di Manlio Cammarata

L'ordinamento giuridico di fronte ai problemi delle tecnologie

Virus e protezione dei dati certezza tecnica o legale?

La trasmissione di virus informatici è un reato previsto e punito dal codice penale. Ma anche l'utente ha il dovere di proteggere i suoi dati. Vediamo che cosa dice la legge e che cosa dovrebbe dire il regolamento sulla sicurezza dei dati personali, che dovrebbe essere emanato tra poco tempo

Mandare in giro un virus è un reato, ma presto lo sarà anche riceverlo. La prima norma è contenuta nel codice penale, la seconda deriva, indirettamente, dalla legge n. 675 del 31 dicembre 1996 sulla protezione dei dati personali.

Leggiamo, prima di tutto, l'articolo 615-*quinquies* del codice penale:

(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) - "Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni".

L'articolo è stato inserito nel codice dalla legge 23 dicembre 1993, n. 547, la cosiddetta "legge sul crimine informatico" e al suo primo apparire ha suscitato allarme tra i tecnici, spesso poco esperti di questioni legali. Infatti la prima lettura del testo fa supporre, a chi non conosca i principi del diritto penale, che il fatto di consegnare a qualcuno, senza saperlo, un dischetto contenente un virus possa far rischiare carcere e multa. Non è così perché, se la norma specifica non dispone altrimenti, l'ipotesi penale si verifica solo in presenza di "dolo", cioè dell'intenzione di produrre un determinato effetto. E' il caso dei "delitti colposi", cioè di quei delitti (come l'omicidio) che sono tali anche se l'autore non aveva l'intenzione di commetterli. Invece nell'articolo 615-*quinquies* non c'è alcuna previsione di colpa e quindi il reato si verifica solo se c'è l'intenzione di commetterlo. Si aggiunga che l'intenzionalità del comportamento, cioè il dolo, deve essere provata dall'accusa.

Il discorso è diverso se dal piano penale ci spostiamo su quello civile. Un soggetto che subisca gravi danni da un virus trovato su un dischetto o ricevuto per via telematica, può chiedere il risarcimento a chi glie lo ha involontariamente consegnato o inviato? La questione è complessa, perché il danneggiato deve dimostrare - oltre all'effettiva esistenza del danno - che la controparte non ha usato la necessaria diligenza per evitare il verificarsi dell'evento dannoso, ma quest'ultima potrebbe facilmente rovesciare l'accusa sulla prima, per non aver verificato il file prima di installarlo o aprirlo. Un'ulteriore complicazione potrebbe nascere a proposito di quale livello di diligenza sia applicabile per evitare questo tipo di danneggiamento: se quella ordinaria o "del buon padre di famiglia" o quella speciale da "valutarsi con riguardo alla natura dell'attività esercitata" nel caso di attività professionali, come prescrive il secondo comma dell'articolo 1176 del codice civile.

Infine è necessario considerare con attenzione un aspetto importante dell'articolo 615-*quinquies*: la norma non parla espressamente di virus, ma di un "programma avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico" eccetera. Cioè include anche i programmi che non rientrano nella categoria dei virus (la cui caratteristica principale è quella di auto-replicarsi), come i "cavalli di Troia", che combinano danni, ma non si autoreplicano. Invece non sono compresi nella previsione del 515-*quinquies* quei subdoli accorgimenti, un tempo usati da alcuni programmatori, che provocavano diversi inconvenienti nel caso in cui il committente non pagasse i diritti d'uso nei termini stabiliti.

Queste azioni sono previste da un altra norma, il

comma aggiunto all'articolo 392 del codice penale (esercizio arbitrario delle proprie ragioni). Il testo originario dice:

Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da se medesimo, mediante violenza sulle cose, è punito a querela della persona offesa con la multa fino a lire un milione.

Agli effetti della legge penale si ha "violenza sulle cose" allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione.

Il comma aggiunto dalla 547/93 dice:

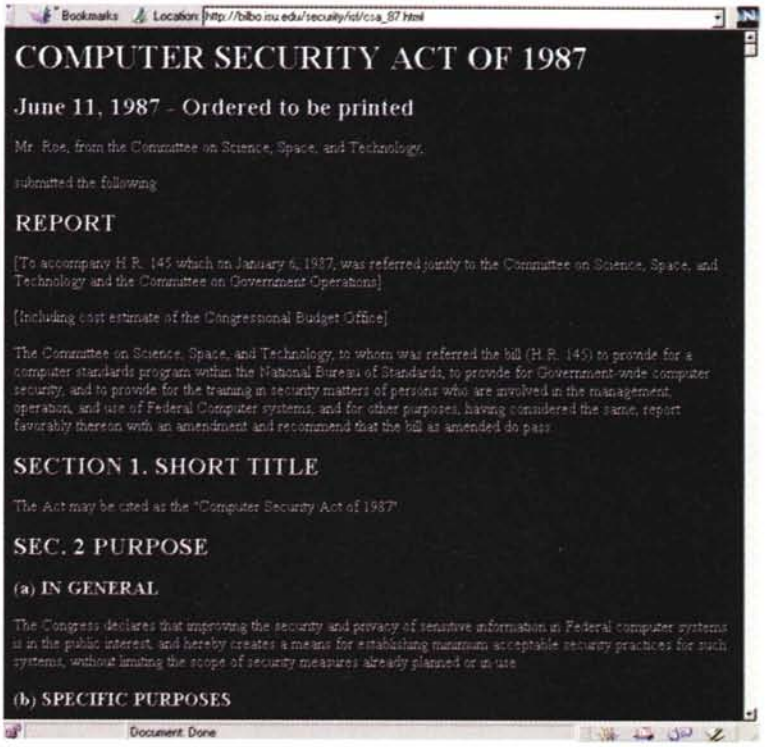
Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.

La pena è severa?

Riassumendo: il codice penale prevede il carcere fino a due anni e una multa fino a venti milioni per chi - volontariamente - diffonde, comunica o consegna un programma che danneggia sistemi informatici, dati o programmi, o ne altera il funzionamento, indipendentemente dal fatto che si tratti di un virus o di un altro tipo di software. Se, invece, il danno viene prodotto nell'ambito di un esercizio arbitrario delle proprie ragioni, c'è una pena pecuniaria fino a un milione e l'accusa scatta solo in seguito alla querela della persona offesa (negli altri casi non occorre querela, l'autorità giudiziaria procede d'ufficio per il solo fatto che l'illecito è stato, o si sospetta che sia stato commesso).

Due anni di galera (come massimo) sono tanti o pochi per punire chi compie il reato previsto dall'articolo 615-*quinquies*? Possono sembrare pochi se si considerano i danni che - in teoria - un virus diffuso su larga scala può cagionare. Si può paragonare questa pena a quella prevista dall'articolo 615-*ter* per l'accesso abusivo a un sistema informatico o telematico, che è come massimo di tre anni per i casi semplici (si procede, anche in questo caso, solo su querela di parte), ma che arriva a cinque anni se ricorrono alcune aggravanti, come l'abuso di poteri da parte di un pubblico ufficiale o di un incaricato di pubblico servizio, o con l'esercizio abusivo della professione di investigatore privato, o con abuso della qualità di operatore del sistema o con violenza sulle cose, o se il colpevole è palesemente armato. Se poi i fatti riguardano sistemi di interesse militare o relativi all'ordine e alla sicurezza pubblica, la pena può essere veramente salata, perché arriva fino a otto anni.

Se andiamo con la memoria a un periodo piuttosto recente, quando si diffondevano frequenti allarmi per virus che, più o meno a una data stabilita, avrebbero messo in crisi milioni di sistemi, si potrebbe concludere che i due anni previsti come massimo per la diffusione di virus sono pochi, e si potrebbe anche osservare che forse potevano essere previste pene differenziate per la diffusione di programmi "semplicemente" destinati a provocare danni e per la messa in circolazione di veri e propri virus. In realtà, se è vero che mettere in giro un virus è senza dubbio un atto criminale, è anche vero che oggi chi subisce gravi conseguenze per colpa di un virus è uno stupido o quanto meno un imprudente, e che sempre o quasi sempre è possibile rimediare ai danni con relativa facilità.


Bookmarks Location: http://bilbo.isu.edu/security/isl/csa_87.html

COMPUTER SECURITY ACT OF 1987

June 11, 1987 - Ordered to be printed

Mr. Roe, from the Committee on Science, Space, and Technology,

submitted the following

REPORT

[To accompany H.R. 145 which on January 6, 1987, was referred jointly to the Committee on Science, Space, and Technology and the Committee on Government Operations]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 145) to provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass

SECTION 1. SHORT TITLE

The Act may be cited as the "Computer Security Act of 1987"

SEC. 2 PURPOSE

(a) IN GENERAL

The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use

(b) SPECIFIC PURPOSES

Document: Done

La legge americana sul computer crime e la sicurezza dei sistemi risale al 1987 (http://bilbo.isu.edu/security/isl/csa_87.html).

Resta da aggiungere che non sono punite né la produzione dei virus, né il loro possesso. E la legge non fa distinzione tra chi diffonde programmi scritti in proprio e chi manda in giro programmi scritti da altri, il reato si verifica solo nel momento in cui il virus viene in qualche modo passato a terzi e con il preciso intento di provocare un danno.

Un'ultima considerazione riguarda il caso, che si è verificato diverse volte e può sempre verificarsi, di un virus messo in circolazione con software riprodotto in grande serie da un editore. Se si tratta di un fatto involontario, come accade normalmente, non c'è il delitto previsto dall'articolo 615-quinquies e quindi non c'è sanzione penale. Rimane, come è ovvio, l'obbligo di risarcire gli eventuali danni.

L'obbligo della protezione

Spostiamoci ora dalla parte della possibile vittima del reato previsto dal 615-*quinquies* o dal 615-*ter*, cioè di chi potrebbe subire danni a causa di un virus, di un programma "killer" o dell'intrusione non

autorizzata di un *hacker* a caccia di informazioni o di un *cracker* che danneggi il sistema o i dati.

A prima vista può sembrare strano, ma per la vittima al danno dell'intrusione si può aggiungere la beffa della sanzione penale, se di beffa si può parlare a proposito di una pena che può arrivare a due anni di reclusione. Stabilisce in fatti l'articolo 36 della legge 675/96 sulla tutela dei dati personali:

1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni.

2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino a un anno.

Ma quali sono le misure necessarie a garantire la sicurezza dei dati personali? Ne parla l'articolo 15 della 675/96:

1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n.

Che cosa dice il codice penale

Ecco le norme fondamentali in materia di virus e protezione dei sistemi negli articoli del codice penale introdotti con la legge n. 547 del 23 dicembre 1993:

Articolo 392 - (Esercizio arbitrario delle proprie ragioni con violenza sulle cose, terzo comma) - Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.

Articolo 420 - (Attentato a impianti di pubblica utilità) - Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.

La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti.

Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni.

Articolo 491-*bis* - (Documenti informatici) - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Articolo 615-*ter* - (Accesso abusivo a un sistema informatico o telematico) - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in essi contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Art.615-*quater* - (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici) - Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni.

La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater.

Art. 615-*quinquies* - (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni.

(Il testo completo della legge 547/93 è alla pagina http://www.interlex.com/testi/l547_93.htm)

400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.

I centottanta giorni sono scaduti il 4 novembre 1997, ma alla metà di gennaio '98 il regolamento non appare ancora all'orizzonte. Si spera che il ritardo sia dovuto a una seria riscrittura di una bozza che era circolata in ottobre, suscitando non poche critiche da parte dei tecnici. E' comunque opportuno mettere a fuoco alcuni aspetti essenziali della materia, rimandando l'analisi dei dettagli all'esame del testo che ormai dovrebbe essere di imminente pubblicazione.

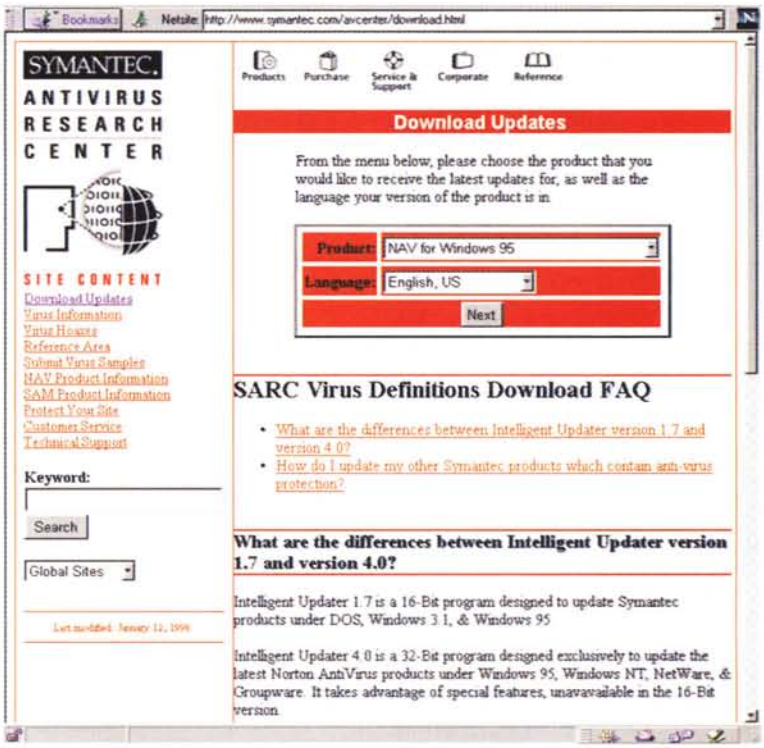
Per capire i termini del problema è utile esaminare la parte relativa alle misure di sicurezza contenuta nel quadro d) del modulo per la notifica dei trattamenti (ne parliamo nelle prossime pagine). Le misure sono divise in tre categorie: organizzative, fisiche e logiche. Tra le prime rientrano azioni come l'analisi dei rischi, la formazione professionale e il piano di *disaster recovery*, tra le seconde la vigilanza della sede, l'ingresso controllato nei locali, il deposito in cassaforte, mentre tra le misure logiche rientrano l'identificazione e l'autenticazione dell'utente, i controlli antivirus, la cifratura dei dati e - con formulazioni diverse - la tenuta di *log* sulle elaborazioni. Soffermiamoci sui controlli antivirus.

La vecchia bozza di regolamento prescriveva l'obbligo di usare programmi, da aggiornare con cadenza almeno semestrale, per proteggere stazioni di lavoro e server di rete contro i rischi di intrusione di virus. Troppo o troppo poco? Semplicemente impossibile, perché non esiste un software che possa offrire protezione contro "l'intrusione" di virus. Un virus può essere rilevato e quindi neutralizzato solo dopo che è entrato nel sistema, contro l'intrusione non c'è altro mezzo che non accendere il computer! Inoltre i tecnici facevano osservare che ci sono sistemi per i quali non esistono antivirus, come gli IBM AS/400 o le macchine Unix, per il semplice motivo che questi sistemi non sono attaccati dai virus.

Ma il problema è che il mancato rispetto delle disposizioni di questo regolamento è un delitto. E allora come si fa? Non c'è dubbio che nella versione definitiva questa norma sarà modificata, ma resta un problema di fondo, sul quale è necessario soffermarsi: il rapporto tra la realtà tecnologica e l'ordinamento giuridico o, per essere più precisi, tra certezza tecnica e certezza legale.

Tra il fatto e la norma

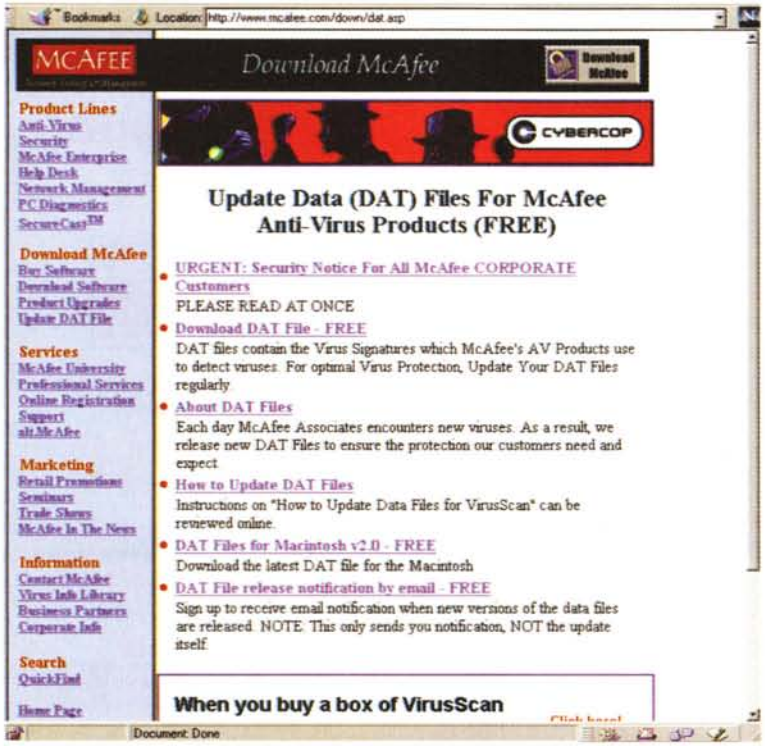
Sia chiaro che prendo la norma sui virus contenuta nella vecchia bozza del regolamento solo come esempio dei problemi che possono nascere dalla mancata rispondenza delle previsioni normative alle fattispecie tecnologiche; delle misure minime di sicurezza per i dati personali parleremo in dettaglio quando il regolamento sarà stato approvato definitivamente. Qui è necessario, per i tecnologi e per i giuristi, riflettere su una questione sempre più delicata.



L'aggiornamento degli antivirus è sempre gratis: questa è la pagina del Norton Antivirus, che ogni mese offre l'elenco aggiornato delle "firme" dei virus (http://www.symantec.com/avcenter/download.html).

Dobbiamo ricordare che ci troviamo di fronte a comportamenti di rilevanza penale, e per di più con un'esplicita ipotesi colposa. L'articolo 36 della legge dice che chi non adotta le misure di sicurezza previste dal regolamento può essere punito anche con due anni di detenzione. E se il regolamento contiene norme che è impossibile rispettare? Nessun timore, perché mai un giudice pronuncerebbe una condanna per il mancato rispetto di una norma che non è possibile rispettare: dicevano i giuristi del buon tempo andato *ad impossibilia nemo tenetur*, nessuno può essere obbligato a cose impossibili. Ma prima di arrivare a una sentenza di assoluzione o a un proscioglimento in istruttoria il titolare del trattamento dovrebbe passare per un autentico calvario, fatto di denuncia, iscrizione nel registro degli indagati, interrogatori, perizie e controperizie... senza considerare l'onorario dell'avvocato.

Ma c'è il rovescio della medaglia: chi rispetta la norma è a posto con la legge. Significa che se il titolare di trattamento installa un programma antivirus e lo aggiorna ogni sei mesi, ma i dati vengono distrutti cinque mesi e ventinove giorni dopo l'ultimo aggiornamento, non c'è alcuna sanzione penale. Insomma, manca una relazione tra la sostanza del fatto e la conseguenza legale. Va ricordato, però, che resta l'aspetto civile: chi fosse danneggiato dalla distruzione dei dati potrebbe chiedere un risarcimento, e il titolare non potrebbe dimostrare di aver adottato tutte le misure necessarie a evitare il verificarsi del danno (come prescrive l'articolo 18 della 675/96, richiamando l'articolo 2050 del codice penale), perché i produttori dei migliori



L'antivirus più conosciuto è quello prodotto da McAfee: ecco la pagina di aggiornamento dell'elenco, naturalmente gratuito (http://www.mcafee.com/down/dat.asp)

antivirus forniscono l'aggiornamento gratuito ogni mese.

Il problema non è solo nel paradosso della maggiore severità della norma civile rispetto alla norma penale, è nel fatto che la norma penale non tiene conto della realtà sostanziale (stiamo sempre ragionando sull'ipotesi che le disposizioni della bozza di regolamento non vengano corrette nella versione definitiva).

Si aggiunga che anche l'aggiornamento mensile dell'antivirus non dà la certezza tecnica della protezione dei dati e dei programmi. Il programma può non funzionare bene, ci può essere un virus recentissimo che non viene rilevato, può non andare a buon fine il ripristino dei dati dopo la "disinfezione" del sistema. Soprattutto i dati possono essere danneggiati o cancellati per errori umani o per malfunzionamenti del sistema (avete presente un *crash* di Windows 95? Può essere più deleterio di qualsiasi virus!).

Il responsabile di un sistema informativo ha un solo sistema che gli dà la certezza tecnica dell'integrità dei dati: la copia di riserva, eseguita con le opportune precauzioni e magari su un sistema remoto, per proteggersi anche da eventi catastrofici come un incendio o un terremoto. Se a intervalli ravvicinati viene effettuato un *back up* dei dati (cifrati!) e la copia di riserva viene custodita in un luogo sicuro, si ha una più che ragionevole "certezza tecnica" dell'integrità delle informazioni.

Invece per il diritto la certezza deriva dall'osservanza di una norma. Nell'esempio della disposizione per la protezione dai virus contenuta nella vecchia bozza di regolamento sulla sicurezza dei dati personali, il responsabile di un trattamento ottiene la certezza legale della protezione per il solo fatto di aver installato un programma e di averlo aggiornato ogni sei mesi.

Certezza tecnica e certezza legale

Naturalmente si possono fare altri esempi. Il più chiaro e più attuale è nel regolamento sulla firma digitale. Con i sistemi tradizionali la certezza giuridica dell'autenticità di un documento deriva dalla presenza di firme, sigilli, filigrane e via discorrendo. Insomma, è una questione formale, al punto che occorre una particolare procedura per dichiarare la falsità di un documento che appare vero. Invece con la firma digitale, se vengono adottate tecniche sicure come la crittografia a chiave pubblica, la certezza dell'autenticità di un documento è molto alta.

Questo portava, prima delle norme previste dalla legge 59/97, a un paradosso: per il diritto una firma tradizionale (facile da falsificare) in un eventuale processo certificava con la sua sola presenza dell'autenticità di un documento, mentre per verificare una firma digitale (molto più sicura) il giudice avrebbe dovuto ordinare una perizia tecnica. Ora, appena le nuove norme saranno operative, la firma digitale avrà la stessa certezza legale della firma autografa, anche se sappiamo che di fatto è di molti ordini di grandezza più attendibile.

Ma non basta. Dal punto di vista tecnico l'attribuibilità di una firma digitale a un soggetto è legata al fatto che la chiave pubblica è verificabile da chiunque, in quanto, appunto "resa pubblica". E' una certezza tecnica. Ma la nuova normativa subordina la validità e l'efficacia legale della firma digitale alla sua pubblicazione da parte di un soggetto iscritto in un apposito elenco, che deve avere i requisiti di un'azienda bancaria, fra i quali un capitale sociale non inferiore a 12,5 miliardi di lire. La certezza legale della firma digitale non corrisponde quindi alla certezza tecnica, perché la norma non dà la sicurezza materiale che un dipendente dell'ente certificatore non combini qualche inghippo sulla data di pubblicazione o di revoca della firma, o nell'accertamento dell'identità del titolare.

Certezza tecnica e certezza legale sono quindi cose molto diverse. Inconciliabili? Questo è il vero problema. Nella nostra cultura diritto e tecnologia sono due mondi diversi e spesso distanti. L'assioma caro ai vecchi "informatici giuridici" di una predisposizione dell'operatore della legge all'uso dei mezzi informatici si rivela ogni giorno più infondato. Non basta che ambedue le materie, il diritto e la tecnologia, siano fondate sul meccanismo della logica aristotelica vero-falso per giungere alle stesse conclusioni. Perché in uno dei due campi a volte può essere presa per vera una premessa che invece è falsa. Per capirlo torniamo all'esempio dell'ipotizzata norma per la protezione dei dati personali dagli effetti dei virus.

Ragiona l'uomo di legge: la norma dice che la

protezione delle informazioni si ottiene con l'adozione di un programma antivirus, il soggetto ha rispettato la prescrizione, dunque ha protetto le informazioni. E invece il poverino è in un mare di guai, perché i suoi dati sono andati persi. Al contrario: la norma dice che la protezione delle informazioni si ottiene con l'adozione di un programma antivirus, il soggetto non ha seguito la norma e quindi deve essere punito. Ma i dati non corrono rischi, perché il tecnico ha predisposto un programma di *disaster recovery* a prova di bomba (fisica e logica). Dov'è l'errore?

Si potrebbe dire che risiede nella logica formalistica del ragionamento giuridico, ma in realtà è falsa la prima premessa, cioè l'assunto che un antivirus aggiornato ogni sei mesi possa proteggere i dati. Dunque è sbagliata la norma.

Di norme "sbagliate" è pieno l'ordinamento, sbagliate nel senso che fanno discendere la certezza tecnica dalla certezza legale, e non viceversa. Prendiamo il caso dell'omologazione dei modem. Se sono provvisti di un certo bollino, che certifica la loro rispondenza a determinati requisiti (necessari per la protezione della rete), il loro uso è legittimo. Anche se, per un guasto o un difetto di fabbrica non rilevabile da chi le utilizza, provocano seri inconvenienti. Invece un apparecchio che funziona perfettamente secondo le prescrizioni tecniche, ma non è provvisto del bollino di omologazione, è causa di multe, sequestri e altri grattacapi. Insomma, per la legge il modem funziona bene se è omologato, per il tecnico funziona bene se... funziona bene.

Ragiona il tecnico: il bollino non certifica il corretto funzionamento dell'apparecchio, ma serve solo a dimostrare che, all'origine, rispondeva a determinati requisiti. Ma allora che valore ha, nella sostanza, questa certificazione? Non c'è dubbio che in determinati casi debba essere obbligatorio rispettare delle norme tecniche, cioè che le norme tecniche abbiano efficacia giuridica, ma affidare alla presenza di un bollino la verifica del rispetto della norma è un nonsenso dal punto di vista tecnico.

C'è un altro problema. La tecnologia evolve a gran velocità e influisce in misura sostanziale sul funzionamento della società, governato dal diritto, e provoca cambiamenti di grande rilevo anche nella percezione e nella definizione di molti aspetti della realtà. Prendiamo di nuovo l'esempio del documento digitale: fino a ieri il concetto di "documento" era legato alla presenza di un supporto fisico determinato e inscindibile dal documento stesso. Un certificato di residenza, per citare un caso molto banale, era (ed è ancora) costituito da un foglio di carta sul quale sono scritte certe informazioni e sono apposti certi timbri. Le stesse informazioni, senza carta e senza timbri, non sono un certificato. Con l'introduzione del documento digitale il certificato esiste senza carta e senza timbri, perché la certificazione può essere incorporata nell'informazione. E' un concetto che la cultura tecnologica ha assimilato da parecchi anni, ma la cultura giuridica se ne è accorta solo di recente ritardo e in qualche caso fatica ancora ad accettarlo.

La conseguenza è che le norme a volte nascono in ritardo, altre volte invecchiano troppo presto. Si può avere questa sensazione proprio leggendo gli articoli del codice penale introdotti dalla legge 547/93. Sono passati solo quattro anni, ma alcuni concetti sono già superati, come quello formulato nell'articolo 491-*bis*:

per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Oggi la definizione di documento informatico è quella che si ricava dall'articolo 15, comma 2, della legge 59/97:

Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge.

E il regolamento applicativo, primo comma dell'articolo 1, chiarisce definitivamente:

Ai fini del presente regolamento s'intende:

a) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il supporto non c'è più, ed è giusto che sia scomparso, dal momento che l'informazione, semplice o certificata, esiste indipendentemente dal supporto. Ma la norma penale, che è sempre tassativa, resta nel codice, e potrebbe causare non poche complicazioni in caso di processi che abbiano

La sicurezza dei dati personali

Queste sono le norme della legge 31 dicembre 1996, n. 675, sulla sicurezza dei dati personali:

Articolo 15 (Sicurezza dei dati) - 1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.

3. Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.

Articolo 36 - (Omessa adozione di misure necessarie alla sicurezza dei dati) - 1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni.

2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino a un anno.

per oggetto alterazioni di documenti, frodi informatiche e simili.

D'altra parte la stessa legge 547/93 ha introdotto concetti innovativi e ancora utili, come quello del "domicilio informatico" applicato a un sistema informativo (gli articoli 614 e 615 del codice penale si riferiscono appunto alla violazione di domicilio). Ma proviamo ad applicare questo concetto a situazioni che con ogni probabilità si verificheranno molto presto, con la diffusione dei "network PC", che lavorano su informazioni archiviate chissà dove sulla rete. In questo caso, qual è il domicilio informatico che può essere violato da un'intrusione illegittima?

A mano a mano che il tempo passa e la tecnologia si evolve, i problemi legali diventano sempre più complicati da risolvere.

Che cosa c'è da rettificare?

Al direttore di MCmicrocomputer è giunta questa e-mail, inviata per conoscenza anche a una quantità di altri indirizzi:

Al Direttore della Rivista MC
.....
Spett. Direttore,

chiedo formalmente un suo diretto intervento in rettifica di quanto erroneamente affermato da Manlio Cammarata sull'ultimo numero (179, 12/97) della rivista MC alle pagine 180-182 ed in particolare nel passo che riporto testualmente di seguito:

''(...) 6 novembre: il presidente del tribunale di Roma ordina l'iscrizione della rivista InterLex nel registro della stampa, prima pubblicazione diffusa esclusivamente attraverso Internet che viene registrata esplicitamente come tale, e non con formule ambigue e soluzioni di ripiego.''

Tale affermazione e' assolutamente priva di fondamento per quanto attiene la presunta priorita' di tale rivista. Le segnalo infatti che chi scrive:

1. e' iscritto nell'Elenco Speciale annesso all'Albo dell'Ordine dei Giornalisti della Puglia (comunicazione prot. n. 1993, del 29.05.97) dal 28 maggio 1997 come direttore responsabile del periodico telematico ''Educazione&Scuola'';

2. a seguito di richiesta del 30.06.97, depositata presso la Segreteria della Presidenza del Tribunale di Lecce in data 01.07.97, ha ricevuto, con Ordinanza dello stesso Tribunale n. 12592, dell'1 luglio 1997 l'iscrizione sul registro della stampa del Tribunale di Lecce della testata giornalistica 'Educazione&Scuola', pubblicazione telematica mensile con aggiornamenti quotidiani, al n. 662, sempre in data 1 luglio 1997;

3. ha dato notizia dell'avvenuta registrazione all'OdG della Puglia con raccomandata AR n. 4767 dell'11.07.97 segnalando che la spedizione di ogni nuovo numero e/o modifica della rivista sarebbe stata comunicata all'Ordine a mezzo posta elettronica all'indirizzo e-mail dello stesso (odg@planio.it) cosa che avveniva (ed avviene senza soluzione di continuita') dal 5 luglio 1997.

Sottolineo che la rivista in questione e' ESCLUSIVAMENTE telematica e che il Tribunale di Lecce ha preso atto nell'ordinanza sopracitata anche degli indirizzi web attraverso i quali avviene la sua distribuzione (di seguito riportati in signature).

Questo per quanto riguarda la registrazione; ne' il tutto termina a questo punto.

Il 18 ottobre us lo scrivente segnalava a Manlio Cammarata la rivista Educazione&Scuola ricevendo risposta dallo stesso il 21 ottobre successivo. In tale email Cammarata chiedeva maggiori indicazioni circa la registrazione di Educazione&Scuola che puntualmente gli venivano comunicate il 23 ottobre successivo (con, in allegato, l'integrale dichiarazione congiunta presentata ed accolta dal Tribunale di Lecce). Poi piu' nulla.

Circa un mese dopo tale scambio di corrispondenza alcune agenzie stampa ed alcuni giornali (anche nelle loro edizioni telematiche) davano notizia della ''storica'' (sic) delibera del Tribunale di Roma.

Anche in quella circostanza chi le scrive comunico' a quanti avevano dato credito e riscontro ufficiale a tale notizia la sua mancanza di fondamento e pubblicava su ''ItaliaOggi'' (A. VII, n. 276, p. 14 del 22 novembre 1997) un breve articolo in cui chiariva la situazione, segnalando altresi' che, per altra testata telematica, tale registrazione era stata effettuata dallo stesso Tribunale di Lecce sin dall'agosto del 1995.

Le lascio quindi immaginare lo stupore con il quale apprendo oggi il reiterarsi di questa incresciosa situazione dalle pagine della sua pubblicazione, anche in considerazione del fatto che lo stesso Cammarata ben conosceva l'erroneita' delle sue affermazioni.

Quanto sopra e' esposto non per spirito polemico o per acquisire la non ricercata ''palma'' del pioniere (che semmai spetterebbe ad altri), quanto per amore del vero e per un senso dell'etica non solo professionale.

In attesa di un suo riscontro a questa mia nonche' della rettifica richiesta invio distinti saluti.

dario cillo

Non c'è nulla da rettificare, perché nell'ordinanza emessa il 6 novembre scorso dal Tribunale di Roma per l'iscrizione di InterLex nel registro della stampa si legge testualmente: "Tecnica Diffusione: INTERNET" e più avanti: "IL PERIODICO TELEMATICO SARA' DIFFUSO DA ROMA A MEZZO RETE TELEFONICA IN FORMATO DIGITALE CON I PROTOCOLLI TECNICI DELLA RETE INTERNET" (per chi volesse leggerla, l'ordinanza è riportata integralmente alla pagina http://www.interlex.com/testi.com/or061197.htm).

E' la prima volta in Italia, per quanto mi risulta e per quanto risulta alla sezione stampa del tribunale di Roma, che Internet viene formalmente riconosciuta come mezzo di diffusione della stampa periodica. Questa è la notizia, che avrà importanti implicazioni sotto il punto di vista giuridico, e non il fatto che InterLex, o un'altra pubblicazione, abbia ottenuto per prima l'importante affermazione di principio.

Invece il periodico diretto dal signor Cillo è stato registrato come diffuso attraverso computer e linea telefonica, secondo la formula introdotta da anni per le testate Videotel (solo per fare un esempio, la testata MC-link è stata iscritta nell'ormai lontano 1990 come diffusa "a mezzo videoterminale").

(Manlio Cammarata)

E' bene fare due conti prima di chiedere le tariffe ridotte

Internet "formula convenienza" conviene solo a Telecom?

Aspettando le "pari opportunità", dal primo gennaio sono in vigore le tariffe agevolate annunciate nello scorso mese di ottobre per il collegamento degli utenti privati a Internet. Ma la lettura dei moduli per la richiesta offre qualche sorpresa, anche per quanto riguarda il diritto alla riservatezza degli utenti.

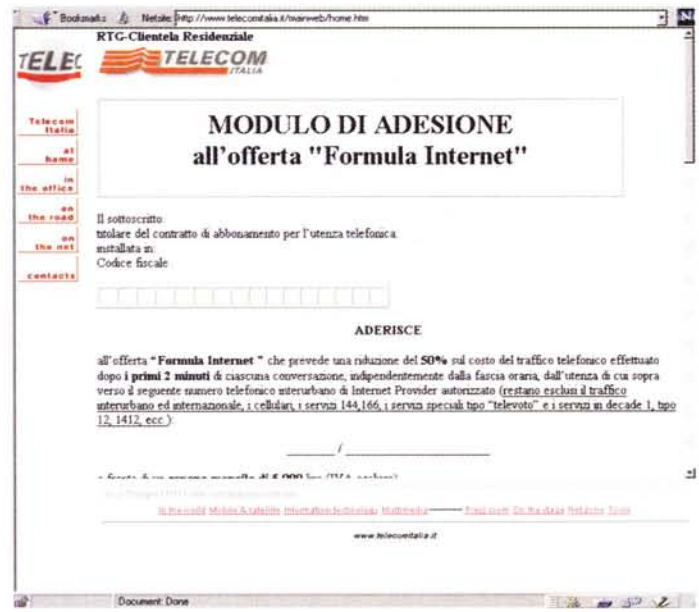
di Manlio Cammarata

Sconti, saldi, offerte speciali... Questa "formula convenienza" mi ricorda tanto i "dieci piani di morbidezza" di un noto prodotto di larghissimo consumo. Ma in tempi di libero mercato (sulla carta) anche gli scatti telefonici sono un prodotto da vendere. Ben vengano dunque le offerte promozionali, se sono a favore di chi compera.

Dunque dall'inizio dell'anno ci si può collegare al proprio Internet provider risparmiando qualcosa sulla bolletta telefonica. Una novità preparata con grande clamore alla fine dello scorso mesi di ottobre: *Il provvedimento "Internet" che viene annunciato oggi è sicuramente unico in Europa ed è stato adottato per contribuire a ridurre il ritardo nello sviluppo della società dell'informazione nel nostro paese. Il Governo è sempre più convinto che il diritto di cittadinanza si esprime anche attraverso la possibilità, per tutti, di partecipare interattivamente al cyberspazio*, si leggeva nel comunicato del ministro Maccanico, che illustrava i punti essenziali della "manovra": sconto del 50 per cento, dopo il primo scatto, con un canone mensile di 2.500 lire per la chiamata urbana e di 5.000 per la teleselezione, *per gli utenti domestici, le scuole e moltissime associazioni non profit.*

In effetti si trattava di una novità abbastanza importante, considerando le resistenze di Telecom Italia a concedere qualsiasi forma di agevolazione per gli utenti della Rete. Ma ora, leggendo i moduli di richiesta predisposti dall'ancora monopolista di fatto, l'entusiasmo si raffredda un po', perché oltre al canone previsto c'è la sorpresa del contributo di attivazione, che ammonta a 10.000 lire *una tantum* sia per le urbane, sia per le interurbane e alza un di bel po' il punto di convenienza dell'offerta. Facciamo due conti.

Naturalmente ci mettiamo nei panni di un utente che cerca di risparmiare il più possibile e quindi si collega nelle ore a tariffa ridotta, dalle 18,30 alle 8 del mattino, il pomeriggio del sabato e tutta la domenica, con uno scatto ogni 400 secondi, cioè 1.372 lire/ora, IVA compresa. Per ammortizzare le 12.000 lire (c'è anche l'IVA) del contributo di attivazione bisogna stare attaccati la bellezza di diciassette ore e mezza, mentre per rifarsi delle 3.000 lire di canone mensile (c'è sempre l'IVA!) bastano circa quattro ore e venti minuti. Ma dopo il primo scatto, che dura 6 minuti e 40 secondi. In pratica, con un collegamento al giorno per trenta giorni, si raggiunge il punto di pareggio dopo circa un quarto d'ora di connessione giornaliera. Ma se si fanno collegamenti più brevi e più volte al giorno (come capita a chi controlla spesso la posta), la convenienza dell'offerta è sempre più lontana.


RTG-Clientela Residenziale

TELECOM ITALIA

MODULO DI ADESIONE
all'offerta "Formula Internet"

Il sottoscritto
titolare del contratto di abbonamento per l'utenza telefonica
installata in
Codice fiscale

ADERISCE

all'offerta "**Formula Internet** " che prevede una riduzione del **50%** sul costo del traffico telefonico effettuato dopo i **primi 2 minuti** di ciascuna conversazione, indipendentemente dalla fascia oraria, dall'utenza di cui sopra verso il seguente numero telefonico interurbano di Internet Provider autorizzato (restano esclusi il traffico interurbano ed internazionale, i cellulari, i servizi 144,166, i servizi speciali tipo "televoto" e i servizi in decade 1, tipo 12, 1412, ecc.):

_____ / _____

www.telecomitalia.it

Document: Done

La pagine del sito di Telecom Italia in cui sono è riportato il modulo di adesione all'offerta convenienza che va presentato o spedito alla filiale Telecom competente per territorio (http://www.telecomitalia.it/mainweb/home.htm).

Ma chi non ha un provider vicino a casa...

Le cose vanno un po' meglio per chi deve usare la teleselezione. Qui lo scatto vale 150 secondi per distanze fino a 15 chilometri, 80 secondi per distanze tra 15 e trenta chilometri e 50 secondi oltre i trenta chilometri, sempre nella fascia più bassa. Il costo normale della connessione è quindi, rispetti-

vamente, di 3.676, 6.858 e 12.192 lire/ora, il che significa che il contributo di attivazione si ammortizza con lo sconto in un tempo che va da meno di due a circa un'ora di collegamento. Per rifarsi del canone di 6.000 lire mensili all'utente più lontano basta un'ora.

Tutto qui? No, perché questi conti valgono solo per gli utenti privati titolari un abbonamento residenziale sulla rete telefonica generale. Per chi ha un abbonamento ISDN il canone mensile raddoppia, 5.000 lire al mese per l'urbana e 10.000 per l'interurbana, raddoppiando quindi il tempo di collegamento necessario per ottenere il pareggio con la tariffa non scontata. Non c'è una ragione tecnica per questa differenza, è un po' come la vecchia sovrattassa sulle automobili con motore diesel: vuoi risparmiare? E io ti punisco!

La maggiorazione per l'ISDN potrebbe essere giustificata con il fatto che questo servizio è oggi utilizzato più dalle imprese che dalle famiglie (se si accetta il principio che l'utenza "affari" deve pagare più dell'utenza privata), ma il fatto è che le agevolazioni sono limitate ai contratti domestici. Non c'è nessuno sconto per aziende, artigiani o professionisti, che dall'uso di Internet possono trarre i maggiori vantaggi, soprattutto se risiedono lontano dai grandi centri. E, per di più, si connettono prevalentemente o esclusivamente nelle ore della tariffa più alta, che in teleselezione è esattamente il doppio dell'altra.

Ma il principale difetto di questa "offerta speciale" è che resta la differenza tra gli abbonati che hanno un provider nello stesso distretto telefonico e quelli che devono usare la teleselezione. Per i primi la tariffa scontata vale 686 lire l'ora, per i secondi va da 1.838 a 6.096 lire l'ora, sempre considerando la fascia oraria più bassa. E se per l'urbana l'importo non si può dire alto, per l'interurbana è una cifra tutt'altro che indifferente.

"Il Ministro è consapevole della necessità di ulteriori interventi e per questo incoraggerà il proseguimento del dialogo con tutte le parti interessate. Esprime infine la soddisfazione per un provvedimento che ha uno straordinario valore sociale, economico e politico". Così si chiudeva il comunicato del 29 ottobre scorso. E il Parlamento, nel votare il collegato alla legge finanziaria per quest'anno, ha stabilito che *Il ministro delle comunicazioni, d'intesa con il ministro dell'università e della ricerca scientifica, adotta provvedimenti finalizzati a garantire la pari opportunità di accesso ad Internet, anche al fine di evitare discriminazioni di tipo territoriale.*

Signori Ministri, è venuto il momento di mettere

Le clausole del contratto

Ecco le clausole della "Formula urbana" per gli abbonati che si collegano al proprio provider in teleselezione. Sono identiche a quelle della "Formula Internet" e della "Formula 3", cambiano solo le cifre. La "Formula 3" prevede uno sconto del 15 per cento su tutte le chiamate urbane e interurbane (esclusi i cellulari) a tre numeri scelti dall'utente; la "Formula urbana" prevede il 50 per cento per un solo numero, che può essere indifferentemente quello di un abbonato al telefono o di un Internet provider; la "Formula Internet" è solo per i collegamenti interurbani a Internet.

[...]

– il numero telefonico suindicato deve appartenere ad un Cliente Telecom Italia;

– al momento della sottoscrizione, al Cliente aderente viene addebitato un contributo di attivazione di 10.000 lire (IVA esclusa);

– l'offerta ha la durata di 1 anno e si rinnova tacitamente di anno in anno salvo quanto previsto in tema di recesso;

– ogni modifica del numero telefonico sopra indicato dovrà essere richiesta per iscritto e decorrerà a partire dal 1° giorno del mese successivo alla ricezione della stessa da parte di Telecom Italia: a fronte di ogni modifica dovrà essere corrisposto un contributo di 10.000 lire (IVA esclusa);

– il canone decorre a partire dal 1° giorno del mese successivo alla ricezione, da parte di Telecom Italia, del presente modulo di adesione e viene addebitato in bolletta posticipatamente;

– la riduzione viene applicata a partire dal 1° giorno del mese successivo alla ricezione, da parte di Telecom Italia, del presente modulo di adesione;

– la riduzione viene applicata esclusivamente sulla parte di traffico urbano effettuato, verso il numero sopra indicato, dopo il primo intervallo temporale di tassazione di ciascuna conversazione;

– la presente riduzione non è compatibile con altri tipi di offerta, salvo quella avente ad oggetto "Formula Internet";

– nel caso di contemporanea sottoscrizione dei moduli di adesione "Formula urbana" e "Formula Internet" è dovuto un solo contributo di attivazione;

– nel caso in cui si verifichi una variazione, per motivi tecnici, del numero telefonico del Cliente aderente o di quello urbano/settoriale sopra indicato, Telecom Italia garantirà la continuità dell'offerta;

– in caso di trasloco della propria utenza telefonica o di richiesta di cambio numero da parte del Cliente, Telecom Italia garantirà la continuità dell'offerta compatibilmente con la disponibilità tecnica e provvederà ad avvertire il cliente nel caso risulti impossibile garantire la continuità dell'offerta stessa;

– in caso di subentro sulla propria linea telefonica da parte di altro Cliente, l'offerta decade a partire dalla data di ricevimento, da parte di Telecom Italia, della richiesta di subentro, ma il canone per il mese di riferimento viene addebitato in bolletta per intero;

– in caso il Cliente disdica la propria linea telefonica, l'offerta decade alle stesse condizioni di cui al punto precedente;

– la trasformazione della linea telefonica del Cliente aderente da Rete Telefonica Generale a ISDN, comporterà automaticamente la cessazione della presente offerta alle stesse condizioni di cui al punto precedente;

– il Cliente ha facoltà di recedere dall'offerta in qualsiasi momento, senza alcun onere aggiuntivo, previo avviso a Telecom Italia inviato mediante raccomandata A/R alla Filiale Telecom territorialmente competente, che produrrà effetto a partire dal primo giorno del mese successivo alla ricezione della medesima; [...]

Segue la parte relativa al trattamento dei dati personali, della quale si parla nell'articolo. La descrizione completa delle offerte e i moduli di adesione si possono trovare sul Web di Telecom Italia, dalla pagina http://www.telecomitalia.it/maiweb/27127.htm. Ma per avere un chiaro quadro riassuntivo è meglio andare su MC-link alla pagina http://www.mclink.it/news/tariffe.htm.

in pratica questi principi, che hanno "uno straordinario valore sociale, economico e politico".

La convenienza del "consenso ampliato"

L'utente che, dopo aver fatto i suoi conti, decida di aderire alla "formula convenienza", si trova davanti a un modulo di due pagine, con poche voci da riempire, la più importante delle quali è il numero telefonico del provider al quale è abbonato. Poi "il sottoscritto dichiara di essere a conoscenza del fatto che..." e segue un lungo elenco di clausole, che si conclude così:

"in relazione alla Legge 675/96 i dati personali del Cliente verranno trattati sulla base dell'indicazione fornita dallo stesso attraverso la sottoscrizione del regime prescelto:

Consenso ampliato

In esecuzione dell'art. 11 della Legge 675/96, recante disposizioni a tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali, il Cliente fornisce il proprio consenso al trattamento dei propri dati personali, direttamente o anche attraverso terzi, oltre che per l'integrale esecuzione della presente offerta o per ottemperare ad obblighi previsti dalla legge, da un regolamento o dalla normativa comunitaria, anche per le seguenti finalità:

a) elaborare studi e ricerche statistiche e di mercato;

b) inviare materiale pubblicitario ed informativo;

c) compiere attività dirette di vendita o di collocamento di prodotti o servizi;

d) inviare informazioni commerciali;

e) effettuare comunicazioni commerciali interattive.

Firma .....

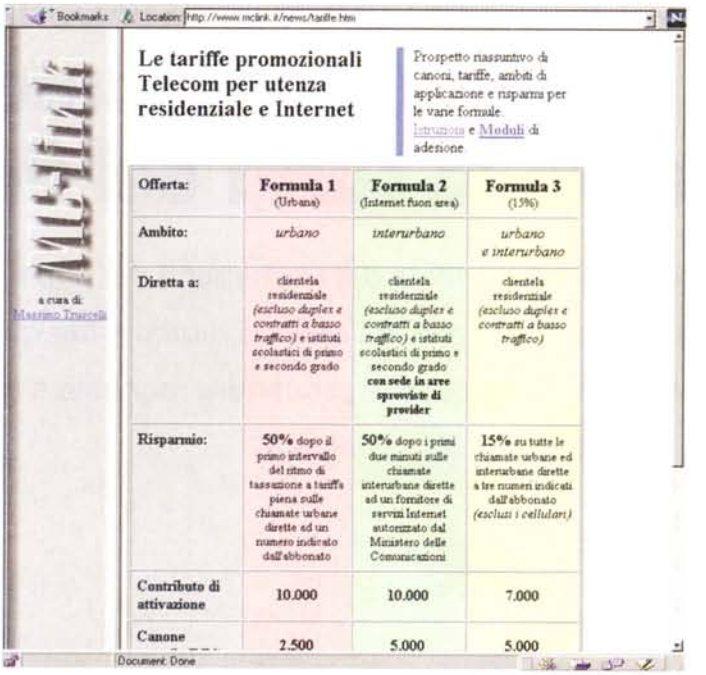
Oppure

Consenso ristretto

I dati personali forniti dal Cliente sono tutelati dalla Legge 675/96, recante disposizioni a tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali, e pertanto saranno utilizzati per l'integrale esecuzione della presente offerta.

Firma.....

Tutto regolare? A prima vista sembra che la legge sui dati personali sia rispettata. Nella prima ipotesi, quella del "consenso ampliato" c'è l'informativa, c'è il consenso, ma molto probabilmente il Garante avrà qualcosa da eccepire. In primo luogo manca l'informazione sui diritti dell'interessato (articolo 13 della legge 675/96), poi non sono specificati i "terzi" che potrebbero trattare i dati, con l'avverbio "attraverso" che fa supporre che i terzi siano incaricati del trattamento per conto di Telecom Italia, ma potrebbe significare anche che i dati vengono ceduti ad altri, per le finalità elencate. Inoltre non



Un quadro riassuntivo molto chiaro degli sconti offerti da Telecom Italia è su MC-link alla pagina http://www.mclink.it/news/tariffe.htm.

c'è l'indicazione sul *nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile*, come prescrive l'articolo 10, comma 1, lettera f) della legge. Siamo sicuri che a un abbonato di Telecom Italia tutti questi dati siano noti, come prevede il secondo comma dello stesso articolo per consentire l'assenza dell'informazione?

Poi, nel caso del "consenso ristretto", non c'è alcuna indicazione delle finalità e delle modalità del trattamento, perché "per l'integrale esecuzione della presente offerta" è una formula troppo generica. E in questo caso basta l'informativa, perché il consenso non è richiesto ai sensi dell'articolo 12, comma 1, lettera b), *quando è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato.*

Ma il punto principale non riguarda tanto il Garante dei dati personali quanto il Garante della concorrenza e del mercato. Perché Telecom Italia con questa offerta viene a conoscenza del nome del provider di ogni abbonato che chiede lo sconto (per attivare il diverso meccanismo degli scatti è necessario conoscere il numero telefonico interessato, e da qui all'identificazione del provider è questione di attimi). Quindi, grazie alla firma sul "consenso ampliato", Telecom può bombardare l'abbonato stesso di offerte e suggestioni che lo convincano a cambiare fornitore. Dunque può approfittare della sua "posizione dominante" nella fornitura dei servizi di rete - anzi del suo monopolio, perché non ci sono ancora alternative a Telecom Italia per gli abbonamenti privati - per fare concorrenza ai fornitori di servizi Internet, proponendo abbonamenti a TIN.

In conclusione, la "formula convenienza" non sempre è conveniente per gli abbonati, ma certamente conviene al gestore della rete telefonica pubblica. Grazie allo "straordinario valore sociale, economico e politico" dell'iniziativa.

La scadenza per i trattamenti già iniziati è il 30 aprile

La notifica al Garante dei dati: meglio la carta del floppy

Il modulo per la notifica dei trattamenti dei dati personali è disponibile sia in versione cartacea che in versione digitale. Ma quest'ultima presenta qualche problema, al punto che la procedura manuale è più veloce e soprattutto meno "stressante". Qual è il problema?

di Manlio Cammarata

Con discreto anticipo sulla data d'inizio delle operazioni, il Garante ha diffuso il modulo per la notifica dei trattamenti di dati personali, prevista dall'articolo 7 della legge 675/96 (ricordiamo che l'obbligo è scattato il 1. gennaio scorso e le scadenze sono fissate al 30 aprile o al 30 giugno, a seconda dei trattamenti).

Il modulo è stato diffuso sia in versione cartacea, sia su floppy disk, e questa è una buona notizia. Ma c'è un particolare: alla fine della compilazione della versione digitale è necessario stampare il tutto e inviare al Garante carta e floppy. Il motivo è che non sono ancora in vigore le norme sulla firma digitale e quindi è necessario un autografo su un pezzo di carta. Però, se si inviano floppy e stampe, si risparmia qualcosa sui diritti di segreteria, che peraltro sono modesti: 15.000 lire per la versione digitale e 25.000 per quella cartacea (per la verità, il comunicato del Garante dice "£ 15.000" e £ 25.000, cioè 15.000 e 25.000 sterline, posto che il simbolo "£" indica il "Pound" di Sua Maestà britannica, e non la lira italiana, che si abbrevia con "L.", "Lit" o "Itl" nelle transazioni internazionali, ma sono dettagli).

Veniamo ai contenuti. Siamo di fronte a una sorta di "740 della privacy", con la non trascurabile differenza che il modulo delle tasse è di quattro pagine e qui sono una ventina, compresi gli allegati. Di fatto l'impostazione della notificazione rispecchia la tendenza di tutta la normativa italiana sui dati personali a curare anche il minimo dettaglio, con il rischio di perdere di vista l'insieme e di giungere a disposizioni di difficile applicazione. La legge, invece, dovrebbe essere il più possibile schematica e generale, lasciando all'interprete la sua applicazione alla fattispecie concreta.

Qui invece si giunge a quello che può essere definito "accanimento normativo", come si vede, per esempio, nel quadro d), relativo alle misure di sicurezza (ne abbiamo parlato poche pagine più indietro nell'articolo sui virus). L'articolo 7, comma 4, della legge 675/96 dice al punto f):

La notificazione contiene:

f) una descrizione generale che permetta di valutare l'adeguatezza delle misure tecniche ed organizzative adottate per la sicurezza dei dati;

Invece il modulo presenta una grande tabella, con l'elenco dettagliato di una lunga serie di misure, divise tra organizzative, fisiche e logiche, e anche le righe in bianco per aggiungerne altre.

Comunque, con un po' di pazienza e consultando gli allegati, con un paio d'ore di lavoro è possibile completare il modulo cartaceo. Ben diverso è il discorso per la versione su floppy disk (che può essere acquisita anche sul Web in diversi siti, fra i quali la pagina http://www.interlex.com/675/modulo.htm di InterLex).

Il "flop" del floppy

In teoria la versione digitale dovrebbe essere più semplice e più veloce da compilare del modulo su carta. Purtroppo non è così.

La procedura, scritta in Visual Basic, si rivela fuori standard fin dall'inizio. Lo scompattamento dei file richiede un tempo inspiegabilmente lungo, al termine del quale appare un terrificante svarione di anglo-italiano: "si vuole leggere *il files* di guida ora?".

Alla partenza su un vecchio sistema 486 con monitor VGA 640x480, usato per simulare le condizioni che con ogni probabilità si verificheranno di frequente soprattutto negli uffici pubblici, è apparso l'avviso "Si consiglia di impostare

la risoluzione di Windows ad un valore superiore a 640x480 pixel". Infatti il formato della finestra non è parametrico (cioè non si adatta automaticamente alla risoluzione dello schermo), ma non è stato nemmeno impostato sul valore massimo consigliato per i monitor standard. Così i riquadri non possono essere visti per intero ed è necessario un continuo *scrolling* nella finestra.

Invano si cerca un pulsante AVVIO sulla finestra di apertura (che non entra tutta nello schermo): una scritta che dice "premere il pulsante sinistro del mouse per proseguire" si scopre solo dopo aver fatto scorrere la finestra verso l'alto.

Si prosegue e appare la prima finestra, con pulsanti e caselle da barrare. Attenzione: arrivati a questo punto è difficilissimo cambiare idea e uscire. Il programma pretende che ogni finestra sia compilata, altrimenti rifiuta di chiudersi persino dopo la pressione di CTRL+ALT+CANC.

Ancora invano il mouse vaga alla ricerca un pulsante AVANTI. Per passare al quadro successivo bisogna fare click sul relativo pulsante che si trova sulla parte alta della finestra, beninteso dopo aver completato il precedente. E qui incominciano i veri guai. Perché compaiono alcuni campi, evidentemente da riempire, ma il cursore rifiuta di fermarsi sul primo (che è una finestra di riepilogo che si riempie automaticamente, ma è messa all'inizio invece che alla fine) e anche sul secondo campo. Poi si scopre che c'è un pulsante INSERISCI in basso. E' la prima volta che vedo un programma sotto Windows in cui il cursore non si ferma automaticamente sul primo campo da riempire in una finestra.

Roba da crisi di nervi. La pressione del tasto F1 non fornisce un aiuto alla compilazione, ma richiama la normativa. Un fumetto con la "i" minuscola, quello che nelle procedure standard contraddistingue i messaggi del sistema, qui fa comparire ancora articoli di legge e norme varie.

Il quadro g), "notizie per facilitare i rapporti con il Garante" rifiuta di farsi riempire; per fortuna quando si fa click sul pulsante del successivo una scritta, mentendo, assicura che le informazioni sono state archiviate e permette di andare avanti.

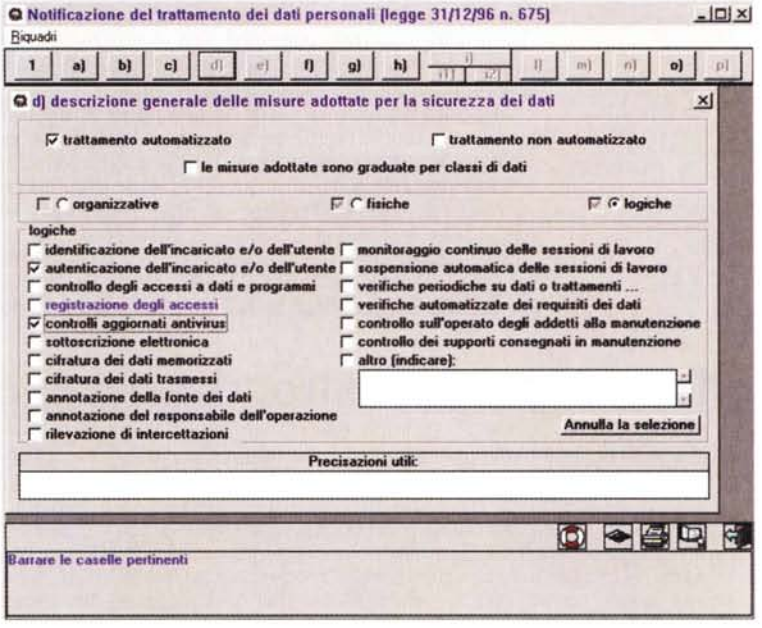
Bene o male e con molta pazienza si arriva all'ultimo quadro, il p), che è quello dove bisogna inserire i dati del notificante e la firma (chi presenta la notifica in forma semplificata trova questo quadro alla h), ma alcune categorie devono riempire anche il quadro "o"). Ma quando si porta il cursore nello spazio dedicato alla firma, compare in basso una scritta: "Il campo collegato alla firma per il momento non è attivo. Sarà usabile a decorrere dalla data indicata dal Garante, successivamente all'entrata in vigore della disciplina concernente la firma elettronica. Al momento è indispensabile apporre la firma sul documento cartaceo che deve essere stampato al termine della compilazione".

Incredibile. La firma elettronica si appone con una procedura di elaborazione del documento finito, che così diventa anche non modificabile Non si "applica" in un campo-modulo, né si può collegare un campo alla procedura della firma, se non è l'ultimo. Procedura che, in questo caso, non si sa nemmeno come finire. Uscendo dal riquadro p) non compare nulla, spostando il cursore sull'icona del salvagente (sic!) compare una scritta che dice: "ATTENZIONE: uscendo dal riquadro con questo pulsante la notificazione risulta incompleta e, conseguentemente, non può essere inviata al Garante".

Occorre un piccolo colpo di genio per pensare di fare click sull'icona della stampante. Che però non fa comparire la solita finestra di stampa di Windows, ma l'ennesima finestra fuori standard. Fatto click sul pulsante STAMPA, ecco l'avviso di errore di Windows, con la croce bianca nel tondo rosso: ATTENZIONE!!! - Errore numero: 482 - Errore descrizione: Printer error.

Questo si è verificato su due diversi computer, collegati a una stampante di rete. Ho tentato di installare il programma su una terza macchina, alla quale è collegata una stampante locale, ma

"Informazioni preliminari, premere il pulsante sinistro del mouse per proseguire"... Ma si passa direttamente al primo quadro da riempire.



Il quadro che contiene il lungo elenco delle misure di sicurezza.

Fine della procedura!

la procedura di installazione è abortita dopo pochi secondi, con il laconico avviso: "I/O Error". Il bello (si fa per dire) è che in questo modo non sono riuscito a stampare neanche il modulo vuoto, per compilarlo a mano!

La "cultura della carta"

Che da una pubblica amministrazione vengano procedure informatiche mal fatte non è una novità. D'altra parte sappiamo bene quanti "bug" si nascondano anche nei prodotti delle più grandi multinazionali del software. Ma il problema non è questo, anche se nel caso del modulo digitale i problemi tecnici sono veramente tanti.

Il punto dolente di tutta l'operazione, messo in evidenza dall'errore concettuale sulla firma digitale, è la mancanza di una "cultura informatica" moderna. Chi ha preparato il contenuto del dischetto è, probabilmente, un informatico più legato alle vecchie procedure a carattere che un utente abituale di Windows, come rivela anche la presenza del pulsante INSERISCI al posto della comparsa automatica del cursore all'inizio del primo campo da riempire. E c'è un altro elemento sul quale si deve fare una riflessione: il fatto che non sia stata adottata la procedura standard dei *wizard*, con i loro pulsanti AVANTI, INDIETRO, OK, FINE eccetera, ma si costringa l'utente a chiamare le pagine una per una premendo i rispettivi pulsanti, indica l'intenzione di trasportare sullo schermo del computer l'esatta sequenza della compilazione del modulo di carta. Ma allora il computer è inutile!

Il vantaggio della compilazione a video della modulistica è dato proprio dalla maggiore velocità e sicurezza consentite da una procedura che guida l'utente passo dopo passo, ma la procedura deve essere quella propria di un'elaborazione automatica, non la trasposizione digitale della scrittura cartacea. In altri termini, il compito che si sarebbe dovuto affidare al programmatore era di scrivere un programma per la notificazione dei trattamenti, invece gli è stato affidato il compito di trasportare sul video il modulo di carta.

Ancora una volta, dunque, la "cultura della prassi" è prevalsa sulla "cultura del risultato". E questo rimane il problema più grave di tutta la nostra pubblica amministrazione.

Rodotà: "Caro Ministro, riscriviamo l'articolo 25"

[Scoppia la polemica tra i giornalisti e il Garante dei dati personali. Motivo del contendere, il codice di autoregolamentazione previsto dall'articolo 25 della legge 675/96, elaborato da un'apposita commissione dell'ordine professionale con l'intervento di insigni giuristi e presentato il 30 dicembre scorso al Garante. Il quale, in un comunicato, afferma che "metterà subito allo studio il testo comunicato per valutarne il merito e dare così la propria valutazione, così come previsto dall'art. 25 della legge 675 del 1996".

Su un primo articolato, presentato alla fine di ottobre, il Garante aveva sollevato alcune obiezioni, recepite solo in parte nella stesura definitiva (né il primo, né il secondo testo sono stati resi pubblici, così è difficile capire esattamente quale sia la sostanza dei problemi).

Ma *l'Espresso* del 15 gennaio pubblica tre pagine di fuoco contro la legge e contro lo stesso Garante, con una "lettera aperta" di Roberto Martinelli, un riassunto del codice a firma di Pierluigi Ficoneri e un commento dell'avvocato Oreste Flammini Minuto.

Alle critiche del settimanale (condivise, con qualche "distinguo", da una buona parte della stampa italiana) risponde punto per punto un comunicato del Garante, che ricorda anche di aver già prospettato al possibilità di una revisione dell'articolo 25. Revisione che, pochi giorni dopo, viene formalmente proposta dallo stesso Garante con una lettera al Ministro di grazia e giustizia.

Nell'attuale formulazione l'articolo 25 dice:

(Trattamento di dati particolari nell'esercizio della professione di giornalista)

1. Salvo che per i dati idonei a rivelare lo stato di salute e la vita sessuale, il consenso dell'interessato non è richiesto quando il trattamento dei dati di cui all'articolo 22 è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità, nei limiti del diritto di cronaca, ed in particolare dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.[...]

2. Il Garante promuove, nei modi di cui all'articolo 31, comma 1, lettera h), l'adozione, da parte del Consiglio nazionale dell'ordine dei giornalisti, di un apposito codice di deontologia relativo al trattamento dei dati di cui al comma 1 del presente articolo effettuato nell'esercizio della professione di giornalista, che preveda misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati. Nella fase di formazione del codice, ovvero successivamente, il Garante prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto e recepire.

3. Ove entro sei mesi dalla proposta del Garante il codice di deontologia di cui al comma 2 non sia stato adottato dal Consiglio nazionale dell'Ordine dei giornalisti, esso è adottato in via sostitutiva dal Garante ed è efficace sino alla adozione di un diverso codice secondo la procedura di cui al comma 2. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 31, comma 1, lettera l). [...]

Il vero problema non è in questo articolo, ma nell'impianto stesso della legge, che prevede una disciplina complessiva (e, come più volte si è detto, di difficile applicazione) per qualsiasi trattamento di dati personali, con alcune eccezioni per i giornalisti. Applicando il dettato della direttiva europea, la legge ignora che l'informazione giornalistica è cosa ben diversa dalla raccolta e dall'elaborazione di dati a fini commerciali, di giustizia o altro. E alcune previsioni dell'articolo 25 stridono un po' nell'accostamento con l'articolo 21 della Costituzione: la stampa non può essere soggetta ad autorizzazioni o censure.

Che la stampa compia qualche "eccesso informativo" è sotto gli occhi di tutti, e dunque un codice di autodisciplina è certamente utile. Ma non si può chiedere che il Garante vada contro la legge che è chiamato ad applicare, e forse non è utile alzare il tono della polemica, anche con argomentazioni inesatte e toni esagitati. La legge è frutto di una lunga discussione parlamentare, che non si è svolta con sufficiente trasparenza e nella pressoché totale disattenzione della stampa, che si è limitata ad alzare alte grida (in parte giustificate) solo per le norme che la riguardano direttamente. Ora l'unica soluzione è cambiare la legge, e cambiarla più presto possibile.

La migliore visione del business

PT775

Colori intensi e brillanti per professionisti della grafica e utenti aziendali

Aperture grille 0,25 mm, per la massima definizione

Trattamento dello schermo ARAG®, per immagini che non disturbano la vista

Controllo delle emissioni conforme ai rigorosi standard TCO e rispondenza alle norme MPR-II e Energy Star®

La gamma di monitor a 17" di ViewSonic è stata creata pensando a coloro che vogliono sfruttare al massimo il loro investimento.

Piccole aziende, utenti che lavorano a casa usando word processor o fogli elettronici, professionisti del CAD o del DTP, appassionati di multimedia o utenti aziendali che devono creare una presentazione: per tutti, la Serie Professional e Graphics dei monitor a 17" di ViewSonic offre la soluzione ideale, combinando elevata risoluzione con alta velocità di refresh e offrendo un'eccellente qualità dell'immagine, priva di sfarfallii.

Tutti i monitor a 17" di ViewSonic sono sottoposti allo speciale trattamento dello schermo ARAG®, per non affaticare la vista.

3 anni di garanzia gratuita

La tradizione di eccellenza di ViewSonic in merito alla qualità ed affidabilità dei nostri prodotti ci permette di offrire per tutti i monitor una garanzia limitata e gratuita di 3 anni.

Monitor ViewSonic a 17"				
	Serie Professional		Serie Graphics	
Modello	**PT775**	**P775**	**GT775**	**17GS**
Dimensione CRT/area visibile	17"/16"	17"/16"	17"/16"	17"/16"
Aperture Grill/Dot Pitch	**0,25 AG**	**0,25 mm**	**0,25 AG**	**0,27 mm**
Risoluzione (max)	1600 x 1280	1600 x 1280	1600 x 1280	1280 x 1024
Risoluzione consigliata	**1600 x 1200 @ 77Hz**	**1600 x 1200 @ 76Hz**	**1280 x 1024 @ 80Hz**	**1024 x 768 @ 86Hz**
Ampiezza di banda input video	200 MHz	200 MHz	135 MHz	86 MHz

Tutti i modelli sono pienamente compatibili con PC o Mac.

Per ulteriori dettagli e per ricevere una guida gratuita alla scelta del monitor, chiamate:

MITAS
tel. 0471.540940
TEST FIRENZE
tel. 055.30171

ViewSonic®

ViewSonic Central Europe
Otto-Brenner Strasse 8,
47877 Willich, Germania
tel. 0049.2154.91880 fax 0049.2154.918810
www.viewsonic.com

I riconoscimenti e le caratteristiche qui sotto indicati sono relativi alla gamma di prodotti ViewSonic e non necessariamente al prodotto qui mostrato.

PT813 - 7/97 · PC Direkt P810 - 12/96 · PT775 - 6/97 · PT770 - 9/96 · P815 - 4/97 · 17PS - 5/96 · PT775 - 6/97 · 17GA - 9/96 · P810 - 2/97