubblicitario o promuovere una sua vendita diretta o per compiere sue ricerche di mercato o di comunicazione commerciale*, purché da un lato tale attività promozionale riguardi beni e servizi del medesimo titolare e analoghi a quelli oggetto della vendita, dall'altro sia consentito all'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le menzionate finalità, di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente, nonché di ottenere un immediato riscontro che confermi l'interruzione di tale trattamento.
Se per certi versi tale previsione sembra una ripetizione di quanto già stabilito dall'art. 130 per le comunicazioni elettroniche, in realtà il Garante ha qui raccolto le esigenze di quegli operatori che, a causa di un'errata o troppo rigida interpretazione della norma, avevano difficoltà a consolidare la clientela e a «conservare un proprio diretto canale comunicativo con i soggetti con i quali abbiano già instaurato un rapporto contrattuale».
Il Garante, inoltre, è tornato sulla questione degli *incaricati*, precisando ancora una volta che il Codice accorda al titolare la possibilità di individuare quale incaricato del trattamento non necessariamente la persona fisica, bensì l'unità organizzativa cui egli appartiene (ad es. 'Ufficio Segreteria' – 'Ufficio Tecnico', ecc.). L'art. 30 del Codice, infatti, nell'ipotesi in cui all'interno di un ufficio vi siano più persone adibite alle stesse mansioni – o comunque 'interscambiabili' – consente di effettuare una sola nomina mediante la sottoscrizione di un unico documento da parte dei componenti quell'ufficio. Si potrebbe così ridurre la produzione cartacea e soprattutto evitare il rischio di dispersione dei documenti.
Si pensi, ad esempio, a quelle realtà aziendali che usufruiscono, anche per brevi periodi all'anno, dell'impiego di lavoratori interinali o comunque con impieghi a tempo determinato: gestire anche gli atti di nomina ad incaricato provocherebbe un inutile appesantimento dell'amministrazione dell'azienda, vanificando di fatto il significato dei provvedimenti del Garante che sono decisamente orientati in senso opposto.
Un altro adempimento – richiesto dalla Legge in particolari e tassative ipo-

tesi – è la 'notificazione' del trattamento, onere che con l'emanazione del Codice Privacy è divenuto da obbligatorio a facoltativo. La notificazione è una dichiarazione con la quale il titolare del trattamento, prima di iniziarlo, rende nota al Garante (che la inserisce nel registro pubblico dei trattamenti consultabile da chiunque sul sito *web* dell'Autorità) l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali. Ma quand'è che bisogna procedere alla notificazione? Il Garante ha specificato che, in linea di principio, i trattamenti ordinari svolti presso piccole realtà produttive non vanno notificati: si pensi ai trattamenti di dati relativi ai dipendenti, ai fornitori o alla clientela. In particolare, 'non devono essere notificati' i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa (i c.d. insoluti).
In questo quadro la notificazione deve essere effettuata in ipotesi particolari (indicate dall'art. 37 del Codice). Con specifico riguardo all'attività di impresa, i trattamenti soggetti a notificazione sono quelli relativi a:

- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti; come detto, non rientrano in quest'ambito i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa;
- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (ad esempio, dati trattati mediante sistemi di geolocalizzazione installati su veicoli al fine di individuarne la posizione);
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo (c.d. profilazione), ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi (non, quindi, quelli trattati direttamente dall'imprenditore), nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie.

Infine, nello svolgimento dell'attività di impresa può risultare necessario trasferire dati personali fuori dell'Unione Europea (ad esempio relativi alla

clientela o ai dipendenti). La disciplina in materia di 'trasferimento di dati' fuori dall'Unione Europea (UE) riguarda principalmente i flussi di dati personali verso i c.d. Paesi terzi, considerato che i Paesi situati all'interno dell'Ue hanno l'obbligo di attuare la direttiva 95/46/Ce, adottando specifiche normative in materia di protezione dei dati personali. Il loro rispetto è considerato idoneo per trasferire dati nell'Ue.
Il trasferimento è sempre consentito in varie ipotesi, tra le quali, con particolare riferimento alle attività d'impresa, possono ricordarsi i casi in cui:

- l'interessato ha manifestato il proprio consenso espresso e, se si tratta di dati sensibili, in forma scritta;
- il trasferimento è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- il trasferimento è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento;
- è necessario ai fini dello svolgimento delle investigazioni difensive oppure per far valere o difendere un diritto in sede giudiziaria.

Qualora non ricorrano le suddette condizioni bisogna fare riferimento:

- alle decisioni di adeguatezza adottate dalla Commissione europea in ordine al livello di protezione dei dati garantito dall'ordinamento del Paese destinatario (artt. 25, par. 6, e 26, par. 4, della direttiva 95/46/CE);
- alla decisione di adeguatezza delle garanzie contenute nel *Safe Harbor* per il trasferimento verso organizzazioni stabilite negli Stati Uniti d'America che ad esso aderiscono;
- all'adozione di clausole contrattuali standard tra 'esportatore' e 'importatore' di dati, il cui contenuto è stato ritenuto idoneo dalla Commissione europea (artt. 25, par. 6, e 26, par. 4, della direttiva 95/46/CE).

SEMPLIFICAZIONI PRIVACY: AUTOCERTIFICAZIONE DEL DPS E MISURE MINIME 'ALLEGGERITE'

Paolo Vicenzotto

Sono due i provvedimenti recentemente emanati in tema di semplificazione degli adempimenti privacy per le imprese, in particolare del Documento Programmatico sulla Sicurezza e delle misure minime di sicurezza: il primo è il decreto del 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133; il secondo – previsto dal medesimo decreto – è il provvedimento del *Garante per la protezione dei dati personali* del 27 novembre 2008, pubblicato in G.U. del 9 dicembre denominato *Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali.*
In generale, prima delle semplificazioni, il D.Lgs. 196/03 prescriveva a tutti i soggetti che trattano dati sensibili con strumenti elettronici (sostanzialmente tutte le aziende) l'adozione delle 8 misure minime di sicurezza dell'art. 34 (profili di autorizzazione, sistemi di autenticazione, antivirus, back up ecc) con le modalità dell'Allegato B, e la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza (DPS), un documento che 'fotografa' le misure di sicurezza adottate in azienda per prevenire violazioni della privacy.
Ora, con i due provvedimenti di semplificazione citati, sono state apportate alcune modifiche.

Il Documento Programmatico sulla Sicurezza e l'autocertificazione
La L. 133/08 ha introdotto l'art. 34 bis al D.Lgs. 196/03, che prevede la possibilità di sostituire il DPS con un'autocertificazione (*rectius*: dichiarazione

sostitutiva dell'atto di notorietà), per quei soggetti che si trovano in una delle seguenti condizioni:

1) trattano dati comuni e gli unici dati sensibili sono i dati sanitari dei dipendenti e collaboratori anche a progetto, ma senza l'indicazione della patologia, come ad esempio tutti quei dati sanitari necessari per la gestione amministrativa e giuslavoristica delle assenze per malattia;
2) trattano dati sindacali, come ad esempio il rilascio di permessi, aspettative, trattenute ed altro.

Chi si trova in queste situazioni, cioè quasi tutte le aziende di produzione nella propria ordinaria attività, può usufruire della semplificazione: anziché redigere il Documento Programmatico sulla Sicurezza con le complesse modalità di cui al punto 19 e seguenti dell'Allegato B al D.Lgs. 196/03, potrà predisporre un'autocertificazione con cui si attesta di trovarsi in una delle due condizioni sopra citate e di trattare tali dati avendo adottato le altre 'misure di sicurezza prescritte'. Si può trovare un modello di autocertificazione all'interno di questo numero di «Techne».

Ma quali sono queste altre 'misure di sicurezza prescritte'? Esse possono essere o le altre misure minime dell'art. 34 secondo le indicazioni dell'Allegato B, o le misure semplificate secondo le indicazioni del provvedimento di semplificazione del Garante del 27 novembre 2008. E ciò a seconda che si ricada o meno nei presupposti soggettivi di questo provvedimento del Garante, di cui parleremo a breve.

Prima di approfondire le misure semplificate, è necessaria un'ulteriore riflessione sull'autocertificazione del DPS. Nella pratica non sarà sempre agevole 'certificare' che l'azienda limita i propri trattamenti previsti dall'art. 34 bis (quelli indicati qui sopra). Possono essere molti, infatti, i casi di trattamenti che esulano da tali ambiti. Basti pensare al caso in cui l'ufficio del personale debba trattare una pratica, ad esempio di infortunio o di malattia, che comporta l'uso di dati contenti la patologia di un dipendente, magari per intrattenere una corrispondenza con l'assicurazione, l'INAIL o il medico del lavoro; oppure alla gestione di permessi concessi ad un proprio dipendente che abbia incarichi politici in quanto eletto in consiglio Comunale o Provinciale; o al caso in cui si renda necessario un controllo, anche solo tecnico, dei file

di navigazione di un dipendente. Queste evenienze possono esservi in origine, o sopravvenire nel corso dell'attività lavorativa. Alla luce di queste considerazioni, è necessario porre la massima attenzione nell'analisi del flusso dei dati trattati. In secondo luogo, qualora nel corso dell'attività intervengano variazioni in ordine alle caratteristiche dei trattamenti o alla tipologia dei dati utilizzati dal titolare tali da fare venir meno i presupposti dell'autocertificazione, il titolare dovrà predisporre il DPS, secondo le indicazioni dell'Allegato B.
Ricordiamo, infine, che l'autocertificazione del DPS, sottoscritta dal titolare dei trattamento (in persona del legale rappresentante) deve essere conservata presso la sede, per essere esibita solo in caso di controlli. È opportuno allegare alla stessa una fotocopia non autenticata di un documento di identità del sottoscrittore (come prescrive l'art. 38 del D.P.R. 445/00).

Le misure minime di sicurezza semplificate. Requisiti delle aziende
Il secondo provvedimento del *Garante per la protezione dei dati personali* del 27 novembre 2008, pubblicato in G.U. del 9 dicembre è denominato *Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali.*
Questo secondo provvedimento prevede che determinate categorie di soggetti non debbano applicare le misure minime di sicurezza nelle modalità previste dall'Allegato B al D.Lgs. 196/03, bensì con altre modalità, che permettono un minor carico di adempimenti per gli imprenditori.
I soggetti che possono avvalersi della semplificazione sono sostanzialmente quelli che già potevano godere dell'autocertificazione nella redazione del Documento Programmatico sulla Sicurezza e cioè:

1) trattano dati comuni e gli unici dati sensibili sono i dati sanitari dei dipendenti e collaboratori anche a progetto, ma senza l'indicazione della patologia;
2) trattano dati sindacali.

Come si può vedere questi due punti coincidono con quelli previsti dal nuovo art. 34 bis sull'autocertificazione del DPS. In più si aggiunge un nuovo requisito:

3) piccole e medie imprese che trattano dati personali unicamente per correnti finalità amministrative e contabili.

La definizione di piccola e media impresa rilevante al fine di individuare l'ambito soggettivo di applicazione del provvedimento di semplificazione è quella prevista dal Decreto 18 aprile 2005 del Ministero delle Attività Produttive, che ha recepito la raccomandazione 2003/361/CE. In modo semplificato possiamo così affermare che per PMI si intendono quelle che hanno meno di 250 occupati, e hanno un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro. Nell'ambito della categoria delle PMI, si definisce piccola impresa l'impresa che ha meno di 50 occupati e ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.

Più complesso è capire quando tali imprese trattino dati «unicamente per correnti finalità amministrative e contabili». In primo luogo l'espressione in esame si riferisce a tutti i trattamenti connessi allo svolgimento delle ordinarie attività d'impresa, sia che si tratti di dati sensibili che comuni. Così potrebbero essere trattamenti riguardanti l'organizzazione aziendale, la tenuta di contratti relativi sia a soggetti interni alla struttura del titolare (es. lavoratori) che terzi (es. clienti, fornitori), la gestione del personale (es. trattamenti sullo stato di salute dei propri lavoratori con indicazione della patologia, anche per gestioni di infortuni sul lavoro, pratiche INAIL, gestione delle trattenute, servizi di mensa in caso di allergie o divieti religiosi, permessi per festività religiose, ecc.), adempimenti nei confronti delle PA. Oppure adempimenti che rientrano nella tenuta della contabilità aziendale, a fini sia civilistici che fiscali, adempimenti di natura finanziaria connessi ai rapporti con banche o altri intermediari finanziari per l'ordinaria gestione di conti correnti (anche di terzi, ad es., nel caso dei propri dipendenti) o per la richiesta di prestiti, linee di credito e garanzie.

Questo requisito è di particolare importanza, in quanto se un'azienda effettua un trattamento che non ricade nelle condizioni del nuovo 34 bis (vedi sopra punti 1 e 2) ma ricade in questo punto sub n. 3 (poniamo ad esempio un trattamento di dati sanitari con indicazione della patologia per una pratica assicurativa di un dipendente con l'INAIL), questa azienda non potrà

applicare l'autocertificazione del DPS, ma solo le misure minime semplificate del provvedimento del Garante, comprensive, come vedremo, di un DPS semplificato rispetto le indicazioni originarie dell'Allegato B. Per chiarire bene a quali adempimenti sono tenute le aziende a seconda delle tipologie di trattamenti, vi invito a consultare la tabella n. 1 in fondo all'articolo.

Descrizione delle misure semplificate

Le semplificazioni riguardano i trattamenti effettuati con strumenti elettronici e non. Nel primo caso vi sono semplificazioni che riguardano le istruzioni agli incaricati del trattamento che potranno essere impartite anche oralmente, con indicazioni di semplice e chiara formulazione. Ciò escluderebbe l'obbligo di formazione analitico previsto invece dall'Allegato B punto 19.6.
Per il sistema di autenticazione informatica, viene data piena legittimità al codice per identificare chi accede ai dati (*username*), associato a una parola chiave (*password*). Cosa comunque, ormai di prassi nelle aziende.
Per ciò che concerne il sistema di autorizzazione, è prevista la possibilità di fornire agli incaricati specifici profili di autorizzazione, tramite il software dei sistemi operativi o dei server. Ad esempio, l'ufficio Clienti sarà autorizzato dal tecnico informatico ad accedere alle sole cartelle di sua competenza, e non a quelle dell'ufficio tecnico o segreteria. E ciò solo con i profili di Windows o del software di sistema.
In tema di sicurezza informatica si individuano dei principi più laschi (anche se quelli dell'Allegato B erano altrettanto 'leggeri'): gli aggiornamenti periodici degli antivirus sono effettuati almeno annualmente e non semestralmente. Il backup deve avvenire con frequenza almeno mensile, anche solo dei dati modificati.
Paradossalmente le misure semplificate riportano la possibilità di redigere un DPS semplificato. Pertanto, non è sempre chiaro capire l'ambito di applicazione di queste modalità semplificate di redazione del DPS, visto che i soggetti che se ne avvalgono possono sostanzialmente sovrapporsi a coloro che usufruiscono dell'autocertificazione sostitutiva del DPS, prevista dal nuovo art. 34 comma 1 bis del D.Lgs. 196/03. Anche in questo caso, per chiarire bene quando un'azienda debba redigere l'autocertificazione, il DPS sem-

plificato o il DPS intero, sarà necessario consultare la tabella 1 in fondo all'articolo.
Come dicevo, il Documento Programmatico sulla Sicurezza riceve dal nuovo provvedimento del Garante alcune semplificazioni rilevanti. Ferma la possibilità per chi ricade nei requisiti 1 e 2 di redigere l'autocertificazione sostitutiva, il nuovo DPS semplificato deve indicare il nome del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Poi deve essere eseguita una descrizione generale dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati. Cosa che si può fare facilmente, utilizzando i modelli di 'informativa' aziendale dove questi dati sono facilmente reperibili. Il documento deve indicare l'elenco, anche per categorie, degli incaricati del trattamento. Come per il DPS dell'Allegato B, è fondamentale una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Nei trattamenti realizzati senza l'ausilio di strumenti elettronici, il titolare potrà fornire agli incaricati, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Resta comunque fermo che per i soggetti sopra indicati, le misure minime di sicurezza obbligatorie sono quelle degli artt. 34 e 35, nelle modalità del qui commentato provvedimento del Garante: tutte le altre disposizioni previste dall'Allegato B al D.Lgs. 196/03 possono non essere adottate.

TABELLA DEGLI ADEMPIMENTI

	Solo dati comuni non sensibili	Dati comuni e unici dati sensibili sono dati sanitari dipendenti e collaboratori anche a progetto, senza patologia	Dati sindacali	Piccole e medie imprese che trattano dati personali unicamente per correnti finalità amministrative e contabili.	Dati sensibili diversi da dati sanitari senza patologia e dati sensibili per finalità diverse da quelle amministrative e contabili
DPS 'intero' secondo disposizione All. B D.Lgs. 196/03 punti 19 e seguenti					X
Misure minime di sicurezza 'intere' ai sensi dell'art. 34 e 35 e modalità All. B					X
Autocertificazione DPS ai sensi dell'art. 34 bis D.Lgs. 196/03		X	X		
Misure minime facilitate (provvedimento Garante)	X	X	X	X	
DPS facilitato (provvedimento Garante)				X	

LA SICUREZZA DEI DATI PERSONALI IN DUE RECENTI PROVVEDIMENTI DEL GARANTE

Luca Zenarolla

La storia della tutela normativa della riservatezza in Italia è emblematica: il nostro paese si dota di una legge in tema con sensibile ritardo rispetto ad altri stati europei, spinto dalla necessità di dare attuazione alla direttiva 95/46/CE che prevedeva, per l'appunto, che ogni paese membro avesse una normativa omogenea in tema di trattamento di dati personali.
Con questa direttiva la libertà di circolazione, quindi, si estende dalle merci e dalle persone a quelle particolari informazioni che sono i dati personali.
L'Italia vi provvede l'ultimo giorno utile per evitare sanzioni, il 31 dicembre del 1996.
Da allora la situazione è cambiata radicalmente: la legge 675/96 – la c.d. Legge Privacy – è stata modificata numerose volte (undici, per la precisione) per poi essere abrogata nel 2004 con l'entrata in vigore del *Codice in materia di protezione dei dati personali*, testo unico che ha rielaborato e unito tutte le norme in tema di riservatezza e che ha costituito il culmine di un'operazione di adattamento e di semplificazione di quella che è, e resta, in Italia una normativa 'imposta' dall'alto piuttosto che il frutto di un'esigenza sentita dalla popolazione.
L'aspetto più singolare è quello che, a fronte del ritardo nell'attuazione della direttiva comunitaria, il Legislatore italiano ha prodotto una delle normative più severe e complesse dell'intera Unione Europea, spingendosi oltre a quella di altri paesi europei già dotati 'tradizionalmente' di norme a tutela della privacy.
Proprio da questo atteggiamento rigido del nostro legislatore deriva quello che è il principale difetto dell'abrogata 675/96 e dell'attuale Codice Privacy,

ossia quello di non riuscire a distinguere tra realtà in cui il trattamento di dati personali è un'operazione routinaria e a basso rischio, rispetto a situazioni in cui l'operazione di trattamento è a tutti gli effetti un'attività pericolosa ai sensi dell'articolo 2050 del codice civile.
Dall'esigenza di porre rimedio a questa problematica è sorto quel movimento di pensiero che, attraverso la modifica del testo normativo o attraverso i provvedimenti del Garante, è culminato nei diversi provvedimenti di semplificazione di cui altri autori si occupano in questo stesso numero della rivista «Techne».
Queste semplificazioni, pur con i limiti e i problemi interpretativi che i miei Colleghi evidenziano nei loro contributi, non devono in ogni caso ingenerare nel lettore il convincimento che la tutela dei dati personali abbia subito nel nostro paese una brusca battuta d'arresto, se non addirittura, una regressione.
Quasi in contemporanea con questi interventi semplificativi, infatti, sono stati pubblicati dall'Authority due provvedimenti che mirano ad aumentare la sicurezza dei dati personali trattati con strumenti elettronici:

- provvedimento del 13 ottobre 2008 *Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*, pubblicato in *G.U. n. 287 del 9 dicembre 2008*;
- provvedimento 27 novembre 2008 *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* pubblicato in *G.U. n. 300 del 24 dicembre 2008.*

Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali

Il primo provvedimento si occupa di due particolari vicende che possono riguardare apparecchiature elettroniche utilizzate per trattare – e in particolare memorizzare – dati personali, ossia la riutilizzazione delle stesse per diverse attività e il loro smaltimento.
Si tratta di operazioni problematiche dal punto di vista privacy, ma troppo spesso sottovalutate: emblematico è il recente caso di una persona che, acquistando da un celebre sito di aste on-line un hard disk di seconda mano,

è entrato in possesso di una vera e propria miniera di nomi, codici, password, numeri di conto e numeri di telefono relativi ad oltre un milione di utenti di American Express, di Natwest e della Royal Bank of Scotland.
La problematica trae origine dal fatto – evidenzia il Garante – che il normale utente tende a ignorare il reale funzionamento delle apparecchiature elettroniche che utilizza quotidianamente: ad esempio, trascinare un file nel cestino del proprio pc per poi 'svuotarlo' non equivale a cancellare il file stesso in maniera definitiva. Semplicemente il file rimane registrato nelle memorie del Pc, in attesa di essere sovrascritto da nuovi dati.
Esemplificando, si può paragonare il disco rigido di un computer agli scaffali di una biblioteca: trascinando un file nel cestino, noi non eliminiamo fisicamente il libro dalla sua scansia, ma, più semplicemente, cancelliamo il nome del file stesso dall'elenco dei libri disponibili.
È quindi evidente che, nel momento in cui ci accingiamo a riutilizzare un computer o a gettare tra i rifiuti i nostri vecchi hard disk, sono necessarie una serie di cautele particolari. È necessario porre in essere – anche attraverso personale esterno specializzato – una serie di operazioni finalizzata a garantire la cancellazione sicura dei dati o loro non intelligibilità.
In particolare:

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche
Il provvedimento distingue in:

1) *Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici*
   In primo luogo si può procedere con la cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file).
   In alternativa si può procedere con la memorizzazione dei dati su hard disk o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di password note al solo utente. Può effettuarsi su interi volumi di

dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un c.d. file-system crittografico in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate.
In questo modo il soggetto che accidentalmente venga in possesso delle nostre apparecchiature, ma che non conosca la password, non potrà accedere alle nostre informazioni.

2) *Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici*
La Cancellazione sicura delle informazioni è ottenibile con appositi programmi informatici (shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione, a scrivere nelle aree del disco precedentemente occupate dalle informazioni eliminate sequenze casuali di numeri binari (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite appositi strumenti elettronici di analisi e recupero di dati. Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere un grado ragionevole di sicurezza varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità possono impiegare diverse ore o alcuni giorni, a secondo delle prestazioni del computer utilizzato.
In alternativa si può puntare sulla formattazione 'a basso livello' degli *hard disk* (la c.d. *low-level formattino*, LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso che possono giungere fino alla possibile successiva inutilizzabilità del supporto.
Infine, l'ultima soluzione è quella della demagnetizzazione (*degaussing*) dei dispositivi di memoria magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici ecc.): questa soluzione presenta il vantaggio di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicate le procedure di cui sopra.

Smaltimento di rifiuti elettrici ed elettronici
In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche si può anche ottenere tramite procedure che, nel rispetto delle normative di settore, prevedano la distruzione dei supporti di memorizzazione in modo da impedire l'acquisizione indebita di dati personali.
La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:
- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
Per quanto riguarda il secondo provvedimento, prima di passare all'esame delle singole misure, è opportuno soffermarsi sulla figura dell'Amministratore di sistema.
Come si legge nelle premesse del provvedimento, con la locuzione 'amministratore di sistema' si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
«Il Codice – a differenza della normativa previdente che prevedeva espressamente l'amministratore di sistema – non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia – continua il Garante – le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione.

Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati), alla custodia delle credenziali, alla gestione dei sistemi di autenticazione e di autorizzazione».
Sulla base di quanto riportato, quindi, sembra inevitabile che chiunque utilizzi strumenti elettronici per trattare dati personali si serva dell'opera di un vero e proprio 'amministratore di sistema': ma è proprio così? Alla luce dell'esperienza maturata sul campo, mi sento di dissentire: numerose sono le realtà in cui le operazioni che il Garante definisce 'tipiche' dell'amministratore di rete sono in realtà svolte da incaricati del trattamento o dal titolare stesso. E come inquadrare il tecnico informatico della cui opera ci si serve saltuariamente, solo in caso di guasti o di nuovi acquisti di attrezzature elettroniche?
Dopo aver illustrato gli aspetti più problematici insiti nel provvedimento, è possibile passare all'analisi delle singole misure prescritte ai titolari dei trattamenti di dati personali effettuati con strumenti elettronici.

a) *Valutazione delle caratteristiche soggettive*
L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Quindi, pur lasciando libero il titolare di attribuire le funzioni di amministratore di sistema ad un soggetto nominato quale incaricato del trattamento ai sensi dell'art. 30 del Codice, egli è tenuto ad osservare criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29. In questo modo, quindi, si viene a creare una figura ibrida, una sorta di 'super incaricato' che condivide i requisiti del responsabile del trattamento ma che da esso si stacca per quel che concerne il profilo della responsabilità.

b) *Designazioni individuali*
La designazione quale amministratore di sistema deve essere individuale e

recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Viene quindi eliminata una delle novità introdotte dal Codice Privacy, ossia la possibilità di nominare delle classi omogenee di incarico in luogo della nomina personale. Non sarà, quindi, più possibile per le aziende nominare come amministratore di sistema l'ufficio a ciò deputato nel suo insieme: si dovrà, invece, procedere a nominare individualmente i singoli membri dell'ufficio stesso. Si tratta, quindi, di un deciso passo indietro rispetto a quel processo di semplificazione che è l'obiettivo dichiarato dei recenti interventi del Legislatore e del Garante Privacy.

c) *Elenco degli amministratori di sistema*
Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Programmatico sulla Sicurezza oppure, nei casi in cui il titolare non sia tenuto a redigerlo, annotati comunque in un apposito documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.
Qualora l'attività degli amministratori di sistema riguardi anche informazioni di carattere personale dei lavoratori, i titolari sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni attraverso diverse modalità alternative:
- avvalendosi dell'informativa resa agli interessati ex art. 13 del Codice;
- tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1º marzo 2007 (in Gazzetta Ufficiale 10 marzo 2007, n. 58);
- mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).

d) *Servizi in* outsourcing
Nel caso di servizi di amministrazione di sistema affidati in outsourcing (ossia all'esterno dell'organizzazione del titolare) il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema,

sulla falsariga di quanto accade nel caso in cui l'amministratore di sistema sia una figura interna all'organizzazione.

e) *Verifica delle attività*
L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle regole previste dalle norme vigenti. Questo punto – pur condivisibile in linea di principio – sembra destinato a rimanere 'sulla carta': se un titolare affida all'esterno la funzione di amministratore di sistema, in quanto ritiene di non possedere nella propria organizzazione sufficente competenza, come potrà svolgere un controllo effettivo ed efficace sull'operato della persona cui si è affidato?

f) *Registrazione degli accessi*
Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Si tratta, quindi, di tenere traccia non solo delle attività di tutti gli incaricati, ma anche degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richiesta. Devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi. Questa prescrizione pone diversi dubbi: cosa si intende per inalterabilità? Può bastare un file in .pdf o è necessario firmare digitalmete il file di log? Per rispondere a questi interrogativi è lecito aspettarsi un ulteriore intervento chiarificatore dell'Authority.

Corso on-line certificato per dipendenti di aziende

PRIVACY E CORRETTO TRATTAMENTO DEI DATI IN AZIENDA

Il D.lgs 196/03 ha comportato un nuovo riassetto dell'impianto normativo.

La formazione in tema di PRIVACY E SICUREZZA:
È UN OBBLIGO DI LEGGE
È UN VALORE AGGIUNTO NELLA QUALITÀ DEL LAVORO
È UN MODO DI PROFESSIONALIZZARE IL RAPPORTO CON IL CLIENTE
È UN MODO PER LIMITARE RISCHI DI SANZIONI O RISARCITORI

Il corso in modalità e-learning è valido ai fini dell'obbligo formativo
L'azienda riceverà report dettagliati sull'esito della formazione di ogni dipendente.

Info: ialweb.it
Diletta Covre **t.** 0434 505553
diletta.covre@ial.fvg.it

SCIOGLI OGNI NODO SULLA PRIVACY

→ D.lgs 196/03

IALweb.it

IAL agenzia formativa Friuli Venezia Giulia

in collaborazione con STUDIO LEGALE RIEM

Il Documento Programmatico sulla Sicurezza

a cura di Glauco Riem e Paolo Vicenzotto

AUTOCERTIFICAZIONE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Ai sensi dell'art. 34, comma 1 bis, del decreto legislativo 30 giugno 2003, n. 196
resa nelle forme e modalità previste dall'art. 47 del D.P.R. 445
del 28 dicembre 2000

Io sottoscritto .....
nato a ..... il .....
in qualità di Legale Rappresentante della

società .....
con sede in .....
P.IVA .....
titolare del trattamento

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere, di formazione o uso di atti falsi, richiamate dall'art. 76 del D.P.R. 445, del 28 dicembre 2000

CERTIFICO

- che in azienda vengono trattati soltanto dati personali non sensibili e come unici dati sensibili quelli costituiti dallo stato di salute o malattia di dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dati relativi all'adesione ad organizzazioni sindacali o a carattere sindacale
- che in relazione a tali trattamenti sono state adottate le altre misure di sicurezza prescritte

data firma

Note a commento

1. La redazione dell'autocertificazione, come documento sostitutivo del DPS, non risulta essere un obbligo, ma rappresenta una facoltà accordata ai soggetti previsti nel comma 1 bis, dell'art. 34 del decreto legislativo 30 giugno 2003 n. 196.

2. Ricordiamo che, se un'azienda effettua un trattamento che non ricade nei requisiti di cui all'art. 34 bis D.Lgs. 196/03 (dati personali non sensibili e come unici dati sensibili quelli costituiti dallo stato di salute o malattia di dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dati relativi all'adesione ad organizzazioni sindacali o a carattere sindacale), ma effettua un trattamento 'per finalità amministrative e contabili' e tale azienda è una PMI (poniamo ad esempio un trattamento di dati sanitari con indicazione della patologia per una pratica assicurativa di un dipendente con l'INAIL), questa azienda non potrà applicare l'autocertificazione del DPS, ma solo le misure minime semplificate del provvedimento del Garante, che sono comprensive di un DPS semplificato rispetto le indicazioni originarie dell'Allegato B.

3. La facoltà di procedere all'autocertificazione dovrà dare luogo ad un'attenta analisi dei flussi documentali contenenti dati sensibili trattati da parte del titolare o del responsabile del trattamento. Ciascun titolare o responsabile dovrà infatti prendere in esame un'ampia casistica documentale dell'impresa la cui analisi preventiva potrebbe essere lunga ed onerosa per cui – al di là della semplificazione – si potrebbe ritenere meno oneroso continuare negli adempimenti annualmente connessi alla redazione del tradizionale Documento Programmatico sulla Sicurezza. In merito ci preme sottolineare come il DPS sia il documento che meglio evidenzia gli approcci, ma anche le soluzioni che il titolare intende adottare per garantire la sicurezza e la protezione dei dati sensibili (e giudiziari) dei soggetti con cui – in ragione della sua attività – viene in contatto. Ci preme anche affermare che la redazione dell'autocertificazione non dà al titolare le stesse possibilità di difesa che potrebbe invece fornire il DPS, redatto secondo le regole previste in materia, ove – in un eventuale controllo – vi fossero delle contestazioni sulle modalità e sulla natura della protezione a tutela dei dati personali sensibili che comunque il titolare o il responsabile sono tenuti ad adottare, secondo i principi generali che postulano la messa a punto di idonee e preventive misure di sicurezza, che sono invece solo genericamente indicate nell'autocertificazione. In punto l'eventuale attività defensionale dovrebbe quindi essere eteroriferita a documenti che attualmente costituiscono invece il corollario del DPS (policy aziendali, note esplicative nella nomina a responsabile o ad incaricato, relazioni tecniche o procedure indicate dall'amministratore di sistema, ecc); tale serie di informazioni risulterebbe 'sparsa' nelle molte

documentazioni dell'impresa e non, come oggi avviene, immediatamente rinvenibile come parte integrante del DPS costituendone le allegazioni.

4. Il titolare che intende utilizzare l'autocertificazione, dovrà poi, successivamente, monitorare attentamente il trattamento di eventuali ed ulteriori dati sensibili, diversi da quelli previsti dal comma 1 bis, dell'art. 34, del decreto legislativo 30 giugno 2003 n. 196, in ragione dell'attività d'impresa, professionale o artigianale, provvedendo eventualmente nell'immediato, alla redazione del Documento Programmatico sulla Sicurezza nelle forme già tradizionalmente previste alla normativa di riferimento del D.Lgs. 196/03 e del suo Allegato B). A titolo esemplificativo e non esaustivo ci preme sottolineare come certi dati personali di natura sensibile possano trovarsi in curriculum vitae dei candidati all'assunzione; nelle richieste di permessi per la partecipazioni ad attività sindacali o politiche, a cerimonie religiose; nelle richieste inoltrate ai responsabili alla mensa aziendale che diano evidenza di eventuali malattie ed altro.

5. Riteniamo poi opportuno che dell'autocertificazione di cui alla previsione dell'art. 34, comma 1 bis, del decreto legislativo 30 giugno 2003, n. 196, sia fatta menzione nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, secondo i principi dettati dal punto n. 26 dell'Allegato B) al D.Lgs. 196/03, analogamente a quanto è attualmente previsto in merito alla redazione o aggiornamento del Documento Programmatico sulla Sicurezza.

Minimo glossario privacy

a cura di Glauco Riem

Accesso selezionato. Da un punto di vista logistico possibilità accordata ad individuati soggetti di ingresso in aree nelle quali si svolgono attività considerate a rischio (aree militarizzate); da un punto di vista logico-informatico abilitazione ad entrare e/o ad aprire determinate applicazioni o banche dati contenenti informazioni riservate (v. art. 9, comma 1, lettera b), D.P.R. 318/99). Ora art. 35, comma 1, sub lettera c) ed Allegato B al D.Lgs. 196/03.

Area militarizzata. Porzione di un edificio o di ufficio nel quale si compiono attività 'pericolose' di trattamento di dati la cui conoscenza è riservata ad una ristretta cerchia di operatori. (v. anche *need to know*).

Amministratore di sistema. Soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema informativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Antivirus. Programma per elaboratore che consente di individuare e neutralizzare altri programmi che modificano, danneggiano o distruggono i dati elaborati ed archiviati nelle memorie magnetiche di un computer.

Back up. È la copia di sicurezza dei dati personali registrati in elaboratori elettronici che deve essere eseguita periodicamente.

Badge. È la tessera, dotata di banda magnetica o di microprocessore, che contiene i dati identificativi di un soggetto. Abbinata spesso all'uso di una

parola chiave è utilizzata, o inserendola o avvicinandola ad appositi lettori elettronici, per attivare una procedura di accesso a determinate aree fisiche o logiche di un sistema di sicurezza.

Casella di posta elettronica certificata. Con questa espressione si intende il sistema di invio di posta elettronica nel quale è fornita, da parte di un gestore di posta qualificato dal CNIPA, al mittente una documentazione elettronica attestante l'invio e la consegna di documenti informatici (ex art. 1, sub lettera g), del D.P.R. 11 febbraio 2005, n. 68).

Chiave biometrica. È la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente.

Chiavi asimmetriche. È la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici.

Cifratura dei dati. Procedura realizzata attraverso specifici programmi per elaboratore che permette di rendere il testo di un documento non intelligibile ai soggetti che non sono dotati delle apposite chiavi il cui uso permette appunto di cifrare e/o decifrare il testo redatto.

Codice identificativo personale. Insieme di caratteri alfanumerici attribuiti ad un singolo soggetto – con appositi programmi per elaboratore – utilizzato per riconoscere l'identità di chi ne è il titolare. Attraverso il predetto codice il suo titolare viene abilitato da un sistema di controllo logico o logistico a compiere determinate attività.

Comunicazione dati (v. anche *diffusione*). È la possibilità, prevista dall'art. 4, comma 1, sub lettera l) del D.Lgs. 196/03 (già l. 675/96 all'art. 10, comma 1, lettera d), di trasmettere i dati personali raccolti da un soggetto, determinati ad altri soggetti.

Credenziali di autenticazione - ex num. 2 dell'Allegato B) del D.Lgs. 196/03. «Consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo [...] oppure ad una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave».

Data log journal. 'Libro giornale' compilato automaticamente da un elaboratore. Il data log permette di verificare analiticamente tutte le attività di elaborazione e di trattamento eseguite e di indicare il tempo in cui le stesse sono state effettuate. Se il sistema informatico è dotato di programmi che consentono l'accesso attraverso parole chiave e/o codici identificativi personali, il *data log journal* permette anche di riferire l'attività ed i tempi di svolgimento ai singoli soggetti che la eseguono.

Dato anonimo - ex primo comma, lettera n), dell'art. 4 del D.Lgs. 196/03. È il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Dato 'sensibile'. Secondo l'art. 4, primo comma, sub lettera d) del D.Lgs. 196/03 (già art. 22, *sub* n. 1, della l. 675/96), sono i dati personali, tassativamente indicati, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dato personale - ex art. 4, comma 1, lettera b), del D.Lgs. 196/03. È qualunque informazione relativa a persona fisica, persona giuridica, ente od associazioni, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Diffusione dati. È l'attività prevista ex art. 4, comma 1, lettera l), del D.Lgs. 196/03 che consiste nel dare conoscenza dei dati personali a soggetti inde-

terminati in qualunque forma, anche mediante la loro messa a disposizione o consultazione (v. anche *comunicazione* dati).

Documento informatico - ex art. 8, comma 1, lettera a). D.P.R. 445/2000. È il documento valido e rilevante a tutti gli effetti da chiunque formato o registrato su supporto informatico e trasmesso con strumenti telematici secondo le regole tecniche previste dall'art. 71 del D.Lgs. 82/05, *Codice dell'amministrazione digitale*.

Elaboratore. «È una apparecchiatura comprendente dispositivi di ingresso e di uscita che, ai segnali di ingresso, portatori di informazione, fa corrispondere in uscita altri segnali, in base a regole stabilite da un programma [...] è quindi essenzialmente una macchina per il trattamento dell'informazione» (G. Fiorentino, *Enciclopedia dell'informatica*, 1979, 125) (v. anche *strumenti informatici ed automatizzati*).

Finalità del trattamento. È l'indicazione dettagliata, che l'interessato deve conoscere in base all'art. 13, comma 1, lettera a), del D.Lgs. 196/03, degli scopi per i quali il trattamento dei dati viene effettuato dal titolare o dal responsabile del trattamento.

Firma digitale. Secondo l'art. 24 del D.Lgs. 82/05, *Codice dell'amministrazione digitale*, è un dispositivo di «firma digitale che deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso».

Firewall. Sistema *hardware* o *software* che – inserito fra la rete Internet e la rete interna – individua e controlla il traffico dei singoli pacchetti TCP.IP facendo transitare solo quelli autorizzati secondo delle regole stabilite dall'*amministratore di sistema* ed eliminando (*drop the packet*) i pacchetti non autorizzati.

Garante. È l'autorità, istituita ex art. 30 della l. 675/96, che come riaffermato dall'art. 153 del D.Lgs. 196/03, ha come compito la protezione dei dati personali ed alla quale è attribuita – *ex* art. 154 – un serie di competenze specifiche e di controllo sulla correttezza e veridicità degli adempimenti messi in essere dai soggetti che sono sottoposti alla norma.

Hardware. È la c.d. parte 'rigida' dell'elaboratore (es.: tastiera, stampante, monitor) in contrapposizione a *software* – la parte 'soffice' – cioè l'algoritmo che permette all'elaboratore di compiere il trattamento delle informazioni secondo le modalità indicategli dal programmatore.

Incaricato del trattamento dei dati personali - ex art. 4, comma 1, lettera h) 153 del D.Lgs. 196/03 (già art. 2, comma 1, del D.P.R. 318/99). È la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Indirizzo elettronico. È l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici.

Interessato - ex art. 4, comma 1, lettera i) del D.Lgs. 196/03 (già art. 1, comma 1, lettera f), della l. 675/96). È la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati.

ITSEC (Information Tecnology Security Evaluation Criteria). È un sistema di valutazione della sicurezza nel trattamento e nel controllo delle informazioni che vengono elaborate con strumenti informatici ed automatizzati. È stato introdotto nel 1992 dalla Commissione delle Comunità Europee (DGXIII) ed è stato utilizzato dagli Stati per gestire la sicurezza nazionale

secondo il concetto per il quale la riservatezza era considerata come «la prevenzione dell'accesso non autorizzato all'informazione». ITSEC prevede un sistema di valutazione della sicurezza secondo sette livelli che vengono indicati con sigle: da C zero (C0) – nessuna sicurezza – a C sei (C6) – massima sicurezza.

Misure minime di sicurezza - ex art. 33 e segg. ed ex Allegato B), del D.Lgs. 196/03 (già art. 1, comma 1 lettera a), del D.P.R. 318/99). È il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel citato regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi prevedibili.

Modello di notifica al Garante. Si tratta di un modello predisposto dal Garante per il trattamento dei dati personali e da utilizzare per i diversi adempimenti previsti ex artt. 37 e 38 del D.Lgs. 196/03 in tema di notifica.

Need to know. È un principio generale sviluppato nella gestione dei sistemi di sicurezza secondo il quale i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento del mansionario loro attribuito.

Preposto alle parole chiave ed/od ai codici identificati personali: Secondo l'Allegato B) del D.Lgs. 196/03 è il soggetto che sovrintende alla custodia, alla gestione ed alla disattivazione delle parole chiave e dei codici identificativi personali attribuiti agli incaricati del trattamento dei dati personali.

Protocollo informatico - ex art. 1, comma 1, lettera c), dell'abrogato D.P.R. 428/98 reiterato nel D.P.R. 445/2000. È l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni, ma anche dalle imprese per la gestione dei documenti.

Responsabile del trattamento - ex art. 4, comma 1, lettera g), del D.Lgs. 196/03 (già art. 1, comma 1, lettera e), della l. 675/96). È la persona fisica, la

persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

Restore. È la possibilità di riottenere immediatamente l'accesso ad informazioni elaborate elettronicamente dopo che le stesse sono state perdute a causa di un evento accidentale o danneggiate intenzionalmente da terzi (vedi *back up).*

Sanzioni privacy. Sono le sanzioni previste dal Titolo III, Capo I ed II del D.Lgs. 196/03 dall'art. 161 al 172 (nella disciplina previgente dal Capo VIII della legge 675/96).

Semplificazione privacy. Complesso di norme in tema di semplificazione degli adempimenti privacy espressamente destinato alle imprese e pubblicato con il decreto del 25 giugno 2008, n. 112, successivamente approvato con modifiche dalla legge di conversione 6 agosto 2008, n. 133; ed altresì con il provvedimento del *Garante per la protezione dei dati personali* del 27 novembre 2008, pubblicato in G.U. del 9 dicembre sotto la rubrica: *Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali.*

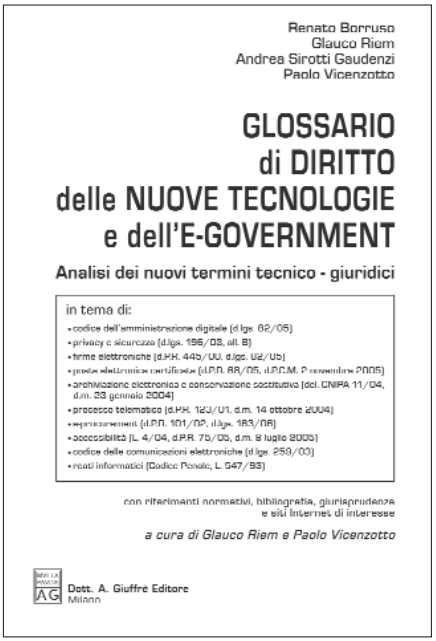
Server. Elaboratore centrale, utilizzato e condiviso da altri elaboratori e terminali ad esso connessi, che conserva nella propria memoria dati e informazioni che ivi vengono registrate.

Software. Programma applicativo che permette all'elaboratore di compiere una serie di attività di trattamento delle informazioni secondo le regole ed i flussi indicati e predeterminati dal programmatore che è autore del programma stesso.

Strumenti elettronici - ex art. 4, comma 3, sub lettera b) del D.Lgs. 196/03. Sono gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Titolare del trattamento - ex art. 4, comma 1, sub lettera f) (già art. 1, comma 1, lettera d), della l. 675/96). È la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza.

Trattamento - ex art. 4, comma 1, sub lettera a) del D.Lgs. 196/03 (già art. 1, comma 1, lettera b), della l. 675/96). È qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzate, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.



Il *Glossario di diritto delle nuove tecnologie e dell'e-government* (Giuffrè, Milano 2007, pp. 548) è una sorta di unicum all'interno del panorama editoriale giuridico sia per la struttura dell'opera, che per i temi trattati. Il testo contiene le definizioni più importanti dei termini giuridici e tecnici di cui alle più recenti produzioni normative in materia di diritto delle nuove tecnologie.
Gli ambiti trattati nell'opera, in particolare, concernono il *codice dell'amministrazione digitale* (d.lgs. 82/05), la *privacy* e sicurezza (d.lgs. 196/03, all. B), le *firme elettroniche* (d.P.R. 445/00, d.lgs. 82/05), la *posta elettronica certificata* (d.P.R. 68/05, d.P.C.M. 2 novembre 2005), l'*archiviazione elettronica e conservazione sostitutiva* (del. CNIPA 11/04, d.m. 23 gennaio 2004), il *processo telematico* (d.P.R. 123/01, d.m. 14 ottobre 2004), l'*e-procurement* (d.P.R. 101/02, d.lgs. 163/06), l'*accessibilità* (L. 4/04, d.P.R. 75/05, d.m. 8 luglio 2005), il *codice delle comunicazioni elettroniche* (d.lgs 259/03), i *reati informatici* (Codice Penale, L. 547/93) oltre ad altri termini più legati alla tradizionale informatica giuridica.
L'opera ha un approccio molto pratico: ciascun termine viene illustrato al lettore attraverso definizioni analitiche, che permettono di chiarire il significato della parola e di ricreare il contesto giuridico ove essa opera nel modo più completo possibile. Quindi sono elencati tutti i 'termini connessi' che trovano una correlazione con la parola definita e che sono anch'essi definiti nel *Glossario*. Poi sono indicate le fonti legislative e regolamentari collegate alla parola analizzata, unitamente alla citazione di altre fonti bibliografiche, ove poter reperire testi per un approfondimento più completo. Gli autori hanno inteso arricchire ciascun vocabolo con pronunce della più recente giurisprudenza in materia. L'ultima parte di ciascun termine prevede l'indicazione di eventuali siti e documenti di interesse reperiti in Internet.

Condizioni di abbonamento

Abbonamento annuale (3 numeri): € 15,00 IVA inclusa.
L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri relativi all'annata. Il pagamento può avvenire con versamento sul conto corrente n. 62833595 - Banco Posta, Via S. Caterina, 8/10 - 33170 Pordenone - ABI 07601, CAB 12500, intestato a: Associazione Culturale per lo Studio del Diritto. Causale: *Abbonamento rivista Techne 2009*.
L'abbonamento si intende rinnovato per l'anno successivo se non disdetto entro 1 mese dalla scadenza. I fascicoli non pervenuti devono essere reclamati al ricevimento del fascicolo successivo. Le variazioni di indirizzo vanno comunicate all'editore.

Pubblicità

Per le inserzioni pubblicitarie contattare: Associazione Culturale per lo Studio del Diritto - Ufficio Pubblicità - Vicolo Chiuso, 5 - 33170 Pordenone, tel. 0434 522866 - fax 0434 246429.

La vignetta di Federico Cecchin

COPIA OMAGGIO

Non soggetto dpr 633/72, art. 12 lettera d

PROMOZIONE
ABBONAMENTI 2009

Condizioni di abbonamento
Abbonamento annuale (3 numeri): € 15,00 IVA inclusa.
L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri relativi all'annata. Il pagamento può avvenire con versamento sul conto corrente n. 62833595 - Banco Posta, Via S. Caterina, 8/10 - 33170 Pordenone
ABI 07601, CAB 12500, intestato a: Associazione Culturale per lo Studio del Diritto.
Causale: Abbonamento rivista Techne 2009.