

ASSOCIAZIONE CULTURALE  
PER LO STUDIO DEL DIRITTO

# techne

EDIZIONE SPECIALE PER IL  
XXIX CONGRESSO NAZIONALE FORENSE

Bologna 13-16 novembre 2008

*Direttore responsabile*

GLAUCO RIEM

*Redazione*

STEFANO CORSINI  
FRANCESCO MIRABELLI  
LUCA ZENAROLLA  
PAOLO VICENZOTTO

Vicolo Chiuso, 5 - 33170 Pordenone  
tel. 0434 522866 - fax 0434 246429 [rivistatechne@yahoo.it](mailto:rivistatechne@yahoo.it)  
[www.rivistatechne.it](http://www.rivistatechne.it)

*Realizzazione editoriale*

Forum, Editrice Universitaria Udinese srl  
Via Palladio, 8 - 33100 Udine  
[www.forumeditrice.it](http://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; già 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**

Membro del CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) già direttore generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia

**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

**PAOLO VICENZOTTO**

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

## **Hanno collaborato a questo numero**

**GIORGIO BATTAGLINI, DAVID D'AGOSTINI, GIULIA FERRARESE, EMANUELE FORNER, DARIO OBIZZI, FABRIZIO PETTOELLO, GLAUCO RIEM, CARLA SECCHIERI, MARCO VIANELLO**

## **SOMMARIO**

<b>EDITORIALE</b> GLAUCO RIEM	<b>5</b>
<b>DA MIHI FACTUM DABO TIBI 'TELEMATICUS' IUS</b> GLAUCO RIEM	<b>8</b>
<b>UN'AVVOCATURA DIGITALE DI RESPIRO EUROPEO</b> MARCO VIANELLO	<b>12</b>
<b>L'OPEN SOURCE NEGLI STUDI LEGALI</b> DAVID D'AGOSTINI	<b>18</b>
<b>PROCESSO CIVILE TELEMATICO TRA ILLUSIONE E NUOVE REALTÀ OPERATIVE</b> CARLA SECCHIERI	<b>27</b>
<b>SICUREZZA INFORMATICA FRA PARANOIA E VIRTÙ</b> GIORGIO BATTAGLINI	<b>32</b>
<b>UN NUOVO APPROCCIO ALL'USO DEI SOFTWARE DI GESTIONE DELL'ATTIVITÀ FORENSE E DEGLI ORDINI DEGLI AVVOCATI</b> FABRIZIO PETTOELLO	<b>38</b>
<b>GLI STANDARD OPERATIVI E LE LIBERTÀ INDIVIDUALI NEL PROCESSO CIVILE TELEMATICO</b> EMANUELE FORNER	<b>43</b>
<b>LA FIRMA DIGITALE E LA POSTA ELETTRONICA CERTIFICATA</b> DARIO OBIZZI	<b>54</b>
<b>I LIMITI DI UTILIZZABILITÀ DEI DATI NELL'AMBITO DEL PROCESSO</b> GIULIA FERRARESE	<b>61</b>
<b>La vignetta</b> di FEDERICO CECCHIN	<b>74</b>

## EDITORIALE

**Giulio Riem**

Techne dedica questo numero alla “digitalizzazione” della professione forense, dello studio legale ed agli aspetti problematici nell’uso delle tecnologie nell’avvocatura.

Sono passati diversi anni dalla pubblicazione del DPR 123/01 sulle regole relative al processo telematico (G.U. n. 89 del 17 aprile 2001) ed è stato recentemente pubblicato il DM il 17 luglio 2008, “*Regole tecnico-operative per l’uso di strumenti informatici e telematica nel processo civile*” corredato da un ponderoso Allegato A), che sostituisce il precedente DM del 14 ottobre 2004, n. 167. Tale decreto sarà probabilmente fatto oggetto di una serie di convegni che l’Avvocatura organizzerà prossimamente e di cui, in questa rivista, si darà conto.

Finita dunque la sperimentazione nelle sedi a suo tempo indicate dal Ministero della Giustizia, molti ordini professionali ed enti si sono abilitati come “*Punti di accesso*” come si può constatare in Internet al link: <http://www.processotelematico.giustizia.it/pdapublic/index.jsp?id=5&pid=5&sid=1>

I tempi della digitalizzazione dell’avvocato sembrano essere maturi e si può pensare possibile un avvio non più sperimentale, ma “ordinario” del processo telematico e ciò anche grazie ad una serie di importanti iniziative intraprese dagli Ordini degli avvocati del Nordest, prima fra tutte quelle di Pordenone ed Udine.

In tali sedi è stato infatti avviato un sistema condiviso di gestione digitale della professione che si basa sull’utilizzo di una *chiave elettronica* (*Business Key*), utilizzata anche da Lextel, e ciò grazie a convenzioni stipulate tra gli

Ordini con le locali Camere di Commercio ed Infocamere.

Il sistema permette di usufruire dei servizi di Posta Elettronica Certificata (P.E.C.) da usare nell'invio di comunicazioni informatiche a norma ed altresì per sottoscrivere, con dispositivi di firma digitale, atti e documenti informatici ai sensi del D.Lgs. 182/05 ed anche per ricevere i biglietti elettronici di Cancelleria spediti dagli Uffici Giudiziari con risparmi (ripetibili ogni anno) che possono sfiorare anche i settantamila euro per Cancelleria.

Naturalmente per stare nel processo telematico gli avvocati dovranno avere una Casella di Posta Elettronica Certificata per il Processo Telematico (C.P.E.C.P.T.) secondo i principi dettati dall'ordinamento.

Una rivoluzione necessaria che implica solo un impegno dell'Avvocatura ed un approccio "possibilista" dell'avvocato.

Se ci si consente un paragone la filosofia di fondo a cui si informa l'approccio info-telematico è la stessa che ha portato gli "scriba" dall'utilizzo dello scalpello e delle tavole di pietra o di creta a quello dell'inchiostro e della pergamena. Sembra allora venuto il tempo che dalla scrittura sulla carta si passi a quella sul bit.

Ma vediamo nel dettaglio.

In apertura GLAUCO RIEM prospetta una visione futuristica della gestione "automatizzata" della Giustizia completamente gestita dalla "macchina" dotata di sistemi esperti che tengano conto della sterminata conoscenza acquisita dall'umanità in questa materia ove l'Uomo-Giuridico sia chiamato solo ad implementare quelle conoscenze che "informano" l'esperienza del sistema.

MARCO VIANELLO, più prammaticamente, indica la via di un'avvocatura digitale proiettata nell'Europa in una E-Justice Strategy ove l'approccio e l'uso delle tecnologie necessariamente coinvolga tutte le parti che a diverso titolo approcciano alla Giustizia.

DAVID D'AGOSTINI ci impegna in una dotta disquisizione sui temi dell'open-source e illustra le opportunità che tali applicazioni offrono all'avvocato digitale.

CARLA SECCHIERI parla del processo telematico nella sede sperimentale del Tribunale di Padova delle traversie di allora e del cauto ottimismo di oggi.

GIORGIO BATTAGLINI affronta, con una sottile e realistica ironia, i temi della sicurezza informatica che tanto occupano l'attività dell'avvocato ai fini sì della tutela della riservatezza, ma anche degli aspetti meramente pratici della cosiddetta security chian che, nel processo telematico, è uno dei temi forse più caldi.

FABRIZIO PETTOELLO illustra le sue fondate teorie sull'approccio metodologico agli applicativi informatici di gestione dell'attività "seriale" forense e degli stessi Ordini degli Avvocati del Triveneto con un occhio attento alla verifica della "produttività" sorta di controllo di gestione a futura memoria.

EMANUELE FORNER affronta invece con un taglio asciutto i temi legati agli standard operativi del processo telematico dandoci una ferma opinione in merito alle libertà individuali così come scaturiscono dall'intento del legislatore che ha scritto la norma e come invece appaiono nella realtà.

DARIO OBIZZI tratta il tormentato e mai abbastanza esaurito tema della firma digitale e ciò anche alla luce dell'utilizzo della posta elettronica certificata e della rilevanza giuridica dei "nuovi sistemi" di gestione documentale che coinvolgono l'Avvocatura.

GIULIA FERRARESE delinea i limiti di utilizzabilità dei dati personali nell'ambito processuale e prospetta i contrapposti interessi tra la protezione delle informazioni ed il diritto alla difesa, delineando le numerose problematiche legate ad un illecito utilizzo delle stesse con notazioni sull'utilizzabilità dei documenti che le contengono. Il tutto è corredato da brevi cenni sull'evoluzione in punto della giurisprudenza.

FEDERICO CECCHIN, nella sua vignetta, illustra, infine, sua personale interpretazione della "mischia info-processuale" fra avvocati misonoisti ed informatici.

## DA MIHI FACTUM DABO TIBI 'TELEMATICUS' IUS

### **Giulio Riem**

Docente di Diritto delle nuove tecnologie, docente del Ministero dell'Interno e della Giustizia

L'ipotesi più spinta è quella secondo la quale chi chiede Giustizia non stia più di fronte ad un *Praetor* al quale esporre la propria vicenda, ma ad un elaboratore dotato di un *programma* che utilizza algoritmi *cellulari* "in grado di *ragionare* direttamente in linguaggio naturale", basati su architetture logiche parallele, dotati altresì di sistemi di coscienza denominati "insight" di tipo MIMD (Multiple Instruction stream Multiple Data stream) che permettono di utilizzare quelle "*conoscenze ulteriori, che restano implicite nella comunicazione umana o fanno parte della comune esperienza*". Tale programma sarà necessariamente fornito di un sistema esperto e di "basi di conoscenza" "pubbliche e private" - prodotte in secoli di esperienza e "dotate" di quella saggezza tipica dello studioso delle discipline umane e giuridiche. Tale elaboratore, in breve, nel rispetto della *vigente procedura*, del contraddittorio sicuramente telematico, del diritto alla difesa e del *giusto processo*, pronuncerà la *soluzione* della controversia e ciò, naturalmente, on-line.

### **Fantadiritto?**

Attualmente senza dubbio sì, ma la risposta potrebbe essere no di qui a breve. Non possiamo, per altro verso infatti, non ricordare che il 24 marzo 1905, Giulio Verne finì di scrivere *Dalla terra alla luna*, romanzo fantascientifico nel quale l'autore *anticipava* modalità e problematiche risolte ed affrontate dall'uomo nella missione Apollo 8 che, nel luglio del 1969, (cioè circa tre generazioni dopo la pubblicazione del libro) portò un *terrestre* a camminare sul suolo del proprio satellite.

Verne *indovino* con esattezza la nazione che avrebbe effettuato il primo lancio, il mese in cui esso sarebbe avvenuto, il numero degli uomini che formavano l'equipaggio, il sistema ed il luogo di rientro sulla terra: ammaraggio sull'Oceano Pacifico.

Pur privi di sfera di cristallo nella quale leggere *auspici* ci sentiamo di dire allora, senza timore di essere in futuro smentiti, che - piacendo a chi l'umanità governa - si potrà giungere - in tempi socialmente brevi - a realizzare un Sistema Automatico di Amministrazione della Giustizia (*Automatic System of Justice Administration*) ove attraverso la rappresentazione del proprio *caso*, in opportuni "modelli" (DTD), preventivamente predisposti, ciascuno potrà ottenere una Giustizia veloce, rapida il cui "prodotto" (soluzione/sentenza) sarà anche immediatamente eseguibile attraverso "sistemi info-telematici" che potranno utilizzare, nei confronti della parte soccombente, *mezzi coercitivi informatici* a fini esecutivi (coattivo prelievo elettronico di somme ovunque esse si trovino depositate) e comminare *pene informatiche* (divieto di operare e/o collegarsi alla rete; pubblicazione della *decisione on-line* e suo invio attraverso poste elettroniche a operatori selezionati che, in ragione dell'attività svolta, la debbano conoscere).

### **Sarà "giusto" arrivare a ciò?**

Riteniamo di dover dare a tale interrogativo una risposta affermativa.

Ed allora dovrà essere rivisitata la nozione di giustizia, di processo, di risarcimento, di esecuzione, di pena e necessariamente di tutti i lemmi che ruotano intorno al pianeta dell'amministrazione giudiziaria.

Questo pensiero sarà poi utile per *reformulare* il modo di svolgere un'attività antica quanto il vivere sociale: amministrare le liti fra le parti *sedandone* l'aggressività delle pretese.

Questo sforzo dovrà comunque essere sottoposto alla coscienza degli individui che compongono la società.

Tutti allora si dovranno nuovamente interrogare sui significati di morale, di etica, del *neminem laedere* e ciò, non solo per meglio razionalizzare i sistemi che utilizzano le nuove tecnologie nella gestione della giustizia, ma - come da tempo e da più parti si chiede - per riaffermare semplicemente i

principi di civiltà, di pacifica convivenza e di una reciproca indefettibile ed inalienabile tolleranza.

Un *algoritmo di soluzione* della Giustizia, che si esprime e formalizza nel continuo, infatti non potrà mai *funzionare* se i suoi ideatori non siano dotati di tutte quelle esperienze e *qualità* necessarie a fare di un uomo un Uomo. La soluzione di questo problema postula poi comunque la soluzione di molti altri problemi che gli sono connessi, ad esempio: nel mondo della *giustizia automatizzata* come si procederà alla creazione, razionalizzazione e uniformità delle leggi?

La Giustizia Telematica, anche quella sperimentale, naturalmente è completamente gestita dall'uomo che, se pur attraverso sistemi complessi, si serve dell'elaboratore e delle reti telematiche per razionalizzare e snellire l'attività giudiziaria che, nella società dell'informatica e dell'informazione, deve dare risposte sempre più adeguate e rapide (vedasi in proposito la dizione dell'art. 17 della direttiva 31/2000 CE ed il D.L.vo 70/03). Tali sistemi, come vedremo, sono noiosamente e puntigliosamente descritti con termini sempre più tecnici e di difficile comprensione che mettono a dura prova la *nuova mente* che il giurista dovrà acquisire nell'approccio a questo scenario futuribile prego di fermenti ed istanze che sommano alla conoscenza delle discipline giuridiche imprescindibili abilità nell'uso degli strumenti informatici e delle logiche che li informano. In proposito ci preme ricordare la pubblicazione del volume *Il glossario del diritto delle nuove tecnologie e dell'e-Government*, Giuffrè, Milano, 2007, ove si affronta sistematicamente e per la prima volta il ventennale problema della nuova terminologia informatico-giuridica:

[http://www.giuffre.it/servlet/page?\\_pageid=68&\\_dad=portal30&\\_schema=PORTAL30&APCodVolume=57663](http://www.giuffre.it/servlet/page?_pageid=68&_dad=portal30&_schema=PORTAL30&APCodVolume=57663)

Le legittime aspettative allora trovano sempre più riscontro in una recente, doviziosa e puntuale legislazione che detta regole giuridiche che indicano precisi adempimenti e procedure tecnico-informatiche che possano garantire quelle certezze che il diritto imprescindibilmente postula per poter attribuire la necessaria validità agli atti compiuti attraverso lo strumento informatico. La pietra angolare del sistema normativo che in Italia ha reso possibile tale rivoluzione è senza dubbio il secondo comma dell'art. 15 della legge 15 marzo 1997, n. 59, pubblicata sulla Gazzetta ufficiale n. 63 del 17 marzo

1997 che recita " *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. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni*".

A questa semplice rivoluzionaria dizione sono seguite numerosissime altre norme e regolamenti tesi a soddisfare una sempre più crescente volontà di amministrare la *res publica* privilegiando il metodo info-telematico e ciò appunto per soddisfare ad esigenze di rapidità, efficienza ed imparzialità. Tale modalità viene sinteticamente indicata con il termine anglosassone e-Government (*governo elettronico*).

La summa di tutte queste norme può essere considerato il DPR del 13 febbraio 2001, n. 123, pubblicato sulla Gazzetta Ufficiale n. 89 del 17 aprile 2001: "Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti" che oggi completata dello strumento regolamentare - così come era nella previsione del comma 3 dell'art. 3 - è il più complesso sistema di gestione amministrativa dello stato italiano per utilizzare ogni tipo di previsione tecnico -informatica- giuridica che è stata approvata nel nostro ordinamento giuridico e che rende possibile una quasi integrale conduzione del processo civile, amministrativo e contabile. Altro fenomenale strumento legislativo risulta essere il Codice dell'amministrazione digitale (D.Lgs 82/05 così come modificato dal D.Lgs 159/06. Ciò obbliga l'amministrazione in genere e quella giudiziaria ad adottare complessi sistemi info-telematici e, per converso, impone ad ogni professionista che presti la sua opera in giudizio a rivisitare completamente le sue abitudini di lavorare.

Questo volume è allora dedicato a chiarire ai Colleghi Avvocati alcuni dei molti aspetti problematici della nuova arte forense dell'evo informatico.

## UN'AVVOCATURA DIGITALE DI RESPIRO EUROPEO

### **Marco Vianello**

Membro della Information Technology Law Committee del C.C.B.E. e segretario dell'Unione Triveneta dei Consigli dell'Ordine degli Avvocati

Riporto alcune notizie di giugno 2008<sup>1</sup>:

- il 23% dei computer italiani è infetto; siamo al 3° posto in Unione Europea e al 10° nel mondo per diffusione di virus informatici;
- dal 2001 al 2008 la Polizia postale ha chiuso 177 siti pedopornografici;
- l'11% del minorenni intervistati ha dichiarato di aver avuto, durante la navigazione in rete, contatti con pedofili o presunti tali;
- il 52% degli utenti on-line ha dichiarato di aver subito almeno un tentativo di accesso non autorizzato.

Come dire che l'utente medio beve e nuota abitualmente nelle acque del Nilo, con le ovvie probabilità di incorrere in pericoli per la salute.

Le aziende di grandi dimensioni hanno approntato misure di protezione adeguate, investendo molto. Le piccole e medie imprese mediamente no. E la media dei nostri studi?

Molte delle soluzioni stanno senza dubbio normativamente già nel codice della privacy<sup>2</sup>.

La Commissione Information Technology Law del CCBE<sup>3</sup> nel 2005 ha approntato un opuscolo - attualmente in corso di aggiornamento - che tenta di offrire alcune linee guida per "l'Avvocato digitale". Ma ormai, seppure in alcuni casi solo in parte, siamo tutti, poco o tanto, digitali.

Voglio citarvi solo un esempio, attinto totalmente "Etica, informatica, diritto" di Claudio Sarra nell'edizione curata da Paolo Moro<sup>4</sup>. L'autore fa emergere un problema di natura deontologica, sul quale può impattare quotidianamente il professionista forense nell'utilizzo degli strumenti informatici.

Solleva il problema dei metadati, delle informazioni nascoste che talvolta

consapevolmente o, più volte, inconsapevolmente si inviano a terzi. L'invio alla controparte per esempio di file contenenti traccia delle informazioni scambiate in due, tre, cinque invii tra avvocato e cliente. La giurisprudenza forense anglosassone si è già occupata dell'argomento, oscillando tra violazione deontologica del ricevente che utilizza informazioni alle quali l'accesso non è autorizzato e violazione deontologica del mittente che viola così la riservatezza tra cliente e avvocato e l'obbligo di aggiornamento, nel saper utilizzare gli strumenti. Per terminare con decisioni più recenti che criticano entrambi i comportamenti<sup>5</sup>.

Certamente non saranno censurabili in equal misura comportamenti tutt'al più colposi (del secondo) e condotte probabilmente volontarie (del primo). L'aggiornamento, comunque, evidentemente non deve riguardare più solo le conoscenze giuridiche in senso stretto, ma anche gli attrezzi utilizzati. Più gli strumenti sono complessi più l'Avvocato deve obbligatoriamente stare al passo; senza scusanti.

A giugno 2008 - ma il documento è stato reso noto solo di recente - la Commissione europea ha rivolto al Consiglio osservazioni, promuovendo in ambito europeo una vera e propria strategia dell'"Electronic Justice"<sup>6</sup>. In due parole che cosa ci propone l'E-Justice Strategy? Alcuni principi e propositi importanti:

1. aiutare la giustizia a essere amministrata con più efficienza attraverso l'Unione europea a favore del Cittadino;
2. creare una rete interoperativa europea che ponga come strumento primario la firma digitale, strumento adeguato per garantire immodificabilità e autenticazione di atti, anche ufficiali; tra le reti già esistenti è possibile visitare il sito [www.juradmin.eu](http://www.juradmin.eu), il portale comune dei casi nazionali della giustizia amministrativa (dell'Italia per esempio sono inseriti i casi del Consiglio di Stato), oltre alla rete europea dei notai e il registro dei testamenti ([www.cnue.be](http://www.cnue.be));
3. creare procedure, software, strumenti informatici in genere che garantiscano l'effettività dell'interoperatività, nonché la facile comprensione tra sistemi di firma digitale e di autenticazione in genere.

Il piano si svilupperà dal 2008 al 2013 e punterà all'agevolazione dell'accesso alla Giustizia da parte di privati, soprattutto vittime di reato, così come

delle imprese, senza barriere di alcun tipo e promuovendo la cooperazione tra tutte le Autorità e i soggetti (nel rispetto delle peculiarità delle funzioni) che si occupano di Giustizia.

Il tutto naturalmente attraverso Internet e un portale dedicato interlinguistico, sì da favorire la conoscenza di diritti e opportunità anche al di fuori del proprio Paese d'origine.

Si punterà, inoltre, ai pagamenti on-line dei diritti delle Corti, così come all'innoltramento delle richieste di attestazione di pendenze a carico.

Nel 2009 sarà diffuso tra gli stati membri un software per scambiare dati dei procedimenti penali.

Si pensi che già nel primo mese di sperimentazione Francia e Germania sono riuscite a scambiare tanti dati quanto era avvenuto complessivamente nei 10 anni precedenti.

Naturalmente sarà tecnicamente garantita la riservatezza delle comunicazioni, facilitato l'utilizzo della videoconferenza, così come saranno implementati strumenti di aiuto alla traduzione dei testi e creato anche un database di traduttori e interpreti disponibili e suddivisi per aree territoriali.

Per meglio comprendere la portata degli interventi del progetto il settore penale costerà approssimativamente 15 milioni di euro nel 2008 e i due settori (civile e penale) complessivamente all'incirca 26 milioni di euro per l'anno corrente.

In calce al testo della Commissione sull'E-Justice Strategy c'è una tabella con una sorta di cronoprogramma del progetto: dalla lettura di questo schema si ricava che per esempio lo studio e la valutazione della situazione attuale della firma digitale occuperà il periodo dal 2009 al 2011, mentre per l'interconnessione dei registri dei fallimenti si prevede la realizzazione entro il 2009.

Non so se si tratterà di un progetto fatto solo di "bit" (non certo solo sulla carta!), ma penso che l'iniziativa della Commissione europea che, come sappiamo, è istituzione di persone e, pertanto, indipendenti da ogni vincolo di natura politica ed economica, sia il segnale di una certa sensibilizzazione. Anche in sede di CCBE a Brussels si è accolta con molto favore questa iniziativa, così come già è avvenuto per iniziative di archivi di dati come Caselex<sup>7</sup>, e Cibex<sup>8</sup>.

Analogamente è avvenuto di recente con PenalNet<sup>9</sup>, portale che agevolerà l'interconnessione di tutti i soggetti dell'Unione (compresi 300 avvocati in Italia e molti altri nel resto d'Europa) che si occupano di diritto penale. Il CCBE, inoltre, da tempo sta cercando di indurre i Consigli Forensi nazionali ad adottare una smart card comune, con il logo del CCBE da un lato e dall'altro il logo nazionale di appartenenza dell'iscritto, che funga prima di tutto da certificato di ruolo, ma che possa anche funzionare con un software comune a tutta Europa per accedere a servizi e banche dati di libero accesso per l'Avvocatura, così come a pagamenti e a molte altre funzioni nazionali o sopranazionali.

Sono certo che anche in ambito nazionale, grazie alle nostre Istituzioni centrali, si potrà fare molto, oltre ad aderire e sollecitare quanto appena descritto: si pensi alla possibilità di istituire un polo unico nazionale per il processo telematico, ma anche allo studio di strumenti informatici comuni a tutta l'Avvocatura, così come hanno già realizzato i Notai, che ci hanno preceduto e insegnato la strada<sup>10</sup>. Non dimentichiamo neppure che sarebbe auspicabile, come l'Unione Triveneta dei Consigli dell'Ordine degli Avvocati afferma da sempre, acquisire il dominio [www.avvocatura.it](http://www.avvocatura.it), così come già è avvenuto per la magistratura ([giustizia.it](http://giustizia.it)) e il notariato ([notariato.it](http://notariato.it)), riuscendo così finalmente a uniformare e identificare la classe forense, abilitando il dominio alla posta elettronica certificata, creando un sotto-dominio di posta certificata dedicata al processo telematico<sup>11</sup>, così come richiesto dalle recentissime regole tecnico-operative emanate dal Ministero<sup>12</sup>.

La speranza è anche che vi siano la volontà e la capacità di realizzare in tempi moderni convenzioni con sistemi che consentano l'accesso a banche dati nazionali comuni con tutti i soggetti della giurisdizione (si pensi per esempio a Italgireweb<sup>13</sup>), ma anche alle banche dati pubbliche, che dovrebbero essere per tutti noi accessibili on-line, senza costi di intermediari.

Siamo Avvocati, talvolta non troppo digitali, ma dobbiamo saper riconoscere le realtà che ci circondano e avanzano, con capacità - questa volta - non solo di adattamento, ma oggi più che mai di anticipazione dei tempi, rinnovandoci per migliorare i nostri servizi, riabilitando sempre più la nostra

immagine a favore del Cittadino e della Giustizia e - perché no - guardando a un profilo moderno della Professione, che punti anche a una miglior accettazione dell'Avvocato da parte dei nostri potenziali clienti e degli altri soggetti della giurisdizione.

Io penso sinceramente che questi strumenti ci possano aiutare a fornire servizi moderni e migliori, ottenendo nel contempo una migliore considerazione complessiva.

#### NOTE

<sup>1</sup> Tratte da un'intervista a Maurizio Masciopinto, direttore della Divisione Investigativa della Polizia Postale e delle Comunicazioni, in occasione della presentazione della prima Settimana nazionale della sicurezza in rete, iniziativa partita il 7 giugno scorso e patrocinata dal Ministero dello Sviluppo Economico e promossa dall'Unione Nazionale Consumatori, con la collaborazione di Polizia Postale, Abi Lab, SicuramenteWeb, Skuola.Net e Agr, e con il sostegno di Microsoft.

<sup>2</sup> Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

<sup>3</sup> Consiglio degli Ordini Forensi d'Europa - [www.ccbe.org](http://www.ccbe.org).

<sup>4</sup> Etica, Informatica, Diritto, a cura di Paolo Moro, 2008, in [http://www.francoangeli.it/Ricerca/Scheda\\_Libro.asp?ID=15907&Tipo=Libro&titolo=Etica+informatica+diritto](http://www.francoangeli.it/Ricerca/Scheda_Libro.asp?ID=15907&Tipo=Libro&titolo=Etica+informatica+diritto).

<sup>5</sup> cfr. O'Neal, Nicole, in Florida Bar Journal, 1 dic. 2007, pubblicato in [http://goliath.ecnext.com/coms2/gj\\_0199-7311833/Metadata-the-future-impact-of.html](http://goliath.ecnext.com/coms2/gj_0199-7311833/Metadata-the-future-impact-of.html) e anche, riguardante aspetti più propriamente disciplinari, Yi, Jonathan, in Florida Bar Journal, 1 dic. 2007, pubblicato in [http://goliath.ecnext.com/coms2/gj\\_0199-7311832/The-effect-of-disciplinary-determinations.html](http://goliath.ecnext.com/coms2/gj_0199-7311832/The-effect-of-disciplinary-determinations.html).

<sup>6</sup> "Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee - Towards a European e-Justice Strategy; COM(2008)329final"; in <http://register.consilium.europa.eu/pdf/en/08/st10/st10285.en08.pdf>

<sup>7</sup> [www.caselex.com](http://www.caselex.com): archivio di casi europei e nazionali dei paesi dell'Unione Europea.

<sup>8</sup> <http://www.cybex.es/defaulten.aspx>, database che raccoglie decisioni e documenti in ambito di prove digitali. L'Unione Triveneta dei Consigli dell'Ordine degli Avvocati ha stretto un accordo di collaborazione e il Collega avv. Giorgio Battaglini è delegato all'invio almeno mensile di documenti, che hanno arricchito nei mesi appena trascorsi la documentazione italiana presente nell'archivio.

<sup>9</sup> Per maggiori informazioni si può consultare <http://cnfpec.it/files/5239/N.%2022-C-2008%20%20%20progetto%20Penalnet.PDF>.

<sup>10</sup> Costituendo una società ad hoc, la Spa Notartel, la quale sviluppa strumenti informatici per la classe notarile.

<sup>11</sup> Per esempio [www.avvocatura.pro](http://www.avvocatura.pro).

<sup>12</sup> Decreto 17 luglio 2008 - Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, in sostituzione del decreto del Ministro della giustizia 14 ottobre 2004, pubblicato nel supplemento ordinario n. 167 alla Gazzetta Ufficiale n. 272 del 19 novembre 2004. (GU n. 180 del 2-8-2008 - Suppl. Ordinario n.184).

<sup>13</sup> [www.italgiure.giustizia.it](http://www.italgiure.giustizia.it).

## L'OPEN SOURCE NEGLI STUDI LEGALI

### **David D'Agostini**

Consigliere del Consiglio dell'Ordine degli Avvocati di Udine, componente della Commissione informatica dell'Unione Triveneta dei Consigli degli Ordini degli Avvocati, docente di Diritto delle nuove tecnologie all'Università degli studi di Udine

### **Premessa**

Il termine "*software*" indica genericamente un programma che funziona su un computer; il software può essere classificato secondo diverse caratteristiche: si distingue tra sistemi operativi (Windows, Linux, MacOS, etc.) e programmi applicativi (Word, Openoffice Writer, Acrobat Reader, etc.) o secondo la funzionalità (programmi di videoscrittura, per l'utilizzo di fogli elettronici, browser per navigare su internet, client di posta elettronica, software gestionali, etc.), oppure in base al linguaggio di programmazione e così via. Per quanto d'interesse in questa sede, a seconda del grado di libertà concesse agli utenti, il software viene classificato in queste categorie.

### ***Software proprietario***

Il codice sorgente di un software proprietario solitamente non viene diffuso e viene tenuto segreto. Vi sono molteplici forme di distribuzione, tra le quali le più diffuse sono le seguenti.

- *Commerciale*: software rilasciato su licenza dietro il pagamento di un corrispettivo per l'uso da parte dell'utente. Alcune volte l'accettazione della licenza avviene per il solo fatto di aprire la confezione, che equivale alla lettura e accettazione delle clausole contrattuali leggibili all'esterno della scatola, ovvero con l'accettazione esplicita delle clausole durante l'installazione del prodotto. Il software commerciale non consente la distribuzione libera ad altri utenti, anche se interni al medesimo studio, ma è possibile installare il software sui computer di altri utenti solo se vengono acquistate le relative licenze.
- *Demo* (o versioni di prova): software di tipo commerciale che il fornitore

distribuisce a titolo gratuito in versione dimostrativa, inibendo o limitando alcune funzioni rispetto alla versione commerciale. Generalmente questo tipo di software non può essere copiato e distribuito liberamente.

- *Shareware*: pacchetti software che si possono ottenere gratuitamente, in cui il programma, a differenza delle demo, si presenta completo delle funzionalità, ma con la possibilità di essere provato per un limitato periodo di tempo. Allo scadere del periodo di prova, è necessario pagare un corrispettivo, altrimenti il programma cessa di funzionare.
- *Ad-ware*: software gratuito che per l'utilizzo visualizza banner pubblicitari o installa nel computer dell'utente programmi spyware (software che raccolgono e inviano dati per usi solitamente commerciali). I costi di licenza sono così coperti in via indiretta dalle aziende inserzioniste.
- *Freeware* (da non confondere con Free Software): software commerciale completo che viene concesso gratuitamente in uso, senza distribuzione del codice sorgente, solitamente per motivi promozionali. In questo caso, l'aggettivo "free" è usato nel solo significato di gratuito e non di libero, al contrario che nell'espressione "free software".

### **Software Libero e Aperto**

Si tratta della categoria di cui fanno parte le due denominazioni di "free software" e software "open source".

### **Software Libero (Free Software)**

Tale dizione indica i programmi distribuiti con licenze elaborate dalla Free Software Foundation (FSF) secondo cui: *l'espressione "software libero" si riferisce alla libertà dell'utente di eseguire, copiare, distribuire, studiare, cambiare e migliorare il software. Più precisamente, esso si riferisce a quattro tipi di libertà per gli utenti del software:*

- *Libertà di eseguire il programma, per qualsiasi scopo (libertà 0)*
- *Libertà di studiare adattare il programma alle proprie necessità (libertà 1)*
- *Libertà di ridistribuire copie del programma (libertà 2)*
- *Libertà di migliorare il programma e distribuirne i miglioramenti (libertà 3)*

L'accesso al codice sorgente da parte dell'utente è un prerequisito di almeno due delle quattro libertà menzionate.

### **Software Open Source**

Tale dizione è frutto di una rivisitazione delle proposte della Free Software Foundation a opera della Open Source Initiative (OSI), con l'obiettivo di avvicinare lo sviluppo del software libero a quello sviluppato dalle imprese commerciali.

I punti fondamentali delle licenze open source sono:

- distribuzione aperta (libera e gratuita): *diritto di fare copie del programma e di ridistribuirle liberamente;*
- accesso aperto (al codice sorgente): *il codice dev'essere disponibile a costo di distribuzione e non obnubilato;*
- modificabilità aperta: *diritto di poter intervenire sul programma e modificarlo* (non si obbliga né si vieta che la licenza si propaghi al lavoro derivato).

### **Public Domain Software**

Infine vi sono i programmi che, per concessione dell'autore, non contengono alcuna indicazione di copyright, tanto da occultarne anche la paternità (aspetto "morale" del diritto d'autore); è perciò possibile utilizzarli, riprodurli e diffonderli liberamente, ma anche eventualmente modificarli e inserirli all'interno di altro software, in quanto non sussiste alcun limite derivante da licenza.

### **Computer e software negli studi legali**

Il computer è uno strumento di lavoro ormai indispensabile in uno studio legale e può essere utilizzato non solo per redigere gli atti, ma anche per navigare su internet, scaricare e inviare la posta elettronica, compiere ricerche giuridiche, gestire le pratiche dei clienti e, in generale, elaborare, salvare e archiviare qualsiasi tipo di dato.

In questi anni un numero sempre maggiore di avvocati sta apprezzando in maniera crescente le potenzialità dell'informatica e della telematica. Ma di quali software necessita un avvocato per il proprio lavoro?

Volendo ridurre la questione ai minimi termini, potremmo pensare che occorranza:

- 1) naturalmente un sistema operativo, ossia il software di base in grado di far funzionare il pc;
- 2) un pacchetto di programmi per elaborare documenti (files di videoscrittura, tabelle, etc.);
- 3) un programma per navigare su internet e uno per la posta elettronica;
- 4) un software gestionale (con clienti, udienze, agenda, scadenze, etc.).

Omettiamo in questa sede i software per la scansione dei documenti o per la masterizzazione di supporti ottici o per il funzionamento di periferiche in generale (solitamente forniti insieme a queste ultime); oppure programmi di messaggistica istantanea o di comunicazione a voce su internet (VOIP, come skype).

Nell'ultimo decennio il mercato del software (non solo quello indirizzato alle realtà professionali, beninteso) si è sviluppando in maniera significativa verso software non proprietario.

Viene, quindi, da chiedersi se un avvocato possa, ed eventualmente in quali termini, dotarsi dei programmi elencati facendo riferimento al software libero e aperto.

### **Sistema operativo**

Il sistema operativo più diffuso tra i personal computer è senza dubbio "*Windows*" prodotto e licenziato dalla Microsoft; le statistiche dicono che anche la maggior parte degli elaboratori presenti sulle nostre scrivanie ha in dotazione tale software di base.

Non mancano i colleghi che hanno deciso di percorrere la strada del Mac della Apple (con sistema operativo MacOS, anch'esso proprietario), né coloro i quali stanno scoprendo con soddisfazione i sistemi operativi open source tra i quali il più noto risulta "*Linux*".

In realtà non esiste un'unica versione di Linux, ma diverse distribuzioni create da comunità di sviluppatori o società, che scelgono, preparano e compilano i pacchetti da includere; tutte le distribuzioni condividono il nucleo Linux, mentre si differenziano tra loro per i pacchetti di strumenti e applicazioni software (tutti comprendono l'installazione guidata del sistema) e per i servizi di assistenza e manutenzione offerti.

Recentemente hanno cominciato a diffondersi anche distribuzioni (chiamate "live") eseguibili direttamente da supporto (CD-ROM, DVD) senza che sia richiesta l'installazione sul proprio hard disk.

Tra le distribuzioni più diffuse, soprattutto per la facilità d'installazione e d'utilizzo e la frequenza degli aggiornamenti, non si può non citare "Ubuntu"; tale sistema operativo fornisce un'interfaccia grafica intuitiva e allo stesso tempo completa. I suoi punti di forza sono l'ottimo riconoscimento dell'hardware e una serie di programmi per la navigazione in internet, la gestione dei documenti, la comunicazione, etc.

Una caratteristica di Ubuntu molto importante, comune alle distribuzioni Linux, è la sua bassa vulnerabilità a programmi dannosi come virus, adware, spyware o malware: nella maggioranza dei casi il programma nocivo non produce danni al di fuori della directory dell'utente infettato.

Inoltre tale sistema operativo risulta molto stabile e resistente: l'installazione o la disinstallazione di nuove applicazioni non rallentano l'avvio o la chiusura del sistema stesso e un eventuale malfunzionamento di un'applicazione raramente blocca il computer.

Per installare Ubuntu si può scaricare l'ultima versione dal sito internet [www.ubuntu-it.org](http://www.ubuntu-it.org) oppure è possibile ordinare gratuitamente il CD-ROM tramite il medesimo sito.

Ubuntu è presente in versione Desktop (consigliata) e Alternate (per computer con meno di 384 MB di RAM); l'installazione avviene in maniera grafica, con istruzioni in italiano, e permette di migrare il proprio profilo utente importando tutti i dati presenti, compresi segnalibri di Internet Explorer o Mozilla Firefox, documenti e altro.

### **Suite Office**

Con il termine "*Suite Office*" si fa riferimento a un insieme di programmi applicativi utilizzati per l'attività d'ufficio, tra i quali spiccano gli elaboratori di testo e i fogli di calcolo.

A prescindere dal sistema operativo installato, è possibile utilizzare una suite open source alternativa a Microsoft Office, vale a dire OpenOffice.

Il progetto OpenOffice, che in Italia ha superato recentemente i tre milioni di

copie scaricate a riprova della maturità di tale iniziativa, si prefigge l'obiettivo di fornire gratuitamente un programma a codice aperto utilizzabile in ogni contesto (pubblico, privato, professionale e aziendale), che possa competere con i prodotti commerciali attualmente dominanti nel settore delle applicazioni per ufficio.

Il fatto che sia gratuita, ma soprattutto che venga reso disponibile il codice sorgente (rilasciato con licenza LGPL), rende la suite OpenOffice particolarmente appetibile da un lato alle Pubbliche Amministrazioni che sono tenute a preferirlo per disposizione normativa, dall'altro a tutti gli utenti privati che vogliono ottenere un risparmio di spesa ovvero una personalizzazione del software.

A favorirne la diffusione è certamente servita la caratteristica di essere compatibile con i formati di file di Microsoft Office, motivo per il quale è possibile aprire, modificare e salvare i file Office (.doc, .xls, etc.) con l'omologo applicativo OpenOffice, senza perdere i propri documenti pregressi.

Inoltre OpenOffice può essere installato non solo su Linux, ma anche su Windows, Mac OS (dalla versione X) e altri sistemi operativi.

L'ultima versione rilasciata include i seguenti programmi:

- Writer: software di videoscrittura molto simile, sia per funzionalità che per l'aspetto grafico, a Microsoft Word; offre la possibilità di esportare i documenti direttamente in formato PDF ed è in grado di leggere la gran parte dei file di testo.
- Calc: foglio di calcolo con funzioni simili a Microsoft Excel; anche in questo caso è possibile salvare il file direttamente in formato PDF; Calc può gestire numerosi formati, compreso il formato proprietario XLS di Excel, sebbene ancora con alcune piccole incompatibilità.
- Impress: programma per presentazioni, appartenente alla stessa categoria di Microsoft Powerpoint, permette di esportare sia in PDF che in formato SWF (per Flash).
- Base: software di creazione e gestione di database, omologo a Microsoft Access.

La suite OpenOffice comprende ulteriori programmi, quali Draw per la grafi-

ca vettoriale, Math quale editor di formule matematiche e altri di minore interesse nell'ambito della professione legale.

Anche in questo caso è possibile installare il software procurandosi il CD-ROM ovvero scaricando l'ultima versione dal sito internet

<http://it.openoffice.org>.

### **Internet e posta elettronica**

Acquistando un personal computer con sistema operativo Windows, l'utente trova installato il browser Internet Explorer e il client di posta elettronica Outlook Express; in alternativa a tali software proprietari potrà comunque utilizzare rispettivamente i due programmi open source Mozilla Firefox e Mozilla Thunderbird.

Firefox è un browser web multipiattaforma in quanto è disponibile per sistemi Linux, Microsoft Windows, Mac OS e permette di importare i preferiti da Internet Explorer.

Tra le sue caratteristiche di maggior pregio vi sono un filtro integrato contro le finestre popup, il supporto per la comunicazione sicura SSL e la funzione di navigazione contemporanea in più siti (cosiddetta navigazione a schede). Oltre alle classiche funzionalità di un browser e a una particolare attenzione al profilo della sicurezza (molto importante se si pensa alla quantità di virus presenti in rete), Firefox offre un elevato grado di personalizzazione.

Di questo browser esiste anche l'edizione Portable per chiavette USB che, consentendo di navigare senza lasciare dati sull'hard disk, appare molto utile ai fini della tutela della propria privacy nel caso di utilizzo del computer altrui; inoltre risulta in via di compilazione pure Firefox Mobile, versione ottimizzata per telefoni cellulari e palmari.

Thunderbird è un client di posta elettronica e permette di gestire i newsgroup e i feed RSS (per leggere le notizie).

Anche questo programma funziona su sistemi Microsoft Windows, Linux, Mac OS e altri, supportando funzionalità aggiuntive da installare a seconda delle esigenze (si pensi a Funambol Mozilla Plugin che permette la sincronizzazione dei contatti e del calendario).

Il suo funzionamento risulta molto intuitivo e, inoltre, il programma ha la

capacità di importare messaggi da altri programmi (tra cui anche Microsoft Outlook) in modo da non perdere la vecchia corrispondenza in caso di migrazione.

Come la maggior parte dei programmi di posta elettronica, Thunderbird tra le sue diverse funzioni annovera la possibilità di creare filtri per smistare automaticamente la posta su diverse cartelle, il raggruppamento dei messaggi secondo data, mittente, priorità o altre caratteristiche e la capacità di posta in arrivo singola per account multipli; ancora una volta molto importante risulta la cura della sicurezza informatica, considerato che la posta elettronica rappresenta il principale veicolo di programmi dannosi e delle frodi on line.

Anche di questo client esiste anche l'edizione Portable per chiavette USB, il che rende concreto il sogno di tenere il proprio studio in tasca.

Entrambi questi applicativi possono essere scaricati gratuitamente in poco tempo, visto il peso contenuto dei file d'installazione, dal sito [www.mozilla-europe.org](http://www.mozilla-europe.org).

### **Software gestionale**

Anche sul versante ben più evoluto dei programmi per la gestione di studi legali non mancano progetti e soluzioni open source di indubbio interesse. I tre esempi più significativi in tal senso, tutti multiutente e multipiattaforma (cioè in grado di essere utilizzati sia con Linux che con Windows e MacOSX), risultano i seguenti:

- Elawoffice ([www.elawoffice.it](http://www.elawoffice.it)), realizzato in linguaggio di programmazione Java, consente:
  - la gestione informatizzata della pratica
  - la gestione automatizzata delle scadenze
  - l'utilizzo di modelli per la creazione di atti e lettere
  - l'interazione con le richieste di utenti del programma e di sviluppatori esterni al programma
  - un'ampia possibilità di personalizzazioni e controllo del programma.
- Knomos ([www.knomos.org](http://www.knomos.org)), pensato per la gestione integrata dello studio legale, risulta principalmente organizzato attorno all'agenda, perso-

nale e condivisa. Gli impegni (udienze, appuntamenti, etc.) vengono registrati mediante riferimento a un codice identificativo, che evita all'utente di digitare la descrizione, ferma restando la facoltà di aggiungere note in formato libero quando necessario. Ciascun impegno è connesso a una pratica il cui record identifica il cliente e le parti, il valore della controversia, l'autorità giudiziaria competente, l'oggetto e così via; ogni pratica è collegata agli impegni relativi, ai dati personali delle parti, ai loro legali, ai documenti e alle registrazioni delle attività e prestazioni.

- JDavide ([www.jdavide.it](http://www.jdavide.it)), anch'esso sviluppato in Java, consente di gestire l'agenda con l'aggiornamento dei rinvii d'udienza e l'inserimento automatico degli adempimenti, di redigere parcelle e notule sia manualmente che automaticamente dall'agenda, di scadenzare i pagamenti.

Estremamente innovativa è la possibilità di accedere al sistema gestionale anche tramite collegamento web, non solo per l'avvocato, ma pure per il cliente che potrà essere autorizzato a visualizzare lo stato della propria pratica direttamente dal computer di casa.

## **Conclusioni**

I tempi sembrano maturi per l'impiego all'interno degli studi legali di strumenti informatici forniti di software open source. Come detto, non è indispensabile utilizzare sia sistemi operativi che applicativi a codice aperto, ben potendo esistere soluzioni miste; a ciascuno sta sperimentare le diverse opportunità proposte e trovare quella che meglio si adatta alle proprie esigenze.

Senza dubbio un numero maggiore di utilizzatori di software open source non potrà che migliorare anche le condizioni di mercato e di riflesso le offerte (sia in termini di prezzo che di qualità dei prodotti) delle software house che distribuiscono programmi commerciale.

## **PROCESSO CIVILE TELEMATICO TRA ILLUSIONE E NUOVE REALTÀ OPERATIVE**

### **Carla Secchieri**

Consigliere tesoriere del Consiglio dell'Ordine degli Avvocati di Padova, coordinatore della Commissione informatica dell'Unione Triveneta dei Consigli degli Ordini degli Avvocati

Nel 2001, ci venne annunciato, in modo trionfale che il nostro Tribunale (Padova) era stato inserito nell'elenco delle sette sedi pilota, che avrebbero dovuto sperimentare uno strumento "rivoluzionario", che avrebbe consentito di abbattere i tempi biblici della Giustizia civile, ed evitato quelle pesanti sanzioni che l'Europa non intendeva più solamente minacciare: il processo civile telematico.

Ci fu spiegato che non si trattava di un nuovo rito (l'ennesimo) bensì l'utilizzo degli strumenti telematici nel processo, con l'obiettivo di creare un'efficiente cooperazione telematica tra gli attori del processo medesimo.

Ci fu detto che gli avvocati sarebbero stati, ovviamente, una parte importantissima della sperimentazione, e quindi ci saremmo dovuti adoperare per trovare, tra i Colleghi, alcuni volontari (non più di 10 - 15) che, esperti, cultori, ovvero solamente curiosi di informatica, dessero il loro prezioso contributo, costituendo un altisonante "laboratorio".

Non solo; poiché il Ministero era a corto di fondi, ci fu chiesto di provvedere a spese nostre alla pulizia delle banche dati degli Avvocati (indispensabile per l'avvio del processo).

Il gruppo fu prontamente formato da entusiasti "smanettoni", pronti ad iniziare il lavoro.

Ed altrettanto prontamente il Consiglio dell'Ordine mise mano al portafoglio, versando in più riprese non poche migliaia di euro.

Nel frattempo, eravamo tutti in ansiosa attesa delle norme tecniche che dovevano disciplinare il funzionamento del tutto, e che, sulla scorta del D.P.R. 13-2-2001 n. 123, avrebbero dovuto essere emanate entro il 30 ottobre

del 2001, ma (si era ormai al 2003 avanzato) ancora non se ne vedeva traccia. Finalmente, nell'ottobre 2004, a soli 3 anni di distanza dal termine previsto, le norme tecniche vennero approntate e noi del "laboratorio" fummo allertati, quasi che l'inizio della sperimentazione dovesse essere di lì a qualche minuto. Fummo invitati a partecipare ad un grande convegno di presentazione (tre giorni a Bologna) nel dicembre, ed a pochi giorni di distanza fu presentato a Padova il progetto, con l'organizzazione di un "road show" (sic!).

A Bologna ebbi modo di conoscere i referenti degli altri Tribunali "pilota", e confrontare i nostri rispettivi stati di avanzamento (praticamente eravamo tutti allo stesso punto: fatto niente).

Con il trascorrere del tempo l'originario ambizioso progetto era già stato completamente stravolto e ridimensionato: niente più deposito di atti, memorie e quant'altro direttamente in un fascicolo d'ufficio "telematico: l'avvio del pct avrebbe riguardato solamente il decreto ingiuntivo.

E nel mentre il Consiglio dell'Ordine pagava i corsi di formazione per i suoi sperimentatori, e per i cancellieri (!), ci affrettammo tutti a scaricare sul nostro pc (non era consentito l'utilizzo di un Mac: il programma "girava" solo in Windows) il c.d. "redattore avvocati", ovvero il software che ci avrebbe consentito di redigere gli atti secondo il formato richiesto dal Ministero, ed a munirci di smart card per poter avere i certificati di ruolo ed essere in grado di firmare digitalmente l'atto.

La fase di sperimentazione vera e propria, che prevedeva un c.d. doppio binario (deposito dell'atto per via telematica senza valore legale e contemporaneo deposito del cartaceo in cancelleria) doveva infatti essere preceduta da una fase preliminare denominata "sala giochi", nella quale, ai fini di testare il redattore avvocati, appunto "per gioco", doveva essere simulato un ricorso per ingiunzione: il ricorrente "Topolino" avrebbe ingiunto al debitore "Pippo" di pagargli la fornitura delle caramelle: non ho memoria se il "Commissario Basettoni" avrebbe poi emesso il provvedimento, perché la sala giochi, per quanto riguarda il Tribunale di Padova, è stata completamente omessa. Forse avevano capito che non eravamo dei "giocherelloni". Ad ogni buon conto, nel corso del 2005, nel mentre mi arrivavano notizie vaghe dalle altre sedi sperimentali, su partenze più o meno imminenti, noi

fummo impegnati in un paio di “riunioni di laboratorio”, nelle quali si facevano programmi più o meno concreti sugli adempimenti che avremmo dovuto adottare (tra i quali anche il rinnovo di quella smart card che i più solerti si erano procurati, e che stava per scadere senza mai essere stata utilizzata in senso più proficuo dall’esibizione a qualche collega che ci chiedeva cosa fosse, appunto, una smart card), perché “era certo”: ben presto avremmo iniziato la sperimentazione sul campo.

E così di due-tre mesi in due-tre mesi.

Poi finalmente, mentre gli altri Tribunali già avevano iniziato il deposito dei ricorsi “sperimentali”, ci dissero: a gennaio (2006) si parte! Anzi no, perché le Cancellerie saranno occupate con una tempestiva ispezione ministeriale della durata di almeno un trimestre.

Giunge giugno e poi fine giugno.

Una breve precisazione: quando il gruppo era stato costituito, da veri pivelli ci eravamo preoccupati di “selezionare” colleghi che con l’informatica avevano dimestichezza, senza curarci del ramo del diritto in cui operavano: la scelta si rivelò completamente sbagliata, perché in realtà il “reclutamento” doveva avvenire tra coloro che più degli altri si occupavano di recupero credito e quindi avevano quasi quotidianamente ricorsi ingiuntivi pronti per il deposito (a nostra discolpa possiamo solo dire che la questione decreti ingiuntivi non era stata palesata che dopo qualche anno): questo ci comportò una qualche difficoltà: tutti noi sperimentatori infatti ci coccolavamo i ricorsi (più o meno all’insaputa dei nostri clienti) tenendoli in serbo per poter dare il nostro contributo alla sperimentazione, fino a che, ovviamente, non potevamo procrastinarne oltre il deposito cartaceo, senza nuocere ai clienti, che desideravano la tutela dei loro diritti e non essere considerati dei pionieri del progresso.

Il 30 giugno, in sordina, perché ormai non ci credevamo più, il Collega Gallese depositò per via telematica il primo ricorso: evviva evviva, la sperimentazione era iniziata!

Peccato che di lì a qualche giorno iniziavano le ferie dei magistrati e quindi non si potè fare molto di più.

A settembre, io stessa mi cimentai nella prova (di forza): purtroppo il redat-

tore era un programma assai rigido, le difficoltà tecniche parecchie, e dopo tre ore di prove e di tentativi, che comportavano ogni volta il dover ricominciare da capo tutta la procedura, spossata, optai per il getto della spugna: i creditori erano tre, ed avrei dovuto per ognuno ripetere l'origine dei miei poteri di rappresentanza, non riuscivo ad imbustare, a spedire non ci ho neppure provato.

Beh sarebbero venuti tempi migliori, al prossimo decreto ingiuntivo: peccato che però una lettera del ministero ci informò che al 31 dicembre la sperimentazione si doveva considerare terminata: al 31 marzo ci sarebbe stata tolta la possibilità di utilizzare il punto di accesso ministeriale (graziosamente concessoci) e avremmo dovuto arrangiarci per conto nostro.

Cos'era successo? Perché tanta fretta?

Facile: il Tribunale di Milano, che non era stato sede sperimentale, e che però aveva molte risorse, aveva concordato con il Ministero la realizzazione del pct ed era pronto a partire, avendo costituito il suo punto di accesso.

Mi affrettai, pertanto, supportata da una formidabile "commissione informatica" a verificare la possibilità di costituire un punto di accesso anche per gli avvocati di Padova: purtroppo però, vi era un'unica società accreditata dal Ministero, ed operando in regime di monopolio, praticava prezzi non sostenibili per il nostro Ordine, in relazione all'effettiva utilità dello strumento (da noi non ci sono settimene o mesi di attesa per l'emissione dei decreti ingiuntivi).

Armata di buona volontà scrissi un'accurata lettera al Ministero, chiedendo di non disperdere il patrimonio di nozioni acquisite nella se pur breve fase sperimentale, e quindi di utilizzare il punto di accesso ministeriale, fino all'individuazione di un nuovo contraente, ma sono ancora in attesa della risposta.

Certo che il 31 marzo 2007 il punto di accesso ministeriale è per noi diventato inaccessibile.

Preso atto che il Consiglio Nazionale Forense era ben lontano dal costituirsi egli stesso punto di accesso, facilitando così il compito ai Consigli territoriali, attendemmo pazientemente che fosse finalmente accreditata una società privata, con i requisiti previsti dalla legge, e alla fine di dicembre concludemmo un contratto con il quale la stessa ci metteva a disposizione il suo punto di accesso.

Era fatta! Potevamo anche noi finalmente partire.

Nossignori: dopo settimane e mesi di silenzio da parte del Ministero e del CISIA locale, apprendiamo che dobbiamo attendere che venga installato il SICID, il nuovo programma del contenzioso civile su base distrettuale, che avrebbe sostituito il vecchio; ma per fare ciò era necessaria l'installazione di nuovi server, che erano già stati forniti, ma non potevano essere posizionati, essendovi dei dubbi sulla tenuta del solaio della sala server (Il che ci riempì di gioia, essendo stato il nostro Tribunale inaugurato in pompa magna nel 1995).

Chiedemmo che ci dessero almeno dei tempi, (si deve organizzare un minimo di formazione, pensare al tecnico per l'help desk e quant'altro: non c'è più spazio per la sperimentazione, se si parte il deposito ha valore legale e non è consentito sbagliare) e ci fu ventilato come definitivo il mese di settembre: notizia girata con grande risalto alla stampa locale, ma giunge luglio e non abbiamo nessuna notizia ufficiale; nel mentre si susseguono articoli di stampa, che danno per imminente la partenza del pct in questo o quel Tribunale, senza mai menzionare Padova.

Finalmente, dopo un incontro piuttosto "vivace" con il CISIA locale, il Ministero ci fa sapere che a settembre ci sarà una riunione per la definizione dei tempi di avvio.

La riunione si è tenuta finalmente a fine ottobre, preceduta da altro incontro con delegati del Ministero, i quali, sorvolando completamente sulla questione del decreto ingiuntivo telematico, ci chiedevano di costituire un nuovo gruppo di volontari disposti ad immolarsi sull'altare della sperimentazione delle esecuzioni "telematiche": Padova infatti era stata individuata ancora una volta come sede sperimentale.

Mi piace pensare che l'improvvisa accelerazione all'avvio del decreto ingiuntivo telematico sia in parte dovuta alla mia reazione (non proprio pacata) a quella richiesta.

Ma forse è solo una questione di tempi ministeriali.

Comunque adesso dobbiamo pensare a tutti gli adempimenti da mettere a punto.

L'avventura, questa volta, seriamente, sta per iniziare.

## SICUREZZA INFORMATICA FRA PARANOIA E VIRTÙ

### **Giorgio Battaglini**

Referente per l'informatica e componente del Comitato scientifico della Camera Civile Veneziana, componente del Circolo Giuristi Telematici per il Veneto, docente della Scuola di giornalismo 'Dino Buzzati' presso l'Ordine dei Giornalisti del Veneto

Molte aziende, ma anche molti professionisti si chiedono il motivo per cui dovrebbero mai interessarsi alle problematiche relative alla sicurezza informatica. Basterebbe per convincerli invitarli ad effettuare delle semplici verifiche, visitando alcuni siti di test online, così da rendersi conto della gravità dei rischi a cui sono esposti - e con essi la loro azienda o il loro studio - nell'utilizzo delle nuove tecnologie. Tramite tali controlli è possibile accertare in tempo reale la presenza di vulnerabilità del sistema informatico utilizzato, ma soprattutto riscontrare la quantità di informazioni personali che vengono rilasciate ai siti visitati, senza saperlo ma soprattutto senza nemmeno sospettarlo.

Si va da semplici indicazioni sul proprio sistema operativo o sul browser utilizzato, a vere e proprie informazioni sensibili quali la cronologia e la tipologia dei siti già visitati, fino alla concreta possibilità di condivisione di intere parti del proprio hard disk e dei dati in esse contenuti. I rischi sono concreti e avere la consapevolezza della loro esistenza è già il primo passo per cercare di trovare un rimedio.

Al di là degli obblighi normativi e delle prescrizioni in materia di sicurezza informatica imposte dal Codice della Privacy, che poi analizzeremo, si ritiene che adottare delle misure di sicurezza per l'utilizzo dei propri sistemi informatici sia oramai un'inevitabile esigenza non solo per i professionisti e le aziende ma anche per i privati.

A differenza di quanto molti credono, il "*processo sicurezza*" non è un semplice prodotto da acquistare ed installare, ma comprende sia un fattore materiale che un fattore umano, il quale notoriamente costituisce l'anello debole della cd. *security chain*. La sicurezza quindi va intesa come un pro-

cesso ove nessuna soluzione è definitiva e che va gestito continuamente, nel quale esistono solo diversi livelli, proporzionati all'importanza del bene da custodire.

Il legislatore, proprio per tali motivi, non pretende la sicurezza assoluta dei dati e dei sistemi ma esige l'adozione di un complesso di misure tecniche, informatiche, organizzative e logistiche, graduandole a seconda della tipologia del bene da tutelare, così da ridurre al minimo i rischi.

Il Codice della Privacy tratta l'argomento sicurezza al titolo V° della parte prima intestandolo "*Sicurezza dei dati e dei sistemi*".

Già da questa prima definizione, s'intuisce quali siano i due ambiti entro i quali bisogna operare per ottenere quel livello di sicurezza richiesto dalla legge, che si orienta non solo verso i dati ma anche verso i sistemi di trattamento e conservazione degli stessi. Per questi due ambiti sono previste le Misure Di Sicurezza.

La prima, e principale, distinzione operata dal legislatore è quella tra le *Misure minime* e le *Misure idonee*.

Il codice prevede l'obbligo di adozione delle citate *misure minime* da parte dei titolari del trattamento e provvede poi ad elencarle analiticamente:

- a) *autenticazione informatica*, che è un processo atto a garantire il controllo di chi accede agli elaboratori, verificandone e convalidandone l'identità. In pratica non è altro che la procedura di riconoscimento e accesso, tramite inserimento di nome utente e password, che utilizziamo normalmente, ad esempio, per accedere al p.c. o al conto di home banking online;
- b) *adozione di procedure di gestione delle credenziali di autenticazione*;
- c) *utilizzazione di un sistema di autorizzazione*, che si rende necessario quando sono previsti profili di autorizzazione di ambito diverso per i vari incaricati. Ad esempio, al titolare di uno studio professionale sarà consentito il trattamento di tutti i dati archiviati mentre alla segretaria addetta al front desk sarà negato accedere ai dati sensibili e/o giudiziari dei clienti dello studio;
- d) *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzio-*

*ne degli strumenti elettronici, e quindi la verifica periodica che ciascun incaricato acceda solo ai dati ad esso necessari per l'espletamento del suo incarico;*

- e) *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; tale misura, certamente basilare ed essenziale, tende ad impedire che i dati siano trattati illecitamente, e/o che si verifichino accessi non consentiti o altri danni ai dati o ai sistemi, causati dall'azione dei cd. *scumware*;*
- f) *adozione di procedure per la custodia di copie di sicurezza, [e per] il ripristino della disponibilità dei dati e dei sistemi; si prescrive in sostanza l'obbligatorietà di effettuare periodicamente, delle copie di back-up dei dati predisponendo apposite procedure di custodia. Ove si trattino dati sensibili e giudiziari, è necessario adottare anche una procedura di *disaster recovery* e cioè l'organizzazione di un vero e proprio sistema per il ripristino dell'accesso ai dati entro il termine massimo di sette giorni dall'evento distruttivo;*
- 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.*

Dopo aver rapidamente dato uno sguardo alle misure tecnico informatiche previste dalla legge, vediamo ora nel concreto quali potrebbero essere i primi essenziali passi per iniziare il *processo sicurezza*, anche utilizzando strumenti gratuiti posto che, come si dice in rete, "*Software is like sex: it's better when it's free*":

- attivare le varie impostazioni di sicurezza del proprio sistema operativo;
- attivare il sistema di autenticazione informatica per l'accesso al pc utilizzando solo password robuste e disattivare il cd. account *guest*;
- attivare, se necessario, un sistema di autorizzazione differenziata per l'accesso ai diversi dati trattati;
- impostare l'attivazione dello *screensaver* protetto da password dopo un'inattività di circa cinque minuti;

- creare un disco di ripristino per il riavvio del sistema operativo in caso di malfunzionamenti o danni;
- effettuare periodici back-up su supporti esterni non riscrivibili (mai sullo stesso hard-disk ove è installato il sistema operativo) e verificare sempre la bontà della copia;
- disabilitare, se non utilizzato, l'accesso remoto al p.c.;
- evitare assolutamente l'installazione di software per il *p2p* e di programmi superflui o di dubbia provenienza;
- disabilitare la condivisione di file e cartelle personali in rete;
- installare alcuni software per la sicurezza tra cui un *firewall* (ancora meglio se hardware), un antivirus e un più specifico software che rimuova i *cookies* e le liste *MRU*.

Ovviamente tali programmi dovranno essere aggiornati costantemente (meglio se manualmente e non in automatico), così come per il sistema operativo e gli altri software utilizzati, installando anche le cd. *patch*.

Essenziale è l'utilizzo regolare di un software di *cancellazione sicura* dei file che ne impedisca il recupero e da impiegare soprattutto per la pulizia dei dispositivi portatili utilizzati per la memorizzazione di dati (floppy disk, penne usb, hd esterni).

Per coloro che si servono di tali supporti, appare indispensabile utilizzare un software di autenticazione e crittografiazione sì da proteggere i dati in essi contenuti e impedirne la visione ad estranei in caso in smarrimento.

Utile è, infine, l'installazione di particolari *plug-in* del *browser web* per la preventiva verifica della sicurezza dei siti che ci si accinge a visitare.

Quanto fin qui illustrato per far intendere, senza pretesa di esaustività, quanti e diversi siano gli ambiti in cui operare per ottenere una maggiore sicurezza del proprio ambiente di lavoro e dei relativi strumenti informatici; ma soprattutto per far capire che, più che l'installazione di hardware e software appositi, è importante prendere coscienza del problema e iniziare a capire il funzionamento degli strumenti che utilizziamo quotidianamente. Purtroppo, anche su una macchina sicura, un utente ingenuo e inesperto rischia che creare danni.

**Link per il download dei software** (link verificati al 7/10/2008)

*Online Armor Personal Firewall* (Ver. 2.1.0.131) Free edition  
<http://www.tallemu.com>, [http://www.download.com/Online-Armor/3000-10435\\_4-10831167.html?tag=lst-1](http://www.download.com/Online-Armor/3000-10435_4-10831167.html?tag=lst-1)

*AVG Anti-Virus Free Edition* Ver. 8.0 (Freeware)  
<http://free.grisoft.com/ww.download?prd=afe>

*Spybot - Search & Destroy* Ver. 1.6.0.30 (Free Open-Source)  
<http://www.spybotsd.org/it/mirrors/index.html>

*CCleaner* Ver. 2.12.660 (Freeware)  
<http://www.ccleaner.com/download>

*Ad-Aware 2008 Free* Ver. 7.1.0.8 (Shareware)  
[http://www.lavasoft.com/single/mirror\\_download.php?f=g20bc772A](http://www.lavasoft.com/single/mirror_download.php?f=g20bc772A)

*SpywareBlaster* Ver. 4.1 (Freeware)  
<http://www.javacoolsoftware.com/sbdownload.html>

*Eraser 5.86a* (Freeware)  
[http://downloads.sourceforge.net/eraser/EraserSetup32.exe?modtime=1199873149&big\\_mirror=0](http://downloads.sourceforge.net/eraser/EraserSetup32.exe?modtime=1199873149&big_mirror=0)

*TrueCrypt* Ver. 6.0a (Free Open-Source)  
<http://www.truecrypt.org/downloads.php>

**Lecture e audio utili free**

*Windows XP in sicurezza* di Mario Pascucci. Apogeo  
[http://www.apogeonline.com/2007/libri/88-503-1008-0/ebook/pdf/8850310080\\_open.pdf](http://www.apogeonline.com/2007/libri/88-503-1008-0/ebook/pdf/8850310080_open.pdf)

*Vademecum per la sicurezza dei p.c.* di G. Costabile  
<http://www.sitoflash.it/costabile/web/index.cfm?id=5CB836BA-F948-159B-BFDD741862B410DB>

*Guida alla sicurezza informatica* Pv. Como - PolPost Lombar  
<http://www.anpsitalia.eu/portale/images/pdf/sicurezza%20informatica%20completo.pdf>

*Corso di sicurezza informatica* di PcOpen  
[http://www.pcopen.it/01NET/HP/0\\_1254\\_4\\_ART\\_61028\\_00.html](http://www.pcopen.it/01NET/HP/0_1254_4_ART_61028_00.html)

*Il podcast di Ventiquattrore Avvocato* del Prof. G. Ziccardi, tra cui

- Sicurezza del professionista, backup e firewall
- Sicurezza e autenticazione: accesso al computer, user id e password
- L'uso corretto dei supporti magnetici
- Le tecnologie di cifratura dei dati e di firma elettronica
- La sicurezza e la privacy delle code di stampa
- Possibile strategia per limitare al minimo i rischi di contagio
- I codici maligni e il computer
- Come difendersi dai virus e dai worm durante l'attività professionale
- Come difendersi dai virus
- Gli adempimenti formali e sostanziali in tema di sicurezza e privacy

<http://www.ilmerito.ilsole24ore.com/podcast.asp>

## Bibliografia

- Marco D'Auria, *Dizionario Internet*, Editori Riuniti, 1996
- Giovanni Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, 1997
- Francesco Brugaletta, *Internet per giuristi*, Simone, 1998
- Ernesto Damiani, *Internet. Guida pratica alla rete internazionale*, Tecniche Nuove, 1999
- Enrico Gianfelici, *La legge sulla privacy*, Fag, 1999
- Emilio Tosi (a cura di), *Il Codice del diritto dell'informatica e di internet*, Tribuna, 2000
- Giorgio Rognetta (a cura di), *Informatica Giuridica*, Simone, 2001
- Glauco Riem, *Privacy e Sicurezza*, Simone, 2002
- Carmelo Giurdanella, *Lo studio legale on line*, Simone, 2003
- Giorgio Zarrelli, *Sicurizza il tuo pc*, Tecniche Nuove, 2003
- AA.VV., *Hacker & sicurezza*, Guide pratiche JCE, 2003
- Andrea Lisi, (a cura di), *La privacy in internet*, Simone, 2003
- Paolo Poli, *Virus & Co - Guida pratica alla sicurezza*, Apogeo 2004
- Luigi Manzo, *Trucchi per la sicurezza del tuo pc*, J. Group Editore, 2004
- Rapetto - Caporale, *Documento Programmatico sulla Sicurezza*, EPC, 2004
- Guido Scorza, *Elementi di diritto dell'informatica*, Simone, 2004
- Ciccia - Fumagalli, *Privacy, Guida agli adempimenti*, Ipsoa, 2004
- G.P. Cirillo (a cura di), *Il Codice sulla protezione dei dati personali*, Giuffrè, 2004
- Imperiali - imperiali, *Codice della privacy*, Il Sole 24 Ore, 2004
- Riccardo Acciai (a cura di), *Il diritto alla protezione dei dati personali*, Maggioli, 2004
- Cardarelli - Sica - Zencovich, *Il codice dei dati personali*, Giuffrè, 2004
- AA.VV., *Codice della privacy*, Giuffrè, 2004
- AA.VV., *Dizionario di Internet e delle reti*, Mondadori informatica, 2004
- AA.VV., *Windows Xp e sicurezza* - Guide Pratiche Computer Magazine, 2004
- AA.VV., *Il registro di Windows* - Guide Pratiche Computer Magazine, 2004
- Gerardo Costabile (a cura di), *Sicurezza e privacy: dalla carta ai bit*, Experta, 2005
- Giovanni Ziccardi, *Telematica giuridica*, Giuffrè, 2005
- Luca Graziano, *Spia e non farti spiare*, FAG, 2005
- David D'Agostini (a cura di), *L'informatica negli studi legali e nel processo civile*, Experta, 2005
- Davide Scullino, *Proteggi il tuo pc da virus, hacker & Co.*, J. Group Editore, 2005
- Giuseppe Santaniello (a cura di), *La protezione dei dati personali, in Trattato di Dir. Amm.*, Cedam, 2005
- AA.VV., *Windows Xp. No Hacker !*, Future Media, 2005
- Alessandro del Ninno, *La tutela dei dati personali*, Cedam, 2006
- Ghirardini - Faggioli, *Computer Forensics*, Apogeo, 2007
- Borrusso - Di Giorgio - Mattioli - Ragona, *L'informatica del diritto*, Giuffrè, 2007
- Bianca - Busnelli (a cura di), *Protezione dei dati personali*, Cedam 2007
- Cajani - Costabile - Mazzaraco, *Phishing e furto d'identità digitale*, Giuffrè, 2008
- Elena Faletti, *E-justice*, Giuffrè, 2008

## **UN NUOVO APPROCCIO ALL'USO DEI SOFTWARE DI GESTIONE DELL'ATTIVITÀ FORENSE E DEGLI ORDINI DEGLI AVVOCATI**

### **Fabrizio Pettoello**

Consigliere tesoriere del Consiglio dell'Ordine degli Avvocati di Udine, coordinatore della Commissione informatica dell'Unione Triveneta dei Consigli degli Ordini degli Avvocati

Quando per la prima volta ho introdotto i computers nel mio studio, oltre a installare gli indispensabili programmi di videoscrittura e di calcolo, mi sono preoccupato di trovare un software gestionale che mi permettesse di semplificare le attività seriali, di verificare la produttività dello studio e di ottenere un efficace memorandum.

Tra i pochi programmi diffusi al tempo nel mio territorio la mia scelta è purtroppo caduta su quello che oggi considero il peggior programma per il rapporto qualità/prezzo.

In seguito ne ho installati, provati e abbandonati ben altri tre, suscitando, come è facile immaginare, grande entusiasmo tra le mie segretarie.

Durante il mio primo mandato nel Consiglio dell'Ordine del mio circondario ho ricevuto la delega per gli aspetti informatici. Per evitare ai miei Colleghi il mio stesso calvario e soprattutto quello delle mie segretarie ho deciso di confrontarmi con diversi di loro. Insieme, al fine di studiare e predisporre una guida all'acquisto di gestionali per studi legali, ne abbiamo analizzati molti: alcuni più diffusi, altri meno conosciuti.

Abbiamo individuato dei criteri di giudizio che ci consentissero di valutare approfonditamente il programma, il prezzo, l'interfaccia, la facilità di utilizzo, la versatilità e l'assistenza. Tutti elementi decisivi per effettuare un acquisto consapevole nella giungla delle offerte commerciali.

Oltre al prezzo, che deve essere proporzionato alla qualità del programma (ce ne sono alcuni, peraltro piuttosto diffusi, con prezzi del tutto fuori mercato), ci sono altri due aspetti molto importanti, che devono essere presi in considerazione per la scelta da operare: il primo, che riguarda tutti gli uten-

ti, attiene alla gradevolezza dell'interfaccia, alla semplicità d'uso, alla facile "navigabilità"; il secondo, interessante per i più esperti, è relativo alla capacità del programma di adattarsi alle esigenze dell'utente, anzi alla possibilità da parte di quest'ultimo di modificarlo e integrarlo.

Ovviamente la recensione soffre di una certa disomogeneità di giudizi, dovuta al fatto che gli autori sono diversi. Abbiamo però cercato di ovviare a tale problema affidando al Collega Mineo il lavoro di coordinamento. Si deve inoltre tener presente che, come tutti i giudizi, anche le valutazioni sui gestionali riflettono le idee dei vari autori. Posso però assicurare che alcuni sono molto qualificati a esprimere i giudizi raccolti nella "Guida all'acquisto di un programma per la gestione dello studio legale", che è scaricabile, gratuitamente e senza bisogno di registrarsi, dal sito dell'Unione Triveneta degli Ordini degli Avvocati

([http://www.avvocatitriveneto.it/allegati/tematiche/897/Guida\\_Gestionali.pdf](http://www.avvocatitriveneto.it/allegati/tematiche/897/Guida_Gestionali.pdf)). L'esperienza di questo lavoro mi ha portato a due considerazioni: quasi mai i programmi sono stati ideati da Avvocati, i programmi *open source* coprono una fascia di mercato troppo marginale.

Per quanto riguarda la prima considerazione, credo che ciò dipenda dal fatto che le softwarehouses cercano di impiegare meno risorse possibile per l'ideazione dei programmi e ciò al fine di trarre il maggior utile con il minimo sforzo. Ne sono un esempio il fatto che poche case hanno sviluppato un redattore atti per il processo civile telematico o un programma per la nota di iscrizione a ruolo con codice e barre. Inoltre i programmi realizzati non sono di grande qualità, basti pensare che la nota di iscrizione a ruolo con codice a barre (sia quello ministeriale sia quello di una software house) non consente l'inserimento di più di un avvocato. Quindi chi non viene inserito non può verificare le sue pratiche sul polisweb!

È peraltro contraddittorio che le case produttrici utilizzino solitamente programmi già esistenti sul mercato dotati di licenza (access, outlook, ecc), [la dipendenza da Microsoft è veramente imbarazzante in questo ambito] e non facciano uso di softwares open source, che consentirebbe un evidente risparmio che potrebbe essere destinato alla ideazione o all'adattamento del programma alle esigenze dell'avvocato. Ritengo infatti che la presenza del-

l'avvocato in fase di ideazione consentirebbe di avere un programma maggiormente fruibile e facile nell'uso. La realizzazione del programma da parte di tecnici costringe invece l'avvocato ad adattare le sue abitudini, i suoi processi logici al programma e non, come dovrebbe essere, il contrario.

Un esempio evidente è l'agenda. È sbagliato pensare che vi sia un diverso modo d'agire tra l'avvocato "digitale" da quello "cartaceo". Le abitudini e le esigenze sono per entrambi le stesse. Come dicevo, uno degli strumenti organizzativi più importanti per l'avvocato è la propria agenda, nella quale si segnano le udienze, gli appuntamenti e le scadenze. Pochi programmi hanno per interfaccia iniziale un calendario giornaliero, dov'è indicato l'orario di inizio e quello di fine delle attività. Ciò consentirebbe, all'organizzazione interna di studio, di ottimizzare il tempo. Infatti molti gestionali hanno un elenco non sempre chiaro di attività, appuntamenti o udienze, dove raramente è indicato il periodo di tempo che l'impegno occupa. Un altro esempio utile a comprendere che raramente l'avvocato è parte essenziale nell'ideazione del programma è la modalità di compilazione della nota spese. Può capitare infatti che la stessa riguardi attività svolte dal dominus e altre dal domiciliatario. Mi spiego meglio: spesso capita che il dominus, nel redigere la nota spese, debba inserire anche attività svolte dal domiciliatario (o viceversa). Così facendo però deve inserire delle voci (quelle dell'attività svolte dal domiciliatario) nella propria contabilità. Ne consegue che il dominus che ha così integrato la nota spese si trova delle prestazioni che non ha effettuato, dato che sono state svolte da un altro soggetto (domiciliatario) a cui competono.

Potrei fare ulteriori esempi, ma credo di essere stato sufficientemente chiaro per far comprendere il concetto che se l'avvocato fosse stato presente al momento della concezione architettonica del programma si sarebbero potuti concepire sistemi più efficaci e soprattutto più adatti ai bisogni dell'avvocato. Per quanto riguarda i programmi open source, ritengo che i tre presenti sul mercato soffrano l'assenza di una comunità di sostegno. Gli stessi sono infatti dipendenti soltanto dall'iniziativa dei singoli ideatori. È mancata - a mio parere - la sensibilità, anche da parte degli Organi istituzionali dell'Avvocatura, di promuovere iniziative volte a favorire l'utilizzo di pro-

grammi open source, che avrebbero consentito alla stessa Avvocatura, mediante l'impiego di risorse relativamente limitate, di utilizzare strumenti efficienti e soprattutto fortemente modificabili, data la disponibilità dei codici sorgente.

È pur vero che, in questo campo, c'è una nuova sensibilità da parte delle Istituzioni dell'Avvocatura. Ne è un esempio il software open source ideato e messo a disposizione di tutti gli Avvocati (e scaricabile dal sito dell'Unione Triveneta degli Ordini degli Avvocati al seguente indirizzo <http://www.avvocatitriveneto.it/download.php>).

In questo senso, si stanno muovendo anche gli Ordini del Friuli Venezia Giulia, che hanno concepito e realizzato un programma open source di gestione dell'Ordine stesso. Propri gestionali sono stati ideati anche da altri Ordini: Bologna, Bolzano, ecc.

Tale programma è stato concepito proprio con l'obiettivo di uscire dalle logiche del profitto, peraltro non contestabili, delle software houses. L'idea è stata quella di concepire un software fortemente innovativo, facilmente implementabile e modificabile. Tale software è una web application e quindi gestibile dal web mediante l'accesso autenticato dal sito di ogni singolo Ordine.

Il programma in questione riguarda la tenuta Albi, il protocollo, la contabilità, la formazione, le difese d'ufficio ed è in previsione la gestione telematica del procedimento disciplinare. In particolare, la tenuta Albi riguarda la gestione di tutti i dati relativi all'Avvocato: quali quelli anagrafici, del praticantato svolto, dei praticanti di studio, dello studio di appartenenza, dei procedimenti disciplinari e delle sanzioni subite.

Il software permette inoltre di avere una conoscenza, in tempo reale, della situazione contabile dell'Ordine; evidenzia, in caso di mancato pagamento nei termini previsti della tassa albo, i nominativi degli iscritti inadempienti, con la possibilità, mediante un semplice click, di inviare un sollecito via *e-mail*.

Per quanto riguarda la formazione, il singolo iscritto potrà iscriversi *on line* alla conferenza, ma anche annullare la prenotazione. In tal caso il software genererà automaticamente una e-mail al primo iscritto in lista d'attesa per

consentirgli di iscriversi, prendendo il posto lasciato libero. Il software tiene altresì la contabilità dei crediti maturati e degli esoneri richiesti e ciò solleva sia l'Avvocato dall'obbligo di redigere una relazione di fine anno sui crediti maturati, sia il Consiglio dell'Ordine dalle verifiche, dato che è il sistema stesso a indicare, al termine del periodo previsto dal regolamento, quali sono gli Avvocati che non hanno raggiunto il punteggio prefissato.

Per quanto riguarda le difese d'ufficio, la Procura della Repubblica e la Polizia Giudiziaria vengono dotati di codici d'accesso al sito. Nell'area loro riservata possono interrogare il sistema per l'indicazione di un avvocato da nominare. Dopo aver compilato i dati utili a individuare il procedimento, il sistema fornisce il nominativo di un avvocato. A quest'ultimo giunge contestualmente una e-mail e/o un eventuale sms. In caso di sostituzione, per esempio per irreperibilità, allo stesso Avvocato giungerà un'ulteriore e-mail e/o sms, che gli consentirà di verificare la correttezza dell'operazione di sostituzione.

Il programma è già stato testato da un anno e sarà attivo entro la fine del 2008. Come dicevo, è prevista la sua implementazione per quanto riguarda l'aspetto disciplinare.

Il sistema prevederà delle macroscadenze che consentiranno di avere sempre sotto controllo lo stato del procedimento.

Dopo la smaterializzazione del fascicolo, i soggetti accreditati potranno anche accedere telematicamente allo stesso, visionare e stampare tutti gli atti e i documenti. Si potranno depositare telematicamente atti e documenti. Ciò potrà avvenire mediante dispositivi di autenticazione che consentano l'accesso sicuro al sistema.

Diverse possono essere le applicazioni per la nostra professione, ma, a mio avviso, da una parte è necessario che gli Avvocati migliorino il loro rapporto con lo strumento informativo effettuando scelte opportune e consapevoli e coerenti alle rispettive necessità, dall'altra le nostre Istituzioni si impegnino a recuperare quel gravissimo ritardo tecnologico che caratterizza la nostra professione, rispetto ad altre, a cui scelte poco felici e per nulla lungimiranti hanno relegato l'Avvocato.

## GLI STANDARD OPERATIVI E LE LIBERTÀ INDIVIDUALI NEL PROCESSO CIVILE TELEMATICO

### Emanuele Forner

Delegato alle comunicazioni telematiche nell'Ufficio per la Formazione della Scuola di Formazione Permanente dell'Ordine degli Avvocati di Venezia, vice presidente della Camera degli Avvocati di Portogruaro

### L'intento del legislatore

Il processo civile telematico (*d'ora in avanti, e per brevità, PCT*) dovrebbe costituire, nelle intenzioni del Legislatore, se non proprio la panacea dei beni noti mali della giustizia civile italiana, quantomeno qualcosa che ci va molto vicino.

In effetti, la realizzazione del PCT adeguerebbe una macchina alquanto sgangherata (*la giustizia civile*) ai mezzi tecnologici che in moltissimi altri campi della vita sociale sono ormai quotidianità. Senza abbandonarci a visionarie fughe in avanti, l'adozione degli strumenti informatici e telematici nell'amministrazione della giustizia potrebbe permettere il recupero di un'efficienza che oramai, più che ricordo, è leggenda, senza richiedere costi proporzionali al risultato.

All'atto pratico, il PCT dovrebbe consistere (*quantomeno nel breve e medio periodo*) nell'utilizzo delle tecnologie informatiche e telematiche per due principali filoni di attività:

- 1) la "digitalizzazione" dei documenti, cioè il progressivo abbandono del tradizionale supporto cartaceo in favore della creazione, memorizzazione, consultazione, conservazione e archiviazione su supporto informatico (*magnetico, ottico e/o elettronico*); in altri termini, anziché in fascicoli e faldoni, atti e documenti del PCT saranno conservati su dischi rigidi, dischi ottici (*CD e DVD*) e dischi allo stato solido (*chiavi USB et similia*); ciò consentirà nel contempo un enorme risparmio in termini di spazi necessari per gli archivi (*non più magazzini stracolmi e debordanti di carte e cartacce, ma armadietti di contenute se non piccole dimensioni*)

e un'accessibilità ai dati in tempo pressoché reale, magari e soprattutto anche dallo studio dell'avvocato via internet;

- 2) la trasmissione dei documenti digitalizzati per via telematica a e dall'ufficio giudiziario, in luogo della tradizionale attività di deposito e prelievo degli omologhi cartacei nel luogo fisico dell'ufficio medesimo; in concreto, niente più avvocati, praticanti, consulenti e tutta quella umanità varia che oggidi suole affollare le cancellerie dei palazzi di giustizia, ma flussi di bit che viaggiano a velocità sempre maggiori lungo le autostrade dell'informazione: l'interazione fra i soggetti pubblici e privati del servizio Giustizia sarà quindi virtuale, tecnologica, asettica, esatta.

### **L'attuale realtà**

L'idea del PCT è assai affascinante; presenta tuttavia lo svantaggio di richiedere un'infrastruttura assai complessa ed esigente in termini di risorse:

- dal lato sistemico, è necessario creare una rete informatica in grado di supportare i flussi di dati in maniera sicura, sia sotto il profilo dell'affidabilità del sistema (*affinché non si verifichino interruzioni dell'attività o perdite di dati*), sia sotto il profilo della protezione dei dati trasmessi (*acciocché nessun malintenzionato o extraneus possa illecitamente intercettare le informazioni*);
- dal lato degli operatori, è necessario formare adeguatamente quanti col PCT finiranno per interagire.

“Or incomincian le dolenti note”<sup>1</sup>: per quanto concerne l'infrastruttura IT, siamo parecchio indietro; tant'è vero che il PCT è stato avviato, per ora, solo in via sperimentale, per un numero ristretto di sedi giudiziarie e solo per la fase di richiesta ed emissione del decreto ingiuntivo.

Sotto un differente aspetto, va un po' meglio con il progetto PolisWeb, nel senso che a oggi risultano caricati sul sito nazionale PolisWeb i dati di 177 Uffici Giudiziari<sup>2</sup>, di cui 66 Sezioni Distaccate di Tribunale e 16 Corti d'Appello; allo stato attuale, PolisWeb consente di consultare *on-line* i dati relativi alle cause pendenti (*l'equivalente - assai evoluto - del vecchio ruolo cartaceo che si è soliti faticosamente sfogliare nelle cancellerie*).

L'aspetto più densamente problematico, tuttavia, è rappresentato dal “fatto-

re umano", ossia la resistenza da parte dei vari operatori del settore (*magistrati, cancellieri e loro collaboratori, ma anche gli avvocati non sono da meno...*) all'introduzione delle nuove tecnologie.

È una storia già sentita, *usque ad nauseam*: i ritornelli più ricorrenti suonano più o meno "io di computer non ci capisco niente" oppure "è troppo difficile/complicato"<sup>3</sup>.

Appare quindi assolutamente necessaria una forte e decisa attività di formazione degli operatori, non solo e tanto sull'utilizzo concreto degli specifici programmi da adoperare, quanto e in primo luogo per un aperto e disponibile approccio al mezzo informatico.

Non sarà facile, ma non si danno alternative: la rivoluzione informatica non consente restaurazioni.

### **Il processo telematico: come dovrebbe essere**

Abbiamo detto che il PCT dovrebbe consentire di effettuare la gran parte delle attuali operazioni di cancelleria (*depositi, iscrizioni etc.*) per via telematica, cioè mediante la trasmissione a distanza di documenti digitali fra le diverse sedi fisiche degli operatori interessati.

Per fare un esempio concreto, per iscrivere a ruolo una causa l'avvocato, anziché recarsi di persona al Tribunale e depositare il fascicolo di parte completo di nota d'iscrizione a ruolo e quant'altro nel tradizionale formato cartaceo, potrà semplicemente trasmetterne l'omologo digitale tramite posta elettronica certificata.

Allo stato attuale, infatti, le specifiche tecniche del PCT prevedono, in estrema sintesi, che atti e documenti siano predisposti in formato PDF<sup>4</sup> e raccolti in una "busta elettronica", indi trasmessi via posta elettronica certificata (*PEC*).

Il Ministero della Giustizia ha predisposto, sinora, alcuni appositi *software*<sup>5</sup>, fra cui merita segnalare:

- *NIR - Nota di Iscrizione a Ruolo*: un'applicazione scritta in Java<sup>6</sup> e disponibile (*lodevolmente*) per diverse piattaforme: Microsoft Windows (*ma non ancora per Windows Vista!*), Linux e MacOS; NIR fornisce un'interfaccia di tipo "*wizard*" per la compilazione e stampa della nota d'iscrizio-

ne a ruolo, comprensiva di codici a barre tridimensionali (*sarebbe interessante già da subito, se fosse stata realizzata meglio, soprattutto per quanto attiene gli aspetti della formattazione e della stampa del documento*);

- *Consolle Avvocato*: già noto come "redattore", è il *software* che si occupa sostanzialmente della predisposizione della "busta elettronica" da inoltrare per via telematica all'Ufficio Giudiziario.

Questi *software* costituiscono gli strumenti indispensabili per utilizzare il PCT, ma non esauriscono le necessità dell'utente, il quale - ovviamente - dovrà disporre anche di un programma di elaborazione di testi per redigere gli atti e di un programma per convertirli in formato PDF (*oltre, naturalmente, ai software necessari per la gestione dei documenti da allegare, incluso un software per convertire anch'essi in formato PDF*); inoltre, saranno necessari *software* per la firma digitale dei documenti e un *account* PEC. Semplificando al massimo la procedura, l'avvocato dovrà predisporre con gli appositi programmi gli atti (*inclusa la nota d'iscrizione a ruolo*) e i documenti allegati, dovrà firmarli digitalmente, dovrà inserirli nella busta digitale e inviare quest'ultima via PEC, il tutto tramite *Consolle Avvocato*; il sistema prevede, poi, modalità di certificazione dell'avvenuto ricevimento dell'invio da parte dell'Ufficio Giudiziario.

### **I requisiti tecnici del sistema visti dalla parte dell'avvocato**

Alquanto incongruamente, *Consolle Avvocato* richiede un sistema dalle seguenti caratteristiche minime:

- PC con CPU Intel Pentium III 500 Mhz e RAM 128 MB (*256 MB consigliata*);
- sistema operativo Microsoft Windows 2000 o Microsoft Windows XP (*aggiornati all'ultimo service pack disponibile*);
- elaboratore di testi Microsoft Word (*versioni 97 oppure 2000 oppure XP, aggiornati all'ultimo service pack disponibile*);
- *browser web* Microsoft Internet Explorer (*versione 6 o superiore*).

L'elaboratore di testi Microsoft Word non è in realtà indispensabile, dal momento che *Consolle Avvocato* e il sistema complessivo del PCT utilizzano

PDF come unico formato di file; di talché, l'avvocato ben potrà redigere i propri atti con qualunque *word processor* purché gli sia possibile alla fine convertire il documento in PDF; tuttavia, Consolle Avvocato è progettato per integrarsi con Microsoft Word e con il *software* di conversione in PDF in modo da consentire la gestione dell'intero procedimento di realizzazione del fascicolo elettronico dall'interfaccia di Consolle Avvocato.

### **Processo civile telematico: gli anelli deboli**

Abbiamo detto che i requisiti di sistema per Consolle Avvocato presentano incongruenze: in primo luogo, c'è da chiedersi perché NIR sia stato realizzato in versione multiplatforma (*cioè, per diversi sistemi operativi*) e Consolle Avvocato solo per Microsoft Windows (*peraltro, escludendo la versione Vista e, pertanto, quanti siano in possesso solo di PC relativamente nuovi*).

A parte questa contraddizione interna, le scelte tecniche alla base del sistema PCT suscitano più d'una perplessità.

Dal lato squisitamente tecnico, occorre chiedersi perché si sia scelto di confinare gli strumenti indispensabili al funzionamento del PCT entro l'ambito di *software* proprietari e chiusi quali i prodotti Microsoft.

È vero che tali prodotti occupano la fascia maggiore del mercato IT, ma negli ultimi tempi le alternative disponibili (*MacOSX e GNU/Linux, per dire che i più noti*) stanno prendendo sempre più piede (*complice anche l'infelice riuscita di Windows Vista*).

Inoltre, è un dato ormai noto che in punto affidabilità e sicurezza del sistema operativo le alternative a Microsoft Windows risultano alquanto preferibili (*si pensi, per esempio, alla vulnerabilità ai virus e al malware in genere: GNU/Linux e MacOSX sono notevolmente meno affetti da tale problema rispetto ai sistemi Microsoft Windows*).

Ma, anche a voler rimanere entro l'ambiente Windows, sotto il profilo del *browser web* vi sono prodotti concorrenti a Internet Explorer (*fra tutti: Mozilla Firefox e Opera*) reputati di gran lunga più sicuri e affidabili.

Per tacere della sempre maggiore diffusione di prodotti alternativi a Microsoft Word e Microsoft Office (*uno su tutti: OpenOffice.org*), anche per

ovviare all'inconveniente dell'elevato costo delle licenze d'utilizzo dei programmi Microsoft (*rimanendo, beninteso, nella legalità...*).

In buona sostanza, confinarsi nell'ambiente Windows, senza un'effettiva giustificazione tecnica e senza offrire alcuna praticabile alternativa, equivale a introdurre surrettiziamente un'imposta occulta, giacché l'avvocato, per utilizzare il PCT, dovrà munirsi di quei determinati programmi pagandone le salate licenze (*oltretutto, neanche a vantaggio dello Stato, ma di un imprenditore commerciale privato!*), con buona pace dell'art. 23 Cost.

Ma non è solo una questione economica (*anche se, di questi tempi, non so quanti - soprattutto fra i colleghi di fresca abilitazione o meno affermati - possano permettersi il lusso di trascurarla tout court*), né le perplessità si limitano a quanto appena esposto.

Sotto altro profilo, dalla documentazione presente sul sito ufficiale del PCT pare evincersi la scelta ministeriale di non realizzare e distribuire *in proprio* i *software* necessari all'interazione tra avvocato e Ufficio Giudiziario, ma di limitarsi a dettarne le specifiche e pubblicare degli abbozzi di codice, lasciando poi alle varie *software house* interessate di sviluppare programmi da lanciare poi sul mercato.

La scelta è decisamente criticabile.

Già i *software* ministeriali non sono completamente *open source*, cioè il codice di programmazione non è liberamente accessibile, quindi non è possibile controllare come quei programmi siano strutturati e quali attività in effetti svolgano; il che solleva questioni di non poco conto in termini di sicurezza e tutela della *privacy*<sup>7</sup>.

Il fatto, poi, che a ciascuna *software house* sia consentito di implementare il codice ministeriale nel proprio prodotto aggiunge ulteriori preoccupazioni, se il programma non sia rilasciato con licenza che contempra l'accesso al codice sorgente (*chi può garantire, altrimenti, che le varie versioni commerciali di Consolle Avvocato non contengano spyware o peggio?*).

Senza contare, infine, i problemi di compatibilità che potrebbero sorgere dal fatto che il *software* non sia unico ma offerto in più varianti<sup>8</sup>.

Resta, comunque, la prospettiva di costringere chi voglia esercitare una determinata professione (*quella di avvocato, nel nostro caso*) a dotarsi di

strumenti indispensabili forniti in regime di oligopolio (*se non di monopolio tout court*), così aprendo un fronte di possibile contrasto con gli artt. 24 e 41 Cost. (*oltre al già rammentato art. 23 Cost.*).

Ma le “stranezze” non finiscono qui.

Consolle Avvocato, dicevamo, si integra con Microsoft Word e con esso soltanto: a che pro, dal momento che poi il formato scelto come standard per il PCT (*PDF, ricordiamo*) non è nativamente supportato da Microsoft Word (*se non, e comunque tramite un plugin aggiuntivo, dalla versione 2007, che peraltro non appare neppure compatibile con Consolle Avvocato*)? È solo perché Microsoft Word risulta essere il *word processor* più diffuso? Dalla perplessità ai sospetti il passo è sgradevolmente breve...

Ancora: se pure PDF è un formato proprietario (*di Adobe Systems*), le sue specifiche sono da tempo pubbliche e sono reperibili abbastanza facilmente programmi liberi e gratuiti in grado di convertire quasi ogni tipo di file in formato PDF, così da non imporre il ricorso ad Adobe Acrobat (*programma soggetto a licenza onerosa, ed alquanto*).

Tuttavia, in punto di principio sarebbe forse stato preferibile adottare tra gli standard per il PCT anche il formato ODF (*che ha il pregio di essere un formato libero, aperto e ufficialmente riconosciuto come standard internazionale: ISO/IEC 26300:2006*).

ODF è il formato predefinito di OpenOffice.org (*un'equivalente alternativa a Microsoft Office, compatibile con i formati proprietari di quest'ultimo, ma libera, gratuita e multiplatforma*), ma anche di altre suite per ufficio (*Lotus Symphony, KOffice*) e in ogni caso liberamente implementabile da chiunque (*anche da Microsoft se, improbabilmente, lo volesse*).

Certo, ODF non potrebbe essere usato per i documenti (*i quali, in buona parte, risulteranno da digitalizzazione di originali cartacei*), ma non si vede perché escluderlo per gli atti:

- se la preoccupazione concerne la modificabilità del documento, a un tanto ovvia la firma digitale (*che garantisce appunto la genuinità del documento e rivela qualsiasi modificazione apocrifa*);
- se, invece, la preoccupazione concerne il puro aspetto del documento, non dovrebbe essere prevalente sul profilo contenutistico; cioè, dal

momento in cui lo standard ISO/IEC garantisce la gestibilità del documento anche tramite un *software* diverso da quello che lo ha creato (*purché conforme alle specifiche dello standard*), eventuali difformità limitate ad aspetti secondari (*i tipi di carattere, prevalentemente*) non dovrebbero assumere più importanza della libertà dell'utente di scegliere quali strumenti adoperare in concreto.

### **L'importanza dell'"opzione software libero"**

Riassumendo, la critica principale all'attuale assetto progettuale del PCT si sostanzia in ciò: non è stata privilegiata una soluzione tecnica improntata ai principi del cosiddetto "*software libero*".

Per quanti volessero approfondire le tematiche del "*software libero*" rimando al sito del Progetto GNU (<http://www.gnu.org/home.it.html>); nel contesto di questo intervento, può essere sufficiente precisare che l'espressione "*Software Libero*" si riferisce alla libertà dell'utente di eseguire, copiare, distribuire, studiare, cambiare e migliorare il *software*.

Ciò comporta (*e presuppone*) che il *software* sia accessibile anche dal sorgente, cioè si possa esaminare il programma nella sua forma "umana", ossia nel linguaggio adoperato dal programmatore e prima di essere tradotto nel cosiddetto "linguaggio macchina", cioè nella forma binaria eseguibile dal computer.

Ciò, comporta, inoltre, che al *software* non sia associata una licenza restrittiva, che riservi cioè tutte le facoltà al produttore e conceda all'utente solo di eseguire il *software* alle condizioni stabilite unilateralmente dal produttore (*per fare un paragone, per quanto grossolano, sarebbe come se con la vostra automobile poteste andare solo dove ha deciso il produttore e non poteste aprire il cofano neanche per cambiare l'olio...*).

La libertà del *software*, invece, consente da un lato il controllo pieno sulle effettive funzionalità del programma (*così da evitare, per esempio, che vi siano incluse istruzioni per carpire fraudolentemente dati*), dall'altro l'effettiva disponibilità dei documenti creati e dei dati gestiti mediante quello specifico *software*.

Un esempio chiarirà meglio quest'ultimo aspetto.

Il formato dei documenti creati con Microsoft Word è di proprietà di Microsoft e non è aperto, cioè le specifiche tecniche sulle quali è costruito sono un segreto industriale del produttore. Cosicché, i documenti creati con Microsoft Word sono legittimamente accessibili - anche dal loro stesso autore - solo e fintantoché si è in possesso di una licenza d'uso rilasciata da Microsoft; è vero che anche altri programmi, realizzati da altri e non soggetti alla licenza Microsoft, possono accedere ai documenti creati con Microsoft Word, ma tali filtri di conversione sono stati realizzati empiricamente, e non sulla scorta delle specifiche di formato, cosicché l'efficacia dei filtri non è garantita al 100%. Inoltre, lo stesso formato proprietario di Microsoft si è evoluto ed è mutato nel tempo, per cui neanche in casa Microsoft è sempre pienamente garantita la cosiddetta "retrocompatibilità" (*cioè, la possibilità di accedere pienamente al contenuto del documento con una versione successiva del software; il rischio aumenta in maniera direttamente proporzionale alla vetustà del file*).

Come si vede, dunque, emerge un problema di non poco momento in ordine alla disponibilità di una propria stessa creazione.

A ciò si affianca il delicato problema di imporre l'utilizzo di specifici prodotti commerciali per l'esercizio di quella che dovrebbe essere una libera professione; utilizzo, lo ribadiamo, non dettato da necessità di qualunque sorta.

L'esistenza stessa di Internet smentisce ogni contrario assunto: il *web* è costruito sopra standard aperti, di modo che sia fruibile dalla più vasta platea senza restrizioni legate a specifici *software*; si può accedere a un sito e ai suoi servizi indipendentemente dal *browser* utilizzato e dal sistema operativo del proprio PC; ciò, perché è conveniente all'operatore raggiungere il più ampio numero di fruitori.

Analogamente dovrebbe essere per un campo di fondamentale importanza come la Giustizia.

### **L'auspicabile agenda dell'Avvocatura in punto**

Come confidiamo si sarà compreso da questo nostro intervento, il PCT è una prospettiva tuttora *in fieri*, la cui entrata a regime non è al momento seriamente calendarizzabile.

Se da un lato ciò è senz'altro motivo di rammarico, dall'altro dev'essere inteso come l'occasione pressoché ultima per l'Avvocatura, affinché un'evoluzione tanto importante della nostra stessa professione - quantomeno per ciò che attiene alle sue concrete modalità operative - avvenga con la fattiva collaborazione dell'Avvocatura stessa e non, come sinora è accaduto, a suo detrimento.

L'Avvocatura associativa, tanto istituzionale quanto libera, dovrebbe dunque attivarsi nei modi a essa consoni e consentiti per imprimere al PCT quella direzione che consenta da un lato il suo più celere e agevole affermarsi, dall'altro che il PCT si riveli uno strumento accessibile a tutti con il minimo di sacrifici e oneri, in forme e modalità che non escludano nessuno.

In tal senso, credo sia fondamentale ribadire la necessità che gli strumenti indispensabili per l'accesso al PCT rispondano ai criteri del già menzionato "software libero", i soli in grado di garantirne l'utilizzabilità da parte di chiunque senza compromettere alcuna libertà o alcun diritto individuale. Parallelamente, l'Avvocatura associativa dovrebbe altresì farsi carico delle opportune attività volte a promuovere e diffondere fra i propri associati una vera e propria cultura informatica, intesa non già e tanto come mero insieme di istruzioni per l'uso di questo o quello strumento (*hardware o software che sia*), bensì come autentica attitudine mentale e comprensione, profonda per quanto minima ed essenziale, di una realtà che è già attuale e dalla quale non è ipotizzabile ritorno.

#### NOTE

<sup>1</sup> Dante Alighieri, *Commedia, Inferno*, Canto V, v. 25.

<sup>2</sup> Fonte: <http://www.processotelematico.giustizia.it/>, sezione Uffici Giudiziari.

<sup>3</sup> Ricordo, solo due o tre anni fa, un noto Sostituto Procuratore della Repubblica di Venezia rammaricarsi perché gli impiegati sostanzialmente si rifiutavano di adoperare il nuovo sistema informatico di gestione del Registro delle notizie di reato; ma la cosa che più mi colpì – in senso sfavorevole – era che il predetto magistrato pareva rassegnato a subire tale atteggiamento; ometto ulteriori commenti...

<sup>4</sup> PDF è l'acronimo per "Portable Document Format": si tratta di formato di file basato su un linguaggio di descrizione di pagina (*sviluppato da Adobe Systems nel 1993*) per rappresentare documenti in modo indipendente dall'hardware e dal software utilizzati per gene-

rarli o per visualizzarli. Un file PDF può descrivere documenti che contengono testo e/o immagini a qualsiasi risoluzione. È un formato aperto, nel senso che chiunque può creare applicazioni che leggono e scrivono file PDF senza pagare *royalties* ad Adobe Systems (*Adobe ha un numero elevato di brevetti relativamente al formato PDF ma le licenze associate non includono il pagamento di diritti per la creazione di programmi associati*).

<sup>5</sup> I *software* sono scaricabili dal sito ufficiale del PCT:

<http://www.processotelematico.giustizia.it>, sezione Download.

<sup>6</sup> Per il funzionamento di NIR è richiesto che nel sistema sia installato Java Runtime Environment 1.4.2 o successivo.

<sup>7</sup> Non molto tempo fa, vi fu un certo clamore quando fu reso pubblico che i documenti realizzati con Microsoft Word includevano al loro interno informazioni (*metadati*) che non avrebbero dovuto esserci (*quali determinati dati dell'autore e, soprattutto, dati relativi ad altri documenti*); tant'è che Microsoft dovette precipitosamente correre ai ripari distribuendo un *software* aggiuntivo per rimuovere tali informazioni (*ma anche così, è da dubitare che tutti gli utenti di Microsoft Word l'abbiano saputo e abbiano provveduto in merito...*).

<sup>8</sup> Gli esperti dell'ambiente GNU/Linux – che, addirittura, è totalmente *open source* – ben sanno quali difficoltà si presentino per far funzionare un medesimo applicativo in tutte le innumerevoli distribuzioni GNU/Linux disponibili sulla piazza.

## LA FIRMA DIGITALE E LA POSTA ELETTRONICA CERTIFICATA

### **Dario Obizzi**

Cultore della materia in Informatica Giuridica presso l'Università degli studi di Udine, delegato dell'Ordine degli Avvocati di Gorizia per le questioni informatiche

L'utilizzo sempre più diffuso delle nuove tecnologie e quindi di elaboratori e di sistemi informatici e telematici ha creato profondi, e non sempre ben sfruttati e compresi, cambiamenti nella vita quotidiana e professionale. La facilità di comunicare e di mettersi in contatto con altri soggetti, inviando fax, e-mail, sms, mms, file allegati e quant'altro, ha indubbiamente consentito un miglioramento delle relazioni interpersonali ed economiche ma, al contempo, ha posto una serie di nuove problematiche. In campo giuridico si è posta da subito la questione relativa al riconoscimento ed al valore da attribuire alle informazioni create, generate, trasmesse o comunque prodotte da sistemi informatici e telematici. Tali informazioni, contenute in un file o in un'e-mail e che possono apparire all'utente come un testo, una fotografia, etc., sono equivalenti ed hanno lo stesso valore di quelle informazioni contenute in un documento cartaceo o in una fotografia analogica? La risposta non è stata semplice ed è giunta solo dopo un cammino legislativo abbastanza lungo. In Italia, infatti, già dagli anni ottanta si erano susseguite delle norme che avevano disciplinato l'uso di strumenti elettronici ed i requisiti per attribuire ai documenti da loro generati o trasmessi efficacia e valenza probatoria (si pensi all'uso del fax nei rapporti tra avvocati<sup>1</sup> oppure all'introduzione dell'art. 491-bis del codice penale in tema di documento informatico<sup>2</sup>), ma nessuna aveva preso una posizione estremamente precisa sul punto. Solo con l'art. 15 della Legge n. 59 del 1997 (cd. legge Bassanini) veniva affrontata di petto la questione, stabilendo che *"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*". Successivamente il D.P.R. 513/97 (ora abrogato) ed il D.P.R. 445/2000 (Testo Unico in materia di documentazione amministrativa) contenevano la definizione di "documento informatico" quale rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Con tali interventi legislativi il nostro ordinamento, quindi, riconosceva espressamente e pienamente validità e rilevanza al documento informatico quale prodotto di un elaboratore o apparato similare. Tuttavia restava ancora irrisolta una questione di primaria importanza: la possibilità di risalire con certezza alla paternità del documento informatico (si pensi, ad esempio, ad una e-mail). La soluzione veniva individuata nell'utilizzo (rectius, nell'apposizione o associazione) della firma digitale, quale sistema, simile alla firma autografa su carta, di autenticazione dei documenti informatici.

La firma digitale, *species* di quello che oggi è il *genus* firma elettronica qualificata, si basa sulla tecnologia della crittografia a chiavi asimmetriche o a chiave pubblica. Ogni utente dispone di una coppia di chiavi: una chiave privata, da non svelare a nessuno e con cui firmare il documento informatico, ed una chiave pubblica, che gli altri utenti utilizzano per decodificare la firma e constatarne quindi l'autenticità. Questa procedura serve a garantire due cose: l'autenticità (certezza del sottoscrittore) e l'integrità (non modificabilità) del documento. Per ottenere la segretezza del documento, si deve utilizzare il procedimento inverso: apponendo la chiave pubblica del titolare della chiave privata si ottiene la codifica del messaggio; solo il titolare, tramite la propria chiave privata, sarà in grado di decodificare il messaggio. La procedura di apposizione della firma digitale, più dettagliatamente, consiste in questo: tramite una funzione di hash, che ha lo scopo di trasformare un testo di qualsiasi lunghezza in una stringa di lunghezza fissa<sup>3</sup>, si ricava l'impronta digitale del documento e, tramite la chiave privata, si codifica l'impronta così ricavata. Questo comporta un notevole vantaggio in quanto la codifica riguarda solo una piccola stringa e non l'intero messaggio o documento che, in alcuni casi, può avere dimensioni molto grandi. La firma viene quindi allegata al documento e chiunque, utilizzando la chiave pubbli-

ca del firmatario, decodifica l'impronta digitale e confronta la stringa così ottenuta con quella che ottiene egli stesso applicando la funzione di hash. Naturalmente tali operazioni vengono eseguite in automatico da appositi software. Qualora i risultati combacino, l'autenticità e l'integrità del documento sono garantite.

Per ottenere la firma digitale bisogna rivolgersi ad un soggetto, denominato ente certificatore (che può essere accreditato o notificato dal CNIPA), che, vista la delicatezza del ruolo, deve assicurare solidità e sicurezza dei sistemi operativi, della struttura organizzativa e finanziaria. Si tratta in sostanza di un ente terzo, neutrale e di fiducia, cui è demandato il compito di fornire il dispositivo di firma sicuro al titolare, verificare ed attestare, emettendo un apposito certificato digitale qualificato, l'identità del titolare, pubblicare sul web il certificato e la chiave pubblica per permettere a chiunque di verificare l'avvenuta certificazione. L'ente certificatore, inoltre, deve essere incluso in un elenco pubblico, consultabile sul sito del CNIPA. Tutto ciò comporta anche l'assunzione di responsabilità da parte del certificatore nei confronti di coloro che abbiano fatto affidamento sul corretto adempimento degli obblighi gravanti sullo stesso certificatore (esattezza delle informazioni necessarie alla verifica della firma, tempestiva registrazione della revoca o sospensione del certificato, etc.).

La firma digitale è quindi molto simile, ma non uguale, alla firma autografa. Mentre la sottoscrizione diventa parte integrante del documento, la firma digitale è in realtà un allegato; la verifica poi segue strade diverse in quanto la firma autografa richiede il confronto con un'altra firma (metodo non molto sicuro), mentre la firma digitale si avvale di un algoritmo e quindi di un sistema più affidabile. L'aspetto che però più distingue i due tipi di firma è quello relativo all'integrità del documento: la firma autografa non è in grado di dare certezza riguardo a eventuali modificazioni, mentre la firma digitale sì. Per converso, la firma digitale manifesta un limite molto evidente: la validità temporale limitata.

Resta a questo punto da verificare il valore giuridico della firma digitale. Come detto, il D.P.R. 10 novembre 1997 n. 513, emanato in attuazione dell'art. 15 della legge 15 marzo 1997, n. 59, prevedeva che il documento infor-

matico, sottoscritto con firma digitale, avesse l'efficacia probatoria di cui all'art. 2702 c.c., riguardante, come ben noto, l'efficacia della scrittura privata. Successivamente tale normativa era stata trasposta nel D.P.R. 28 dicembre 2000, n. 445 che, a sua volta, ha subito molteplici modifiche, dovute anche alla necessità di adattare la legislazione nazionale alla Direttiva europea 99/93. Attualmente la materia è disciplinata dal Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005 n. 82, così come modificato dal D.Lgs. 4 aprile 2006 n. 159), il quale prevede tre (recitius, due) tipi di firme elettroniche: la "firma elettronica" e la "firma elettronica qualificata". La "firma digitale" è un particolare tipo di firma elettronica qualificata. La firma elettronica cd. "semplice" è definita come un insieme di dati in forma elettronica, allegati o connessi ad altri dati, utilizzati come metodo di identificazione informatica (ad es. gli header dell'e-mail). La firma elettronica qualificata, invece, richiede in più un'identificazione univoca del titolare, tramite mezzi nell'esclusiva disponibilità del firmatario (quindi smart-card, token USB), e la certificazione del titolare da parte di un soggetto terzo e tramite un certificato qualificato. La firma digitale, oltre ad essere una firma qualificata, è contraddistinta dall'utilizzo della tecnologia della crittografia a chiavi asimmetriche. Ciò premesso, l'art. 20 del D.L.vo 82/05 stabilisce che l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile nel giudizio; se vi è apposta la firma digitale, il documento informatico si presume riconducibile al titolare, salvo che questi dia prova contraria (quindi vige il principio inverso rispetto alla sottoscrizione in cui la controparte deve dimostrare la riconducibilità al firmatario), e soddisfa il requisito della forma scritta. L'art. 21 aggiunge che il documento informatico cui è apposta una firma elettronica è liberamente valutabile nel giudizio sul piano probatorio, mentre, nel caso di apposizione di firma digitale, l'efficacia è quella dell'art. 2702 c.c.

Riassumendo, il documento informatico ha validità e rilevanza nel nostro ordinamento: se è apposta una firma elettronica avrà un'efficacia probatoria da valutare caso per caso, mentre in presenza di una firma digitale il documento informatico diventa una vera e propria scrittura privata sottoscritta (salvo l'inversione dell'onere della prova per quanto riguarda il disconoscimento).

L'utilizzo della firma digitale può essere quindi il più vario: dai rapporti con le pubbliche amministrazioni (si pensi, ad esempio, al principio sancito dall'art. 3-bis della L. 241/90: *per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*), alle dichiarazioni fiscali, alle transazioni finanziarie e bancarie, ai rapporti contrattuali, alla fornitura elettronica di beni e servizi, alle operazioni di identificazione e autorizzazione, etc.

Di pari passo con la regolamentazione della firma digitale, si è cercato di risolvere anche il problema relativo alla trasmissione del documento informatico. Il ricorso alla posta elettronica per l'invio del messaggio informatico, infatti, si è rivelato inadatto a garantire la provenienza del documento da parte di un soggetto determinato, l'integrità del contenuto e, soprattutto, la volontarietà dell'invio. Per ottenere gli stessi effetti prodotti da una lettera raccomandata con ricevuta di ritorno si è quindi fatto ricorso alla Posta Elettronica Certificata (PEC). Con tale sistema il mittente riceve l'attestazione, da parte del gestore della posta elettronica, dell'invio e della consegna dei documenti informatici (anche privi di firma digitale) al destinatario (recitius, al provider del destinatario). La certificazione fornita dal gestore di PEC costituisce prova legale dell'avvenuta trasmissione di un messaggio, come accade per l'avviso di ricevimento nella raccomandata<sup>4</sup>. Per ottenere tale risultato è però necessario che anche il destinatario abbia un indirizzo di posta elettronica certificata; in caso contrario, l'effetto ottenuto sarà assimilabile ad una raccomandata senza ricevuta.

Il D.P.R. 11 febbraio 2005 n. 68 disciplina le modalità di utilizzo della PEC<sup>5</sup>: i provider della posta elettronica certificata, enti autorizzati e molto simili ai certificatori della firma digitale, appena ricevono il messaggio da inviare forniscono al mittente la ricevuta di accettazione. Subito dopo il messaggio viene inserito dal gestore in una busta di trasporto, unitamente alla relativa ricevuta fornita. La busta e la ricevuta vengono quindi sottoscritte con firma elettronica avanzata e ad ogni messaggio viene apposta una marcatura temporale (time stamping). La busta viene quindi inviata al destinatario: il gestore della PEC del destinatario invia al gestore del mittente una ricevuta

di presa in carico ed effettua dei controlli sulla presenza di virus o altre anomalie. Terminati tali controlli, il gestore del destinatario invia una ricevuta di avvenuta consegna che, indipendentemente dalla avvenuta lettura, certifica che il messaggio è stato consegnato nella casella di PEC del destinatario. Qualora l'e-mail non sia consegnabile (ad es. account non più attivo), il gestore comunica al mittente nelle ventiquattro ore successive la mancata consegna.

Tale procedura di trasmissione è valida agli effetti di legge<sup>6</sup>.

Il sistema così come è attualmente configurato e previsto presenta però due inconvenienti che ne rallentano la diffusione<sup>7</sup>: il primo è la conoscibilità dell'indirizzo di posta elettronica certificato del destinatario (la legge parla di indirizzo "dichiarato" o addirittura "espressamente dichiarato"<sup>8</sup>); il secondo è quello relativo ai costi, soprattutto se rapportato all'e-mail, quasi sempre gratuita.

#### NOTE

<sup>1</sup> Si veda la Legge 7 giugno 1993, n. 183 (in Gazz. Uff., 14 giugno, n. 137). - Norme in materia di utilizzazione dei mezzi di telecomunicazione per la trasmissione degli atti relativi a procedimenti giurisdizionali. L'art. 1 prevede che, in presenza di determinati requisiti, "*la copia fotocopiatrice di un atto del processo redatto e sottoscritto da un avvocato o da un procuratore e trasmesso a distanza attraverso i mezzi di telecomunicazione ad altro avvocato [o procuratore], si considera conforme all'atto trasmesso*".

<sup>2</sup> Secondo tale norma "*per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*".

<sup>3</sup> L'hash MD5 è rappresentato come una sequenza di 32 cifre esadecimali. Il famoso incipit dell'Iliade "Contami o diva del pelide Achille l'ira funesta" corrisponde alla seguente stringa: b4dd7f0b0ca6c25dd46cc096e45158eb. Basta cambiare una lettera "Contami o diva del pelide Achille l'ira funesta" e la stringa cambia completamente: f065b51db9c592bf6ecf66a76e39f8d0. Tale esempio è riportato su

<http://it.wikipedia.org/wiki/MD5>

<sup>4</sup> L'art. 45 del Codice dell'Amministrazione Digitale è chiaro sul punto: il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

<sup>5</sup> Per le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica è stato emanato il D.P.C.M. - Dipartimento per l'innovazione e le Tecnologie 2 novembre 2005 (in Gazz.Uff., 15 novembre, n. 266). - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.

<sup>6</sup> Si veda l'art. 14 D.P.R. 445/2000 (ora abrogato) ed il D.P.R. 11 febbraio 2005 n.68 (in Gazz. Uff., 28 aprile, n. 97). - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata. Sul punto anche l'art. 48 del Codice dell'Amministrazione Digitale che riconosce alla trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, la stessa efficacia, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

<sup>7</sup> Si veda a tal proposito la Legge 16 gennaio 2003 n. 3 (in Suppl. ordinario n. 5 alla Gazz. Uff., 20 gennaio, n. 15). - Disposizioni ordinamentali in materia di pubblica amministrazione. L'art 27 prevede, tra i vari obiettivi da conseguire, la diffusione dell'uso delle firme elettroniche.

<sup>8</sup> È previsto, ad esempio, che le imprese, nei rapporti tra loro intercorrenti, possano dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese.

Da ultimo va segnalato che la Legge 6 agosto 2008, n. 133 ha previsto espressamente all'art. 51 che le notificazioni e le comunicazioni di cui al primo comma dell'articolo 170 del codice di procedura civile, la notificazione di cui al primo comma dell'articolo 192 del codice di procedura civile e ogni altra comunicazione al consulente vengano effettuate per via telematica all'indirizzo elettronico "comunicato" ai sensi dell'articolo 7 del regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2001, n. 123.

## **I LIMITI DI UTILIZZABILITÀ DEI DATI NELL'AMBITO DEL PROCESSO**

**Giulia Ferrarese**

Avvocato in Verona

### **I riferimenti normativi**

Come noto, per trattare lecitamente i dati personali del cliente nell'ambito del processo è innanzitutto necessario rendere allo stesso l'informativa di cui all'art. 13 D.Lgs. 196/03<sup>1</sup>.

Non è invece necessario rendere l'informativa ai terzi di cui si trattano i dati nel processo (ad esempio controparte, testimoni, terzo chiamato etc.), atteso il disposto dell'art. 13, 5° D. Lgs. cit.

Con riferimento all'altro adempimento preliminare al trattamento dei dati personali e cioè il rilascio del consenso al trattamento dei dati, due norme del D.Lgs. cit. (artt. 24, lett. f) e 26 lett. c)<sup>2</sup> per i trattamenti posti in essere nell'ambito del processo esonerano da tale adempimento purché i dati siano trattati esclusivamente per la finalità della difesa in giudizio e per il tempo a ciò strettamente necessario.

Le altre modalità da rispettare per un corretto e lecito trattamento dei dati nell'ambito del processo sono dettate dall'art. 11 D.Lgs. cit. il quale prevede la necessità che i dati personali siano:

- 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.

Il secondo comma del medesimo art. 11<sup>3</sup> dispone che i dati personali trattati in violazione delle modalità sopra indicate non possono essere utilizzati. Oltre che la parti ed i loro difensori, nell'ambito del processo sono tenuti a rispettare le modalità per il trattamento dei dati indicate dall'art. 11 anche il giudice ed i suoi ausiliari (l'art. 47<sup>4</sup> D.Lgs. cit., dettato con riferimento ai trattamenti effettuati presso gli uffici giudiziari, non esonera infatti dall'osservanza del disposto fondamentale di cui all'art. 11).

### **Il conflitto tra protezione dei dati personali e diritto di difesa**

Come noto, il diritto di difesa è garantito dall'art. 24 cost. mentre il diritto alla protezione dei dati personali, pur essendo considerato un diritto fondamentale, non è di rango costituzionale.

È pertanto lecito utilizzare nell'ambito del processo dati personali, anche di terzi, per far valere o difendere un diritto.

Per agevolare il diritto di difesa nell'ambito del processo, come visto, non è nemmeno richiesto il consenso del cliente o di terzi di cui si trattino dati personali.

Il D. Lgs. cit. pone tuttavia come limite e condizione per il trattamento lecito dei dati, anche per le finalità di difesa nell'ambito del processo, il rispetto delle modalità di cui all'art. 11<sup>5</sup>.

Quando poi il trattamento riguarda dati di terzi particolarmente sensibili (idonei a rivelare lo stato di salute o la vita sessuale) non è consentito utilizzare detti dati nel processo se il diritto che si vuole difendere o far valere non è di rango almeno pari a quello del diritto alla protezione dei dati personali (e pertanto deve trattarsi quanto meno di far valere un diritto fondamentale).

### **Le conseguenze dell'utilizzo illecito dei dati**

Si ritiene che esista un limite generale all'assunzione ed acquisizione di prove nel processo nei casi di illiceità della loro formazione o assunzione o di indisponibilità della prova. Ci si riferisce al concetto di "prova illecita", definita come prova vietata perché contraria a divieti di legge.

La violazione di ogni divieto posto dalla legge comporta l'inutilizzabilità della prova.

Anche la prova assunta in violazione dei limiti stabiliti dall'art. 11 per il trattamento dei dati è pertanto contraria ad un divieto di legge e può essere considerata una prova illecita.

La conseguenza è dunque la non utilizzabilità ai fini probatori delle prove e pertanto dei dati introdotti nel processo in violazione dell'art. 11.

Il secondo comma dell'art. 11, d'altronde, espressamente sancisce che "I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati".

### **L'utilizzabilità dei documenti**

Anche per le prove c.d. precostituite (i documenti) è necessario, per la loro corretta utilizzazione nel processo, valutare innanzitutto se siano state lecitamente acquisite.

Un documento illecitamente sottratto alla controparte o a terzi ovvero ottenuto ad esempio senza il rispetto dei limiti di accesso ai documenti amministrativi non può essere utilizzato nel processo.

Bisognerà poi valutare se le produzioni documentali siano pertinenti rispetto all'oggetto del giudizio e non eccedenti rispetto alla finalità della causa, se siano corretti ed aggiornati.

Se dunque vengono prodotti in giudizio documenti illecitamente acquisiti ovvero che non rispettano le modalità indicate dall'art. 11, il giudice li dovrà espungere dal processo e non ne dovrà tenere conto.

Analogamente, per le prove costituente il giudice dovrà avere cura di non ammettere e non assumere prove che comportino violazione della normativa sulla protezione dei dati in quanto prove illecite<sup>6</sup>.

### **L'evoluzione della giurisprudenza**

La tematica in esame ha cominciato ad essere oggetto delle prime pronunce da parte dei Tribunali.

Va segnalata in particolare l'ordinanza 14.07.07 resa dal Tribunale di Roma nel procedimento cautelare n. 26125 R.G. tra Techland e Peppermint GmbH. contro Wind telecomunicazioni, in cui è intervenuto il Garante. Nel provvedimento si precisa che l'art. 24 D.Lgs. cit.,(che consente l'uso di dati personali

senza il consenso dell'interessato ove gli stessi siano strumentali a far valere o difendere un diritto in giudizio) presuppone che il dato personale utilizzato nel processo senza il consenso del terzo sia già in possesso dell'utilizzatore e, soprattutto, che tale possesso sia avvenuto legittimamente. Nel caso esaminato il Giudice aveva osservato che il possesso parziale di dati personali dei presunti autori delle violazioni era stato ottenuto dalle ricorrenti (che avevano avanzato richiesta di esibizione di dati personali) in modo illecito, trattandosi di dati acquisiti senza l'autorizzazione dell'Autorità garante (art. 37 D.Lgs. cit.) e del consenso informato degli interessati.

Detti dati erano stati infatti acquisiti dalle ricorrenti avvalendosi del servizio di una società terza che aveva svolto un'opera di monitoraggio inserendosi nella rete peer to peer e simulando di essere un fruitore di servizi, in violazione dei diritti di segretezza delle comunicazioni elettroniche e telematiche tra privati (divieti che è lecito superare solo per la repressione di illeciti penali di particolare gravità, come quelli mafiosi, o quelli in danno di sistemi informatici).

Il Tribunale ha pertanto ritenuto che la connotazione illecita dei dati parziali già acquisiti (codici IP e GUID) abbia determinato, ai sensi dell'art. 11, comma 2 D.Lgs. cit., la completa inutilizzabilità dei dati in sede giudiziale. Nel caso di specie, il Tribunale ha quindi respinto l'istanza cautelare considerando i predetti dati non utilizzabili come prova della sussistenza di seri elementi per valutare la fondatezza della domanda.

Di segno diverso una precedente pronuncia del Tribunale di Bari (sentenza 16.02.2007) nella quale si afferma che "qualsiasi violazione di leggi o regolamenti nell'utilizzo processuale delle prove (ivi comprese le norme del c.d. codice della privacy) può trovare esito solo nell'ambito dei rispettivi sistemi processuali e siccome nel processo civile non esisterebbe un divieto esplicito di utilizzo; siccome nel campo delle prove precostituite i momenti di illiceità sarebbero tutti di natura preprocessuale, un documento illecitamente ottenuto in danno della parte avversa e/o utilizzato fuori delle condizioni dell'art. 26 del citato codice sarebbe comunque utilizzabile come prova, salve le conseguenze extraprocessuali, civili e penali, del comportamento illecito che si è consumato", da farsi valere cioè in altra sede processuale (art. 152 D. Lgs.).

Il ragionamento non convince in quanto, con riferimento alla prova precostituita (documento), l'illiceità, benché avvenuta in tempo anteriore alla produzione del documento in giudizio, si estende alle conseguenze volute o prevedibili, e pertanto ne consegue che la "qualifica di illecito si estende anche alla produzione in giudizio, qualora, questa costituisca lo scopo ovvero sia percepita come possibile scopo dall'autore dell'illecito"<sup>7</sup>.

Di recente la Corte di Cassazione (leggasi per intero la sentenza 22602 del 14 maggio 2008) ha implicitamente riconosciuto il principio della non utilizzabilità delle prove "illecite", principio che (con l'eccezione di alcune pronunce di segno contrario) si viene man mano affermando sia a livello giurisprudenziale che di dottrina e che, come vedremo, è stato richiamato anche nello schema preliminare di codice di buona condotta.

Non si dimentichi poi che tramite la consultazione dei pubblici registri ed il diritto di accesso (oggi esteso anche a favore di terzi, purché portatori di un interesse tutelabile in sede giudiziaria per la cui difesa sia indispensabile conoscere i dati personali di altri soggetti<sup>8</sup>) o altri strumenti processuali (art. 210 e segg. cpc: ordini di esibizione o informazioni) è possibile entrare lecitamente in possesso di documenti utili ai fini della prova nel giudizio.

### **Il recente documento del Garante in tema di trattamenti da parte dei consulenti tecnici e dei periti (linee guida)**

Con riferimento ai trattamenti effettuati nell'ambito del processo da parte di consulenti tecnici e periti, il Garante ha emanato in data 26.06.08 alcune "linee guida" volte a prevenire i rischi connessi a detti trattamenti.

Nel documento si precisa che ai trattamenti posti in essere dai predetti ausiliari del giudice si applicano le norme del Codice (D.Lgs. n. 196/03) relative ai trattamenti effettuati presso uffici giudiziari "per ragioni di giustizia" e pertanto l'art. 47 D.Lgs. cit.. Detta norma esonera dall'osservanza di alcune disposizioni del Codice mentre restano pienamente applicabili altre norme ed in particolare l'art. 11 che prescrive il rispetto dei principi di liceità e correttezza e l'osservanza delle altre modalità di trattamento indicate<sup>9</sup>.

I consulenti ed i periti possono pertanto trattare i dati personali nei limiti in cui ciò è necessario per l'espletamento dell'incarico e devono adottare

modalità di trattamento proporzionate allo scopo perseguito. L'utilizzo incrociato di dati è consentito solo se collegato alle indagini ed autorizzato dalle autorità giudiziari e competenti.

Le informazioni aventi ad oggetto dati personali sono utilizzabili solo se contribuiscono a fornire un quadro corretto e completo del caso e se effettivamente necessarie all'accertamento nonché pertinenti, specie se di natura sensibile o di carattere giudiziario o relative a soggetti estranei al procedimento.

Espletato l'incarico, il consulente od il perito devono depositare nel giudizio la relazione redatta nonché la documentazione agli stessi consegnata e quella acquisita nel corso dell'attività e non possono conservare (in originale o in copia, in formato elettronico o in cartaceo) informazioni e dati personali acquisiti nel corso dell'incarico.

Ai fini fiscali o contabili è consentito conservare solo i dati personali effettivamente necessari. In caso di richiesta di chiarimenti o di supplemento di indagine, i consulenti e periti potranno sempre acquisire dal fascicolo di causa la documentazione necessaria.

Al fine di evitare una indebita divulgazione delle informazioni acquisite nonché la loro perdita o distruzione, devono essere adottate dagli ausiliari le misure idonee e preventive nonché le misure minime prescritte dalla legge e, nell'ipotesi di trattamento di dati sensibili o giudiziari, dovrà essere altresì redatto il documento programmatico.

Anche i consulenti di parte potranno trattare solo i dati necessari, pertinenti e non eccedenti ed i dati sensibile o giudiziari se indispensabile. Dovranno anch'essi adottare le misure idonee e quelle minime di legge e, se del caso, redigere il documento programmatico.

### **I limiti nella pubblicazione delle sentenze**

Non è consentita la diffusione (su riviste giuridiche, supporti elettronici o reti di comunicazioni elettroniche) di sentenze o altri provvedimenti contenenti i dati identificativi di minori o delle parti dei procedimenti in materia di famiglia o stato delle persone.

Vanno parimenti omessi, nei casi di diffusione di cui sopra, i dati identificati-

vi dei soggetti interessati qualora gli stessi ne abbiano fatto richiesta (prima della definizione del procedimento) ovvero l'autorità giudiziaria ne abbia disposto d'ufficio l'omissione (a tutela della dignità o dei diritti di tali soggetti). Negli altri casi è consentita la diffusione anche integrale delle sentenze e degli altri provvedimenti giurisdizionali (art. 52D. Lgs. cit.).

### **Lo schema preliminare del Garante per il codice di deontologia e buona condotta per il trattamento dei dati personali effettuato per far valere o difendere un diritto in sede giudiziaria**

È stato recentemente elaborato uno "schema preliminare" di codice di deontologia e buona condotta la cui adozione è prevista dall'art. 12 D.Lgs. cit. Attualmente lo stesso è in corso di approvazione.

Nello schema preliminare si ribadisce che è consentito il trattamento dei dati per esigenze difensive (sia nel corso di un procedimento che nella fase propedeutica allo stesso) purché i dati siano strettamente funzionali all'esercizio del diritto di difesa ed il trattamento sia effettuato in conformità ai principi di proporzionalità, pertinenza, completezza e non eccedenza rispetto alle finalità difensive contenuti nell'art. 11 D.Lgs.

Nel preambolo dello schema si precisa che, se non vengono rispettate le garanzie e gli accorgimenti per la protezione dei dati previsti dalla legge, i dati trattati sono inutilizzabili (art. 11, comma 2 D.Lgs.). Atteso che lo schema preliminare disciplina proprio i trattamenti effettuati per far valere un diritto in sede giudiziaria (o in fase propedeutica al giudizio), viene in tal modo confermato che la conseguenza dell'inutilizzabilità dei dati (ad esempio sotto il profilo probatorio) verifica anche nell'ambito del processo.

Nello schema preliminare sono contenute alcune regole complementari (ulteriori rispetto alle disposizioni contenute nel D.Lgs. 196/03 e nelle altre fonti in materia), che sono anch'esse condizione di liceità e correttezza del trattamento.

Viene in particolare raccomandata l'adozione di idonee cautele per il trattamento dei dati nei casi di acquisizione di dati con alto grado di confidenzialità o che comportano rischi specifici per gli interessati, scambio di corrispondenza per via telematica, esercizio contiguo di attività autonome all'in-

terno dello studio, utilizzo di dati di cui è dubbio l'impiego lecito per il ricorso a tecniche invasive, utilizzo di dati riportati su supporti elettronici (registrazioni audio video) o documenti (tabulati di flussi telefonici e informatici, relazioni di investigatori privati), ricerche su banche dati a uso interno, consultabili anche da uffici situati altrove, acquisizione di dati e documenti da terzi (verificando se si abbia titolo per ottenerli), conservazione di atti relativi ad affari definiti.

Con riferimento alla conservazione dei dati, nello schema si precisa che atti e documenti possono essere conservati (in originale ed in copia ed anche in formato elettronico) anche dopo l'estinzione del procedimento qualora ciò sia necessario per altre ipotizzabili esigenze difensive della parte o dell'avvocato. Se la conservazione è prevista per adempiere ad un obbligo normativo (ad esempio in materia fiscale) vanno conservati i soli dati effettivamente necessari.

Si richiamano per approfondimenti bibliografici:

F. Antezza, *Prove illecite, dati sensibili ed utilizzabilità processuale*, in "Il merito" n. 4/07, p. 22 e segg.

G.F. Ricci, *Le prove illecite nel processo civile*

M. Conte, *Le prove civili*, Giuffrè. 2005

G. Ferrarese, *Deontologia, processo civile e trattamento dati*, in "Rassegna forense", luglio-dicembre 2005, n. 3-4, p.1017 e segg.

*Lo schema preliminare del Garante del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per far valere o difendere un diritto in sede giudiziaria*, relazione del convegno su "L'informatizzazione dello studio legale" tenutosi a Verona il 16.06.08.

#### NOTE

<sup>1</sup> Art. 13. Informativa (omissis)

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

<sup>2</sup> Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento: (omissis)

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

Art. 26. Garanzie per i dati sensibili (omissis)

I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

<sup>3</sup> Art. 11. Modalità del trattamento e requisiti dei dati (omissis)

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

<sup>4</sup> Art. 47. Trattamenti per ragioni di giustizia

1. In caso di trattamento di dati personali effettuato presso uffici giudiziari di ogni ordine e grado, presso il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia, non si applicano, se il trattamento è effettuato per ragioni di giustizia, le seguenti disposizioni del codice:

a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;

b) articoli da 145 a 151.

2. Agli effetti del presente codice si intendono effettuati per ragioni di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controver-

sie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari. Le medesime ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione.

<sup>5</sup> Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

- 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.

(omissis)

<sup>6</sup> Va osservato che in relazione al trattamento di dati effettuato per ragioni di giustizia (dal magistrato, dalle cancellerie e segreterie giudiziarie e dagli ausiliari del giudice) non è consentito al parti proporre ricorso al Garante. Quest'ultimo conserva peraltro il proprio autonomo potere di svolgere accertamenti nei riguardi di trattamenti effettuati da magistrati ed uffici giudiziari (sia pure con modalità che garantiscano il rispetto delle reciproche attribuzioni). L'intervento del Garante che accerti violazioni della normativa sulla protezione dei dati non produce automaticamente i propri effetti sulla "validità, efficacia e utilizzabilità di atti, documenti e provvedimenti giudiziari basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento (che) restano disciplinate dalle pertinenti disposizioni processuali nella materia civile o penale" (art. 160, comma 6 D. Lgs. 196/03). Come osservato (Codice della privacy, Giuffrè editore, 2004, p. 2109) l'art. 160 D. Lgs. cit. ha inteso evitare automatici effetti caducatori sugli atti e i documenti, utilizzati in procedimenti giudiziari penali e civili, che siano il risultato di trattamenti di dati che, a seguito di accertamenti effettuati dal Garante, siano giudicati non conformi alle disposizioni di legge.

<sup>7</sup> Sul punto leggasi Conte, *Le prove civili*, Giuffrè, 2005, p. 591, il quale richiamando anche il De Stefano, conclude che: " diversamente opinando si verrebbe ad ammettere l'utilizzabilità di tutte le prove precostruite illecite, in quanto per le stesse il vizio attiene evidentemente soltanto alla fonte".

<sup>8</sup> Con riferimento poi alla richiesta di accesso a dati personali di terzi (nella fattispecie richiesti ad una Compagnia di assicurazione in funzione propedeutica all'instaurazione di un eventuale giudizio) vi è da segnalare la sentenza 19.12.2007 n. 13988 del Tribunale di Milano che ha statuito che l'art. 24 D.Lgs. cit. non può interpretarsi nel senso restrittivo di consentire il trattamento solo da parte del titolare dei dati e per esigenze di difesa proprie di questo ma anche a favore di terzi purché portatori di un interesse tutelabile in sede giu-

diziaria e per la cui difesa sia indispensabile conoscere i dati personali di altri soggetti (senza che sia peraltro necessario provare la fondatezza del diritto che si vuole tutelare). Il Tribunale (adito a seguito del diniego di accesso ai dati) ha pertanto ordinato alla Compagnia di Assicurazione di esibire ai ricorrenti (genitori legittimari pretermessi nelle disposizioni testamentarie del figlio e che intendevano proporre azione di riduzione contro la nuora) le polizze assicurative aventi quale contraente o beneficiaria la nuora stessa, erede testamentaria del figlio deceduto.

<sup>9</sup> Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero in Gazzetta Ufficiale n. 178 del 31 luglio 2008.



**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 2008*.

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 2008*

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* 2008.