

ASSOCIAZIONE CULTURALE
PER LO STUDIO DEL DIRITTO

techne

Direttore responsabile

GLAUCO RIEM

Redazione

STEFANO CORSINI
FRANCESCO MIRABELLI
LUCA ZENAROLLA
PAOLO VICENZOTTO

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

Direttore responsabile

GLAUCO RIEM

Comitato scientifico

RENATO BORRUSO (direttore del comitato scientifico)

Presidente onorario aggiunto della Corte di Cassazione; professore di Informatica giuridica

MASSIMILIANO ATELLI

Magistrato del TAR; già avvocato Ufficio del Garante per la protezione dei dati personali

GIANLUIGI CIACCI

Professore di Informatica giuridica, Università Luiss 'Guido Carli' di Roma; dottore di ricerca in

Diritto dell'informatica e Informatica giuridica, Università degli Studi 'La Sapienza' di Roma

CRISTIANA COMPAGNO

Magnifico Rettore, Università degli Studi di Udine

GIAN LUCA FORESTI

Professore di Informatica, Università degli Studi di Udine

FURIO HONSELL

Professore di Informatica, Università degli Studi di Udine

DONATO LIMONE

Professore di Informatica giuridica, Università degli Studi 'La Sapienza' di Roma e Università telematica 'Telma' di Roma

PATRIZIO MENCHETTI

Membro del Legal Advisory Board (comitato consultivo giuridico) della Direzione generale 'Società dell'Informazione' della Commissione Europea

PIER LUCA MONTESSORO

Professore di Sistemi di elaborazione e direttore del Dipartimento di Ingegneria Elettrica, Gestionale e Meccanica, Università degli Studi di Udine

ROCCO PANETTA

Avvocato; dirigente dell'Ufficio del Garante per la protezione dei dati personali; professore di Istituzioni di diritto privato, Università degli Studi 'Roma Tre' di Roma

UMBERTO RAPETTO

Comandante del Nucleo Speciale Anticrimine Tecnologico della Guardia di Finanza

FLORETTA ROLLERI

Direttore generale del Centro di Eccellenza del Ministro della Giustizia in Castel Capuano in Napoli

PIEREMILIO SAMMARCO

Professore di Diritto dell'informatica, Università degli Studi 'Roma Tre' di Roma; dottore di ricerca in Diritto dell'informatica e Informatica giuridica, Università degli Studi 'La Sapienza' di Roma

ROBERTO SANTOLAMAZZA

Direttore di 'Treviso Tecnologia', azienda speciale della CCIAA di Treviso

ANDREA SIROTTI GAUDENZI

Professore nel Master in Diritto della Rete, Università degli Studi di Padova

MARZIO VAGLIO

Professore nel Master in Diritto della Rete, Università degli Studi di Padova

PAOLO VICENZOTTO

Avvocato del Foro di Pordenone, autore di pubblicazioni di Diritto dell'informatica

Hanno collaborato a questo numero

???????

SOMMARIO

EDITORIALE GLAUCO RIEM	5
TECHNE & STUDI PROFESSIONALI PIERANTONIO BIASOTTO	XX
PRIVACY: LA SEMPLIFICAZIONE PRIVACY EX ART. 6 DEL DECRETO SVILUPPO (D.L. N. 70/2011). IL TESTO DELLA NORMA E BREVI NOTE A COMMENTO GLAUCO RIEM	XX
L'APPLICAZIONE DEL D.LGS. 196/2003 NEGLI STUDI PROFESSIONALI ALLA LUCE DEL COMUNICATO DELL'AGENZIA DELLE ENTRATE DEL 3.8.2011 'VIGILANZA SUGLI INTERMEDIARI ENTRATEL' STEFANO CORSINI	XX
SEMPLIFICAZIONI PRIVACY: AUTOCERTIFICAZIONE DEL DPS E MISURE MINIME 'ALLEGGERITE' ALLA LUCE DELLE MODIFICHE LEGISLATIVE AL CODICE PRIVACY 2011 PAOLO VICENZOTTO	XX
LA SICUREZZA DEI DATI PERSONALI IN DUE PROVVEDIMENTI DEL GARANTE LUCA ZENAROLLA	XX
MINIMO GLOSSARIO PRIVACY	XX
Le vignetta di FEDERICO CECCHIN	XX

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 di professionisti ed imprese contenuto nel cosiddetto decreto sviluppo D.L. 70/2010 così come recepito con modifiche dalla legge n. 106.

In apertura una breve nota del Presidente dell'«Unione dei giovani commercialisti ed esperti contabili» di Treviso PIERANTONIO BIASOTTO illustra i motivi che hanno determinato l'intenzione di pubblicare questo numero della rivista «Techne» onde informare i propri professionisti associati delle novità legislative in merito alla semplificazione privacy ed ad organizzare il convegno del 10 ottobre 2011 scorso con la collaborazione dell'Associazione culturale per lo studio del diritto e dell'informatica di Pordenone e lo Studio Legale Riem.

GLAUCO RIEM delinea i temi generali sull'attuale assetto normativo in tema di trattamento e protezione dei dati personali così come modificato dalla recente normativa.

STEFANO CORSINI delinea l'approccio alla privacy negli studi professionali alla luce del Comunicato dell'Agenzia delle Entrate del 3 agosto 2011 sulla *Vigilanza sugli intermediari Entratel*.

PAOLO VICENZOTTO commenta gli adempimenti relativi all'autocertificazione ed al documento programmatico **steso** in forma semplificata.

LUCA ZENAROLLA analizza i due più recenti provvedimenti del Garante in tema di sicurezza nel trattamento dei dati personali e segnatamente sulla radiazione dei *Rifiuti di apparecchiature elettriche ed elettroniche (Raee)* e *misure di sicurezza dei dati personali* e sulle *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*.

Infine la vignetta di FEDERICO CECCHIN illustra, *suo modo*, le semplificazioni introdotte dal decreto sviluppo in punto privacy.

«Technè» contiene inoltre dei materiali conoscitivi di supporto per lo studio professionale quali un glossario privacy, l'elenco delle nuove sanzioni privacy per le violazioni amministrative e per gli illeciti penali attualmente in vigore.

TECHNE & STUDI PROFESSIONALI

DI PIERANTONIO BIASOTTO

Presidente Unione Giovani Dottori Commercialisti ed Esperti Contabili di Treviso

La privacy è comunemente intesa come un complesso di norme e di comportamenti finalizzati alla protezione e alla tutela del diritto alla riservatezza delle informazioni che riguardano anche aspetti 'sensibili' delle persone. La disciplina è in costante evoluzione, condizionata anche dalla continua innovazione tecnologica che interessa i rapporti economici, giuridici e fiscali.

La stratificazione prodotta negli anni da novelle normative emanate con intento di apportare delle semplificazioni ha prodotto, in realtà, una disciplina per niente chiara e di facile applicazione. Disciplina che, peraltro, trova critiche severe non solo nella sua reale capacità di raggiungere gli obiettivi prefissati ma anche negli elevati costi a cui sottopone la società a fronte di risultati marginali.

Certo è che l'evoluzione informatica obbliga sempre più persone a regole severe per proteggere i dati sensibili in quanto la loro diffusione potrebbe ledere diritti fondamentali dell'individuo.

Il 10 ottobre 2011, nel convegno di Mogliano Veneto (TV) organizzato dall'UGDCEC di Treviso, ci si è posti l'obiettivo di fare il punto sulle norme in tema di privacy.

Il quadro emerso non sembra rassicurante e le semplificazioni introdotte, di 'semplice' paiono avere soltanto il nome.

In questo numero della rivista «Techne» abbiamo domandato ad alcuni esperti della materia di fornirci chiarimenti, delucidazioni e spunti operativi sulle numerose modifiche normative di recente introduzione, ponendo attenzione anche ai *rumour* presenti all'interno della bozza del 'nuovo

decreto sviluppo' che sembra introdurre ulteriori 'semplificazioni'.
Con questo lavoro auspichiamo di essere riusciti a fornire ai colleghi un piccolo contributo focalizzato proprio su tematiche legate alla privacy che quotidianamente dobbiamo affrontare nella gestione dei nostri studi professionali.

PRIVACY: LA SEMPLIFICAZIONE PRIVACY EX ART. 6 DEL DECRETO SVILUPPO (D.L. N. 70/2011). IL TESTO DELLA NORMA E BREVI NOTE A COMMENTO

GLAUCO RIEM

Il Garante, nel corso di un'audizione di fronte alla Commissione Bilancio e Finanze della Camera, ha manifestato il suo giudizio sulla novella al codice privacy affermando che il testo della norma approvato «appare assolutamente censurabile, non solo per il linguaggio, l'incertezza del suo contenuto e la sua incoerenza col sistema delle fonti, ma anche perché muove da presupposti e contiene affermazioni del tutto prive di ogni fondamento».

Lo stesso Garante della Privacy poi «non ritiene che il decreto sviluppo escluda l'applicazione del codice nei rapporti dell'impresa con i dipendenti», così come da una prima lettura dell'art. 6 del decreto legge 70 del 2010 convertito con la legge n. 106 il 12 luglio 2011, era, *prima facie*, sembrato ad alcuni commentatori.

In punto, una precisa circolare di Confindustria (n. 19439 del 18 luglio 2011), ha illustrato la norma alle imprese che troppo presto avevano pensato di liberarsi di una serie di adempimenti legati alla tutela della riservatezza. Ma vediamo il testo recato dalla novella.

Il D.L. 70/2011 modifica nell'ordine i seguenti articoli del D.Lgs. 196/2003:

- art. 5. *Oggetto ed ambito di applicazione*, aggiungendovi il comma 3 *bis*:

3-bis.⁽¹⁾ Il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo-contabili, come definite all'articolo 34, comma 1-ter, non è soggetto all'applicazione del presente codice.

- art. 13. *Informativa*, aggiungendovi il comma 5 *bis*:

5-bis.⁽¹⁾ L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f).

- art. 24. *Casi nei quali può essere effettuato il trattamento senza consenso*, aggiungendo al comma 1) la lettera g):

g)⁽¹⁾ con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.

- art. 24. *Casi nei quali può essere effettuato il trattamento senza consenso*, aggiungendo al comma 1) le lettere i) *bis* ed i) *ter*.

i-bis)⁽²⁾ riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis (19);

i-ter)⁽²⁾ con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.

- art. 26. *Garanzie per i dati sensibili*, aggiungendo al comma 3) la lettera b) *bis*:

b-bis)⁽¹⁾ dei dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis.

- art. 34. *Trattamenti con strumenti elettronici*, aggiungendo i commi 1) *bis* ed 1) *ter*.

1-bis.⁽¹⁾ Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita 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 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B). In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrativo-contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentiti il Ministro per la semplificazione normativa e il Ministro per la pubblica amministrazione e l'innovazione, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico contenuto nel citato allegato B) in ordine all'adozione delle misure minime di cui al comma 1.

1-ter.⁽¹⁾ Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempiimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

- art. 130 aggiungendo i commi 3) *bis*, 3) *ter* e 3) *quater*:

3-*bis*.⁽²⁾ In deroga a quanto previsto dall'articolo 129, il trattamento dei dati di cui all'articolo 129, comma 1, mediante l'impiego del telefono e della posta cartacea per le finalità di cui all'articolo 7, comma 4, lettera b), è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario e degli altri dati personali di cui all'articolo 129, comma 1, in un registro pubblico delle opposizioni.

3-ter.⁽²⁾ Il registro di cui al comma 3-bis è istituito con decreto del Presidente della Repubblica da adottare ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, previa deliberazione del Consiglio dei ministri, acquisito il parere del Consiglio di Stato e delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, nonché, per i relativi profili di competenza, il parere dell'Autorità per le garanzie nelle comunicazioni, che si esprime entro il medesimo termine, secondo i seguenti criteri e principi generali:

a) attribuzione dell'istituzione e della gestione del registro ad un ente o organismo pubblico titolare di competenze inerenti alla materia; **b)** previsione che l'ente o organismo deputato all'istituzione e alla gestione del registro vi provveda con le risorse umane e strumentali di cui dispone o affidandone la realizzazione e la gestione a terzi, che se ne assumono interamente gli oneri finanziari e organizzativi, mediante contratto di servizio, nel rispetto del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 12 aprile 2006, n. 163. I soggetti che si avvalgono del registro per effettuare le comunicazioni corrispondono tariffe di accesso basate sugli effettivi costi di funzionamento e di manutenzione. Il Ministro dello sviluppo economico, con proprio provvedimento, determina tali tariffe; **c)** previsione che le modalità tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale è intestatario secondo modalità semplificate ed anche in via telematica o telefonica; **d)** previsione di modalità tecniche di funzionamento e di accesso al registro mediante interrogazioni selettive che non consentano il trasferimento dei dati presenti nel registro stesso, prevedendo il tracciamento delle operazioni compiute e la conservazione dei dati relativi agli accessi; **e)** disciplina delle tempistiche e delle modalità dell'iscrizione al registro, senza distinzione di settore di attività o di categoria merceologica, e del relativo aggiornamento, nonché del correlativo periodo massimo di utilizzabilità dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente; **f)** obbligo per i soggetti che effettuano trattamenti di dati per le finalità di cui all'articolo 7, comma 4, lettera b), di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilità e sulle modalità di iscrizione nel registro per opporsi a futuri contatti; **g)** previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli 23 e 24.

3-quater.⁽²⁾ La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3-bis e sul trattamento dei dati sono attribuiti al Garante.

Abbiamo già anticipato del dissenso espresso dal Garante alla novella recata dal decreto sviluppo n. 70/2011 e dalla successiva legge di recepimento n. 106 il 12 luglio 2011. Il Garante ha anche affermato che «si tratta di norme di difficile interpretazione che non semplificano il tessuto normativo del Codice».

Dalla lettura delle norme già riportate in dettaglio non possiamo che concordare con quanto affermato dal Garante.

La maggiore perplessità è suscitata *in primis* dalla nuova dizione dell'art. 34 *Trattamenti con strumenti elettronici*, là dove si afferma che per coloro che

trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita 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 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B).

Coloro (titolari e/o responsabili) che avevano scelto di redigere l'autocertificazione - possibilità introdotta dal decreto n. 112/2008 convertito nella legge n. 133/2008, sulla *Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'allegato B) al Codice in materia di protezione dei dati personali* - erano stati 'facilitati' nell'immediato ma, avevano dovuto costantemente monitorare i flussi documentali contenenti dati sensibili di terzi, non ricompresi nell'elenco previsto dalla norma e ricaduti successivamente alla dichiarazione nell'ambito del trattamento.

L'ampia casistica dei dati trattati nell'impresa poneva infatti, in capo al 'dichiarante', una diligenza ed un'attenzione nell'analisi della tipologia di dati trattati che non giustificava, né tuttora giustifica, l'abbandono della redazione del DPS così come postulato dall'allegato B) al D.Lgs. 196/2003 e successive modifiche. Infatti una volta redatto o aggiornato correttamente il DPS 'classico' basta seguirne le indicazioni; si evitano così - a nostro avviso - i doveri e costanti controlli per verificare se il trattamento abbia riguardato

solo quelle categorie di dati e di persone che sono elencate nella dizione normativa (art. 34) che prevede la semplice autocertificazione del dichiarante ai sensi dell'art. 47 del d.P.R. 445/2000.

In punto riteniamo difficile che i professionisti possano redigere l'autocertificazione così come prevista dalla norma in vigore essendo quasi impossibile che il professionista tratti «soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti».

In relazione all'obbligo deve sicuramente essere chiarito che l'obbligatorietà è in relazione alle scelte del titolare del trattamento e cioè: se non si ritiene di redigere il DPS ex allegato B) al Codice Privacy sussiste l'obbligo di redigere e sottoscrivere la dichiarazione sostitutiva e ciò sempre se siano presenti le condizioni previste dalla attuale dizione dell'art. 34 sub comma 1) *bis*. A nostro avviso quindi, chi continua a redigere ed aggiornare il DPS non è sicuramente obbligato a redigere la dichiarazione sostitutiva.

Chi invece, trovandosi nella suddetta previsione normativa, rinuncia ad adottare il DPS ex allegato B) al Codice privacy dovrà obbligatoriamente redigere la dichiarazione sostitutiva ex comma 1) *bis*; affrontando però l'alea che detta dichiarazione venga, a posteriori, vanificata da successivi trattamenti di dati diversi ed eccedenti quelli tassativamente indicati dalla norma da inserire nella dichiarazione stessa.

Ulteriore perplessità reca poi la nuova dizione dell'art. 130 ove il legislatore, nel passaggio dalle regole contenute dalla legge 675/96 al D.Lgs. 196/2003, aveva fatto una precisa scelta di campo abbandonando la regola dell'*opt-out* per abbracciare quella dell'*opt-in*: niente più comunicazioni indesiderate all'interessato cui i dati o l'indirizzo mail si riferiscono, ma solo dietro il suo preventivo consenso (*opt-in*): quindi niente spedizioni con l'indicazione che, se lo desideri, «ti cancelliamo dalla lista» (*opt-out*), ma «o hai il consenso preventivo dell'interessato oppure non devi spedirgli comunicazioni di sorta».

Tutti abbiamo sotto gli occhi le migliaia di comunicazioni non desiderate di cui indistintamente siamo fatti oggetto da parte di coloro che, dall'intero mondo urbi terracqueo elettronico, utilizzano '*recent inventions and new*

business methods': la scelta di un obbligatorio e preventivo consenso avrebbe dovuto porre allora un reale freno a detta 'attività' e ciò anche in relazione al fatto che detto divieto era allora rafforzato dall'art. 167 del Codice sul *Trattamento illecito di dati*, che poneva a carico dei trasgressori del dettato dell'art. 130 la sanzione della reclusione.

L'odierna novella, derogando alla previsione dell'art 129 del Codice, apre una ulteriore breccia nel sistema dell'*opt in*, affermando che

il trattamento dei dati di cui all'articolo 129, comma 1, mediante l'impiego del telefono e della posta cartacea per le finalità di cui all'articolo 7, comma 4, lettera b), è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario e degli altri dati personali di cui all'articolo 129, comma 1, in un registro pubblico delle opposizioni.

Consentire l'uso del telefono e della posta cartacea ove non vi sia la dichiarazione di opposizione dell'interessato al trattamento dei propri dati formalizzata nel pubblico registro delle opposizioni significa di fatto permettere quello 'scempio' che il legislatore - coerentemente allo spirito del Codice privacy del 2003 e della Convenzione di Strasburgo n. 108 del 1981 - voleva evitare e che aveva già subito un primo affronto normativo con la modifica dell'art 130, comma 3-*bis*, inserito dall'art. 20-*bis* della legge 166/2009, di conversione del D.L. n. 135/2009, che aveva introdotto il **cosiddetto** regime dell'*opt-out* per le chiamate telefoniche a fini commerciali esteso anche alle promozioni con l'invio della posta cartacea.

Al lettore quindi consigliamo allora l'iscrizione al pubblico Registro delle opposizioni al seguente link: <http://www.registrodelleopposizioni.it/>.

Sicuramente le comunicazioni commerciali avranno maggiore possibilità di raggiungere il cittadino a cui i dati personali si riferiscono, lasciando comunque indenne chi le invia anche perché il cittadino - nella maggioranza dei casi - non sa come tutelarsi e, spesso, non ha le conoscenze informatiche per farlo autonomamente.

Ulteriori novità erano poi sono contenute nella bozza del decreto sviluppo

pubblicata anche *on line*, nella sua versione del 18 ottobre scorso che postulava le sottoindicate modifiche che segnaliamo in quanto appare probabile troveranno ingresso in un prossimo immediato futuro:

Ecco le modifiche predicate:

- verrebbe sostituita la dizione dell'art. 4, primo comma, sub lettera b) del Codice sulla nozione di dato personale che risulta essere:

b) 'dato personale', qualunque informazione relativa a persona fisica, nonché, limitatamente al settore delle comunicazioni elettroniche, qualunque informazione relativa a persona giuridica, ente od associazione abbonati ad un servizio di comunicazione elettronica accessibile al pubblico, sempre che si tratti di soggetti identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

- il citato articolo verrebbe poi modificato alla lettera i):

i) le parole «la persona giuridica, l'ente o l'associazione» sono soppresse e sono aggiunte, in fine le seguenti: «nonché la persona giuridica, l'ente o l'associazione abbonati ad un servizio di comunicazione elettronica accessibile al pubblico, limitatamente al trattamento dei dati personali nel settore delle comunicazioni elettroniche».

- verrebbe abrogato il primo comma, sub lettera g) sull'obbligo di tenere un aggiornato documento programmatico sulla sicurezza ed altresì muta il comma 1-*bis* recentemente aggiunto dal D.L. 70/2010. Riportiamo per intero (onde evitare fraintendimenti) il nuovo testo dell'art. 34 (**in corsivo il testo che si voleva introdurre ed in corsivo sottolineato il testo che si sarebbe dovuto abrogare**):

Art. 34. Trattamenti con strumenti elettronici 1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli

incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; ***[g] tenuta di un aggiornato documento programmatico sulla sicurezza;*** h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari. 1-bis.⁽¹⁾ *Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita 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 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B). In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrativo-contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentiti il Ministro per la semplificazione normativa e il Ministro per la pubblica amministrazione e l'innovazione, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico contenuto nel citato allegato B) in ordine all'adozione delle misure minime di cui al comma 1.*

- all'art. 43, sub lettera h), dopo la parola 'dati' verrebbe inserito il seguente testo (**in corsivo la modifica**):

h) il trattamento concerne dati personali trattati nel settore delle comunicazioni elettroniche riguardanti persone giuridiche, enti o associazioni abbonati ad un servizio di comunicazione elettronica accessibile al pubblico.

- ulteriore modificazione si sarebbe voluta inserire relativamente al testo dell'art. 26, sub lettera d) del quarto comma (**in corsivo le modificazioni postulate**):

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento, da contratti collettivi o dalla normativa comunitaria

per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

Qualche riflessione sulle modifiche che il legislatore avrebbe voluto introdurre.

La prima è che il legislatore sembra volersi/doversi piegare alle esigenze 'operative' delle grandi società ed imprese alle quali le norme sulla tutela della riservatezza nel trattamento di dati personali erano da subito sembrate eccessive e - nel tempo - sempre più gravemente sanzionate sia da un punto di vista amministrativo che penale. Abrogare la norma che impone la tenuta di un aggiornato documento programmatico costituisce da sempre, per tutte le categorie produttive, un adempimento da cancellare dal tessuto normativo.

L'aggiornamento del DPS va, per converso, invece considerato una delle condizioni cardine di un costante monitoraggio della correttezza dei trattamenti effettuati dal titolare. *Quid iuris* allora delle attività previste del punto 19 dell'allegato B) al Codice Privacy?

Si potrebbero allora *scolorare*, nel mancato 'aggiornamento' del DPS, le tutele accordate agli interessati al trattamento? *Quid iuris* poi nelle more del provvedimento di individuazione delle modalità semplificate di applicazione del disciplinare tecnico contenuto nel citato allegato B) in ordine all'adozione delle misure minime, così come recita l'ultima parte dell'art. 34 *sub* comma 1-*bis*?

A questo punto riteniamo che l'intero Codice andrebbe *realmente semplificato* rivisitando l'intera materia recata dal D.Lgs. 193/2003 e dalle successive modifiche; ciò alla luce di un misurato compendio degli interessi di tutti gli 'attori' che intorno alla tutela dei dati personali si muovono, mitigando la rigidità della norma adattandola alle contrapposte esigenze degli operatori. Una rivisitazione coordinata insomma in ordine anche alla considerazione che non si possa continuare a procedere con interventi *spot* a seconda delle pressioni esercitate dalle grandi società che operano nel settore delle tele-

comunicazioni, del telemarketing, del commercio dei beni e servizi, dalle associazioni di categoria.

Cartina al tornasole di questo ondeggiare del legislatore sono, tra le altre, le regole sull'*opt-in* e sull'*opt-out* che introducono macchinosi sistemi di tutela nelle comunicazioni come quello del *Registro delle opposizioni*: **'non** vuoi ricevere comunicazioni opponiti **on line'**.

Già ci sembra di vedere che l'*interessato* - che fa fatica ad arrivare a fine mese - si diletti in rete con l'anzidetto registro.

La semplificazione, a nostro avviso, dovrebbe partire dalla rivisitazione di quella semplice, chiara e diretta dizione contenuta nella Convenzione di Strasburgo del 1981 sulla *Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale* che, *in nuce*, conteneva tutte le tutele necessarie alla riservatezza ed era priva di quei minuziosi, dettagliati e spesso contraddittori precetti difficili da coordinare e da comprendere in specie a causa della disordinata stratificazione normativa.

In difetto ogni semplificazione risulterà essere solo una pericolosa e compiacente complicanza.

LINK DI APPROFONDIMENTO

Confindustria: Privacy: le novità del decreto sviluppo

http://search.confindustria.it/search?q=decreto+sviluppo&btnG=Cerca+con+Google&access=p&entqr=0&output=xml_no_dtd&sort=date%3AD%3AL%3Ad1&client=default_frontend&ud=1&oe=UTF-8&ie=UTF-8&proxystylesheet=default_frontend&site=default_collection

Sito del Registro delle opposizioni

<http://www.registrodelleopposizioni.it/>

La bozza del testo del nuovo decreto sviluppo

http://www.leggioggi.it/wp-content/uploads/2011/10/decreto_sviluppo_completo_bozza_18_ottobre.pdf

L'APPLICAZIONE DEL D.LGS. 196/2003 NEGLI STUDI PROFESSIONALI ALLA LUCE DEL COMUNICATO DELL'AGENZIA DELLE ENTRATE DEL 3.8.2011 'VIGILANZA SUGLI INTERMEDIARI ENTRATEL'

STEFANO CORSINI

Il presente contributo vuole rappresentare uno strumento di supporto per tutti quei professionisti che, a distanza di oltre sette anni dall'entrata in vigore del D.Lgs. 196/2003 *Codice in materia di protezione dei dati personali*, ancora non sanno quali sono gli adempimenti davvero necessari per la propria attività e quali sono gli aspetti rilevanti che in sede ispettiva vengono analizzati.

L'applicazione del D.Lgs. 196/2003 *Codice in materia di protezione dei dati personali* negli studi professionali è un argomento su cui si è già a lungo dibattuto. È pacifico oramai che, alla pari di ogni titolare di trattamento di dati, anche i commercialisti devono adempiere ai precetti della norma ponendo in essere tutta una serie di misure, sia fisiche che organizzative, volte a tutelare la riservatezza degli interessati (clienti, dipendenti, fornitori di beni e servizi).

Particolare preoccupazione ha destato nei professionisti commercialisti, la Circolare dell'Agenzia delle Entrate del 3 agosto 2011 ove l'Ente annunciava per il secondo semestre del corrente anno l'inizio di nuovi controlli per la verifica del rispetto del Codice Privacy da parte di tutti i soggetti, persone fisiche o giuridiche, intermediari abilitati alla trasmissione delle dichiarazioni attraverso il Canale Entratel dell'Agenzia medesima.

L'iniziativa dell'Agenzia delle Entrate trae fondamento da quanto previsto dall'art. 11 del decreto del 31 luglio 1998 e dall'art. 5 del provvedimento del Direttore dell'Agenzia delle Entrate del 10 giugno 2009. Esiste anche un provvedimento specifico del Garante Privacy del 18 settembre 2008 (*doc. web n. 1549548*) che ha rintuzzato gli obblighi di vigilanza, ma sarà sufficiente analizzare i due provvedimenti su menzionati.

Il primo prevede che gli utenti (tra cui CAF e professionisti iscritti ad albi) possono trattare i dati contenuti nelle dichiarazioni per le sole finalità del servizio di trasmissione telematica e per il tempo a ciò necessario. Costoro si configurano quali autonomi titolari del trattamento dei dati personali e il trattamento dei dati personali contenuti nelle dichiarazioni è consentito solo ai soggetti individuati e nominati quali responsabili o incaricati del trattamento. In particolare, inoltre, è previsto che tali utenti, oltre a fornire apposite istruzioni ai soggetti come sopra individuati, si impegnino altresì a mantenere riservate le informazioni che consentono l'accesso al servizio telematico, adottando procedure per la consegna e la custodia di tali informazioni (codici, password, ecc.). Profetico, infine, è il comma 7, che testualmente recita «l'Amministrazione finanziaria verifica periodicamente, anche con controlli a campione, il rispetto delle disposizioni contenute nel presente articolo».

Il secondo provvedimento ricalca il primo, quasi a voler rimarcare l'importanza della riservatezza durante l'attività di trasmissione e conservazione delle dichiarazioni.

Oggetto dell'attività di verifica, secondo la circolare di agosto, saranno:

1) La struttura organizzativa dell'intermediario/titolare del trattamento.

Sarà verificata l'eventuale designazione, da parte del titolare del trattamento dei dati (CAF o altro intermediario abilitato al Servizio Entratel), dei *responsabili* (anche esterni) del trattamento dei dati e la redazione di istruzioni operative riservate agli stessi. Solitamente si rinviene la necessità di attribuire la qualifica di responsabile del trattamento, ai sensi dell'art. 29 del D.Lgs. 196/2003, a quelle società, **cd.** 'di elaborazione dati', che svolgono la strumentale attività di elaborazione dati fiscali e contabili per conto terzi e di cui da anni migliaia di studi si avvalgono. Quasi sempre, poi, tali società condividono la sede con i professionisti, risultando altresì proprietarie di tutti i beni (compresi computer e software) nonché titolari del rapporto di lavoro con i soggetti che materialmente trattano dati per conto del professionista abilitato Entratel.

Tale situazione crea una promiscuità di informazioni che spesso risulta difficile mappare e gestire da un punto di vista della 'privacy dello studio', sic-

ché è indispensabile procedere alla corretta individuazione e designazione di tutti i soggetti a vario titolo coinvolti nel trattamento dei dati e nell'utilizzo delle credenziali di accesso ai canali telematici.

2) L'esistenza del documento programmatico per la sicurezza (di seguito DPS) previsto dall'art. 34, comma 1, lett. g) del D.Lgs. 196/2003 e dalle disposizioni contenute nel suo allegato **B**), regola 19.

In attesa di conoscere quale sarà la sorte del DPS, attesa la paventata riforma del Codice Privacy che vorrebbe abolirlo, è opportuno continuare a tenere un aggiornato documento che riporti e descriva tutti gli elementi previsti ex lege (elenco dei trattamenti di dati, ruoli, compiti, responsabilità, misure minime di sicurezza, formazione, ecc.). Si ricorda che i commercialisti, così come gli avvocati, considerata la peculiare attività e la varietà di informazioni di cui dispongono, non possono beneficiare delle semplificazioni recentemente introdotte (art. 34, comma 1-bis: autocertificazione al posto del DPS).

3) La designazione degli incaricati per il trattamento dei dati e l'attribuzione dell'ambito di trattamento consentito.

Come sopra ricordato, i soggetti che trattano dati o dispongono di codici di accesso per conto del titolare (o del responsabile se sono dipendenti delle società di elaborazione dati) devono essere formalmente incaricati ai sensi dell'art. 30 del D.Lgs. n. 196 del 2003 e art. 11, comma 4 del decreto 31 luglio 1998. È consigliato specificare nell'atto di nomina quali sono le responsabilità connesse alla condivisione o comunicazione a persone non legittimate dei dati acquisiti nello svolgimento delle proprie funzioni, calcando la mano sulle procedure di conservazione dei documenti e delle credenziali di accesso ai canali telematici.

4) L'adozione di una procedura di controllo del rispetto delle misure di sicurezza e dell'adempimento degli obblighi previsti dal D.Lgs. n. 196 del 2003. Tale previsione della circolare in questione appare poco chiara, dal momento che l'obbligatoria tenuta di un aggiornato Documento Programmatico sulla Sicurezza risponde già alle esigenze dettate dal presente punto 4).

5) *L'adozione di una corretta politica di gestione delle password*, che preveda l'attribuzione a uno o più soggetti specifici dell'incarico di amministrare le utenze per l'accesso ai sistemi informatici, l'utilizzo di credenziali di accesso nominative e note solo all'utente responsabile della loro conservazione, l'indicazione da parte dell'intermediario ai propri collaboratori dei criteri che le password utilizzate devono rispettare, secondo quanto previsto dall'allegato **B**), regola 5, del D.Lgs. n. 196 del 2003, del corretto uso delle stesse nonché delle responsabilità derivanti dalla loro eventuale condivisione, l'adozione di misure volte a mantenere riservate le informazioni che consentono l'accesso ai servizi telematici.

Detto aspetto descrive quanto già dovrebbe essere in atto nello studio del professionista 'virtuoso', dal momento che l'allegato **B**) del D.Lgs. n. 196 del 2003 e l'art. 5, comma 6 del provvedimento 10 giugno 2009 già prevedono quanto sopra. In ogni caso ciò richiede a tutti gli operatori una rinfrescata delle proprie misure minime di sicurezza, considerato che nel corso di tutti i miei *audit* presso aziende e studi professionali a partire dal 2004 ho sempre rilevato una atavica recalcitranza alla sostituzione delle password secondo le tempistiche di legge (3 mesi se si trattano dati sensibili) e con le caratteristiche richieste (senza riferimenti agevolmente riconducibili all'incaricato). È indispensabile che il titolare del trattamento, se vuole essere certo dell'applicazione di tale misura, si assuma tale onere in prima persona senza sperare di affidarlo al collaboratore e potersene dimenticare. Diversamente dovrà delegare tale responsabilità ad un soggetto qualificato (tecnico informatico o consulente privacy).

6) *La previsione, nel ciclo di vita delle credenziali*, di procedure per garantire la costante aderenza tra i privilegi di accesso ai dati e il ruolo organizzativo del personale che vi accede (art. 34 del D.Lgs. n. 196 del 2003).

L'ente ha qui voluto ricordare che l'aggiornamento periodico dell'ambito di trattamento consentito all'incaricato deve essere verificato e aggiornato con cadenza periodica (almeno annuale) oppure ad ogni effettivo cambiamento di mansioni. Mutando le mansioni assegnate possono cambiare le informazioni a cui si ha accesso, compresi i codici di accesso ai Pc e alle

piattaforme telematiche rese disponibili dagli enti pubblici (INAIL, INPS, Adeline, Entratel, ecc.).

7) *La designazione, come responsabili del trattamento, delle società esterne* diverse dalle società di servizi di cui l'intermediario si avvalga per operazioni meramente strumentali all'esercizio dell'assistenza fiscale (ad esempio quelle di natura tecnica quali il ripristino di un server o la sostituzione di un supporto hardware), qualora lo svolgimento di tali operazioni implichi il possibile trattamento di dati nonché l'adozione di procedure volte a garantire la riservatezza dei dati e/o di clausole contrattuali che prevedano la salvaguardia della riservatezza delle informazioni.

Se non è una ripetizione, ciò consiste nella specificazione di quanto illustrato al punto 1), con la differenza che il responsabile in questo caso deve essere necessariamente esterno.

8) *Misure di sicurezza relative ai supporti tecnologici utilizzati.*

Al riguardo sarà verificata l'adozione di misure di protezione delle postazioni di lavoro, dei server e dell'infrastruttura di rete, conformi alle disposizioni contenute nell'allegato **B)** del D.Lgs. n. 196 del 2003. In particolare, sarà riscontrata la sussistenza delle seguenti condizioni:

- configurazione delle stazioni di lavoro che preveda il blocco automatico delle stesse dopo un certo tempo di inattività dell'operatore (screensaver con password per il ripristino);
- installazione di programmi di protezione per le stazioni di lavoro e server al fine di mitigare i rischi di accesso ai dati o la loro manomissione (soprattutto antivirus e firewall, ma anche applicazioni *antimalware*);
- aggiornamento periodico del sistema operativo e del software di protezione (quasi sempre tali strumenti hanno impostato l'aggiornamento automatico ad ogni *release* della *software house*);
- in caso di utilizzo di reti senza fili (*wireless*), adozione di protocolli di sicurezza idonei a limitare il rischio che le trasmissioni dati siano intercettabili da parte di soggetti esterni non autorizzati (poiché le chiavi di accesso alla connessione wi-fi del router sono preimpostate ed astratta-

mente rilevabili tramite appositi strumenti, l'ente qui consiglia di fatto di sostituirle con altre scelte dal titolare).

- 9) Ulteriori misure di sicurezza. La Circolare prevede il controllo circa:
- a) La conservazione delle dichiarazioni e della relativa documentazione separatamente dai documenti acquisiti dall'intermediario per altre attività dallo stesso svolte (allegato **B**) del D.Lgs. n. 196 del 2003). Appare, a mio avviso, di difficile realizzazione tale intento, considerato che all'interno di un fascicolo i documenti contengono sia dati personali che dati sensibili e comunque, anche qualora fosse possibile separarli, a mio parere si rischia di dover stravolgere l'ordine logico del fascicolo. Solitamente ogni pratica ha una sua 'cronologia', con gli atti e i documenti fascicolati secondo un ordine temporale. Separarli potrebbe pregiudicare tale metodo di gestione documentale cartacea. Inoltre si ritiene che per le dichiarazioni, essendo le stesse dei dati sensibili, non ha senso separarle dai documenti che concorrono alla loro elaborazione, ma piuttosto conviene considerare l'intero fascicolo quale dato sensibile.
 - b) La conservazione separata dei documenti contenenti dati sensibili dal resto della documentazione archiviata (art. 22, commi 6 e 7 del D.Lgs. n. 196 del 2003).

Riporto testualmente il comma 6 per sottolineare la sua oggettiva difficoltà applicativa: «I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, *tenuti con l'ausilio di strumenti elettronici*, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità». Dal tenore della norma sembrerebbe necessario criptare i dati sensibili o filtrare l'accesso con altre non meglio specificate soluzioni.

In ogni caso, stando a quanto annunciato, sarà bene per tutti gli intermediari valutare l'ipotesi, ove possibile, di conservare i documenti di cui alle lett. a) e b) secondo le modalità ivi stabilite.

10) *Presenza di spazi idonei ed accessibili esclusivamente a personale autorizzato* per la conservazione dei documenti relativi all'attività di trasmissione delle dichiarazioni fiscali e dei supporti contenenti il *backup* dei dati stessi (allegato **B**) del D.Lgs. n. 196 del 2003).

Questa regola è il 'distillato' del Codice Privacy: bisogna evitare situazioni di promiscuità con soggetto terzi o anche con soggetti incaricati ma privi della necessaria autorizzazione per accedere a tali informazioni. Talvolta negli studi che visito mi capita di rilevare che l'archivio, storico o corrente, si trova nei pressi della sala d'aspetto dei clienti, così come il fax. Ciò può essere dettato da esigenze contingenti di spazio, tuttavia la norma e gli ispettori non vedono di buon occhio tale scelta, che in ogni caso sarà difficile da giustificare in sede di ispezione.

11) *Esistenza, nei casi in cui l'attività di assistenza/trasmisione non si risolve in un'opera pressoché personale del soggetto abilitato*, ma si dispieghi, piuttosto, in base ad un'articolata struttura organizzativa, di procedure per l'accesso e la gestione degli archivi (allegato **B**) del D.Lgs. n. 196 del 2003).

Secondo l'intento della circolare i soggetti, diversi dall'intermediario, che hanno accesso agli archivi cartacei devono essere controllati o, quantomeno, tutti gli accessi vanno mappati. A parere dello scrivente questa misura può essere garantita solo attraverso la predisposizione di archivi *ad hoc* e la loro sorveglianza diretta da parte del titolare, del responsabile o degli incaricati stessi. Se poi l'archivio cartaceo è quello delle pratiche evase, che di solito si trova in una stanza apposita nel seminterrato della **sede dello studio**, il controllo potrà avvenire prevedendo la custodia delle chiavi in capo al titolare o soggetto di fiducia e la consegna *brevi manu* agli incaricati ad ogni evenienza.

Per gli archivi elettronici, vale quanto scritto sopra relativamente al controllo degli accessi, ai profili di autorizzazione, all'aggiornamento dell'ambito di trattamento consentito agli incaricati.

12) *Conservazione della documentazione fiscale* secondo le modalità e per il periodo previsti dalle vigenti disposizioni (art. 11 decreto 31 luglio 1998, art. 5 del provvedimento 10 giugno 2009, art. 11 del D.Lgs. n. 196 del 2003).

I tempi di conservazione sono quelli dell'art. 43 del D.P.R. 600/1973 (31 dicembre del quinto anno successivo a quello in cui è stata presentata la dichiarazione o 31 dicembre del sesto anno successivo a quello in cui la dichiarazione avrebbe dovuto essere presentata) e delle altre norme di settore vigenti ed applicabili, mentre per quanto riguarda le modalità i dati personali oggetto di trattamento devono essere:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. Inoltre i danni per scorretto trattamento causati con violazione dell'art. 11 D.Lgs. 196/2003 possono comportare il risarcimento dei danni non patrimoniali.

Nonostante tutto ciò non rappresenti una novità, visto che il decreto ministeriale di riferimento risale all'anno 1998, è davvero opportuno non sottovalutare il contenuto della circolare, considerato che, se l'esito dei controlli porta a rilevare una o più infrazioni, la conseguenza è la possibile revoca dell'abilitazione al canale Entratel, che per molti, se non per tutti, vorrebbe dire interrompere una consistente percentuale della propria attività. La circolare, in verità, fa riferimento ai soggetti abilitati Entratel, ma alla luce delle possibili conseguenze non conviene limitare la propria attenzione solo a tale ambito.

Le sanzioni privacy per le violazioni amministrative e gli illeciti penali attualmente in vigore

Disposizioni in materia di tutela della riservatezza (D.Lgs. 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 'tre mila euro-dieciottomila 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 è sanzionata da ventimila euro a centoventimila euro (articolo 163);
- più che raddoppiata invece è la sanzione per omessa informazione o esibizione al cioè 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».*

Riteniamo in merito alle sanzioni, non ci sia bisogno di molti commenti se non quello che esprime il disagio che le diverse categorie professionali ed economiche provano nel gestire gli adempimenti di un apparato normativo complesso, rigido e veramente severo.

SEMPLIFICAZIONI PRIVACY: AUTOCERTIFICAZIONE DEL DPS E MISURE MINIME 'ALLEGGERITE' ALLA LUCE DELLE MODIFICHE LEGISLATIVE AL CODICE PRIVACY 2011

PAOLO VICENZOTTO

In tema di semplificazioni in materia di privacy, il recente articolo 6, comma 2, lettera b), numero 5), del D.L. 13 maggio 2011, n. 70 ha sostituito e aggiornato l'art. 34 1 bis del D.Lgs. 196/2003 *Codice in materia di protezione dei dati personali* ed ha introdotto il successivo comma 1 ter.

Questo provvedimento completa e migliora il progetto di semplificazione degli adempimenti previsti dal D.Lgs. 196/2003 per le imprese, già introdotti con il decreto del 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133, e dal 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. 196/2003 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 provvedimenti di semplificazione citati, sono state apportate rilevanti modifiche.

Il documento programmatico sulla sicurezza e l'autocertificazione

L'art. 34 comma 1 bis del D.Lgs. 196/2003 prevede la possibilità di sostituire

il DPS con un'autocertificazione (*rectius*: dichiarazione sostitutiva dell'atto di notorietà) per tutti quei soggetti che:

- trattano soltanto dati personali non sensibili e trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti;
- trattano dati personali per correnti finalità amministrativo-contabili.

Pertanto chi si trovi in una di queste condizioni, e cioè quasi tutte le aziende 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. 196/2003, potrà predisporre un'autocertificazione con cui si attesta, in primo luogo, di trovarsi in una delle due condizioni sopra citate e quindi di trattare tali dati «in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato **B)**».

Il legislatore, nel 2011 ha altresì introdotto il comma 1 ter, che specifica in modo esplicito cosa si intenda per trattamenti con 'finalità amministrativo-contabili'. In tal modo sembrano chiariti - ma non certo in modo definitivo - alcuni dubbi interpretativi sorti con la riforma del 2008:

ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale - assistenziale, di salute, igiene e sicurezza sul lavoro.

Ritengo infine *che gli studi professionali di avvocati e commercialisti non rientrano* fra i soggetti che possono avvantaggiarsi delle semplificazioni di cui all'art. 34 comma 1 bis e 1 ter del D.Lgs. 196/2003. Essi dovranno continuare ad adottare le misure minime di sicurezza e a redigere annualmente il Documento programmatico sulla sicurezza.

Le misure minime di sicurezza semplificate

Chi si trova nelle condizioni di poter autocertificare il DPS, di fatto potrà avvalersi delle misure semplificate emanate dal Garante per la protezione dei dati personali a norma dell'ultima parte dell'art. 34 comma 1 bis. Il provvedimento di riferimento è 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*.

Le semplificazioni introdotte dal Garante 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 il provvedimento prevede la possibilità di redigere un DPS semplificato. Non si capisce la *ratio* di tale misura, visto che per i soggetti che potrebbero avvantaggiarsene, già esiste la possibilità di sostituire il DPS stesso con l'autocertificazione.

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. A mio parere, infine, anche chi può usufruire dei provvedimenti di semplificazione dovrà invece adottare le misure di sicurezza imposte dal Garante con provvedimenti di carattere generale ai sensi dell'art. 154 del D.Lgs. 196/2003, come ad esempio il provvedimento sulla videosorveglianza (*8 aprile 2010 in Gazzetta Ufficiale n. 99 del 29 aprile 2010*) e sull'uso di mail e Internet nei luoghi di lavoro (*Linee guida del Garante per posta elettronica e internet - Gazzetta Ufficiale n. 58 del 10 marzo 2007*). In caso di semplificazione, invece, è esclusa l'applicazione del provvedimento sugli amministratori di sistema *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 - G.U. n. 300 del 24 dicembre 2008*.

LA SICUREZZA DEI DATI PERSONALI IN DUE PROVVEDIMENTI DEL GARANTE

LUCA ZENAROLLA

Le semplificazioni pur con i limiti e i problemi interpretativi che i miei colleghi evidenziano nei loro contributi, non devono 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 (Raee) 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 (Raee) 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 regi-

strati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un **cosiddetto** 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 seconda delle prestazioni del computer utilizzato.

In alternativa si può puntare sulla formattazione 'a basso livello' degli hard disk (la **cosiddetta** 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 seconda del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.

Il provvedimento del Garante Privacy sugli amministratori di sistema alla luce delle modifiche introdotte dalla legge 12 luglio 2011, n. 106

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 previgente 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».

Questo non vuol dire, però, che chiunque utilizzi strumenti elettronici per trattare dati personali si serva dell'opera di un vero e proprio 'amministratore di sistema'. Numerose sono le realtà in cui le operazioni che il Garante definisce 'tipiche' dell'amministratore sono in realtà svolte da incaricati del trattamento o dal titolare stesso oppure da tecnici informatici che solo occasionalmente intervengono (per esempio, per manutenzioni a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi *software*.

Le singole misure previste dal Provvedimento

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 1° marzo 2007 (in Gazzetta Ufficiale 10 marzo 2007, n. 58);
- mediante altri strumenti di comunicazione interna (ad esempio, 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 sufficiente 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 delle attività di tutti gli incaricati, ma solo 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 richieste. 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. A questo proposito si segnala che lo stesso Garante ha precisato che «caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e 'certificati'».

Le modifiche della legge 12 luglio 2011, n. 106

Il D.L. 13 maggio 2011, n. 79, convertito con modifiche dalla legge 12 luglio 2011, n. 106, ha modificato, tra l'altro, il disposto dell'articolo 34 del D.Lgs. 196/2003. Nello specifico ha introdotto il comma 1-ter che definisce il concetto di 'finalità amministrativo-contabili' su cui tanto si era discusso in dottrina.

Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della con-

tabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

Alla luce di questo intervento, quindi, si può capire come rientrano in questa definizione anche alcune particolari attività di trattamento effettuate in ambito lavorativo e che, prima di luglio, si pensava non potessero essere incluse in questa tipologia di finalità. Si pensi, ad esempio, alle attività di controllo sul regolare funzionamento del sistema informatico aziendale, che possono comportare il trattamento di dati anche sensibili del singolo lavoratore e che, prudenzialmente, si riteneva non potessero rientrare nel novero dei trattamenti effettuati per finalità amministrativo-contabili. La novella di luglio, quindi, finisce per ampliare in modo sensibile l'ambito di applicazione delle misure di semplificazione introdotte dal Legislatore a partire dal 2008 e che, sino a questo intervento, erano rimaste sostanzialmente inapplicate.

Le conseguenze sull'applicazione del Provvedimento in tema di AdS

Questa modifica ha, poi, un'importante conseguenza in relazione all'ambito di applicabilità del Provvedimento sugli Amministratori di Sistema: è lo stesso provvedimento a stabilire espressamente che «i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 **D.L.** 25 giugno 2008, n. 112, conv., con mod., con **legge** 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento».

La nuova formulazione dell'articolo 34, con l'interpretazione estensiva del concetto di 'finalità amministrativo-contabili', comporta, quindi, come conseguenza, l'aumento dei titolari esonerati dal rispetto del Provvedimento del 27 novembre 2008.

Dichiarazione sostitutiva dell'atto di notorietà

(Ai sensi dell'art. 34, co. 1-bis, D.Lgs. n. 196/2003, e dell'art. 47, D.P.R. 28 dicembre 2000, n. 445)

Il/La sottoscritto/a _____ (cognome e nome)
nato/a a _____ (_____) il _____ (luogo, data)
residente a _____ (_____) in via _____ n. _____
(indirizzo), in qualità di legale rappresentante *pro tempore* (amministratore
delegato/presidente del consiglio di amministrazione) della società
' _____ ' con
sede in _____, Via _____, n. _____, quale
Titolare del Trattamento ai sensi e per gli effetti di cui all' art. 4, co. 1, lett. f) del D.Lgs.
n. 196/2003 - cd.'Codice privacy';

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

DICHIARA

di trattare soltanto dati personali non sensibili e come unici dati sensibili e giudiziari
quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi
quelli relativi al coniuge e ai parenti, in osservanza delle misure minime di sicurezza
previste dal Codice privacy e dal Disciplinare tecnico di cui all'allegato B) al Codice.
La presente dichiarazione sostitutiva dell'obbligo di tenuta di un aggiornato
Documento Programmatico sulla Sicurezza è resa ai sensi e per gli effetti di cui all'art.
34, co. 1-bis, Codice privacy.

_____ (luogo, data)

Il dichiarante

Si allega: 1) Copia del documento di identità.

Note a commento

1. La redazione dell'autocertificazione, come documento sostitutivo del D.P.S., 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 così come modificato dal D.L. 70/2010.

2. Ricordiamo che se un'impresa o un professionista effettua un trattamento che non ricade nei requisiti di cui all'art. 34 bis D.Lgs. 196/2003 (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 una l'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 difensiva 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 dall'art. 34 (comma 1.bis) 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. 196/2003 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 le 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. 196/2003, 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. 318/1999**). Ora art. 35, comma 1, sub lettera c) ed allegato **B**) al **D.Lgs. 196/2003**.

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. *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 conservati su supporto magnetico 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. 196/2003**, di trasmettere i dati personali raccolti da un soggetto, previo il suo consenso e fatte salve le previste esclusioni dello stesso, ad altri soggetti per previste ed individuate finalità.

CONTROLLO DEL TRATTAMENTO. Attività e procedure organizzative, fisiche e logiche messe in essere - secondo le previsioni dell'allegato B) al **D.Lgs.** 196/2003 - da un operatore al fine di proteggere i dati personali ed il loro trattamento dai rischi di distruzione e di perdita ed altresì onde non consentire un accesso ai dati da parte di terzi non autorizzati.

CREDENZIALI DI AUTENTICAZIONE. Ex num. 2 dell'allegato B) del **D.Lgs.** 196/2003: 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.** 196/2003: è il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

DATI 'SENSIBILE'. Ex art. 4, primo comma, sub lettera d) del **D.Lgs.** 196/2003: 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.** 196/2003: 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. 196/2003** che consiste nel dare conoscenza dei dati personali a soggetti indeterminati 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 informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del citato testo unico.

ELABORATORE. (G. Fiorentino, *Enciclopedia dell'informatica*, 1979, **p. 125**): «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» (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. 196/2003**, degli scopi per i quali il trattamento dei dati viene effettuato dal titolare o dal responsabile del trattamento.

FIRME CON DISPOSITIVI DIGITALI. Ex art. 1 (definizioni) del D.Lgs. 82/2005 come novellato dal D.Lgs. 235/2010 sub lettera q) e seguenti:

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

q-bis) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firma-

tario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

r) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

FIREWALL. Sistema *hardware* e *software* che - inserito fra la rete Internet e la rete interna di un ente o di un'impresa - individua e controlla il traffico dei singoli pacchetti TCP/IP facendo transitare solo i pacchetti 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 **legge** 675/96, che come riaffermato dall'art. 153 del **D.Lgs.** 196/2003, ha come compito la protezione dei dati personali ed alla quale è attribuita - ex art. 154 - una 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 **cosiddetta** parte 'rigida' dell'elaboratore e delle varie sue periferiche (esempio: 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.** 196/2003: 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. 196/2003** (già art. 1, comma 1, lettera f), della **legge 675/1996**): è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati.

INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (ITSEC). 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 (CO) - nessuna sicurezza, a C sei (C6) - massima sicurezza.

MISURE MINIME DI SICUREZZA. Ex art. 33 e segg. ed ex allegato B), del **D.Lgs. 196/2003**: 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 art. 37 e 38 del **D.Lgs. 196/2003** 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 (v. allegato **B**) del **D.Lgs. 196/2003**).

PREPOSTO ALLE PAROLE CHIAVE ED/OD AI CODICI IDENTIFICATI PERSONALI. Ex allegato B) del **D.Lgs. 196/2003**: 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 DPR 428/98 reiterato nel DPR 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.** 196/2003 (già art. 1, comma 1, lettera e), della **legge** 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 fornita da un apposito sistema informatico di riottenere immediatamente l'accesso ad informazioni elaborate elettronicamente dopo che le stesse sono state perse 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.** 196/2003 dall'art. 161 al 172 (nella disciplina previgente dal Capo VIII della legge 675/**1996**).

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*; le ulteriori norme introdotte dall'art. 6 del decreto legge 70 **del** 2010 convertito con la legge n. 106 il 12 luglio 2011.

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.** 196/2003: 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): 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.** 196/2003: è qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

WEB AZIENDALE. Rete di comunicazione elettronica all'interno di una azienda che, attraverso cavi, raggi infrarosso od altri sistemi di connessione, permette a più elaboratori e/o terminali di trasferire e condividere informazioni e dati.

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 2010*.

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 2011

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* 2010.