

Diritto dell'Internet

Bimestrale di dottrina, giurisprudenza, prassi sulle nuove tecnologie, privacy, e-government e processo telematico

DIRETTORE SCIENTIFICO:
Giuseppe Cassano

COMITATO SCIENTIFICO:

Michele Ainis
Mario Bessone
Renato Borruso
Renato Clarizia
Giovanni Comandè
Pasquale Costanzo
Astolfo Di Amato
Ugo Draetta
Giovanni Duni
Vincenzo Franceschelli
Aurelio Gentili
Mario Jori
Adelmo Manna
Mario Morcellini
Nicola Palazzolo
Lorenzo Picotti
Giovanni Sartor
Filippo Satta
Paolo Spada
Luigi Carlo Ubertazzi

ANNO IV - LUGLIO-AGOSTO 2008
Direzione e redazione
Strada 1 Palazzo F6
20090 Milanofiori Assago (MI)

00093022

TARIFFA R.O.C.: POSTE ITALIANE SPA - SPEDIZIONE
IN ABBONAMENTO POSTALE - D.L. 353/2003 (CONV. IN
L. 27/02/2004 N. 46) ART. 1, COMMA 1, DCB MILANO


Diritto
dell'Internet
on-line

4

2008

www.ipsoa.it

Pubblicazione *on-line*
dei redditi



Procura telematica

**Regole tecniche del casellario
giudiziario telematico**



IPSOA

Gruppo Wolters Kluwer

SOMMARIO

■ ATTUALITA'

REDDITI <i>ON-LINE</i> di <i>Giuseppe Cassano</i>	329
LA PUBBLICAZIONE <i>ON-LINE</i> DELLE DICHIARAZIONI DEI REDDITI di <i>Renato Clarizia</i>	333

■ NORMATIVA

Osservatorio della normativa italiana a cura di <i>Fulvio Sarzana di Sant'Ippolito e Enzo Maria Tripodi</i>	335
--	-----

■ GIURISPRUDENZA

Civile	
IL NOME (DI DOMINIO) DI ASSOCIAZIONI (POLITICHE) TRA PROFILI IDEOLOGICI E INTERESSI MEDIATICI Tribunale di Roma, 12 marzo 2008	339
commento di <i>Lara Trucco</i>	340
L'ATTO DIGITALE E LA PROCURA: UNA RAGIONEVOLE SOLUZIONE SUL RILASCIO DELLA PROCURA SPECIALE Tribunale di Milano 1 febbraio 2008, ord.	347
commento di <i>Alessandra Villecco</i>	349
LA COMUNICAZIONE DI CANCELLERIA A MEZZO <i>E-MAIL</i> Cassazione civile, sez. Lavoro, 19 febbraio 2008, n. 4061	356
commento di <i>Francesco Buffa</i>	359
Penale	
PER LA CONFIGURABILITÀ DEL REATO DI ABUSIVO MANTENIMENTO NEL SISTEMA INFORMATICO È NECESSARIO CHE L'AGENTE SIA CONSAPEVOLE DI AGIRE <i>INVITO DOMINO</i> Tribunale di Nola 11 dicembre 2007, n. 488	365
commento di <i>Giovanni Garbagnati</i>	366
Amministrativa	
PROCEDURA DI GARA E ANNOTAZIONE NEL CASELLARIO INFORMATICO PER LA MANCATA DIMOSTRAZIONE DEL POSSESSO DEI REQUISITI DICHIARATI T.A.R. Lazio, Roma, Sez. III, 1 aprile 2008, n. 2773	375
commento di <i>Mattia Pani</i>	376
LA POSTA ELETTRONICA: UNA COMPLESSA QUALIFICAZIONE TRA PRASSI, GIURISPRUDENZA E LEGGE T.A.R. Puglia, Lecce, sez. I, 21 febbraio 2008, n. 562	383
commento di <i>Daniele Marongiu</i>	386
Osservatorio della giurisprudenza italiana a cura di <i>Iacopo Pietro Cimino e Francesco Di Ciommo</i>	389
Osservatorio di diritto internazionale ed europeo a cura di <i>Giovanni Mario Riccio, Guido Scorza e Giovanni Ziccardi</i>	392
■ ARGOMENTI	
IL SISTEMA UNICO NAZIONALE D'INTERCETTAZIONE TRA CONTENIMENTO DELLA SPESA E REGOLE PROCESSUALI di <i>Alberto Cisterna</i>	394
L'INFORMAZIONE DEL CONSUMATORE NELLA COMMERCIALIZZAZIONE A DISTANZA DI SERVIZI FINANZIARI di <i>Valerio Sangiovanni</i>	399

■ PRASSI

LE REGOLE TECNICHE DEL NUOVO CASELLARIO GIUDIZIARIO TELEMATICO

di Alfonso Contaldo e Michele Gorga

411

PHISHING: STRATEGIE OPERATIVE DELL'INGANNO

di Monia Fantini

421

■ RASSEGNA BIBLIOGRAFICA

a cura di Francesco Brugaletta, Carmelo Giurandella, Andrea Lisi, Giuseppe Vaciago

427

■ INDICI

AUTORI

429

CRONOLOGICO

429

ANALITICO

430

ERRATA CORRIGE

Il commento alla sentenza "Tribunale Firenze, sez. lavoro, 7 gennaio 2008, n. 1218", pubblicato sul n. 3/2008 a pagina 291, è a cura dell'avv. Umberto Galasso.

L'articolo è stato pubblicato l'8 marzo u.s. su Teutas.it ed è reperibile nella sua interezza a quest'indirizzo: <http://www.teutas.it/societa-informazione/tutela-dei-dati-personali/33-tutela-dei-dati-personali/62-utilizzo-di-internet-per-motivi-extralavorativi.html>

Diritto dell'Internet

Bimestrale di dottrina, giurisprudenza, prassi sulle nuove tecnologie, privacy, e-government e processo telematico

La rivista si cita: *Dir. Internet*

EDITRICE

Wolters Kluwer Italia S.r.l.
Strada 1, Palazzo F6 - 20090 Milanofiori Assago (MI)

DIRETTORE RESPONSABILE

Donatella Treu

REDAZIONE IPSOA

Manuela Plebani, Isabella Viscardi

INDIRIZZO INTERNET

<http://www.ipsoa.it/dirittoellinternet>

COMITATO DI REDAZIONE

Ercole Aprile, Stefano Aterno, Ernesto Belisario, Francesco Brugaletta, Francesco Buffa, Francesco Giuseppe Catullo, Francesco Celentano, Iacopo Pietro Cimino, Francesco Di Ciommo, Pasquale Fava, Paolo Galdieri, Carmelo Giurandella, Michele Iaselli, Andrea Lisi, Luca Lupària, Massimo Melica, Giovanni Marco Riccio, Fulvio Sarzana di Sant'Ippolito, Guido Scorza, Enzo Maria Tripodi, Giuseppe Vaciago, Giovanni Ziccardi

REALIZZAZIONE GRAFICA

Ipsosa

FOTOCOMPOSIZIONE

ABCompos Srl
via Pavese, 1/3 - 20089 Rozzano (Mi)
Tel. 02 57789422

STAMPA

Arti Grafiche Stefano Pinelli - Via Farneti, 8
20129 Milano

REDAZIONE

Per informazioni in merito a contributi, articoli ed argomenti trattati scrivere o telefonare a:

IPSOA Redazione

Diritto dell'Internet

Caseella postale 12055 - 20120 Milano
telefono (02) 82476.831 - telefax (02) 82476.055
e.mail: redazione.dirittodellinternet.ipsoa@wki.it

AMMINISTRAZIONE

Per informazioni su gestione abbonamenti, numeri arretrati, cambi d'indirizzo, ecc.

scrivere o telefonare a:

IPSOA Servizio Clienti
Caseella postale 12055 - 20120 Milano
telefono (02) 824761 - telefax (02) 82476.799
Servizio risposta automatica
telefono (02) 82.476.999

PUBBLICITÀ:



db Consulting srl Events & Advertising
via Leopoldo Gasparotto 168
21100 Varese
tel. 0332/282160
fax 0332/282483
e-mail: info@db-consult.it
www.db-consult.it

Spedizione in abbonamento postale - 45% - art. 2 comma 20/b legge 662/96 - Filiale di Milano
Iscritta al R.O.C. n. 1702 in data 4 settembre 2001

ABBONAMENTI

Gli abbonamenti hanno durata annuale, solare: gennaio-dicembre; rolling: 12 mesi dalla data di sottoscrizione, e si intendono rinnovati, in assenza di disdetta da comunicarsi entro 30 gg. prima della data di scadenza a mezzo raccomandata A.R. da inviare a Wolters Kluwer Italia s.r.l. Strada 1 Pal. F6 Milanofiori 20090 Assago (MI)
Servizio Clienti: tel. 02 824761
e-mail: servizio_clienti@ipsoa.it
www.ipsoa.it/servizioclienti

INDIRIZZO INTERNET

Compresa nel prezzo dell'abbonamento l'estensione *on line* della Rivista, consultabile all'indirizzo www.ipsoa.it/dirittoellinternet

ITALIA

Abbonamento annuale 2008: € 120,00
Abbonamento annuale 2008 + codici legali: € 173,00

ESTERO

Abbonamento annuale 2008: € 240,00

MAGISTRATI e UDITORI GIUDIZIARI - sconto del 30% sull'acquisto dell'abbonamento annuale alla rivista, applicabile rivolgendosi alle Agenzie Ipsosa di zona (www.ipsoa.it/agenzie) o inviando l'ordine via posta

a Wolters Kluwer Italia S.r.l., Strada 1 Pal. F6, 20090 Milanofiori Assago (MI) o via fax al n. 02-82476403 o rivolgendosi al Servizio Informazioni Commerciali al n. 02-82476794.

Nell'ordine di acquisto i magistrati dovranno allegare fotocopia del proprio tesserino identificativo attestante l'appartenenza alla magistratura e dichiarare di essere iscritti all'Associazione Nazionale Magistrati.

MODALITA' DI PAGAMENTO

Versare l'importo sul C/C/P n. 583203 intestato a WKI S.r.l. Gestione incassi - Strada 1, Palazzo F6, Milanofiori oppure

Inviare assegno bancario/circolare non trasferibile intestato a Wolters Kluwer Italia S.r.l. Indicare nella causale del versamento il titolo della rivista e l'anno di abbonamento

Prezzo copia: € 26,00

Arretrati: prezzo dell'anno in corso all'atto della richiesta

DISTRIBUZIONE

Vendita esclusiva per abbonamento

Il corrispettivo per l'abbonamento a questo periodico è comprensivo dell'IVA assolta dall'editore ai sensi e per gli effetti del combinato disposto dell'art. 74 del D.P.R. 26/10/1972, n. 633 e del D.M. 29/12/1989 e successive modificazioni e integrazioni.

Egregio abbonato,

Ai sensi dell'art. 13 del D.Lgs. n. 30.6.2003 n. 196. La informiamo che i Suoi dati sono conservati nel data base informatico del titolare del trattamento, Wolters Kluwer Italia S.r.l. Responsabile del trattamento: Ufficio MID. L'elenco aggiornato di tutti i responsabili del trattamento potrà essere richiesto per iscritto all'Ufficio MID presso la sede della società. I Suoi dati saranno utilizzati dalla nostra società, da enti e società esterne ad essa collegati, nonché da soggetti terzi, titolari autonomi del trattamento, solo per l'invio di materiale amministrativo-contabile, commerciale e promozionale. Ai sensi dell'art. 7 del citato D.Lgs., Lei ha diritto di conoscere, aggiornare, rettificare, cancellare i Suoi dati, nonché di esercitare tutti i restanti diritti ivi previsti, mediante comunicazione scritta a Wolters Kluwer Italia S.r.l., Ufficio MID, Milanofiori, Strada 1-Palazzo F6, 20090 Assago (MI).

Pubblicazione dei redditi *on-line*

Redditi *on-line*

di Giuseppe Cassano

La pubblicazione su Internet dei redditi degli italiani relativi all'anno 2005 è stata un'importante occasione di riflessione sia per gli studiosi che per gli operatori sulla rilevanza della *privacy* nell'attuale era tecnologica, sull'effettivo significato di *privacy* e quindi di "riservatezza" non da tutti compreso, sull'incapacità del legislatore di far fronte alle continue ed ormai quotidiane problematiche create dalle nuove tecnologie, sull'inadeguatezza di organi come l'Autorità Garante preposti alla vigilanza sul rispetto della normativa in materia di protezione dei dati personali e più di ogni altra cosa sulle insidie talvolta imprevedibili che gli strumenti della Rete possono presentare se non utilizzati in maniera legittima ed equilibrata (1).

Il caso è ormai noto: l'Agenzia delle Entrate sulla base di quanto previsto dall'art. 69 d.p.r. 29 settembre 1973, n. 600, come mod. dall'art. 19 l. 30 dicembre 1991, n. 413 e dall'art. 66 bis d.p.r. 26 ottobre 1972, n. 633 ha deciso di pubblicare in un'apposita sezione del proprio sito internet, ai fini della consultazione, gli elenchi nominativi dei contribuenti che hanno presentato le dichiarazioni ai fini dell'imposta sui redditi e dell'imposta sul valore aggiunto, ritenendo in tal modo di dare applicazione alla attuale disciplina che regola la pubblicazione di tali elenchi (2).

Questa decisione ha sollevato pesanti polemiche con forti reazioni sia politiche che sociali e prese di posizione tra l'altro nettamente distanti tra chi era a favore della iniziativa dell'Agenzia e chi decisamente contro. La questione è inevitabilmente giunta sul tavolo dell'Autorità Garante per la protezione dei dati personali che con un provvedimento finale del 6 maggio 2008 ha concluso per l'illegittimità della diffusione dei dati sul sito internet dell'Agenzia delle Entrate.

Ma vediamo di capire le motivazioni di carattere giuridico che hanno indotto l'Agenzia ad assumere tale iniziativa e le motivazioni che giustificano il provvedimento dell'Autorità Garante.

La normativa di riferimento è rappresentata dall'art. 69 del d.p.r. n. 600/1973 che al comma 1 stabilisce che «il Ministro delle finanze dispone annualmente la pubblicazione degli elenchi dei contribuenti il cui reddito imponibile è stato accertato dagli uffici delle imposte dirette e di quelli sottoposti a controlli globali a sorteggio a norma delle vigenti disposizioni nell'ambito dell'attività di programmazione svolta dagli uffici nell'anno precedente», più in particolare il comma 4 sostiene che «il centro informativo delle imposte dirette, entro il 31 dicembre

dell'anno successivo a quello di presentazione delle dichiarazioni dei redditi, forma per ciascun Comune, gli elenchi nominativi da distribuire agli uffici delle imposte territorialmente competenti" i quali secondo il comma 6 "sono depositati per la durata di 1 anno, ai fini della consultazione da parte di chiunque, sia presso lo stesso ufficio delle imposte sia presso i Comuni interessati". Inoltre, analogo adempimento è previsto dall'art. 66 bis del d.p.r. n. 633/1972 relativamente ai contribuenti che hanno presentato la dichiarazione annuale afferente l'imposta sul valore aggiunto.

L'Agenzia delle Entrate ritenendo che la finalità principale di tali disposizioni fosse quella di realizzare un quadro di trasparenza e di circolazione dei dati relativi alla materia fiscale in possesso dell'Amministrazione finanziaria, nel rispetto di quanto sancito dall'art. 2, comma 1 del Codice dell'amministrazione digitale (d.lgs. n. 82/2005) (3) sull'utilizzo delle più appropriate tecnologie dell'informazione e della comunicazione ha proceduto alla pubblicazione dei predetti dati su internet a seguito di specifico provvedimento del Direttore della stessa Agenzia del 5 marzo 2008.

La decisione dell'Agenzia si fondava anche su alcuni provvedimenti dell'Autorità Garante del 17 gennaio 2001 e del 2 luglio 2003, che pur senza entrare nel merito specifico della questione ribadivano come principio di carattere generale che la disposizione in materia di pubblicità degli elenchi dei contribuenti reca «una precisa scelta normativa di consultabilità da parte di chiunque di determinate fonti (elenchi nominativi dei contribuenti che hanno presentato la dichiarazione dei redditi o che esercitano imprese commerciali, arti e professioni), demandando ad un d.m. la previsione solo di alcuni aspetti integrativi della fattispecie attinenti ai termini e alle modalità per la formazione degli elenchi, che sono stati quindi individuati dal Ministero anche per quanto riguarda l'indicazione dei dati reddituali». L'individuazione di tali "termini e modalità" risulta di recente effettuata non più con decreto ministeriale, ma con provvedimento adottato dal Direttore dell'Agenzia delle entrate in quanto di natura tecnico-gestionale.

Note:

(1) Ne avevamo fatto cenno nella mia Presentazione a questa Rivista, 2005, I.

(2) Cfr. Provv. Direttore dell'Agenzia 5 marzo 2008, prot. 197587/2007.

(3) Per le varie delucidazioni sul punto rimandiamo a G. Cassano e C. Giurdanella, *Il codice della pubblica amministrazione digitale*. Commentario

Di contrario avviso è stato il Garante per la protezione dei dati personali che dopo alcuni provvedimenti interlocutori che già lasciavano intendere il proprio orientamento ha redatto in data 6 maggio 2008 un provvedimento con il quale ha accertato l'illegittimità della pubblicazione dei dati reddituali su Internet intesa come vera e propria diffusione inibendo all'Agenzia l'ulteriore medesima diffusione dei dati per i periodi di imposta successivi al 2005, in carenza di idonea base normativa e della preventiva consultazione dell'Autorità. Nel contempo l'Autorità ha anche contestato all'Agenzia delle entrate la specifica violazione amministrativa per l'assenza di un'idonea e preventiva informativa ai contribuenti interessati.

Il Garante, dopo aver ricevuto specifici chiarimenti dall'Agenzia delle entrate, ha fondato la propria decisione su tre punti:

1. la mancanza di una base giuridica di riferimento per la pubblicazione su Internet dei dati reddituali ritenuta tra l'altro una modalità di diffusione sproporzionata in rapporto alle finalità per le quali l'attuale disciplina prevede una relativa trasparenza in quanto i dati, per le caratteristiche intrinseche della Rete, sono stati resi consultabili non presso ciascun ambito territoriale interessato, ma liberamente su tutto il territorio nazionale e all'estero. Inoltre e questo è un aspetto che il Garante ha ritenuto estremamente importante, l'Agenzia non ha previsto alcun limite per la consultazione on-line consentendo a diversi utenti di scaricare i file con i dati dei contribuenti italiani sul loro computer e trattarli liberamente e cosa ancor più grave inserendoli in vari circuiti P2P al fine di metterli in condivisione e permetterne la diffusione a chiunque e senza alcun accorgimento, si colleghi con i vari programmi di *file-sharing*.

2. Il Codice dell'amministrazione digitale per quanto incentivi l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione da parte della P.A. fa espressamente salvi i limiti alla conoscibilità dei dati previsti da leggi e regolamenti (come avviene nel menzionato art. 69), nonché le norme e le garanzie in tema di protezione dei dati personali (artt. 2, comma 5 e 50 d.lgs. 7 marzo 2005, n. 82).

3. L'Autorità non è stata consultata preventivamente dall'Agenzia come prescritto rispetto ai regolamenti e agli atti amministrativi attinenti alla protezione dei dati personali (art. 154, comma 4 del Codice).

In effetti, ad integrazione di quanto affermato dal Garante, va rilevato che per quanto i dati reddituali non possano rientrare nell'ambito di quelli sensibili la cui definizione è fornita dal Codice in maniera tassativa (4), possono essere tranquillamente classificati come dati il cui trattamento ai sensi dell'art. 17 del Codice presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (5).

Inoltre, nell'art. 69 del d.p.r. n. 600/1973 ed in particolare al comma 6, non si parla di pubblicazione, ma di libera consultazione il che è potenzialmente un concetto

molto diverso: la pubblicazione su Internet equivale ad una vera e propria diffusione dei dati non consentita, mentre la consultazione viene limitata a chi ne abbia interesse e ne faccia richiesta esplicita. Lo spirito della norma appare chiaro ed è in questo senso che può lecitamente coniugarsi l'esigenza di trasparenza dell'azione amministrativa con la necessità di tutela della privacy dei cittadini.

D'altro canto il concetto di trasparenza è strettamente legato all'azione amministrativa di un ente pubblico e difatti il comma 1 dell'art. 69 parla esplicitamente di pubblicazione degli elenchi dei contribuenti il cui reddito imponibile è stato accertato dagli uffici delle imposte dirette e di quelli sottoposti a controlli globali a sorteggio, proprio perché in questo caso si tende a far conoscere alla collettività gli accertamenti svolti dagli uffici finanziari. Ben diverso è il caso di specie dove tra l'altro non si ravvisa l'effettiva necessità della pubblicazione *on-line* di questi elenchi connessi esclusivamente a dichiarazioni unilaterali dei cittadini non oggetto di riscontro da parte degli uffici finanziari.

Lo stesso codice dell'amministrazione digitale riconosce un diritto del cittadino all'uso delle nuove tecnologie da parte della P.A. dietro richiesta da parte dei cittadini (art. 3) o comunque riconosce l'uso delle nuove tecnologie nell'ambito di un procedimento amministrativo anche ai fini dell'accesso agli atti endoprocedimentali ricorrendosi alla legge n. 241/1990 (art. 4).

In definitiva l'uso delle nuove tecnologie da parte della P.A. si ricollega ad una logica di trasparenza che sfugge nel caso specifico alla pubblicazione *on-line* di questi elenchi che pare fine a se stessa.

Molti, invece, proprio per la ragione opposta hanno approvato l'iniziativa dell'Agenzia che avrebbe avuto il merito di rendere trasparenti questi dati fiscali e quindi di evidenziare l'urgenza della lotta all'evasione fiscale e l'abnorme divaricarsi della forbice della disuguaglianza fra cittadini. Addirittura molti hanno rilevato che quello dell'Agenzia è stato "un atto dovuto e civile per un Paese che intende emergere da una giungla di furbizie e mezze verità" (6). Ora aldilà di tali dichiarazioni ad effetto appare che, come già detto, nella sostanza giuridica tale atto non sembrerebbe giustificato né dalla legge né dai principi generali in tema di trasparenza amministrativa.

Note:

al D.Lgs. n. 82 del 7 marzo 2005, Milano, 2005, 1-708.

(4) Si tratta di quei dati personali - come noto - idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dei dati personali idonei a rivelare lo stato di salute e la vita sessuale.

(5) Lo riafferma in relazione alla questione di cui discutiamo A. Monti, *Vuoto normativo? La legge che vieta è già in vigore*, in *Il sole 24ore*, Milano, quotidiano del 3 maggio 2008.

(6) Così risulta da un *Comunicato CGIL* ripreso dalla maggiori agenzie stampa, dei primi di maggio c.a..

Ovviamente, di converso, sono tutte da verificare le iniziative di molte associazioni di consumatori che sono direttamente partite con esplicite richieste di risarcimento danni in mancanza di un accertamento effettivo dell'esistenza del reato o del fatto illecito e senza aver dimostrato in concreto il pregiudizio subito (7).

Ma come sottolineato in premessa e come anticipato del resto dalla stessa Autorità nel proprio provvedimento il caso di specie ha evidenziato i pericoli che non la Rete in quanto tale, ma un uso distorto della stessa possono rappresentare per la collettività (8). Difatti, anche una semplice disattenzione o negligenza commessa per il tramite della rete può tradursi in una catastrofe poiché dati estremamente delicati possono essere immediatamente catturati e condivisi poi nei circuiti P2P i quali sono difficilmente tracciabili o comunque controllabili. Nei confronti di questi soggetti si potrebbe configurare l'applicazione dell'art. 167 del Codice per la protezione dei dati personali anche se rimane difficile la dimostrazione dell'effettiva volontà di arrecare danno agli interessati. Il problema, purtroppo, non sta tanto nella punibilità di questi soggetti, ma nell'inadeguatezza degli attuali strumenti legislativi a disciplinare i fenomeni connessi alle nuove tecnologie.

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati. Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche (9).

Il rischio che la diffusione dei documenti elettronici e l'interconnessione di archivi informatici possano comportare una riduzione dei diritti della persona e della riservatezza dei dati personali è estremamente alto. Ciò anche in considerazione del fatto che su questi profili l'Italia non è dotata di una legislazione in tutto idonea a contemperare le esigenze di semplificazione e razionalizzazione dell'attività economica e commerciale con quelle di tutela della persona, anche in attuazione delle prescrizioni e dei principi generali già contenuti nella normativa comunitaria.

Lo sviluppo della rete ha inoltre contribuito, secondo il Garante, alla concezione di un "corpo elettronico" della persona ripartito in diverse banche dati. Oggi le potenziali aggressioni del diritto all'identità personale non provengono esclusivamente da atti, fisici o immateriali, che comportano un'invasione della propria sfera privata. L'evoluzione tecnologica, infatti, se da un lato ha reso sempre più semplici ed accessibili i meccanismi attraverso i quali la pretesa di solitudine dell'individuo tende ad

essere compressa, dall'altro ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate che consentono di risolvere o quanto meno di attenuare in radice questo fenomeno. Cioché diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto. Difatti, nell'attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. "persona elettronica" attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto (10). Sul punto, in Italia, il recente Codice per la protezione dei dati personali ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato, ma tale approccio non impedisce che quando la legge interviene è già troppo tardi in merito ai danni provocati alla collettività e la stessa Autorità ha dimostrato di non poter agire alla luce dell'attuale normativa con la necessaria tempestività che l'uso dello strumento elettronico e/o telematico richiederebbe (11).

Note:

(7) Sulla bontà delle nuove forme di danno non patrimoniale e nella specie del danno esistenziale, e con le precisazioni del caso di evitare danni bagatellari, si rimanda a G. Cassano, *Provare, risarcire e liquidare il danno esistenziale. Valutazione e quantificazione del nuovo danno non patrimoniale*. Introduzione di Pier Giuseppe Monateri. Premessa di Paolo Cendon, Milano 2005, 1-505.

(8) Ne sottolinea questo profilo M. Melica, *Redditi on-line: una questione di diritto mentre la rete resta sconosciuta*, nella *Rivista telematica* www.altalex.com consultata il 2 giugno 2008.

(9) È l'indagine condotta - nel mio primo capitolo - in G. Cassano, *Diritto dell'Internet*. Il sistema di tutele della persona, Milano 2005, 1-401. Sulle interferenze in tema, avevamo già discusso in G. Cassano, *La tutela della reputazione*. Casistica giurisprudenziale in tema di diffamazione, aggiornata alle problematiche legate all'avvento di Internet, alle questioni di competenza ed alla responsabilità dei c.d. "soggetti neutri", Piacenza, 2002, 1-480.

(10) Le ricostruzioni più lucide si devono a Stefano Rodotà. Cfr. da ultimo S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano 2006 e, per completezza della sintesi delle questioni, cfr. M. Iaselli, *Compendio di informatica giuridica*, Napoli, 2007.

(11) Sul tema specifico il suggerimento è di M. Cammarata, *Quella che manca è la cultura della privacy*, nella *Rivista telematica* www.interlex.com consultata il 2 giugno 2008.

Per risolvere questa non facile problematica si dovrebbe agire su due versanti. Innanzitutto, da un lato intensificare quelle misure di sicurezza che specialmente su Internet devono in qualche modo controbilanciare l'enorme flessibilità della Rete ed introdurre una sorta di "educazione civica all'uso della rete" poiché spesso chi usa gli strumenti della Rete non ne comprende le conseguenze. Dall'altro porre mano, qualora sia possibile, ad una revisione normativa di tutte quelle disposizioni che vanno in qualche modo adeguate all'evoluzione tecnologica, e così in questo modo soddisfare l'esigenza di individuare opportune soluzioni e misure di protezione per garantire un giusto equilibrio tra l'esigenza di forme proporzionate di conoscenza dei dati personali e la tutela dei diritti degli interessati (12).

Non va comunque mai dimenticato che il concetto di privacy rientra in un ambito per certi versi più ampio di "riservatezza" ed è estremamente connesso alla tutela di valori di rango costituzionale come la libertà, dignità, in-

tegrità della persona. Tale concetto con l'avvento della Rete e delle nuove tecnologie si è sicuramente evoluto, ma non affievolito, anzi va difeso strenuamente a tutela della persona in quanto tale (13).

Note:

(12) Pur a fronte di considerazioni in parte diverse, sembra che l'auspicio sia lo stesso di R. Clarizia, *La pubblicazione on-line delle dichiarazioni dei redditi*, in questa *Rivista*, 4, 2008, 333.

(13) La questione in esame potrebbe essere per eccellenza uno di quei casi in cui la risposta da darsi potrebbe essere ragionevolmente diversa per mezzo di argomentazioni differenti. In questi casi una chiarezza normativa certamente avrebbe agevolato la soluzione del caso, che al di là della fermezza delle proprie opinioni, potrebbe essere un ottimo spunto per esercitazioni seminariali ad uso degli studenti in tema di argomentazioni giuridiche, oppure per gli studiosi, che, a fronte del coacervo normativo da dipanarsi, a difesa delle proprie soluzioni, potrebbero essere meglio supportati dalla lettura - ed è amara conclusione - di (pubblicato postumo nel 1864) A. Schopenhauer, *L'arte di ottenere ragione esposta in 38 stratagemmi*, nella edizione di Adelphi, 1991, 1-124, che da un ferreo argomentare giuridico.

RIVISTE

Danno e responsabilità

La rivista più autorevole e tempestiva sulla responsabilità civile

Direzione scientifica: Vincenzo Carbone, Pier Giuseppe Monateri, Roberto Pardolesi, Giulio Ponzanelli, Vincenzo Roppo
Periodicità: mensile



La rivista è interamente dedicata alla tematica del risarcimento del danno patrimoniale e non patrimoniale, attraverso l'analisi completa e tempestiva dell'evoluzione legislativa e giurisprudenziale in materia. Il mensile si articola in due macro-sezioni. Materiali e opinioni: articoli di dottrina, tabelle per la quantificazione dei risarcimenti di determinate classi di danni; Giurisprudenza: le sentenze più innovative e interessanti della Corte costituzionale, della Corte di giustizia CE, delle Corti straniere, della Corte di Cassazione e dei giudici di merito pubblicate per esteso e commentate dagli esperti della materia.

Il **servizio online**, riservato esclusivamente agli abbonati e consultabile all'indirizzo www.ipsoa.it/dannoeresponsabilita, permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 178,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 – fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- www.ipsoa.it

Pubblicazione dei redditi *on-line*

La pubblicazione *on-line* delle dichiarazioni dei redditi

di Renato Clarizia

Il caso della pubblicazione *on-line* delle dichiarazioni dei redditi ha dato occasione a valutazioni di carattere politico e giuridico, ma, talvolta, giustificazioni "politiche" hanno supportato considerazioni giuridiche e ciò è sbagliato ed ha generato confusione (1).

Restiamo sul piano della normativa vigente: il d.p.r. n. 660/1973 all'art. 69, nel disciplinare la pubblicazione degli elenchi dei contribuenti, espressamente dispone che "gli elenchi sono depositati per la durata di un anno ai fini della consultazione da parte di chiunque, sia presso lo stesso ufficio delle imposte sia presso i comuni interessati"; la legge sulla *privacy* (d.lgs. 196/2003) all'art. 19 ultimo comma dispone che la diffusione di dati diversi da quelli sensibili e giudiziari da parte di soggetti pubblici è consentita quando vi sia la previsione di una norma di legge o regolamentare; il codice dell'amministrazione digitale (d.lgs. n. 82/2005) all'art. 2 incentiva l'utilizzazione da parte dei soggetti pubblici delle "tecnologie dell'informazione e della comunicazione" e all'art. 12, comma 5, precisa che "le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni...". Una lettura della richiamata normativa, assolutamente sgombra da ogni preconcetto "politico", porta a ritenere che il legislatore del 1973 non ha voluto che le dichiarazioni dei redditi dei contribuenti italiani fossero tenute riservate, il legislatore del codice del trattamento dei dati personali si preoccupa che sia assicurata la riservatezza soprattutto dei dati sensibili e giudiziari, il legislatore del 2005 addirittura dispone che l'accesso alla "consultazione" di dati da parte dei privati sia dato attraverso l'utilizzazione delle tecnologie "dell'informazione e della comunicazione". È significativo che il legislatore del 1973 e del 2005 adoperino lo stesso termine "consultazione", anche se, evidentemente, nel primo caso si presupponeva un accesso fisico del privato presso l'agenzia delle entrate o del Comune mentre nel secondo caso tale "accesso" avviene in via informatica.

Comunque, mi pare che la finalità di trasparenza, di pubblicità e di libera consultazione degli elenchi dei contribuenti, sicuramente perseguita dal legislatore del 1973, sia correttamente attuata - salvo le perplessità che dirò tra breve - anche con la pubblicazione *on-line*, in quanto

la "consultazione" e l'"accesso" a quei dati è oggi consentita in via informatica in ragione della richiamata normativa.

L'unico profilo problematico mi pare che sia quello del limite di un anno del deposito degli elenchi dei contribuenti ai fini della consultazione da parte di chiunque, ai sensi del più volte citato art. 69. Non mi sembrerebbe, però, eccessivamente forzato, in una logica di interpretazione evolutiva della normativa, ritenere che quel limite temporale alla luce della odierna possibilità di "accesso informatico", possa ritenersi superato perché esso era posto in quanto gli elenchi dei contribuenti e delle loro dichiarazioni dei redditi erano consultabili esclusivamente su supporto cartaceo e quindi avrebbe creato problemi logistici ed organizzativi per il soggetto pubblico il consentirne la consultazione anche per anni diversi da quello della richiesta da parte del privato.

E veniamo, in conclusione, al vero problema che ha nuovamente e con grande evidenza manifestato il caso in questione, quello della "rivoluzione" informatica, nel senso che sempre più viene a configurarsi una sorta di società civile parallela a quella "tradizionale", in cui le relazioni interpersonali, le transazioni, le attività si svolgono avvalendosi di tali nuove tecniche, modificandosi così non solo le loro forme e modalità attuative ma anche, talvolta, la loro sostanza (2). Sicché può accadere - ed è accaduto in questo caso - che la "vecchia" normativa (che non conosceva il fenomeno informatico) debba convivere con quella "nuova" (emanata proprio per sviluppare e diffondere il fenomeno informatico) senza che siano state emanate opportune norme di coordinamento (3). Non si è considerato così che nell'ambito informatico e di internet non esiste la dimensione temporale e spaziale, sicché il termine di un anno da un lato e dal-

Note:

(1) Cfr. il quadro completo della normativa proposto da G. Cassano, *Redditi on-line*, in questa *Rivista*, 4, 2008, 329, che sembra propendere per la illegittimità della diffusione.

(2) Interessante è la ricostruzione storica fatta da E. Tosi, *Diritto privato dell'informatica e di internet*, Torino, 2006, 32, del rapporto tra informatica e diritto.

(3) Analoga denuncia di difficile convivenza in R. Clarizia, *I contratti e l'informatica*, in R. Clarizia (a cura di), *I contratti informatici*, Torino, 2007, 3.

l'altro la consultabilità solo delle dichiarazioni dei redditi relative a quel particolare Comune o Ufficio dell'Agenzia delle entrate, sono limitazioni che il "trattamento" informatico dei dati non sopporta: una volta pubblicato su internet il dato diventa non soltanto fruibile da tutti e senza termini temporali, ma completo, infatti sono state pubblicate le dichiarazioni dei redditi di tutti i contribuenti, e non quelli solo di un determinato Comune o di un determinato ufficio dell'agenzia delle entrate. Si badi bene anche senza l'informatica è possibile conservare la memoria di quanto si consulta, ma con enorme dispendio di tempo e comunque limitatamente agli elenchi depositati presso una determinata Agenzia o un determinato Comune.

In effetti, quando il legislatore ha ritenuto che la mera interpretazione della normativa vigente non riuscisse a "disciplinare" correttamente il fenomeno informatico, è intervenuto con una regolamentazione *ad hoc*, ad esempio - sintetizzando al massimo - sancendo l'equivalenza al documento giuridico cartaceo del documento informatico con firma digitale. Meglio sarebbe stato che il legislatore fin dall'inizio avesse affrontato le problematiche giuridiche suscitate dall'informatica, costruendo un "sistema" autonomo e distinto rispetto a quello "tradizionale", con proprie regole e principi (4).

Allora, se l'interesse e il risultato perseguiti dal legislatore del 1973 con la norma sulla consultabilità degli elen-

chi dei contribuenti non coincidono con (o contraddicono addirittura) quelli perseguiti con la normativa successivamente emanata (codice della *privacy*, codice dell'amministrazione digitale, ecc.), sarebbe stata auspicabile e necessaria una espressa ed inequivoca presa di posizione del legislatore.

In conclusione, a me non appare *prima facie* evidente la violazione della normativa sulla *privacy*, né tanto meno la sicura emersione dell'imputabilità di chi ha autorizzato siffatta pubblicazione, ma emerge prepotentemente nel contempo l'esigenza che il legislatore intervenga con chiarezza sul punto e non lasci ancora una volta al giudice il compito di supplire a carenze normative e di sciogliere dubbi interpretativi di cui è colpevole il Parlamento e/o il Governo (5).

Note:

(4) D'altro canto già negli anni ottanta G. Alpa, *Il diritto dei computers*, in G. Alpa (a cura di), *I contratti di utilizzazione del computer*, Milano, 1984, 9, si interrogava se non si stesse andando "verso una nuova branca del diritto".

(5) A. Gentili, *Documento elettronico: validità ed efficacia probatoria*, in R. Clarizia (a cura di), *I contratti informatici*, cit., 121, evidenzia che l'intervento del legislatore in materia informatica, ad esempio con il Codice dell'amministrazione digitale, si presenta "fiacco", laddove lascia ancora al libero apprezzamento del giudice, ad esempio, la valutazione dell'equivalenza, sotto il profilo sostanziale e probatorio, del documento informatico con firma elettronica alla scrittura privata.

RIVISTE

Il Notariato

Il punto di riferimento per i notai italiani

Direttore scientifico: Giancarlo Laurini

Comitato Scientifico: Ernesto Briganti, Piergaetano Marchetti, Gennaro Mariconda, Umberto Morello, Remigio Perchinunno, Giovanni Tatarano

Periodicità: bimestrale



La rivista offre una panoramica di giurisprudenza, leggi, regolamenti e circolari di origine nazionale ed europea, presentando anche modelli contrattuali rispondenti a tecniche ed esigenze pratiche nuove. I documenti sono accompagnati da un commento di prima mano (in ogni caso rigoroso e puntuale), esteso a misura dell'interesse dell'argomento e centrato sui punti qualificanti, svolto secondo uno schema che agevolerà il lettore in un approccio semplice e immediato. Destinata agli operatori e agli studiosi del diritto particolarmente interessati alla materia contrattuale e societaria, oltre a quanti frequentano studi e Scuole di specializzazione, preparandosi all'attività professionale, la Rivista dedica attenzione

agli effetti che le problematiche trattate hanno sull'attività pratica.

Il nuovo servizio on-line, riservato agli abbonati e compreso nel prezzo dell'abbonamento, è disponibile all'indirizzo www.ipsoa.it/notariato e permette di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 140,00

Per informazioni

- Servizio Informazioni Commerciali (tel. 02.82476794 - fax 02.82476403)
- Agente Ipsoa di zona (www.ipsoa.it/agenzie)
- www.ipsoa.it

Osservatorio della normativa italiana

a cura di Fulvio Sarzana di Sant'Ippolito ed Enzo Maria Tripodi

■ Criminalità informatica

**CONTRASTO AL TERRORISMO
INTERNAZIONALE - INDIVIDUATI I SOGGETTI
LE CUI INFRASTRUTTURE TELEMATICHE
SONO DI INTERESSE NAZIONALE - ISTITUITO
IL CENTRO NAZIONALE ANTICRIMINE
INFORMATICO PER LA PROTEZIONE DELLE
INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.)**

Ministero dell'Interno, decreto 9 gennaio 2008
«Individuazione delle infrastrutture critiche informatiche
di interesse nazionale»
(G.U. 30 aprile 2008, n. 101)

Il decreto è stato emanato in attuazione dell'art. 7 bis della legge n. 155/2005 (di conversione del d.l. 27 luglio 2005, n. 144, recante "Misure urgenti per il contrasto del terrorismo internazionale") che stabilisce l'individuazione - ad opera del Ministero dell'interno - delle infrastrutture critiche informatizzate di interesse nazionale.

L'art. 1 del decreto stabilisce che sono infrastrutture critiche i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di:

- Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute;
- Banca d'Italia ed autorità indipendenti;
- società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque;
- ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti - autorità provinciali di pubblica sicurezza.

Il Ministero dell'interno collabora - ex art. 2 - alla protezione informatica delle infrastrutture informatizzate degli organi costituzionali, secondo forme e modalità da concordare con gli organi medesimi.

Viene poi istituito - mediante decreto demandato al Capo della polizia - il C.N.A.I.P.I.C., ossia il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche.

■ Diritto e concorrenza nel settore delle comunicazioni

**TERMINE PER LA PARTECIPAZIONE
ALLA PROCEDURA SELETTIVA
PER LA CAPACITÀ TRASMISSIVA
SUL DIGITALE TERRESTRE**

Autorità per le garanzie nelle comunicazioni
«Procedura selettiva per la cessione del quaranta per cento della capacità trasmissiva delle reti digitali terrestri - termine per la presentazione delle domande»
(G.U. 2 maggio 2008, n. 102)

L'AGCOM ha fissato nel 23 giugno 2008 (alle ore 18) il termine per la presentazione delle domande inerenti la procedura selettiva per l'individuazione dei soggetti che possono accedere al quaranta per cento della capacità trasmissiva delle reti digitali terrestri oggetto di cessione ai sensi della delibera n. 109/07/CONS del 7 marzo 2007.

Il disciplinare per lo svolgimento della procedura selettiva è pubblicato sul sito dell'Autorità (www.agcom.it) e sui siti web degli operatori tenuti alla cessione delle capacità trasmissiva (RAI, Elettronica Industriale e Telecom Italia Media).

Si ricorda che la domanda deve essere presentata esclusivamente a mano - in un plico chiuso o sigillato - presso la sede romana dell'Autorità (Via delle Muratte, 25).

**PROCEDURE SANZIONATORIE
E IMPEGNI PROPOSTI DAGLI OPERATORI:
MODIFICHE ALLA DELIBERA N. 54/08/CONS**

Autorità per le garanzie nelle comunicazioni, deliberazione 12 marzo 2008, n. 130/08/CONS
«Modificazione della delibera n. 54/08/CONS, recante "Modifiche ed integrazioni al regolamento in materia di procedure sanzionatorie in attuazione dell'articolo 14 bis del decreto-legge 4 luglio 2006, n. 223, convertito dalla legge 4 agosto 2006, n. 248, e del regolamento in materia di impegni di cui alla delibera n. 645/06/CONS"».
(G.U. 23 aprile 2008, n. 96)

L'AGCOM, con la delibera n. 130/08/CONS, ha apportato alcune modifiche al regolamento in materia di procedure

Nota:

(*) Il testo integrale delle disposizioni illustrate è pubblicato sul sito www.ipsoa.it/diritto dellinternet.

sanzionatorie, di cui alla delibera n. 54/08/CONS (che, a sua volta, le introduceva nella delibera n. 136/06/CONS). In particolare, viene sostituito l'art. 12 bis (*Proposta di impegni*) e l'art. 12 ter (*Decisione*). Sulla base del primo articolo indicato, l'operatore al quale sia stata contestata una violazione in materia di fornitura di reti e servizi di comunicazione elettronica può presentare una proposta preliminare di impegni, finalizzata a rimuovere le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure. Tale proposta, che deve diventare definitiva entro sessanta giorni dalla notifica dell'atto di contestazione da parte dell'Autorità, viene trasmessa all'organo collegiale che può dichiararla inammissibile nei seguenti casi:

- a) quando la proposta di impegni, per la sua genericità, si manifesti carente di serietà o appaia presentata per finalità dilatorie;
- b) qualora gli impegni assunti appaiano manifestamente inadeguati a migliorare le condizioni della concorrenza nel settore rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure.

Se non viene comunicata l'inammissibilità all'operatore la sua proposta viene resa pubblica attraverso il sito Internet dell'Autorità, e i soggetti interessati hanno facoltà di presentare osservazioni entro i successivi trenta giorni.

L'art. 12 ter stabilisce che l'organo collegiale valuta se la proposta di impegni sia idonea a migliorare le condizioni della concorrenza nello stesso settore rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure. Ove tale giudizio sia positivo, l'organo collegiale approva gli impegni e ne ordina l'esecuzione, così rendendoli obbligatori per l'operatore proponente.

L'attuazione degli impegni comporta la successiva archiviazione del procedimento sanzionatorio.

Qualora gli impegni assunti non vengano rispettati (ovvero siano stati approvati sulla base di informazioni incomplete, colpevolmente inesatte o fuorvianti da parte dell'operatore), dopo una diffida, viene revocato il provvedimento di approvazione degli impegni stessi e riprende il procedimento sanzionatorio per la violazione precedentemente contestata. La mancata esecuzione degli impegni comporta inoltre l'applicazione della sanzione di cui all'art. 98 del Codice delle comunicazioni elettroniche.

La delibera - molto opportunamente - abroga la delibera n. 54/08/CONS e provvede alla pubblicazione, in allegato, del testo "consolidato" della delibera n. 136/06/CONS.

**PROCEDURE SANZIONATORIE
E IMPEGNI PROPOSTI DAGLI OPERATORI:
MODIFICHE ALLA DELIBERA N. 645/06/CONS**

Autorità per le garanzie nelle comunicazioni, deliberazione 12 marzo 2008, n. 131/08/CONS

«Modifiche al regolamento in materia di impegni di cui alla delibera n. 645/06/CONS»

(G.U. 3 maggio 2008, n. 103 - Suppl. ord. n. 112)

Posta la delibera n. 130/08/CONS presentata in questa Ru-

brica, l'AGCOM ha ritenuto opportuno modificare anche la delibera 645/06/CONS al fine di specificare il percorso istruttorio attraverso il quale la proposta di impegni giunge all'esame dell'organo collegiale e di regolare l'ipotesi della presentazione di impegni nell'ambito di più procedimenti diversi, dettando le relative disposizioni di raccordo.

Le modifiche sono analoghe a quelle di cui alla delibera n. 130/08/CONS, tenuto conto della diversa organizzazione dell'articolato della delibera n. 645/06/CONS.

Si segnala all'attenzione l'art. 8 bis recante il "Coordinamento tra più procedimenti". Una proposta di impegni da parte dell'operatore può infatti essere presentata nell'ambito di più procedimenti anche di natura diversa. In tal caso l'istruttoria dell'Autorità si concentra integralmente e ad ogni effetto nell'ambito del solo procedimento che, tra quelli interessati, ha natura regolatoria, o, nell'ipotesi di più procedimenti aventi tale natura, nell'ambito del procedimento avente l'oggetto più ampio.

E-Government

**FATTURAZIONE ELETTRONICA:
INDIVIDUATO NELLA SOGEI IL GESTORE
DEL SISTEMA DI INTERSCAMBIO**

Ministero dell'Economia e delle Finanze, decreto 7 marzo 2008

«Individuazione del gestore del sistema di interscambio della fatturazione elettronica nonché delle relative attribuzioni e competenze»

(G.U. 3 maggio 2008, n. 103)

Il decreto è emanato in attuazione della legge finanziaria 2008 (art. 1, commi 211 e 212, della legge 24 dicembre 2007, n. 244), laddove si prevede l'individuazione del gestore del sistema di interscambio sulle fatturazioni elettroniche. Al riguardo, vale la pena di ricordare che, nel nostro ordinamento, la fatturazione elettronica è stata introdotta con il d.lgs. 20 febbraio 2004, n. 52 (in materia di semplificazione e armonizzazione delle modalità di fatturazione in materia di IVA) e che il suo obbligo è stato previsto - ex art. 1, comma 209, della legge 24 dicembre 2007, n. 244 - per quanto concerne l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture, emesse nei rapporti con le amministrazioni dello Stato, anche ad ordinamento autonomo, e con gli enti pubblici nazionali.

Di conseguenza, con il decreto in commento il gestore del sistema di interscambio istituito dall'allora Ministero delle finanze (ora dell'Economia e delle finanze) è stato individuato nella SOGEI (Società Generale d'Informatica S.p.A.).

Ai sensi dell'art. 2, il decreto demanda all'Agenzia delle entrate specifiche attribuzioni di indirizzo, di coordinamento e di controllo del sistema di interscambio, gravando altresì sulla stessa l'obbligo semestrale di riferire al Ministero dell'economia e delle finanze in merito all'evoluzione del sistema di interscambio.

Con il successivo art. 3 sono demandate alla SOGEI le attività di sviluppo, di gestione e di conduzione dell'infrastruttura tecnologica e dei servizi informatici del sistema di interscambio.

Infine, l'art. 5, stabilisce che le attività svolte dalla SOGEI sono regolate dal contratto di servizi quadro concluso in data 23 dicembre 2005 ed efficace fino alla fine del 2011, nonché da appositi contratti esecutivi che verranno conclusi con Agenzia delle entrate nei limiti degli ordinari stanziamenti di bilancio.

■ Informatizzazione della Pubblica Amministrazione

TRASMISSIONE TELEMATICA DELLE RICETTE MEDICHE: PROROGA DEI TERMINI PER L'ADEGUAMENTO DELLE FARMACIE

Ministero dell'economia e delle finanze, decreto 29 aprile 2008

«Modifica del decreto 18 marzo 2008, concernente i parametri tecnici per la trasmissione telematica delle ricette» (G.U. 10 maggio 2008, n. 109)

Con il decreto 18 marzo 2008, il Ministero dell'economia ha stabilito - tra l'altro - che le ricette utilizzate presso le strutture di erogazione dei servizi sanitari a partire dal 1° giugno 2008 devono essere trasmesse esclusivamente secondo le modalità definite dal decreto, in attuazione della legge 24 novembre 2003, n. 326. Tale legge affidava a detto Ministero il compito di stabilire i parametri tecnici per la realizzazione del *software* certificato che è stato installato dalle strutture di erogazione di servizi sanitari per la periodica trasmissione dei dati previsti.

A seguito di una richiesta di proroga avanzata da Federfarma per l'adeguamento dei sistemi informatici delle farmacie, il Ministero ha differito, al 1° settembre 2008, la data a partire dalla quale le ricette utilizzate presso le strutture di erogazione dei servizi sanitari devono essere trasmesse esclusivamente secondo le modalità di cui al citato decreto del 18 marzo 2008.

■ Tutela dei dati personali

PUBBLICAZIONE ON-LINE DELLE DICHIARAZIONI DEI REDDITI: IL GARANTE CHIARISCE I LIMITI DELLA DISCIPLINA LEGISLATIVA

Garante per la protezione dei dati personali, provvedimento 6 maggio 2008

«Misure in ordine alla pubblicazione in Internet di dati relativi alle dichiarazioni dei redditi» (G.U. 8 maggio 2008, n. 107)

La questione è fin troppo nota da dover dedicare troppo

spazio in questa rubrica, trattandosi della pubblicazione *on-line* delle dichiarazioni dei redditi e IVA (riferite al 2005) di circa 38 milioni di contribuenti italiani.

La disciplina attualmente vigente (art. 69, d.p.r. 29 settembre 1973, n. 600, come modificato dall'art. 19, legge 30 dicembre 1991, n. 413; art. 66 *bis*, d.p.r. 26 ottobre 1972, n. 633) prevede che gli elenchi di detti contribuenti sono formati annualmente e depositati per un anno, ai fini della consultazione da parte di chiunque, presso i comuni interessati e gli uffici dell'Agenzia competenti territorialmente. È poi previsto che, con apposito decreto, devono essere stabiliti annualmente «i termini e le modalità» per la formazione di detti elenchi.

L'Agenzia delle entrate con un improvvido provvedimento ha invece disposto la pubblicazione nel sito Internet www.agenziaentrate.gov.it (Prov. direttore dell'Agenzia 5 marzo 2008, prot. 197587/2007).

Il Garante, dopo aver invitato in via d'urgenza l'Agenzia a sospendere la pubblicazione (e fornire chiarimenti sull'accaduto), ha rilevato i seguenti profili di criticità:

- il provvedimento dell'Agenzia poteva stabilire solo «i termini e le modalità» per la formazione degli elenchi. La conoscibilità di questi ultimi è infatti regolata direttamente dalla legge;
- il Codice dell'amministrazione digitale, seppur incentiva l'uso delle tecnologie dell'informazione, fa espressamente salvi i limiti alla conoscibilità dei dati previsti da leggi e regolamenti, nonché le norme e le garanzie in tema di protezione dei dati personali;
- la predetta messa in circolazione in Internet dei dati, oltre a essere di per sé illegittima perché carente di una base giuridica e disposta senza metterne a conoscenza il Garante, ha comportato anche una modalità di diffusione sproporzionata in rapporto alle finalità per le quali l'attuale disciplina prevede una relativa trasparenza. I dati sono stati resi consultabili non presso ciascun ambito territoriale interessato, ma liberamente su tutto il territorio nazionale e all'estero;
- infine, il Garante non è stato consultato preventivamente, come prescritto rispetto ai regolamenti e agli atti amministrativi attinenti alla protezione dei dati personali (art. 154, comma 4, del citato Codice).

Di conseguenza il Garante ha stabilito di:

- 1) confermare la sospensione della pubblicazione degli elenchi nominativi per l'anno 2005 dei contribuenti che hanno presentato dichiarazioni ai fini dell'imposta sui redditi e dell'imposta sul valore aggiunto, inibendo all'Agenzia delle entrate di diffondere ulteriormente in Internet detti elenchi, nonché di diffonderli in modo analogo per i periodi di imposta successivi al 2005, in carenza di idonea base normativa e della preventiva consultazione del Garante;
- 2) demandare l'Ufficio a contestare all'Agenzia la violazione amministrativa per l'assenza di un'idonea e preventiva informativa ai contribuenti interessati.

Infine il Garante ha disposto che sia curata la più ampia pubblicità del provvedimento, «al fine di rendere edotti coloro che hanno ottenuto i dati dei contribuenti provenienti, anche indirettamente, dal sito Internet dell'Agenzia,

della circostanza che essi non possono continuare a metterli in circolazione stante la suesposta violazione di legge e che tale ulteriore messa in circolazione configura un fatto illecito che, ricorrendo determinate circostanze, può avere anche natura di reato».

Per un commento più analitico della vicenda, si rimanda ai due editoriali di G. Cassano, *Redditi on-line*, in questa *Rivista*, 2008, xxx e di R. Clarizia, *La pubblicazione on-line delle dichiarazioni dei redditi*, in questa *Rivista*, 2008, xxx.

RIVISTE



Diritto penale e processo

Mensile di giurisprudenza, legislazione e dottrina

Direzione scientifica: Giorgio Spangher, Paolo Pisa (condirettore)

Comitato scientifico: Paolo Ferrua, Francesco Palazzo, Sergio Seminara, Paolo Tonini

Periodicità: mensile

La Rivista costituisce un attento osservatorio giuridico dei problemi creati dall'evoluzione del diritto penale sostanziale e processuale. Pubblica tutta la normativa di rilevanza penale, corredata da approfonditi commenti. Ampio spazio è dedicato alla giurisprudenza e, accanto agli Osservatori che segnalano in forma sintetica le più recenti pronunce, sono pubblicati i provvedimenti di maggior interesse riportati per esteso con qualificati commenti. Un'apposita sezione tratta gli istituti di diritto penale internazionale riportando fra l'altro le sintesi delle decisioni della Corte europea dei diritti dell'uomo, della Corte di giustizia CE, dei Tribunali

penali internazionali e degli organi non giurisdizionali.

Il **servizio online**, riservato esclusivamente agli abbonati e consultabile all'indirizzo **www.ipsoa.it/dirittopenaleeprocesso**, permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 200,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 – fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- **www.ipsoa.it**

Nome e *domain name*

Il nome (di dominio) di associazioni (politiche) tra profili ideologici e interessi mediatici

Tribunale di Roma, 12 marzo 2008 - Rel. Ienzi

Uso di nome e domain names da parte di associazioni politiche non riconosciute - Confondibilità - Estensione della disciplina dei segni distintivi ai domain names - Applicazione dell'art. 7 c.c. e richiamo del diritto all'identità personale - Inibizione della prosecuzione dell'uso del segno distintivo - Trasferimento dei domain names - Pubblicazione del dispositivo della sentenza

(c.c. art. 7)

La denominazione degli enti, in quanto equivalente del nome, gode della medesima tutela attribuita dall'art. 7 c.c. nel caso in cui il nome (o la denominazione) sia da altri usurpato con un pregiudizio di carattere economico o morale per il titolare. Il diritto di usare un nome a dominio spetta al titolare del diritto al nome e a chi ha provveduto per primo a registrarlo.

...*Omissis*...

I ricorrenti agiscono sia per la tutela del nome e dell'identità personale dell'associazione Rosa bianca, che per quella dei diritti anteriori sul proprio *domain name* «rosabianca.org» registrato il 9 giugno 2000.

Con riferimento al primo aspetto, è ormai pacifico in giurisprudenza il principio secondo cui la denominazione degli enti, in quanto equivalente del nome, gode della medesima tutela a quest'ultimo attribuita dall'art. 7 c.c., nel caso in cui il nome o denominazione sia da altri usurpato con un pregiudizio di carattere economico o morale per il titolare.

In particolare l'ordinamento tutela non solo il nome ma il diritto all'identità personale intesa come interesse del soggetto ad essere se stesso, cioè come diritto della persona ad essere tutelata contro attribuzioni estranee alla propria personalità, ad evitare che questa ne risulti travisata.

Nel caso di specie è evidente il diritto dell'associazione ricorrente ad agire per chiedere la tutela del proprio nome e della propria identità personale.

Invero il nome «Rosa Bianca» identifica da decenni l'attività della ricorrente, come dimostrato da tutta la documentazione prodotta, individuando l'identità storica, politica e culturale dell'associazione.

Come specificato nel ricorso si tratta di un'associazione di cultura e impegno politico, che prende il nome e l'ispirazione da un gruppo di studenti tedeschi che si oppo-

sero al regime nazista, e che fin dal 1978 opera con lo scopo di diffondere la cultura cattolico-progressista.

Lo stesso nome dunque non può essere usato da un altro e diverso movimento politico, differente per storia e orientamento politico, essendo quell'uso idoneo a creare confusione ed a ledere l'identità personale dell'associazione ricorrente.

In particolare idoneo a creare confusione è l'uso del proprio nome come *domain name* da parte del sig. Sanseverino, dal momento che si tratta di nomi a dominio («larosabianca.net» e «larosabianca.com») praticamente identici a quello dell'associazione Rosa Bianca (rosabianca.org), che costituisce segno distintivo dell'associazione non riconosciuta ricorrente.

I *domain names* si differenziano solo per la presenza di un articolo determinativo. Inoltre per giurisprudenza costante le particelle quali «.it» o «.com», che indicano il c.d. *top level domain name* non sono sufficienti a differenziare il segno distintivo. Del resto i ricorrenti hanno dimostrato che la confusione si è in pratica verificata fin dall'inizio quando tutti gli utenti di internet, ricercando il sito del nuovo partito digitavano direttamente il nome dello stesso «rosabianca» andando così a finire sul sito dell'associazione esponente ed inviando moltissime e-mail all'indirizzo di posta elettronica segnalato dal sito rosabianca.org. La confusione si è poi aggravata quando il nuovo

movimento politico ha attivato il proprio sito Internet,

a causa della compresenza di sue siti, che presentano sostanzialmente lo stesso nome a dominio, riconducibili tuttavia a due ben distinti movimenti politici.

Evidentemente il diritto di usare un nome a dominio caratterizzato dal nome «Rosa Bianca» spetta all'associazione ricorrente, sia per il diritto al nome sia per il poizore diritto sul nome a dominio rosabianca.org, la cui registrazione risale al 2000.

Il danno che si può verificare per l'associazione ricorrente deriva inevitabilmente dall'oscuramento conseguente alla massiccia presentazione agli elettori del

neo-costituito movimento politico e dal suo sito Internet.

Sussiste conseguentemente anche il pericolo nel ritardo, in quanto attendere l'esito del giudizio di primo grado danneggerebbe l'associazione Rosa Bianca, che non avrebbe modo di far conoscere pienamente la propria attività discendente dalla sua identità culturale, con grave lesione dei diritti personalissimi.

Il ricorso va pertanto accolto nelle conclusioni richieste con conseguente condanna alle spese di parte resistente. ... *Omissis*...

IL COMMENTO

di Lara Trucco

Nell'articolo si esamina a chi spetti il diritto di utilizzo di nome e domain name in caso di riscontrata «confusione» con altri «segni distintivi» e la possibile rilevanza, in tale determinazione, del diritto all'identità personale.

1. I fatti all'origine della controversia

Denominazioni del tipo, «il corsaro nero», «la lanterna blu», «bandiera gialla» si può dire che appartengano ormai alla toponomastica più comune, se non addirittura all'immaginario collettivo. Qualcosa del genere avviene anche per «la rosa bianca», che evoca immagini bucoliche ed insieme momenti romantici ed idilliaci.

Niente però di tutto questo ha a che vedere col caso di specie, in cui oggetto del contenzioso è stato l'utilizzo della medesima denominazione da parte di due associazioni «politicamente impegnate». Situazione, per vero, che forse non avrebbe nemmeno destato molta attenzione, considerata la predilezione che i partiti dimostrano per certi tipi di nomi (tra cui quelli di piante e fiori), e la rissosità manifestata negli ultimi tempi, specie in campagna elettorale... non fosse stato che la controversia ha riguardato altresì, segno dei tempi che cambiano, l'utilizzo di un analogo *domain name*: «rosabianca.org» e «rosabianca.com» e «.net».

Più nello specifico, l'associazione ricorrente si è rivolta in via d'urgenza all'autorità giudiziaria lamentando il fatto che la recente costituzione di una formazione politica, differente per storia e orientamento politico, egualmente denominata, avesse prodotto una «gravissima» confusione identitaria. Neppure la presunta fusione con un'altra formazione politica, poi, secondo la ricorrente, avrebbe risolto le cose, dal momento che l'associazione si era presentata autonomamente alle elezioni amministrative in varie realtà locali, con la conseguenza che in seno agli organi di stampa - e conseguen-

temente tra il pubblico - l'associazione neo-costituita sarebbe continuata ad essere identificata come «Rosa Bianca», senza che fosse mai intervenuta nessuna rettifica o smentita pubblica da parte dell'associazione stessa. Che, anzi, da ultimo, si era presentata sul web con un sito con identica denominazione, nonostante la parte ricorrente avesse già provveduto a registrare in precedenza un *domain name* analogo, aggravando, secondo parte attrice, la situazione per «la confusione» e l'«oscuramento» provocati in suo danno a causa della compresenza di due siti, aventi lo stesso nome a dominio, riconducibili tuttavia a due ben distinti movimenti politici. Di qui la lamentata violazione davanti ai giudici di nome ed identità personale, nonché dei diritti anteriori sul *domain name* «rosabianca.org».

2. Le concezioni «identificativa» e «individuativa» del *domain name*

A quest'ultimo riguardo, benché sia ormai copiosa la giurisprudenza in materia di «nome a dominio», tuttavia più unici che rari sono i casi in cui compaiono associazioni, in particolare, di «natura politica». Piuttosto, da quando internet ha fatto la sua comparsa nella società, le controversie direttamente o indirettamente riguardanti il *domain name* hanno visto coinvolte soprattutto società e imprese (di vario genere), ed in qualche caso persone fisiche.

Com'è noto, sin dalle prime controversie sorte in materia, un profilo particolarmente discusso è stato quello della natura del *domain name*.

In estrema sintesi, tale questione ha visto contendersi il campo fondamentalmente due tesi (1): quella, per così dire «identificatoria», assolutamente minoritaria, equiparante il *domain name* ad un mero indirizzo te-

Note:

(1) Cfr. sul tema G. Cassano, *Il domain name appartiene alla categoria dei segni distintivi?*, in *Dir. Radiodiffusioni e Telecomunicazioni*, 2001, 82.

lematico (2), e, quella «individuativa», invece attenta a considerare anche i contenuti a cui il *domain name* stesso si collega, e dunque «il prodotto» nella sua ben distinta globalità (3).

Il fatto è che, al di là del profilo «nominalistico», alla luce del silenzio serbato in proposito dal legislatore, la scelta per l'uno piuttosto che per l'altro profilo non manca di avere conseguenze di rilievo sulla riconducibilità - negata dal primo approccio (4) ed invece ammessa dal secondo - dei nomi di dominio ai segni distintivi conformati dal legislatore, il fondamento della cui tutela sta proprio nell'assunto della loro capacità di distinguere e rappresentare in un *flash* visivo l'entità a cui ineriscono, nella consapevolezza del danno che la loro confusione con altri segni analoghi può provocare per il titolare dell'entità «rappresentata».

Ora, è cosa piuttosto notoria che la giurisprudenza, pressoché unanimemente ha sposato l'approccio «individuativo», con ciò dunque valorizzando - e presupponendo - «le caratteristiche e la funzione di un vero e proprio segno distintivo» del *domain name*, idoneo, come tale, ad individuare sul web una determinata entità, lasciandosi conseguentemente aperta la possibilità di entrare nel merito delle questioni che possono porsi sul piano dell'effettivo utilizzo di questo tipo di «segno» (5).

Tale scelta ha fatto sì che si presentassero ulteriori questioni, *in primis*, circa la «tipologia» di «segno» (distintivo) del *domain name*: a tale riguardo, accanto a coloro i quali, particolarmente attenti a mettere in evidenza il rilievo che il *domain name* presenta per l'esercizio di attività economiche e commerciali, ne propugnano la riconduzione, a seconda dei casi, alla «ditta» (6), o all'«insegna» (7) (della quale il primo costituirebbe l'aspetto virtuale di cui l'imprenditore si avvale per manifestare la propria attività al potenziale cliente fino a concludere il contratto) o, ancora, in modo preponderante, «al marchio» (ora in riferimento alle norme contenute nel c.d. «Codice sulla proprietà industriale» (8)) - a seconda delle diverse situazioni e tesi in campo, «tipico» (9), o «atipico» (10), o, ancora, «complesso» (11), o «indifferen-

considerazione della funzione distintiva dei nomi a dominio «dell'utilizzatore del sito», ha ricavato la loro assimilabilità ai segni distintivi dell'impresa, e l'applicabilità, in caso di conflitto, delle norme a tutela del marchio (nello stesso senso, successivamente, tra gli altri, v. Trib. Parma 22 febbraio 1999, in *Dir. comunitario scambi internaz.*, 1999, 492; Trib. Pistoia 10 novembre 2000, in *Giur. dir. ind.*, 2001, 474; Trib. Prato 19 agosto 2000, in *Dir. ind.*, 2002, 51; Trib. Verona 10 gennaio 2001, in *Giur. dir. ind.*, 2001, 544; Trib. Teramo 5 novembre 2002, in *P.Q.M.*, 2003, 78; Trib. Milano 31 maggio 2005, ined.).

(4) A meno di non voler condividere l'idea della possibilità, ex art. 1 bis, comma 1, l. marchi, «che anche l'uso di un indirizzo costituisca violazione di un altrui segno distintivo» come affermato *en passant* da Trib. Napoli, sent. 13 marzo 2003, in *Foro it.*, 2003, I, 3185.

(5) *Leading case* al proposito è considerato il «caso Amadeus», deciso da Trib. Milano, 10 giugno 1997 e 22 luglio 1997, in *Foro it.*, 1998, I, 923. Conseguentemente, l'uso di un *domain name* confondibile con un segno distintivo altrui anteriore viene considerato illecito anche, ma non solo, nei casi in cui la sua appropriazione avvenga all'esclusivo scopo di ottenere un ingiusto profitto (v. tra gli altri, Trib. Milano 7 agosto 2001, in *Riv. dir. ind.*, 2001, II, 444 e Trib. Viterbo 24 gennaio 2000, in *Foro it.*, 2000, I, 2334).

(6) Cfr. Trib. Modena 1 agosto 2000, in *Giur. merito*, 2001, 329.

(7) Cfr., in questo senso, Trib. Milano 13 aprile 2000, in *Annali it. dir. autore*, 2000, 971; e Trib. Milano 3 giugno 1997, in *Giur. it.*, 1997, 697, che motiva l'affinità tra *domain name* ed insegna considerando «il sito web» alla stregua di un «luogo virtuale» ove l'imprenditore contatterebbe il cliente fino a concludere con esso il contratto (riprendono l'immagine del «luogo virtuale», tra gli altri, Trib. Roma 22 dicembre 1999, in *Annali it. dir. autore*, 2000, 851; Trib. Parma 26 febbraio 2001, in *Riv. dir. ind.*, 2002, II, 350).

(8) Sulla linea di continuità del D.Lgs. 10 febbraio 2004, n. 30 rispetto al quadro venutosi a comporre in precedenza in materia si veda per tutti Corte App. Firenze, 19 settembre 2005, ined.; e, da ultimo, Trib. Bologna 29 agosto 2007, in questa *Rivista*, nell'Osservatorio della giurisprudenza italiana (a cura di) I.P. Cimino e F. Di Ciommo, 2007, 605. In dottrina, rileva come il codice, abbia «voluto assicurare ai *domain names* una tutela non solo sostanziale ma anche formale, in quanto per la prima volta, il nome a dominio, viene equiparato, a livello legislativo, agli altri segni distintivi», seguendo un approccio «unitario», G. Cassano, *L'impatto del codice dei diritti di proprietà industriale sulle nuove tecnologie e sul regime giuridico di Internet*, in questa *Rivista*, 2005, 115.

(9) Cfr., tra gli altri, in questo senso, Pret. 27 maggio 1998, in *Giur. it.*, 1998, 1875; Trib. Parma 12 ottobre 1998, in *Dir. comunitario scambi internaz.*, 1999, 491; Trib. Verona ord. 25 maggio 1999, in *Foro it.*, 1999, I, 3061; Trib. Modena 28 luglio 2000, in *Giur. merito*, 2001, 329 (con commento di G. Cassano, *L'utilizzo del domain name quale atto di concorrenza sleale*, ivi, 339, che esamina i vari tipi di «marchi» e la loro possibile associazione col *domain name*); nonché Trib. Genova 13 ottobre 1999, in *Dir. inf. e inf.*, 2000, 494 (con commenti, che dimostrano una certa «cautela» da parte degli autori, di G. Tarizzo, *L'applicabilità della disciplina sui marchi ai nomi di dominio: certezze e dubbi*, ivi 500, e G. Cassano, *In tema di domain name*, ivi, 495, che ritiene che allo stato attuale l'estensione dei principi in materia di marchi ai *domain names* sia la più corretta e a ben vedere l'unica praticabile, «anche se non del tutto appagante») in cui viene ravvisata la permanenza della violazione anche quando il *domain name* venga utilizzato come *link* per accedere ad un altro sito. Per diverso profilo, Trib. Roma 24 gennaio 2001 (in *Annali it. dir. autore*, 2001, 642), ha reputato legittimo l'uso da parte di un concorrente, del *domain name* altrui, quale *meta-tag* del proprio sito internet.

(10) Cfr., da ultimo, Trib. Catania 5 luglio 2004, ined. Di un qualche interesse può essere inoltre Trib. Palermo 4 dicembre 2001, in *Riv. dir. ind.*, 2002, II, 287, che nel caso di utilizzazione «abusiva», come *domain name*, di un marchio di fatto, ritiene di doversi fare riferimento non già alle norme della c.d. l. marchi, o, quanto meno, non esclusivamente a queste, bensì alle previsioni del codice civile in tema di marchi, ed in particolare all'art. 2571 c.c., che si riferisce appunto al marchio non registrato.

(11) V. in commento a Trib. Bergamo 5 maggio 2001 (in *Dir. inf. e inf.*, 2001, 735) P. Sammarco, *La riconducibilità a nome a dominio dei marchi* (segue)

Note:

(2) Questa la posizione sposata dal Trib. Bari, nella nota ord. del 24 luglio 1996 (in *Foro it.*, 1997, I, 2316), che rappresenta uno dei pochi casi in cui è stato sostenuto, appunto, che il *domain name* «costituisce un semplice codice d'accesso ai servizi telematici», ovvero «un'entità per identificare univocamente dei gruppi di oggetti (servizi, macchine, caselle postali, ecc.) presenti sulla rete». Tale approccio è stato successivamente ripreso da Trib. Firenze-Empoli 23 novembre 2000 (in *Giur. Merito*, 2001, 923), in una decisione che, tuttavia, è stata immediatamente riformata in senso conforme alla tesi maggioritaria da Trib. Firenze 28 maggio 2001 (in *Foro toscano* 2002, 109), per essere poi pressoché abbandonato.

(3) Cfr., in questo senso, tra i primi, Trib. Modena 23 ottobre 1996 (in *Foro it.*, 1997, I, 2316), che ha affermato l'illegittimità dell'impiego dell'abbreviazione del titolo di una rivista notoria: il «Foro Italiano», come *domain name* identificativo di una *chat* attivata all'interno di un apposito «sito» internet e avente ad oggetto la discussione di problematiche analoghe a quelle trattate dalla rivista medesima, per la sua idoneità a creare una situazione di «confusione»; e la «pionieristica» decisione del Trib. Reggio Emilia 30 maggio 2000 (in *Dir. inf. e inf.*, 2000, 669), che dalla

temente inteso» (12) -; si è posto chi, osservando invece come non sempre il sito contrassegnato dal *domain name* sia strumento per l'esercizio di un'attività economica, considera possibile ed anzi doveroso quando in gioco vi siano profili «non patrimoniali» ricondurne la tutela alla disciplina prevista per la salvaguardia del «nome» (13) o, a seconda dei casi, del «diritto d'autore» (14).

A questo stesso riguardo, il Tribunale di Roma, nel caso in esame, ha seguito una strada «unitaria», applicando, combinatamente, le norme sulla tutela del nome e del marchio, senza tuttavia fare di queste ultime espressamente menzione, ma rilevando, si direbbe, in «via diretta» l'idoneità del *domain name* della formazione politica neocostituita («larosabianca.net» e «larosabianca.com») «a creare confusione» con quello dell'associazione ricorrente («rosabianca.org»).

3. Segue: La «confondibilità» del «segno»...e del *domain name*

Proprio con riguardo al profilo della «confondibilità», può essere di un qualche interesse rilevare come, in genere, la giurisprudenza abbia escluso l'«effetto confusorio» del *domain name* per il pubblico, o a motivo della sua evidente diversità di «forma» (15); o perché composto da termini generici «come tali privi di capacità distintiva» (16); o, ancora, trattandosi di un segno utilizzato in «numerossimi» siti (nel mondo) (17); o, comunque, più in generale, constatandone la «scarsa capacità identificativa» (18).

In alcuni casi, poi, la mancanza di rischi di confusione è stata dedotta in considerazione della diversa attività effettivamente svolta (19), e tenendo altresì conto dei soggetti coinvolti e delle circostanze (20), nonché «della capacità di discernimento media dei consumatori» riguardati (21), e, non in ultimo, della non («allegata» (22) o «comprovata» (23)) rinomanza, del segno distintivo.

Per contro, si ravvisa il rischio di confusione nelle situazioni per così dire «speculari» a quelle appena menzionate, quindi, in estrema sintesi: identità di aspetto dei «segni», nonché il fatto che essi si compongano di termini specifici, come tali maggiormente idonei a distinguere ciò a cui si riferiscono e che riguardino entità operanti in un medesimo settore o, comunque aventi attività affini. Per altro verso, la giurisprudenza presume esservi pericolo di confusione quando di mezzo c'è un

Note:

(segue nota 11)

complessi e la loro tutela, ivi, 737, che esamina la questione della riconducibilità del nome a dominio alla figura del marchio c.d. «complesso» (quel particolare tipo di marchio, cioè, che riunisce in sé elementi emblematici o figurativi accanto ad elementi nominativi).

(12) Cfr. Trib. Napoli, 13 marzo 2003, cit., che, peraltro, reputa tale questione di «rilievo non decisivo».

(13) In particolare, applicano la tutela del nome prevista dall'art. 7 c.c.: Trib. Torino 23 dicembre 2000, nel noto caso che ha vista coinvolta la *show girl* Alessia Merz (in *Dir. inf. e inf.*, 2001, 539, con commento di La

tutela dei nomi a dominio come tutela del diritto al nome, ivi 546, che esamina i presupposti della tutela prevista dall'art. 7 c.c., nonché la dottrina e la giurisprudenza in proposito); e Trib. Napoli 27 maggio 2000, in *Annali it. dir. autore*, 2001, 464.

(14) Così, per esempio, per riconoscere il diritto all'uso del *domain name* applicano le norme sul diritto d'autore Trib. Padova ord. 14 dicembre 1998, in *Foro It.*, 1999, I, 3061; Trib. Macerata 2 dicembre 1998, in *Dir. ind.*, 1999, 35; Trib. Roma 23 dicembre 1999, in *Giur. dir. ind.*, 1999, 1407; nonché Trib. Modena ord. 23 ottobre 1996, cit.

(15) Ci sembra che possa essere letta in questa chiave, in particolare, la decisione del Trib. Firenze 5 gennaio 2000, in *Foro toscano*, 2000, 14.

(16) Così Trib. Bergamo 5 maggio 2001, cit., 735; v. altresì Trib. Mantova, 5 giugno 2004, ined.; e Trib. Torino, sez. IX, 7 dicembre 2005, ined.

(17) V. Trib. Gorizia 25 giugno 1999, in *Annali it. dir. autore*, 2000, 760, che su tale base ha considerato privo della capacità distintiva necessaria ad essere tutelato ex art. 2598 n. 1 c.c. il *domain name* «icon-it».

(18) Cfr. Trib. Messina 20 giugno 2001, in *Foro it.*, 2001, I, 2975 (con nota adesiva di P. Laghezza, «Nomina nuda tenemus», ovvero: della testata giornalistica e del «domain name», un conflitto annunciato nella guerra dei nomi, ivi, 2975).

(19) Cfr. sul punto Trib. Bari 24 luglio 1996, cit., secondo cui si deve aver riguardo «alla concreta attività svolta dalla resistente e non invece alle enunciazioni contenute nell'atto costitutivo», considerato che queste «molto spesso contengono previsioni di attività ben più ampie e variegiate di quelle effettivamente svolte». Da questo punto di vista, fatte ovviamente le dovute differenze del caso, può essere di qualche interesse rilevare come, nella fattispecie in esame, forse anche constatata la possibile confusione di ruoli con altre associazioni, la convenuta decise, ad un certo punto, di nominarsi «Una Rosa per l'Italia-Libertà e Solidarietà»: tuttavia sulla considerazione di questo ha fatto premio il rilievo del nome con cui l'associazione è continuata ad essere identificata dagli organi di stampa e (conseguentemente) dall'opinione pubblica.

(20) Così nella menzionata vicenda decisa dal Tribunale di Bari 24 luglio 1996, cit., si aveva a che fare con due società (con attività) diverse: una svolgente esclusivamente attività di *provider*, e l'altra, invece, di produzione e progettazione di apparecchiature elettroniche ed elettromeccaniche per il controllo di processi industriali nel settore calzaturario; di assistenza tecnica per la relativa manutenzione e di elaborazione di *software*, senza però alcuna attività di *provider*. Ancora, per esempio, Trib. Gorizia 25 giugno 1999, cit. ha ritenuto diverse e dunque «inconfondibili» l'attività di produzione e di elaborazione di immagini fotografiche pubblicitaria con quella di produzione multimediale. Cfr. altresì Trib. Pistoia 10 novembre 2000, cit., che non ha ravvisato alcun elemento di confusione tra il marchio *Wimmerland*, relativo a servizi promozionali e commerciali di prodotti di largo consumo, e il *domain name Wimmerland.it*, identificativo di un sito sportivo, considerandoli «segni» relativi a servizi diversi; e Trib. Roma (dec. del 9 marzo 2000, in *Foro it.*, 2000, I, 2333) che ha escluso la confondibilità dei *domain names* considerando come i siti (nella fattispecie, contenenti informazioni sulle caratteristiche di autovetture e sulle opportunità per il loro acquisto), avessero ad oggetto mercati diversi: riferito l'uno all'acquisto di autovetture negli Usa, l'altro in Italia.

(21) In particolare, Trib. Modena (23 agosto 2000 in *Arch. civ.*, 2001, 895), fa attenzione a verificare se il segno distintivo fa riferimento al medesimo «bacino di utenza».

(22) Cfr. sul punto Trib. Modena 24 gennaio 2001, in *Annali it. dir. autore*, 2001, 646.

(23) Cfr. al proposito Trib. Verona 10 gennaio 2001, cit. che vedeva contrapposti da un lato l'utilizzazione come *domain name* da parte di un'impresa operante nel settore delle attrezzature elettriche e dei servizi informatici e, dall'altro lato, il marchio registrato per articoli di abbigliamento: il giudice ha ritenuto che i «segni» non fossero confondibili «data la totale mancanza di affinità tra i rispettivi ambiti merceologici, in difetto di ogni prova in ordine alla rinomanza del marchio da tutelare e all'assunto del titolare del marchio secondo cui il *domain name* in questione [sarebbe stato] impiegato allo scopo di trarre indebito vantaggio dalla notorietà del marchio, convogliando verso il sito contraddistinto da tale *domain name* un gran numero di visitatori».

nome che gode di una certa rinomanza: in questi casi, infatti, il suo impiego come *domain name* viene ritenuto di per sé lesivo dei diritti del titolare (dunque indipendentemente dall'attività svolta), comportando «l'immediato vantaggio di ricollegare la propria attività a quella del titolare» «famoso» stesso, attirando con ciò la clientela e dunque traendo un indebito vantaggio dallo sfruttamento della notorietà «altrui» (24). Vanno poi considerate le ipotesi in cui la registrazione di *domain name* corrispondente al segno distintivo da altri precedentemente registrato - siano essi più o meno noti - viene realizzata per mera finalità di disturbo: in questi casi, infatti, la giurisprudenza tende a tutelare il titolare «in buona fede», facendo premio la consapevolezza della limitatezza del *domain name* come risorsa (25), e dunque l'opportunità di sorvegliarne la legittima acquisizione, indipendentemente dall'effettivo utilizzo (26).

Nel caso di specie, il contenzioso è sorto tra due soggetti aventi la medesima natura e svolgenti analoga attività (significativo è notare come, invece, se si digita l'indirizzo www.rosabianca.it si sia introdotti in un ambiente bucolico, facente peraltro da sfondo ad un'attività d'indole invece marcatamente economica) con *domain names* tutt'altro che generici (al punto da poter essere considerati veri e propri nomi di persona), distinguendosi per la (sola) presenza di un articolo determinativo, e, ovviamente per il fatto di essere denotati da diversi *top level domain* («.net»; «.com» e «.org») che, in linea peraltro, con l'orientamento giurisprudenziale predominante, l'autorità giudicante ha considerato insufficienti a operare una sufficiente differenziazione (27).

Del resto, ancora una volta in linea, per certi versi, con la giurisprudenza predominante, della «confusione» prodotta da tale omonimia - «in particolare», di *domain names* - il Tribunale considera contro-prova il fatto che gli utenti, digitando l'indirizzo (*rectius*, componendo il *domain name*) non si collegavano con il sito Internet cercato, ma con quello dell'associazione ricorrente (28) inviando erroneamente all'indirizzo di posta elettronica ivi segnalato «moltissime» e-mail.

4. La titolarità dell'uso del (*domain*) name

Posta la confondibilità del «segno», si è trattato di stabilire a chi dunque esso spettasse, ovvero chi ne fosse il legittimo titolare.

Al proposito si deve intanto del tutto preliminarmente ricordare come per giurisprudenza costante, i soggetti istituzionali, costituiti su base convenzionale (29), a cui spetta nel nostro Paese di assegnare i (nomi dei) siti internet (in estrema sintesi, la *Registration Authority* e gli organismi ad essa connessi, facenti capo, com'è noto, all'*Internet Assigned Numbers Authority*: IANA), si limitino a svolgere un'attività di carattere tecnico (30), consistente, fondamentalmente, per quanto qui rileva, nel verificare la rispondenza delle richieste di assegnazione dei *domain names* al relativo regolamento (le c.d. regole di *namings*, appunto, di assegnazione e gestione dei do-

Note:

(24) Così Trib. Salerno 30 giugno 2000, in *Giur. dir. ind.*, 2000, 1019; nello stesso senso v. Trib. Napoli 19 febbraio 2002, in *Dir. inf. e inf.*, 2002, 362; e Trib. Vicenza 6 luglio 1998, cit. In dottrina, sui «tipi di conflitto» tra i segni contrapposti che possono presentarsi, v. da ultimo L. Albertini (in commento a Trib. Arezzo, 7 novembre 2006), *Sulla contraffazione del marchio "striscia la notizia" tramite domain name (con cenni all'uso "civile" di internet)*, in questa *Rivista*, 2007, 570.

(25) Cfr., tra gli altri, Trib. Macerata 2 dicembre 1998, cit.; e Trib. Parma 26 febbraio 2001, in *Riv. dir. ind.*, 2002, II, 350; più specificamente incentrate sul profilo della violazione delle norme che presiedono alla correttezza e lealtà della concorrenza, sono invece Trib. Genova 13 ottobre 1999, in *Dir. e pratica società*, 1999, 76; Trib. Genova 17 luglio 1999, in *Dir. e pratica società*, 1999, 73; Trib. Roma 22 dicembre 1999, in *Annali it. dir. autore*, 2000, 851; e Trib. Torino 21 luglio 2000, in *Giur. it.*, 2001, 774. Sempre in tema di concorrenza sleale, derivante dall'appropriazione di un marchio altrui come *domain name* v. altresì Trib. Crema 24 luglio 2000, in *Discipl. comm.*, 2001, 27; Trib. Roma 18 luglio 2002, in *Impresa*, 2002, 1627; Trib. Perugia 5 ottobre 2000, in *Giur. dir. ind.*, 2000, 1183; Trib. Reggio Emilia 5 dicembre 2001 in *Riv. dir. ind.*, 2002, II, 399; e Trib. Modena, sez. I, 18 ottobre 2005, ined. (là dove sembrerebbe invece avere percorso una strada meno lineare Trib. Milano, 13 aprile 2000, in *Annali it. dir. autore*, 2000, 971, col reputare illecita la registrazione di un *domain name* contenente la denominazione sociale di un imprenditore concorrente per il rischio di «confondibilità in astratto» - contraria, come tale, agli art. 2564 e 2598 n. 1 c.c. -, derivante dall'uso potenziale del *domain name* stesso).

Da questo punto di vista è stata fatta ampia luce da parte della dottrina sull'idoneità della registrazione (abusiva) di determinati *domain name*, di procurare un duplice danno all'avente diritto: e per l'ingiusto profitto che traibile dall'utilizzazione del segno distintivo altrui, e per l'impossibilità che ne deriva per il legittimo titolare di registrare il proprio dominio internet al fine di pubblicizzare la propria attività e i propri prodotti. In alcuni casi il fatto stesso di registrare il *domain name* (in particolare, della denominazione sociale di un concorrente) col deliberato intento di precludere l'uso della denominazione per i siti web, è stato configurato come concorrenza sleale ex art. 2598 n. 3, «anche quando non ricorra in concreto l'intento estorsivo e speculativo proprio del *domain grabbing*» (così Trib. Milano 13 aprile 2000, in *Annali it. dir. autore*, 2000, 971; v. altresì Trib. Parma 26 febbraio 2001, in *Riv. dir. ind.*, 2002, II, 350). Per una «proposta interpretativa» di differenziare il c.d. *domain name grabbing* (che si avrebbe nel caso di incidenza della attività illecita sulla sfera patrimoniale del danneggiato) rispetto al *cybersquatting* (che invece si avrebbe nell'ipotesi di incidenza nella sfera personale), v. G. Cassano, *Cybersquatting*, in *Dir. inf. e inf.*, 2001, pagg. 88. Ancora, sul nuovo fenomeno che si va diffondendo via internet, meglio noto come *typosquatting* (consistente nel registrare un nome di dominio molto simile a quello utilizzato da altri, magari invertendone le lettere o sostituendone alcune, mossi dall'obiettivo di intercettare il traffico indirizzato verso il «sito ufficiale») v. C. Tack, in questa *Rivista*, 2007, 382.

(26) Trib. Milano 7 agosto 2001, in *Riv. dir. ind.*, 2001, II, 444.

(27) Cfr., tra i primi, Trib. Milano 3 giugno 1997 (in *Giur. it.*, 1997, I, 697), che ha ritenuto «priva di attitudine distintiva» la particella indicante il *top level domain name* in quanto «relativa alla mera localizzazione geografica dell'elaboratore». Successivamente nello stesso senso v. Trib. Roma 22 dicembre 1999, in *Annali it. dir. autore*, 2000, 851; Trib. Siracusa-Lentini 23 marzo 2001, in *Foro It.*, 2001, I, 3705; Trib. Napoli 8 gennaio 2002, in *Dir. inf. e inf.*, 2002, 359.

(28) Cfr. Trib. Teramo 5 novembre 2002, cit., attento a distinguere tale situazione con quella «affatto diversa» dell'utente che esegue ricerche ipertestuali attraverso i motori di ricerca, in quanto mentre componendo un *domain name* si digiterebbe un indirizzo/nome identificativo di un sito Internet ben preciso, diversamente, effettuando una ricerca ipertestuale si avrebbe il generico scopo di ottenere un elenco di siti, i quali richiederebbero di venire ulteriormente selezionati.

(29) Cfr. Trib. Genova 17 luglio 1999, cit.

(30) Così, tra gli altri, Trib. Napoli 26 febbraio 2002, in *Arch. civ.*, 2002, 706; e Trib. Pistoia 10 novembre 2000, in *Giur. dir. ind.*, 2001, 474.

main names), non dando corso all'assegnazione in uso dei domain names, riservati a soggetti determinati (in genere istituzionali) (31) o, secondo il criterio c.d. «first come first served», di quelli già registrati (32). Per contro, la ricerca di anteriorità identiche non si estende al confronto con antecedenti registrazioni del medesimo segno come marchio o come altro segno distintivo (a differenza all'attività svolta dall'Ufficio italiano brevetti e marchi) (33), rivelandosi con ciò stesso inidonea ad assicurare un idoneo filtro a tutela dei segni distintivi (34).

La considerazione delle regole per l'attribuzione dei domain name alla stregua di mere regole tecniche o, al più, di natura «contrattuale» (35), ha favorito l'affermarsi dell'idea dell'inidoneità della, pur regolare, registrazione (effettuata, come s'è visto, sulla base della regola del first) a conferire diritti di sorta (36), non potendo né essere opposta a terzi (37), né tanto meno vincolare l'attività dell'autorità giurisdizionale (38) - che, anzi, in alcuni casi si è trovata a censurare la stessa registrazione del name (39) -; e della possibilità, al più, di tener conto delle regole di naming «in via sussidiaria ed interpretativa», in quanto pur sempre espressive delle peculiarità del sistema internet.

In quest'ultimo senso pare muoversi quella giurisprudenza che al fine di accertare il preuso del segno distintivo ha riconosciuto un qualche rilievo alla data di avvenuta registrazione del domain name presso la Registration Authority (40). Nondimeno, si ispira a ben diverso principio la giurisprudenza preponderante che, nel caso di rilevata confondibilità di domain name con altri segni distintivi «comuni», ne riconosce la titolarità in capo a chi per primo ha «registrato» (non il domain name) il segno distintivo, applicando solo in tale contesto la regola del first, tanto da «trascinare» con sé l'eventuale utilizzabilità del domain name (41). Là dove in presenza, invece, di nomi «notori» (42) continua ad imporsi la fondamentale regola contenuta nell'art. 21 l. marchi - che vuole che essi possano essere registrati come marchio solo dall'avente diritto o con il suo consenso (43) - ren-

Note:

(31) V. sul tema P. Costanzo, *Nomi di dominio della Pubblica Amministrazione*, in <http://www.costituzionale.unige.it/dottorato/Costanzo.pdf>.

(32) Sul ruolo delle Autorità di registrazione v. E. Bassoli, *Domain grabbing e tutela inibitoria*, in *Dir. inf. e inf.*, 2001, 524.

(33) V. sul punto Trib. Genova 18 dicembre 2000, in *Dir. inf. e inf.*, 2001, 521.

(34) Così da ultimo, Corte app. Firenze, sez. I, 9 settembre 2005, n. 1284, ined.; nello stesso senso, precedentemente, cfr. Trib. Pistoia 10 novembre 2000, in *Giur. dir. ind.*, 2001, 474; e Trib. Napoli 26 febbraio 2002, in *Arch. civ.*, 2002, 706.

(35) Così Pret. Vicenza 6 luglio 1998, in *Annali it. dir. autore*, 1999, 526.

(36) V. Trib. Cagliari 25 febbraio 2000 (relativa alla tutela di un marchio celebre "di fatto"); Trib. Vicenza 6 luglio 1998, *Giur. it.*, 1998, 2342; Trib. Roma 2 agosto 1997, in *Foro it.*, 1998, I, 923; Trib. Firenze 28 maggio 2001, cit.

(37) Cfr. in questo senso, Trib. Roma 2 agosto 1997, cit.; Trib. Parma 22 febbraio 1999, cit.; Trib. Torino 21 luglio 2000, cit.; e Trib. Genova 18 dicembre 2000 in *Dir. inf. e inf.*, 2001, 521.

(38) Per contro, sono rimaste isolate quelle pronunce in cui o si è riconosciuto un qualche rilievo alla data di registrazione del domain name presso la Registration Authority (v. per esempio Trib. Catania 5 luglio 2004 in *Giur.* 2004, 3649); o, in aggiunta al preteso utilizzatore abusivo del domain name, è stata chiamata in causa anche la Registration Authority italiana (v. per tutte Trib. Modena 7 dicembre 2000, in *Giur. merito*, 2001, 328). Così come quelle in cui è stato individuato in capo al gestore di rete, assimilandone la figura a quella dell'"editore", l'obbligo di vigilare affinché attraverso la sua pubblicazione non venissero compiute, tra l'altro, registrazioni di domain name abusive (cfr. Trib. Macerata 2 dicembre 1998, cit.; Trib. Milano 22 luglio 1997, cit.); sulla responsabilità del provider, v. P. Sammarco, *Assegnazione di nomi a dominio su Internet, interferenze con il marchio, domain grabbing e responsabilità del provider*, in *Dir. inf. e inf.*, 2000, 78; più in generale, sul "ruolo" dei provider e sulla (problematica) possibilità di rinvenire nei loro confronti precisi obblighi controllo, in particolare, estendendo loro la normativa sulla stampa, v. per tutti, P. Costanzo, *Libertà di manifestazione del pensiero e "pubblicazione" in Internet*, in *Dir. informaz. e inf.*, 1998, 377; e V. Zencovich, *La pretesa estensione alla telematica del regime della stampa, note critiche*, *ibidem*, 27.

(39) Cfr., per esempio, Trib. Napoli, sent. 13 marzo 2003, cit.

(40) Così Trib. Catania 5 luglio 2004, cit.

(41) Così, per esempio, da ultimo la Corte app. Firenze (sez. I, 19 settembre 2005, n. 1463, ined.) dinanzi a segni distintivi di pari rilievo e appartenenti al medesimo settore ha accordato la preferenza «al soggetto che con priorità ha registrato il proprio», ritenendo che così facendo esso abbia acquisito il diritto ad ottenere un corrispondente domain name.

Di un qualche interesse può essere segnalare come per questa strada si sia giunti a ritenere che l'autorizzazione all'uso di un marchio conferita da un'impresa a terzi per pubblicizzare i propri prodotti comprendesse anche la sua registrazione, come domain name, di un sito Internet (cfr. Trib. Firenze, 5 gennaio 2000, cit.); diversamente, sposano l'idea secondo cui il titolare di un marchio non vanta un positivo diritto ad ottenere un domain name corrispondente al marchio, Trib. Firenze 29 giugno 2000, in *Dir. inf. e inf.*, 2000, 672, successivamente confermata dal Trib. di Firenze il 10 luglio 2000, in *Annali it. dir. autore*, 2000, 1000; Trib. Pistoia 10 novembre 2000, cit. Ancora più radicale, da questo punto di vista è la pronuncia, ancora una volta (tanto da indurre la più attenta dottrina a interrogarsi sulla possibilità di parlare di una "giurisprudenza toscana" in materia: cfr. G. Cassano, *Una "giurisprudenza toscana" sui nomi di dominio?*, in *Dir. inf. e inf.*, 2001, 511 e Id., *Un filone giurisprudenziale anarchico: la giurisprudenza toscana e i nomi di dominio*, in *Giur. it.*, 2001, 1902) del Trib. Firenze, 23 novembre 2000, cit., che non condivide la possibilità di equiparare il marchio con il domain name, perché mentre il primo sarebbe caratterizzato da vari tipi di segni grafici "idonei a formare infinite combinazioni", finalizzati a tutelare il prodotto di una impresa, il secondo potrebbe invece essere formato soltanto da lettere o numeri e costituire nient'altro che un indirizzo telematico.

(42) Affrontano il particolare profilo della "notorietà", tra gli altri, Trib. Parma 9 giugno 2000, in *Impresa*, 2000, 1148; Trib. Verona 14 luglio 1999, in *Giur. it.*, 2000, 341; Trib. Vallo Lucania 10 giugno 2005, ined.

(43) Con più stretto riguardo ai nomi di persona ci limitiamo qui ad osservare come a fronte della tesi favorevole al divieto di utilizzo di "nomi di persona" per la composizione di "segni distintivi" (per la "degradazione" che si produrrebbe a scapito del nome patronimico, che, da attributo della personalità, si ridurrebbe a mero strumento di individuazione di prodotti: al proposito, ricordiamo che nel 2001 era stato approvato in Commissione al Senato un disegno di legge sui nomi a dominio, il "d.d.l. Pasigli", reperibile su <http://www.interlex.it/nomiadom/testo.htm>, che all'art. 2 disponeva il divieto di registrazione di nomi a dominio corrispondenti, tra l'altro, a nomi identificanti persone fisiche), per giurisprudenza ormai costante li si ritiene di massima leciti, nel rispetto, ovviamente, della normativa di riferimento ed in particolare a patto che non si tratti di nomi notori e che non venga lesa l'immagine di chi porta quel nome (v. App. Milano 30 luglio 1996, ined.). A quest'ultimo riguardo, peraltro, è tutt'ora aperto il dibattito sulla possibilità di configurare limiti (ulteriori) in materia tenuto conto del "Codice in materia di protezione dei dati personali". Al proposito, mentre la prospettiva tendente ad equiparare la disciplina "industrialistica" rispetto a quella civilistica porta ad estendere il controllo individuale su ogni aspetto della propria personalità, ivi inclu-

(segue)

dendo possibile che la persona notoria (si tratti di persona fisica o di altro tipo) possa «riappropriarsi» del proprio *domain name*, anche se registrato prima da altri (44).

5. Il rilievo dell'«identità personale» nella definizione della controversia

Posto dunque il carattere recessivo della registrazione del *domain name* rispetto a quello dei segni distintivi «tradizionali», qualche problema si pone quando si ha a che fare con un segno distintivo non registrato e nemmeno, in certi casi, registrabile, né tanto meno notorio...

In queste situazioni (a fronte della possibile riemersione del principio del *first*), la giurisprudenza prevalente percorre una strada per certi versi speculare (o, se si vuole, complementare) a quella intrapresa nel caso di «notorietà», valorizzando l'idea della presenza, al di là del segno distintivo (già, peraltro, «identificatorio», come s'è visto al §2) di un «valore aggiunto» - sia esso di ordine industriale o intellettuale, anche se poi, nella maggior parte dei casi le due cose si tengono... - precipitato della storia e dell'attività dell'ente, meritevole, come tale, della più adeguata tutela

È in quest'ottica che, talvolta, si chiama in campo l'«identità personale» (45), identificando in essa il diritto del soggetto «ad essere sé stesso», ovvero «ad essere tutelato contro attribuzioni estranee alla propria personalità», idonee a «trasfigurarla o travisarla», tra l'altro, confondendola con altre entità. Ed è quello che fa nel caso in esame il Tribunale di Roma, dapprima ravvisando una violazione del nome «tradizionale», tutelato dall'art. 7 c.c., essendo «ormai pacifico in giurisprudenza il principio secondo cui la denominazione degli enti, in quanto equivalente del nome, gode della medesima tutela a quest'ultimo attribuita dall'art. 7 c.c., nel caso in cui il nome o denominazione sia da altri usurpato con un pregiudizio di carattere economico o morale per il titolare»; e, quindi, evidenziando che «si tratta di un'associazione di cultura e impegno politico, che prende il nome e l'ispirazione da un gruppo di studenti tedeschi che si opposero al regime nazista, e che fin dal 1978 opera con lo scopo di diffondere la cultura cattolico-progressista». Ritenendo con ciò «evidente» la lesione dell'identità personale della ricorrente, non potendo lo stesso nome «essere usato da un altro e diverso movimento politico, differente per storia e orientamento politico», a motivo della confusione che quell'uso è idoneo a ingenerare.

La decisione a cui approda il giudice induce ad interrogarsi in particolare sulle ragioni del richiamo del diritto all'«identità personale», specie se si condivide l'idea che la lettura «unitaria» ed estremamente estensiva della normativa di riferimento sarebbe stata già di per sé idonea a condurre ad analoghe conclusioni con riguardo alle lesioni ravvisate e alle tutele apprestate.

Del resto la stessa autorità giudicante riconosce infine il diritto dell'associazione ricorrente ad usare in via esclusiva il nome a dominio in questione «sia per il diritto al nome sia per il poizore diritto sul nome a dominio

rosabianca.org, la cui registrazione risale al 2000», riferendosi dunque essenzialmente alle norme sul nome e sul marchio. Inoltre, applica in via d'urgenza, ex art. 700 c.p.c. (46), le tutele richieste dall'associazione ricorrente, ancora, sulla base delle norme sul marchio (inibizione dell'uso di segni identici o simili al nome oggetto del contendere e al suo nome a dominio; immediato trasferimento dei nomi a dominio «abusivi» a favore dei ricorrenti; fissazione di una sanzione per ogni violazione o inosservanza del provvedimento e della sua esecuzione); e sul nome (pubblicazione sui quotidiani e sui i siti concesi, del dispositivo della sentenza; condanna alle spese di lite), facendo con ciò venir meno uno dei motivi che tradizionalmente ha condotto ad invocare tale diritto: quello, appunto, di mancanza di adeguati strumenti di tutela. Senza voler poi qui considerare le problematiche che desta l'estensione del riconoscimento del diritto all'identità personale, anche nei confronti di soggetti diversi dalle persone fisiche, specie là dove si dia risalto al suo radicamento nelle norme costituzionali inerenti alla dignità umana (47).

Tutto ciò considerato ci pare che la chiamata in campo del diritto all'identità personale, al di là della comprova della perdurante vitalità dell'associazione (da notare al proposito che il giudice nella decisione in commento evidenzia il fatto che «il nome «Rosa Bianca» identifica da decenni l'attività della ricorrente»), sia riuscita utile, in qualche misura, nel dotare il «nome» - e,

Note:

(segue nota 43)

sa la gestione del «proprio» *domain name*, concludendo a favore dell'illegittimità dell'uso di segni distintivi composti da nomi altrui senza il consenso dell'avente diritto, sia esso persona notoria o meno (al punto da ritenere implicitamente abrogato l'art. 21, comma 2, l. marchi); diversamente, in un'ottica volta ad affermare la prevalenza della disciplina industrialistica su quella civilistica si è indotti a sostenere che la normativa sulla *privacy* incida del tutto relativamente sulla legge marchi, specie nei casi in cui la persona non è «famosa», dal momento che proprio la mancata notorietà del nome renderebbe inattuabile la «trasmissione» del suo «valore aggiunto», nonché dell'«informazione-dato personale», al prodotto o servizio «marcato», rendendo conseguentemente «inutile» il consenso dell'avente diritto (salvo i casi del tutto «improbabili» in cui la persona, anche non nota, il cui nome risulti ricompreso nel marchio, sia identificabile).

(44) V. il noto caso, già menzionato, che ha riguardato il marchio «Porta Portese», deciso dal Trib. Roma, il 2 agosto 1997, cit.; successivamente, nello stesso senso, tra gli altri, si vedano Trib. Napoli, 26 marzo 2004, in *Foro it.*, 2004, I, 1548; e Trib. Perugia, 5 ottobre 2000, inedit.

(45) Al proposito, ci si consenta di rinviare a L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino 2004, 207.

(46) Come rivela il Tribunale di Napoli nella sent. del 13 marzo 2003, cit., ormai in questa materia (ma a ben vedere sin dall'inizio: v. le decisioni capostipiti dei Trib. di Bari e di Modena) la tutela è «quasi sempre cautelare», al punto da portare taluni giudici a censurare la mancata tempestività dell'azione a tutela del diritto all'uso esclusivo del proprio segno distintivo, individuandovi un'ipotesi di decadenza, specificamente prevista, tra l'altro, dall'art. 42, comma 1, l. marchi.

(47) V. al proposito, L. Trucco, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, cit., 233.

conseguentemente, nell'ottica «unitaria» sposata dal giudice, il «domain name» - di un «peso» (ulteriore) tale da renderlo al possibile resistente bilanciamento con la «notorietà» (non tanto dell'altra associazione, quanto, soprattutto) dei componenti del movimento politico convenuto, che, in un'ottica volta alla valorizzazione dell'interesse mediatico rispetto a quello ideologico, avrebbe potuto condurre ad una diversa definizione della vicenda (48).

Del resto viene considerata ormai «diritto vivente (49)», quella giurisprudenza che, dinnanzi al conflitto - quanto all'identificazione della norma applicabile -, tra gli art. 7 c.c. e 21 l. marchi, privilegia la seconda disposizione, ritenendo che solo compito dell'art. 7 c.c. sia quello di vietare l'uso pregiudizievole del nome altrui posto in essere a scopo di identificazione personale, spettando invece all'art. 21 l. marchi disciplinare più ampiamente l'ipotesi di uso del nome altrui, anche se patronimico, come marchio, perché l'impiego del nome patronimico per distinguere i prodotti o i servizi di una determinata impresa lo emanciperebbe dalla persona fisica (ma potrebbe anche essere una persona giuridica o un'associazione non riconosciuta) a cui originariamente appartiene (50).

Note:

(48) Cfr. Trib. Napoli (26 febbraio 2002, in *Arch. civ.*, 2002, 706), nel noto caso in cui oggetto del contendere era nome di dominio "Playboy.it", riferito ad un sito di contenuto pornografico e di cui la società *Playboy enterprises inc.* aveva chiesto l'assegnazione, posto il presunto esclusivo diritto di marchio, come termine *Playboy*, anche come *domain name*. Il giudice nel caso di specie evidenzia come l'*initial confusion* possa rivelarsi già di per sé idonea a produrre l'effetto utile per il titolare del sito, che, grazie al "momento del contatto" riesce a farsi conoscere "drenando" la clientela da una parte (il titolare del marchio da tutelare) all'altra (il titolare del nome di dominio). Per diverso profilo, mettono in luce l'idoneità del *domain name* (utilizzato) a rafforzare la "notorietà" (anche degli altri segni distintivi) del soggetto e le scelte del consumatore, rispettivamente, Trib. Biella, 16 maggio 2000, in *Giur. piemontese*, 2000, 443; e Trib. Firenze, 7 giugno 2001, in *Dir. e pratica società*, 2001, 80.

(49) Così Trib. Napoli, sent. 13 marzo 2003, cit.

(50) V. in particolare, Cass. 21 ottobre 1988, n. 5716, in *Foro it.*, 1989, I, 764, che evidenzia come in tali ipotesi debba trovare applicazione la disciplina delineata dall'art. 2564 c.c. e legge marchi; più di recente, v. Cass. 13 marzo 1998, n. 2735, *Riv. dir. ind.* 1999, II, 477; Cass. 3 luglio 1992, n. 8157, in ed.; e Cass. 6 aprile 1995, n. 4036, in ed., secondo cui «al fine di verificare se l'uso di un nome altrui, in occasione dell'adozione di una ditta commerciale o di un marchio, possa ritenersi o meno indebito, deve farsi riferimento alla disciplina specifica che la legge riserva a tali segni distintivi nell'ambito del diritto commerciale, non già alla tutela riservata dalla legge ai diritti della personalità (art. 7 c.c.), con la conseguenza che un provvedimento giudiziario che inibisca ad altri l'uso del proprio nome può essere chiesto solo quando questa utilizzazione si traduca in un uso arbitrario di segni distintivi dell'attività imprenditoriale».

RIVISTE

I Contratti

Rivista di dottrina e giurisprudenza

Direzione scientifica: Giorgio De Nova, Guido Alpa, Ugo Carnevali
Comitato di redazione: Carmen Leo, Arturo Maniàci, Christian Romeo
 Periodicità: mensile



Una Rivista che, grazie all'ampia rilevanza data alla giurisprudenza e all'analisi della contrattualistica nazionale e internazionale delle problematiche connesse con l'arbitrato, fornisce una risposta completa e tempestiva alla sempre più diffusa esigenza di informazione in materia. Le numerose sezioni in cui è articolata la Rivista - Giurisprudenza, Normativa, Argomenti, Quesiti, Panorama fiscale, Osservatorio comunitario - privilegiano questioni di rilevanza professionale. La rubrica Modelli contrattuali segnala l'elaborazione, anche da parte di enti e di associazioni, di schemi contrattuali tipici ed atipici.

Il **servizio online**, riservato esclusivamente agli abbonati e consultabile all'indirizzo www.ipsoa.it/icontratti, permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 199,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 - fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- www.ipsoa.it

Processo civile telematico

L'atto digitale e la procura: una ragionevole soluzione sul rilascio della procura speciale

Tribunale di Milano 1 febbraio 2008, ord.

Processo telematico - Ricorso per decreto ingiuntivo telematico - Copia informatica della procura alle liti - Busta contenente ricorso e procura firmata con firma digitale dell'avvocato - Costituzione in giudizio valida - Requisito congiunzione materiale ex art. 83, comma 3, c.p.c. - Sussistenza

(d.lgs. n. 82/2005 artt. 20, comma 2, 71; c.p.c. art. 83, comma 3)

È valida la costituzione in giudizio compiuta col deposito telematico del ricorso per decreto ingiuntivo, quando viene soddisfatto il requisito della congiunzione materiale all'atto della procura alle liti in formato digitale, richiesta dall'art. 83, comma 3, ultima parte, c.p.c. Ciò si verifica quando la copia informatica della procura medesima viene spedita all'interno della busta telematica sottoscritta con firma digitale dall'avvocato che ha depositato telematicamente il ricorso monitorio. Infatti, la busta telematica firmata digitalmente dal difensore rappresenta un insieme di atti informatici tra loro congiunti in modo assolutamente inscindibile e immodificabile. La firma digitale del difensore apposta sulla busta è inoltre idonea a garantire la provenienza, nonché a soddisfare il requisito della forma scritta.

...Omissis...

Rilevato

Rileva la rituale costituzione in giudizio delle parti e in particolare che l'eccezione di inammissibilità dell'opposizione dell'Azienda agricola Castellone s.r.l. non pare fondata in quanto dall'esame della busta verde contenente l'atto (decreto opposto) notificato a mezzo posta risulta che l'ingiunta destinataria è stata avvisata del deposito del plico con raccomandata del 27 aprile 2007; ragionevolmente deve ritenersi che il medesimo giorno l'atto sia stato depositato nell'ufficio postale per il decorso del termine di giacenza di dieci giorni; risulta altresì che l'atto di citazione è stato presentato all'ufficiale giudiziario per le notifiche il 6 giugno 2007 dunque nel termine di quaranta giorni dal 27 aprile 2007; osserva sulla costituzione in giudizio della ricorrente quanto segue: la difesa dell'opponente ha posto in via preliminare una serie di questioni circa la validità della procura alle liti in capo al difensore della società ricorrente con conseguente ricaduta sulla validità/esistenza del ricorso per decreto ingiuntivo. Ha dedotto: 1) la nullità della procura perché sarebbe stata rilasciata su un foglio separato dal ricorso che non è stato allegato al medesimo ma semplicemente prodotto quale documento del fascicolo monitorio e ciò sebbene nell'intestazione dell'atto fosse stato dichiarato che l'avv. Ru-

sconi rappresentava la società ricorrente «in forza di procura allegata al presente atto» dunque il tutto in violazione di quanto disposto dall'art. 83, comma 2 e 3. c.p.c.; 2) l'omessa trascrizione, nelle copie autentiche del ricorso e del decreto ingiuntivo notificate ai debitori ingiunti, della procura asseritamente allegata al ricorso; 3) il vizio della procura per difetto di rappresentanza della società di colui che avrebbe conferito il mandato al difensore che ha presentato e firmato il ricorso monitorio.

Nell'esaminare la valida costituzione in giudizio della ricorrente va premesso che il procedimento della fase monitoria si è svolto in via telematica.

Dall'esame del fascicolo monitorio telematico, prodotto in forma cartacea nella presente fase di opposizione dalla opposta, e dall'esame del ricorso monitorio risulta che Italfondario s.p.a. ricorrente, ha agito in giudizio quale procuratore di Intesa Mediocredito s.p.a. rappresentata e difesa dall'avv. Rusconi «in forza di procura allegata al presente atto», così come si legge nell'epigrafe del ricorso; la procura alle liti è stata prodotta quale doc. 8 del fascicolo telematico; la procura alle liti è procura rilasciata su documento cartaceo dal dott. Angelo Bruno Braschi la cui firma è stata certificata dall'avv. Rusconi, nel testo della procura c'è l'esplicito riferimento all'azione contro le attuali opposenti poiché si dà mandato al legale di agire in via monitoria e nella successiva eventuale fase di

opposizione contro Azienda agricola Castellone e fideiussori dinanzi al Tribunale di Milano.

Ritiene il tribunale valida la costituzione in giudizio della ricorrente opposta poiché quello che è stato denunciato come vizio della procura alle liti, perché materialmente non spillata al ricorso monitorio, pare carente nei suoi presupposti di fatto. Si è detto che la procura alle liti risulta prodotta quale doc. 8 del ricorso monitorio, essa è stata spedita all'interno della busta telematica sottoscritta con firma digitale dall'avvocato che ha presentato e depositato telematicamente il ricorso monitorio; la busta telematica è un insieme di documenti informatici: il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; la busta informatica è sottoscritta con firma digitale e soddisfa il requisito legale della forma scritta ai sensi degli art. 20 e 71 d.lgs. n. 82/2005, la firma digitale apposta sulla busta garantisce l'identificabilità dell'autore e l'integrità del documento (art. 20, comma 2, d.lgs. n. 82/2005): la procura alle liti in quanto contenuta nella busta telematica è stata regolarmente prodotta in giudizio al momento della costituzione in giudizio della parte ricorrente (risulta effettivamente presente nel fascicolo monitorio oltre che essere indicata nell'indice delle produzioni contenute nella busta telematica); la circostanza che essa sia contenuta nella busta telematica unitamente al ricorso monitorio, busta firmata dall'avvocato con firma digitale, soddisfa il requisito della congiunzione materiale all'atto richiesta dall'art. 83, comma 3, ultima parte, c.p.c. atteso che l'art. 10 d.p.r. n. 123/2001 stabilisce che: «Se la procura alle liti è stata conferita su supporto cartaceo, il difensore, che si costituisce per via telematica, trasmette la copia informatica della procura medesima, asseverata come conforme all'originale mediante sottoscrizione con firma digitale». Dunque la normativa del codice di procedura civile sulla procura alle liti non è stata modificata dal sistema normativo in vigore che regola il processo civile telematico nel senso che la procura alle liti, anche nel procedimento monitorio telematico, può essere conferita, oltre che a margine o in calce al ricorso, anche su foglio separato purché esso sia congiunto materialmente all'atto (ricorso) cui si riferisce; l'inserimento del foglio separato contenente la procura nella busta telematica firmata dal difensore con firma digitale costituisce la congiunzione materiale, nel sistema telematico, della procura all'atto dato anche il disposto dell'art. 10 d.p.r. n. 123/2001 che richiede, per la procura su supporto cartaceo, che essa sia trasmessa in copia informatica asseverata conforme con firma digitale; nel caso di specie, per altro, specifici elementi contenuti nel testo della procura alle liti (nome delle controparti, individuazione dell'azione e modalità di presentazione, indicazione dell'autorità giudiziaria competente) non lasciano dubbi sul riferimento concreto di quella procura al ricorso depositato e contenuto nella medesima busta telematica.

La procura alle liti rilasciata dal dott. Braschi quale rappresentante di Italfondario s.p.a. è valida perché dal

doc. 2 prodotto dalla ricorrente nella fase monitoria risulta che l'amministratore delegato di Italfondario s.p.a. con procura speciale e sottoscrizione autenticata da notaio, aveva conferito al dott. Bruno Angelo Braschi una serie di poteri tra cui quello al fine di tutelare ragioni di credito presentare ricorsi per decreti di ingiunzione, eleggere domicili, nominare avvocati conferendo ad essi mandati generali o speciali alle liti per rappresentanza e difesa della società in tutti i gradi di giudizio. Risulta altresì dal doc. 1 monitorio che Banca Intesa Mediocredito s.p.a. aveva nominato quale suo procuratore speciale ex art. 77 c.p.c. Castello gestione crediti s.p.a. e che Italfondario s.p.a. quale società incorporante si è fusa con Castello gestione crediti s.p.a. il 2 agosto 2006; infine si rileva che la circostanza che il ricorso e il decreto ingiuntivo siano stati notificati alle parti debentriche senza la trascrizione della procura alle liti non può dare luogo alla nullità insanabile del ricorso e del decreto considerando che numerosi elementi agli atti, tra cui la certificazione di cancelleria con il depositato della busta contenente il ricorso e i documenti informatici, consentono di ritenere l'avvenuto conferimento della procura alle liti prima della costituzione in giudizio della parte ricorrente.

La difesa delle parti opposte ha chiesto di sospendere la provvisoria esecuzione del decreto ingiuntivo opposto; la richiesta non può essere accolta: si rileva che l'eccezione di incompetenza per territorio non pare tale da precludere l'esame nel merito dell'opposizione; che i documenti prodotti nella fase monitoria sono idonei a dare dimostrazione scritta, nella suddetta fase monitoria, del credito dedotto in giudizio della banca; il contratto di finanziamento, stipulato nel 2002, risulta, quanto alla pattuizione sugli interessi moratori, conforme al T.U.F., art. 120, e alla delibera CICR del febbraio 2000; rilevato che le difese hanno chiesto i termini ex art. 183, comma 6, c.p.c. e che è opportuno che essi siano dati in udienza per avere certezza dell'uguale decorso per tutte le parti processuali.

IL COMMENTO

di Alessandra Vилlecco

Il commento alla pronuncia in epigrafe analizza la questione sia sotto il profilo della normativa processuale, sia nella prospettiva tecnica per spiegare il significato della "materiale congiunzione" a cui fa riferimento il comma 3 dell'art. 83 nel caso di ricorso informatico depositato telematicamente. In particolare, viene esaminata anche la delicata questione della procura rilasciata su foglio autonomo come un'apertura verso la procura presunta, che proprio nella previsione dell'art. 10 del decreto presidenziale n. 123/2001 sul processo telematico sembra trovare un pieno riconoscimento.

1. Introduzione

Questo provvedimento giurisprudenziale che riguarda una delle prime esperienze attuative del processo telematico, dimostra chiaramente come il formalismo digitale possa dare anche maggior efficacia all'attuazione degli scopi cui tende la disciplina processuale che regge la delicata materia della procura alle liti e i suoi riflessi sulla regolare costituzione delle parti.

I giudici del tribunale ambrosiano hanno ritenuto valida la costituzione del ricorrente per ingiunzione avvenuta con il deposito per via telematica del ricorso, in quanto la procedura elettronica per apporre la procura speciale si sarebbe dimostrata rispettosa delle regole contenute nell'ultima parte del comma 3 dell'art. 83 c.p.c. (come modificato dall'art. 1, legge 27 maggio 1997, n. 141), che ha parificato la procura rilasciata su foglio separato alla procura in calce all'atto con lo stabilire che la procura speciale rilasciata su foglio separato si considera apposta in calce all'atto cui si riferisce se a quest'ultimo sia "congiunto materialmente".

Nel caso di specie, i giudici hanno ritenuto che la procedura informatica e telematica per redigere il ricorso e prepararlo per il deposito nella busta telematica con allegati tutti gli atti e i documenti che servono per la regolare costituzione telematica ai sensi della disciplina sul processo telematico abbia assolto questo requisito.

Di sicuro la vicenda assume toni di maggiore interesse proprio perché è incentrata sul futuro processo telematico, cioè il processo basato sull'infrastruttura informatica e telematica la cui disciplina è contenuta nel regolamento di cui al d.p.r. 13 febbraio 2001, n. 123, un processo che ha già trovato applicazione per iniziativa del tribunale di Milano sia pure con limitato (per ora) riferimento al procedimento per ingiunzione (1).

Questo regolamento detta le regole per la trasmissione e la conservazione degli atti processuali elettronici richiamando, per quanto riguarda la forma e il valore probatorio, la disciplina sostanziale di cui al Codice del-

l'Amministrazione Digitale (CAD) (2). Il processo c.d. telematico (3) è essenzialmente basato su un sistema informativo unitario per la creazione e la gestione di un fascicolo elettronico e lo scambio telematico degli atti processuali anche se, almeno per ora, la forma digitale non esclude affatto la tradizionale forma cartacea: invece, quanto ha forma digitale dovrà essere riprodotto in forma cartacea e viceversa, sempre che tali operazioni affidate agli uffici di cancelleria non comportino un eccessivo dispendio economico e siano facilmente realizzabili.

Così la costituzione in giudizio, come la produzione di documenti elettronici, può avvenire in via telematica, ma anche attraverso la forma cartacea (4). Per quanto

Note:

(1) A. Torrice, *Il decreto ingiuntivo telematico: innovazione tecnologica, normativa, sociale e organizzativa. L'esperienza del tribunale di Milano*, Roma, "Forum P.A. 2007" http://www.forumpa.it/forumpa2007/convegni/relazioni/1043_amelia_torrice/1043_amelia_torrice_1.pdf; P. Pacchioli e F. Pappalardo, *Il decreto ingiuntivo telematico con valore legale: l'esperienza del Tribunale di Milano*, in questa Rivista, 2, 2007, 203 ss.

(2) Il CAD è contenuto nel d.lgs. 7 marzo 2005, n. 82.

(3) M. Jacchia, *Il processo telematico*, (a cura di), Bologna, 2000; P. Liccardo, *Introduzione al processo civile telematico*, in *Il processo telematico*, cit.; F. Buffa, *Il processo civile telematico: la giustizia informatizzata*, Milano, 2002; A. Vилlecco, voce *Processo telematico*, in *Dig. It. disc. priv.*, sez. civ. Torino, 2003 e *Due facce di una stessa medaglia: il processo tradizionale ed il nuovo processo tecnologico*, in *Cyberspazio e diritto*, 2004; G. Buonomo, *Processo telematico e firma digitale*, Milano, 2004; A. Vилlecco, *The Employment of XML Standards in Electronic Judicial Proceedings*, Institute of Mining of Technology, Socorro-New York, 2005; F. Buffa, *Al via il processo civile telematico: le nuove opportunità per gli avvocati*, in questa Rivista, 1, 2005, 9 ss.; G. Rem e A. Sirotti Gaudenzi, *La giustizia telematica e la procedura informatizzata*, Rimini, 2005; S. Brescia e P. Liccardo, *Processo telematico*, in *Enc. giur. it.*, Roma, 2006; M. De Cristofaro, *Il nuovo processo civile "competitivo" secondo la l. 80/2005*, in www.judicium.it, 2005; D. Intravaia, *Processo civile telematico: Disciplina normativa e infrastruttura tecnologica*, in *Elementi di informatica giuridica*, M. Jori (a cura), Torino, 2006; M. Fabri, *Tecnologie della giustizia*, Bologna, 2006; G. Taddei Elmi, *Il processo telematico*, (a cura di), Napoli, 2007; A. Vилlecco, *Fair On-Line Civil Trial: An Important Aspect of E-Government*, in *IPSI Journal*, 2007.

(4) La redazione degli atti da parte dell'avvocato avviene mediante un comune sistema di videoscrittura con uno strumento integrato che preliminarmente consente di selezionare il modello di atto da predisporre, con l'automatico inserimento di dati nei campi obbligatori che identificano l'autore dell'atto. Successivamente, dopo la redazione l'atto viene imbastito insieme a tutti gli altri documenti, inclusa la procura in originale, se è stata rilasciata con firma digitale dal soggetto che la conferisce, oppure la copia informatica della medesima eseguita mediante scansione, qualora sia stata rilasciata in formato cartaceo ai sensi dell'art. 10 D.P.R. 123/2001. In argomento si veda lo scritto di A. Contaldo e M. Gorga, *Le regole del processo civile telematico anche alla luce della più recente disciplina del SICI*, in questa Rivista, 1, 2008, 5 ss.

Tali atti e documenti potranno essere salvati in formato pdf, rtf, txt, jpg, gif, tiff, xml, in assenza di elementi attivi come macro o campi variabili. La busta verrà poi firmata con la firma digitale del difensore ed anche criptata mediante l'impiego dell'algoritmo 3DES per l'invio telematico, attraverso un sistema di posta elettronica certificata (PEC), all'ufficio giudiziario (UG) di destinazione, il quale si servirà per il controllo della chiave pubblica contenuta nel certificato dell'ufficio giudiziario destina-

(segue)

riguarda, in particolare, la procura, l'art. 10 d.p.r. n. 123 ammette il suo rilascio anche su supporto cartaceo, purché il difensore trasmetta "la copia informatica della procura medesima, asseverata come conforme all'originale mediante sottoscrizione con firma digitale". La norma in questione si preoccupa di disciplinare solo questa ipotesi, in quanto in riferimento alla procura firmata con la firma digitale del soggetto che la conferisce il documento originale verrà allegato all'atto digitale prima dell'imbustamento, proprio in piena sintonia con l'art. 83, comma 3, c.p.c. (5).

Il provvedimento che si annota rappresenta un confortante punto di partenza, anche se non pienamente condivisibile appare il profilo argomentativo, per dare risposta non solo alla specifica questione sottoposta al suo vaglio, ma anche per far luce su una materia che per lungo tempo ha impegnato la giurisprudenza, spesso in modo disarmonico e contraddittorio. Infatti, diversi sono i temi evocati dalla questione in esame: la natura della procura rilasciata su foglio separato; il significato della "materiale congiunzione" ai sensi dell'art. 83, comma 3, c.p.c.; i vizi collegati alla procura, alla loro rilevanza e all'eventuale sanzione; il potere certificatorio dell'avvocato riguardo alla firma del cliente che in definitiva si ricollega alla prospettiva della rilevanza da attribuire alla presunzione di esistenza della procura, la c.d. procura "presunta".

2. La procura su foglio separato

Le questioni sulla forma della procura hanno trovato nuovo alimento con la riforma del 1997 che ha dato legittimità alla procura rilasciata su foglio separato attraverso la modifica del comma 3 dell'art. 83 c.p.c., un'eventualità che aveva suscitato in giurisprudenza contrasti non sopiti, sia prima sia dopo la novella e di cui vi è stata anche ampia eco in dottrina (6), su quali fossero i requisiti, per dare validità a procure speciali scritte non a margine e neppure in calce ad atti processuali che debbono essere sottoscritti da un difensore ritualmente investito dello *ius postulandi* (7).

La prassi forense nel ricorrere con frequenza al conferimento della procura redatto su fogli separati, autonomi rispetto all'atto processuale a cui avrebbe dovuto essere apposta, ha provocato in principio una reazione di natura garantista assai rigorosa della Corte di legittimità che, in assenza di una specifica disciplina sul punto, ha ritenuto l'invalidità di questa modalità di rilascio della procura, provocando quella che è stata definita con buona ironia la "strage degli innocenti" (8).

Solo successivamente, forse sotto la pressione della realtà dei fatti che spesso scavalca la regola *iuris*, nonché l'avvento delle nuove tecnologie che hanno reso più agevole la stampa degli atti con fogli separati uniti poi dalla fascicolazione, il legislatore è stato indotto ad operare un cambiamento della disciplina processuale con lo stabilire, nel nuovo comma 3 dell'art. 83 c.p.c. che "la procura si considera apposta in calce anche se rilasciata

su foglio separato che sia però congiunto materialmente all'atto cui si riferisce".

Una formula che suscita vari interrogativi. Infatti ci si può chiedere cosa si intenda per congiunzione materiale. O, ancora, se la specialità della procura risulta dalla materiale congiunzione del foglio che la contiene all'atto per la redazione del quale risulta rilasciata e non anche da espressioni che ne evidenziano il legame col processo o con l'atto.

La maggior parte della giurisprudenza ha ritenuto, in un primo tempo, di utilizzare la "taumaturgica virtù" (9) di *ammenicola* meccanici per dare validità all'atto di procura su foglio separato, solo che questa sua "materiale congiunzione" fosse realizzata con la spillatura mecca-

Note:

(segue nota 4)

tario dell'atto, dopo che il gestore centrale (GC) - il primo punto di accesso alla rete interna della giustizia - avrà effettuato un controllo preliminare sulla busta.

Sul sito del Ministero di Giustizia <http://processotelematico.giustizia.it/pdapublic/index.jsp?sid=1&id=1&pid=1> sono reperibili una serie di informazioni sul processo telematico, anche in riferimento alle specifiche tecniche, e sui vari progetti.

(5) Infatti, è proprio in questo caso, come si avrà modo di spiegare, che si ha l'equivalenza, sotto ogni profilo, alla procura di parte su foglio separato ai sensi del 3° comma dell'art. 83, per cui la firma digitale del difensore apposta sulla busta che contiene tutti gli atti processuali e i documenti che devono essere depositati al momento della costituzione assolve al requisito della "congiunzione materiale".

(6) G. Balena, *Sulle conseguenze del difetto di procura "ad litem"*, in *Foro it.*, 1987, I, 552; G. Guarnieri, *Ancora sulla procura in foglio più o meno separato o allungato*, in *Riv. dir. proc.*, 1989, 291 ss.; S. Chiarloni, *Senza fondo gli abissi formalistici in tema di pretesi vizi della procura alle liti*, in *Giur. it.*, 1993, I, 1, 1013 ss.; G. De Luca, *Sulla specialità della procura a margine del ricorso per cassazione*, in *Foro it.*, 1994, I, I, 3170 e *Procura alle liti, commento alla legge del 24 maggio 1997*, n. 141, in *Nuove leggi civili commentate*, 1997, 1298; M. Giorgetti, *Sulla leggibilità della firma in calce alla procura ad litem*, in *Riv. dir. proc.*, 1995, 287 ss.; R. Murra, *La procura alle liti tra colombi ed angeli neri*, in *Giust. civ.*, 1995, I, 381; F. Cipriani, *La procura su foglio autonomo tra la certificazione e gli spilli del difensore*, in *Foro it.*, 1995, I, 537 ss.; F. Cipriani - G. Costantino - A. Proto Pisani - G. Verde, *L'infinita "historia" della procura speciale*, *ivi*, I, 3430 ss.; L. Di Bartolomeo, *Braccio di ferro tra Parlamento e Corte di Cassazione sulla procura speciale alle liti*, in *Riv. trim. dir. proc. civ.*, 1998, 695 ss., nota a Cass. 21 giugno 1997, n. 5569; F. Cipriani, *Procura su foglio separato o procura presunta?*, in *Foro it.*, 1997, I, 3152, nota critica a Cass., 2 settembre 1997, n. 8347 e Cass., 21 giugno 1997, n. 5569; M. Acone, *La procura speciale alle liti tra tiepidezza del legislatore e i contrasti nella corte*, in *Corr. giur.*, 1997, 1159 ss., nota critica a Cass., 21 giugno 1997, n. 5569.

(7) All'inizio degli anni '60 già S. Satta, *La procura in foglio più o meno separato o allungato*, in *Giust. civ.*, 1961, I, 1890 s. aveva precisato che il "metafisico" sforzo interpretativo del legislatore nell'equiparare la procura in calce a quella su foglio separato non ha mai tenuto conto del fatto che il termine "calce", meramente empirico, perché non ha mai voluto evocare alcun preciso riferimento ad "una connessione strutturale con l'atto al quale fa riferimento e prima ancora è termine empirico il foglio che, rispetto all'atto, non ha alcuna rilevanza giuridica, almeno per quello che riguarda gli atti processuali", poiché "quando la legge parla di calce vuol dire soltanto che la procura può essere rilasciata successivamente all'atto".

(8) G. Guarnieri, *Risolto "ex lege" l'annoso problema della validità della procura spillata*, in *Riv. dir. proc.*, 1997, 486.

(9) F. Cipriani, *Procura su foglio separato o procura presunta?*, *cit.*, 3157.

nica del foglio ad un atto processuale idoneo veicolo della procura alle liti. Si precisava ancora che questa congiunzione dovesse emergere da una numerazione progressiva coerente con quella data alle pagine dell'atto oppure, in alternativa, che l'unione risultasse dal timbro di congiunzione. Infine, si esigeva che il foglio separato fosse poi seguito da un'ultima pagina con l'istanza e la relazione di notificazione.

Per fortuna, la Cassazione, forse spinta dal ragionevole dubbio dell'inconsistenza di tali ragionamenti, si è poi orientata su argomentazioni dettate dal buon senso (10). Così, ha ritenuto che il foglio separato contenente la procura potesse anche essere inserito nella prima pagina o in mezzo all'atto (11), senza la necessità della spillatura come requisito di "congiunzione materiale", poiché tale requisito è individuabile in una serie di elementi, basati sull'interpretazione di fatti e circostanze, che rendono certa la provenienza dalla parte del potere di rappresentanza (12) ed alla riferibilità della procura stessa al giudizio a cui si riferisce.

Riguardo alla specialità della procura in margine o in calce la giurisprudenza ha per lo più specificato che non si rendono necessarie formule sacramentali, ma è sufficiente che si evinca dalla procura la volontà di conferire la rappresentanza al difensore, soprattutto quando con l'atto al quale è apposta formi un corpo unico per realizzare il requisito della "contestualità", quale giustificazione della riferibilità all'atto medesimo (13).

Il famoso timbro di congiunzione, usato e abusato, per utilizzare procure speciali seriali, cioè predisposte per adattarsi a qualunque tipo di lite, assolveva all'onere della riferibilità della procura a quello specifico giudizio, comportando sul piano pratico formulazioni generiche come ad esempio: "nomina procuratore e difensore nel processo di cui al presente atto in ogni stato e grado" oppure "per il presente procedimento" e per timore di non tralasciare nulla si eccedeva utilizzando espressioni generiche quali "in ogni fase e grado anche di appello, opposizione, esecuzione, opposizione all'esecuzione, chiamata in causa di terzi, ecc..." (14).

Per salvaguardare da nullità un numero indefinito di procure rilasciate su foglio separato e contestualizzate all'atto solo tramite la frequente prassi dei timbri di congiunzione, i giudici di legittimità hanno elaborato la tesi della specialità *per relationem* della procura, facendola derivare direttamente dalla sua relazione fisica con l'atto quando con esso costituisce un vero e proprio *corpus* inscindibile, con la precisazione della non tassatività degli atti indicati all'art. 83, comma 3, che anzi, sulla base della "specialità" *per relationem* della procura, il principio del comma 3 può essere esteso "a qualsiasi atto processuale, anche proveniente dall'avversario e comunque necessario ai fini della decisione" (15).

La dottrina ha cercato di sciogliere tali dubbi in senso positivo, nel senso di ritenere valida la procura su foglio separato, anche quando il foglio sia, ad esempio, semplicemente allegato al fascicolo di parte e, anche se

la procura non si riferisce esplicitamente a quel giudizio, venendo a fondare sul fatto dell'utilizzazione del foglio di procura una sorta di "procura presunta" (16). Insomma, un tema collocato in un panorama incerto, confuso, ed è stato detto, a ragione, che "la travagliata vicenda della procura speciale alle liti non può certamente essere aditata come esempio di civiltà giuridica" (17).

Sussistono peraltro dubbi sugli effettivi raccordi tra quanto dispone la nuova disciplina della procura su foglio separato e l'esercizio del potere di certificazione attribuito al difensore per quanto riguarda l'autografia della sottoscrizione della parte. Conviene notare che il legislatore non ha certo voluto introdurre una nuova tecnica di conferimento della procura alle liti rispetto a quella della procura in calce o in margine all'atto cui accede: è stato soltanto elaborato un metodo per rilasciare la procura. Infatti, occorre rilevare che l'assenza dal dato normativo di un espresso richiamo al potere di certificazione avrebbe potuto apparire come un modo, utilizzato dal legislatore, per evitare di chiarire i limiti dei poteri di certificazione dell'avvocato in riferimento a procure che non si trovano a margine o in calce all'atto, lasciando

Note:

(10) Cass. 23 aprile 2004, n. 7731, in *Gius.*, 2004, 3440; Cass., 24 settembre 2002, n. 13910, in *Ragiusan*, 2003, 227, 38.

(11) Il Cons. Stato sez. VI 10 ottobre 2006, n. 6011 in *Giustizia civile*, 2007, fasc. 4, 1002 ss., con nota critica di R. Murra, *Procura su foglio separato: ma è davvero questione di centimetri?*, ha ritenuto che una procura conferita su foglio separato per un giudizio dinanzi al tribunale amministrativo non sia idonea allo scopo qualora se sull'ultima pagina nella quale è redatto il ricorso esiste spazio a sufficienza per ivi apporre la procura medesima. La giurisprudenza amministrativa sembra considerare rilevante l'assenza di spazio fisico nell'atto T.A.R. Emilia-Romagna Parma Sez. I Sent., 10/03/2008, n. 131. Sempre in senso critico a questa interpretazione giurisprudenziale. Deluca, *Procura alle liti*, cit., 1997, 1298; Cass., 24 settembre 2002, n. 13910, cit.

(12) Cass., 5 marzo 2001, n. 3189, in *Mass. Giur. it.*, 2001 e di recente anche C. App. Roma Sez. II, 07/02/2008.

(13) In tal senso la Cass., S.U., 22 novembre 1994, n. 9869, in *Foro it.*, 1995, I, 537 nota di F. Cipriani, *Giust. Civ.*, 1995, I, 377 nota di R. Murra, *Procura su foglio separato: ma è davvero una questione di centimetri?*, in *Nuova Giur. Civ.*, 1995, I, 928 nota di Genesi, *Nuova Giur. Civ.*, 1995, I, 1087 nota di P. Della Vedova. Con questa pronuncia le Sezioni Unite hanno risolto il contrasto sorto in giurisprudenza su questo punto. In seguito, Cass., S.U., 13 giugno 1995, n. 444, ord., in *Foro it.*, 1995, I, 3433.

(14) La Cassazione, in riferimento al ricorso per cassazione e al controricorso, ha sovente ritenuto non valide tali formule generiche Cass., 14 marzo 1997, n. 2262; Cass., 15 maggio 1997, n. 4281, in *Foro it.*, *Mass.*, 1997, 393; Cass., 10 aprile 1997, n. 3110, in *Guida al diritto*, 1997, n. 27, 57.

(15) La prima in tal senso Cass. 18 maggio 1953, n. 1401, in *Giur. compl. Cass. civ.*, 1953, VI, 401, con nota di Bianchi D'Espinosa e tra le ultime in ordine di tempo la Cass., 16 giugno 1992, n. 7323, in *Giur. it.*, 1993, I, 1, 1013, con nota di S. Chiarloni, *Senza fondo gli abissi formalistici in tema di pretesi vizi della procura alle liti*, cit., Cass., S.U., 22 novembre 1994, n. 9869, in *Foro it.*, 1995, I, 537 ss. con nota critica di F. Cipriani, *La procura su foglio autonomo tra la certificazione e gli spilli del difensore*, cit.

(16) F. Cipriani, *Procura su foglio autonomo o procura presunta*, cit., 3159.

(17) M. Acone, *La procura speciali alle liti tra tiepidezza del legislatore e i contrasti nella corte*, in *Corr. giur.*, 1997, 1163.

l'operatore nel dubbio se nella specie sia ancora essenziale la certificazione del difensore (18).

Ad avviso di chi scrive, non vi è ragione di dubitare che data la piena parificazione della procura in foglio separato con quella apposta in calce, i poteri di certificazione del difensore debbano essere esercitati anche nel nuovo contesto, poteri, conviene rilevarlo, che servono a conferire alla procura quel rilievo giuridico che supera la materialità insita nelle caratteristiche "fisiche" della combinazione tra atto e procura e ciò per la ragione che, sotto il profilo giuridico, ben "può costituire un *corpus* inscindibile anche una combinazione di atti che sono fisicamente distinti" (19).

Si è visto come la giurisprudenza abbia assunto sul tema della procura su foglio separato varietà di atteggiamenti. L'incidenza poi di un valido rilascio della procura sulla valida costituzione in giudizio porta a riflettere anche sull'orientamento, invero rigido, assunto dalla Suprema Corte quanto all'ambito d'applicazione del comma 2 dell'art. 125 c.p.c. (20) che ammette il rilascio della procura anche in un momento successivo alla notificazione dell'atto di citazione, purché anteriore alla costituzione (21). A prescindere dagli effetti derivanti dalla produzione della procura successiva, ma antecedente alla costituzione, la dottrina e la giurisprudenza vi ravvisa, da un lato, un'attività di mera documentazione di una procura preesistente in forma verbale (22) dall'altra, come una sorta di convalida del difetto di rappresentanza in capo al difensore (23)- (24).

La nuova formulazione dell'art. 83, comma 3, sembra meglio adattarsi alla citata norma dell'art. 125 nel consentire il rilascio della procura non solo in forma d'atto pubblico e di scrittura privata autenticata (25). Infatti, la giurisprudenza precisa che anche un documento diverso da quelli espressamente contemplati dalla legge, depositato in cancelleria al momento della costituzione in giudizio è da ritenersi valida documentazione della procura rilasciata, purché la controparte non sollevi specifiche contestazioni circa l'esistenza e la tempestività della procura (26).

Una conclusione questa non condivisibile poiché la procura non ha lo scopo, come pure è stato detto, "di fornire alla controparte la giuridica certezza della riferibilità dell'attività svolta dal difensore al titolare della posizione sostanziale controversa" (27): invero, la procura e la sua regolarità formale sono nell'esclusivo interesse della parte che la rilascia (28) e che manifesta la volontà di essere rappresentata in giudizio da un determinato difensore e anche nell'interesse di quest'ultimo che non vuol correre il rischio che il proprio cliente disconosca il suo operato per aver egli agito senza procura (29).

3. Procedimento ingiuntivo telematico: copia informatica della procura

In questa cornice di problemi e di questioni tutt'altro che compiutamente definiti, si colloca la norma di cui all'art. 10 del regolamento sul processo telematico e

Note:

(18) A tal proposito si consiglia vivamente la lettura del vivace, ma quanto mai preciso e sensato scritto di F. Cipriani, *Procura su foglio separato o procura presunta?*, in *Foro it.*, 1997, I, 3152, in nota alle pronunce della Cassazione sezione lavoro, del 21 giugno, 1997, n. 5569, che ha dichiarato la nullità della procura su foglio separato anche in assenza di un riferimento all'atto e la sentenza 2 settembre 1997, n. 8347 di segno opposto alla precedente, entrambe emesse dopo la legge del 27 maggio 1997, n. 141. L'autore sostiene che il silenzio del legislatore sul punto in questione sia da attribuire limitatamente ai casi della procura a margine e in calce, e perciò al di fuori di questi due casi questo potere non potrebbe sussistere perché comunque sarebbe inidoneo a raggiungere lo scopo, nonché incapace a fornire la giuridica certezza della riferibilità dell'attività svolta dal difensore. Infatti, si sarebbe trattato di un'esclusione esplicita, perché nell'ambito della discussione alla Commissione giustizia del Senato successiva al disegno di legge, d.d.l. 335/S/XIII, si decise di sopprimere il riferimento alla certificazione contenuto nell'art. 1 del disegno di legge, che per iniziativa del senatore Palumbo e altri doveva essere un'interpretazione autentica del comma 3 dell'art. 83 c.p.c. Il d.d.l. 334/S/XIII "Interpretazione autentica del terzo comma dell'art. 83 del codice di procedura civile" - Art. 1: «il terzo comma dell'art. 83 del codice di procedura civile deve essere interpretato nel senso che si considera come apposta in calce anche la procura rilasciata su uno o più fogli congiunti all'atto al quale si riferisce, a condizione che essa sia stata sottoscritta dalla parte e l'autografia della sottoscrizione sia stata certificata dal difensore prima della notificazione o del deposito».

(19) M. Acone, *op. cit.*, 1167

(20) Su tale argomento si suggerisce lo scritto di V. Andrioli, *Commento al codice di procedura civile*, III ed., I, Napoli, rist. 1957.

(21) Cass., 21 febbraio 2001, n. 2476, in *Mass. Giur. it.*, 2001; Cass., 21 gennaio 1986, n. 630, in *Mass. Giur. it.*, 1986; Cass., 27 giugno 2003, n. 10251, in *Mass. Giur. It.*, 2003, *Gius.*, 2003, 24, 2813, in *Arch. Civ.*, 2004, 549, che ammette la validità della procura su foglio separato solo se la procura sia dotata della forma scritta e comunemente sia stata depositata prima della costituzione.

(22) C. Mandrioli, *Dei difensori*, in *Commentario UTET*, I, 2, Torino, 1980, 950-951.

(23) B. Cormio, *Degli atti in generale*, in *Commentario UTET*, I, 2, Torino, 1973, 1346. In giurisprudenza Cass., 9 luglio 1993, n. 7569, in *Giur. it.*, 1994, I, 1, 731.

(24) A. Villecco, *Due facce di una stessa medaglia: il processo tradizionale ed il nuovo processo tecnologico*, cit. 213, su alcune riflessioni tra la compatibilità dell'art. 125, comma 2, c.p.c. e l'art. 10 d.p.r. n. 123/2001.

(25) Cass., 23 maggio 2002, n. 7539, in *Mass. Giur. It.*, 2002, *Arch. Civ.*, 2003, 304; Cass., 4 febbraio 2002, n. 1430, in *Mass. Giur. It.*, 2002; Cass. 21 febbraio 2001, n. 2476, in *Mass. Giur. It.*, 2001, *contra* Cass., 26 novembre 2004, n. 22285, in *Mass. Giur. It.*, 2004, *CED Cassazione*, 2004, *Impresa*, 2005, 2, 313.

(26) Cass., 27 giugno 2003, n. 10251, in *Mass. Giur. It.*, 2003, *Gius.*, 2003, 24, 2813, in *Arch. Civ.*, 2004, 549; Cass., 7 aprile 2000, n. 4384, in *Mass. Giur. It.*, 2000.

(27) M. Acone, *La procura speciale alle liti tra tiepidezza del legislatore e i contrasti nella corte*, cit., 1170. Già L. Mortara, *Commentario del codice e delle leggi di procedura civile*, II, Milano, 1923, 755 nota 1., aveva ben spiegato il collegamento tra diritto alla difesa tecnica e diritto costituzionale di difesa nelle "facilitazioni accordate alla costituzione della difesa che è, nel suo esercizio, un diritto imprescindibile di ciascun litigante".

(28) F. Cipriani, *Procura su foglio separato o procura presunta?*, cit., 3155.

(29) In Francia in base al vecchio codice esisteva in capo alla parte, non certo alla controparte, la possibilità di disconoscere l'operato del difensore, il *désaveu* (art. 352 ss. *ancien c.p.c.*). Oggi, pur essendo stato abolito il *désaveu*, il difensore non ha comunque il dovere di esibire il mandato (art. 416, comma 2, *nouveau c.p.c.*). La regola del mandato presunto opera anche in altri paesi europei, come Austria e Germania, nei processi davanti alla Corte di giustizia dell'Unione Europea, così pure negli Stati Uniti d'America.

gli interrogativi che sottende quanto alle modalità del suo rilascio e all'esercizio del potere di certificazione del difensore.

È interessante notare come nel provvedimento che si annota venga affermato che la regola di cui all'art. 10 cit., nell'ammettere il rilascio della procura alle liti anche in formato cartaceo, purché il difensore dichiari la conformità della copia informatica della procura apponendo la propria firma digitale, "non è assolutamente derogatoria alla disciplina del codice di procedura civile sulla procura alle liti conferita su foglio separato" di cui al comma 3 dell'art. 83 c.p.c. sulla procura alle liti.

Il giudice ambrosiano ritiene che l'inserimento della copia informatica della procura, rilasciata in originale su supporto cartaceo, insieme all'atto nella busta telematica firmata dal difensore con firma digitale, attui quella congiunzione materiale a cui fa riferimento l'art. 83, comma 3, c.p.c., nel senso che nell'ambito del sistema telematico, il disposto dell'art. 10 d.p.r. n. 123/2001 debba essere così interpretato per quanto riguarda la copia informatica della procura asseverata con firma digitale conforme all'originale cartaceo.

Ecco dunque che le perplessità sul potere di certificazione dell'avvocato nell'autenticare la firma del cliente sulla procura rilasciata su foglio separato trovano in quest'ambito un'adeguata soluzione, anche se, come già precisato, non si poteva dubitare che la legge n. 141/1997 avesse consentito l'ampliamento del potere certificatorio del difensore, nonostante il diverso avviso della giurisprudenza che continua a limitarlo ai soli casi della procura a margine o in calce, come se il *topos* documentale possa costituire il limite del potere certificatorio del difensore (30).

Infatti, dal combinato disposto dell'art. 83, comma 3, e l'art. 10 d.p.r. n. 123/2001 emerge la soluzione a quanto da tempo si attendeva in tema di procura speciale rilasciata per scrittura privata sul ruolo fidefacente dell'avvocato, nel senso che la certificazione dell'autografia della sottoscrizione del conferente il mandato alla lite è effettuata "dall'unica firma con la quale il difensore, avvalendosi della procura, dà paternità all'atto processuale" (31).

Ciò significa che viene attribuita piena validità alla c.d. procura presunta ai fini della costituzione in giudizio, ossia che la sottoscrizione dell'atto e, nel caso di specie, l'apposizione della firma digitale sulla busta che contiene la copia informatica della procura assicura la riferibilità dell'attività difensiva a quel giudizio ed al tempo stesso renderebbe superflua la produzione del documento contenente la procura originale al momento della costituzione e persino in un momento successivo.

La firma digitale del difensore, apposta sulla busta telematica che contiene l'atto e la copia informatica della procura, varrebbe come dichiarazione sull'esistenza della procura. Va poi considerato che, alla luce della disciplina dettata dall'art. 10, viene meno la necessità di produrre in giudizio la prova documentale/procura, se

non nel caso in cui sorgano eventuali contestazioni, al fine di evitare un giudizio di querela di falso, qualora fosse posto in discussione il potere certificatorio del difensore.

In sintesi, la firma digitale dell'avvocato, garantisce la provenienza certa e l'integrità dei documenti in virtù delle regole tecniche che governano il flusso dei *bit* nelle funzioni matematiche della crittografia asimmetrica deputata alla generazione della firma digitale apposta alla busta con tutto il suo contenuto: atto processuale, copia informatica della procura e documenti offerti in produzione, mentre sul piano sostanziale la firma digitale è a tutti gli effetti una dichiarazione sia di paternità dell'atto e dell'avvenuto rilascio della procura da parte del suo titolare, ottemperando in questo modo alla disposizione di cui all'art. 10 del d.p.r. n. 123/2001. Alla luce della nuova disciplina il potere di certificazione del difensore mostra la propria giustificazione obiettiva quale esercizio di una funzione per dare pubblica fede sulla provenienza della procura e ciò "per fornire alla controparte la giuridica certezza della riferibilità dell'attività svolta dal difensore al titolare della posizione sostanziale controversa" (32).

È proprio grazie alla tecnica che ha portato alla "dematerializzazione" delle cose in generale e dei documenti in particolare che si può comprendere in pieno il senso della "materiale congiunzione" a cui si è riferito il legislatore del 1997. Infatti, in base all'orientamento dottrinale e giurisprudenziale a cui attribuire maggiore credito, non vi è dubbio che la materialità debba essere intesa come la pertinenza della procura all'atto, e non è certo la presenza di strumenti da fabbro o da mesticheria come ferri, spilli o colla che possono incidere sulla validità di un atto processuale (33), bensì la dichiarazione espressa attraverso l'apposizione della firma digitale del difensore alla busta contenente la copia informatica della

Note:

(30) Su questo aspetto, anche riguardo al profilo storico si veda M. Acone, *La procura speciale alle liti tra tiepidezza del legislatore e i contrasti nella corte*, in *Corr. giur.*, 1997, n. 10, 1164.

(31) Cass., S.U. 28 novembre 2005, n. 25032, in *Foro it.*, 2006, 4, 1, 1065 con nota di G. Deluca, *Procura speciale: continua l'infinita "historia"*, i giudici di legittimità in questo provvedimento inoltre precisano che non si rendono necessarie specifiche diciture e, soprattutto in relazione alla funzione dell'autentica, la non necessità della vicinanza cartolare delle sottoscrizioni. Per cui la sottoscrizione dell'atto da parte del difensore rappresenterebbe una certificazione implicita dell'autenticità della sottoscrizione della procura.

(32) Così ipotizzavano le Sezioni Unite della Cassazione con la citata sentenza n. 9869/1994 sulla funzione della certificazione di conferire pubblica fede alle sottoscrizioni a suo favore.

(33) Chiaramente nello scritto *Procura su foglio separato o procura presunta?* Cipriani afferma che: "[...] essendosi il legislatore ben guardato dal dire che la procura su foglio separato è valida solo se il foglio è spillato all'atto, e non potendosi ragionevolmente pensare che gli spilli abbiano la taumaturgica virtù di far diventare validi gli atti nulli, le procure speciali su foglio autonomo, ossia le procure per mera e classica scrittura privata, anche se non spillate all'atto, sono perfettamente valide: del resto davanti al giudice di pace, il mandato può ben essere rilasciato anche "in atto separato".

procura sarà idonea a soddisfare la riferibilità della procura al giudizio.

Del resto, come più volte precisato, con la norma contenuta nel comma 3 dell'art. 83 c.p.c. il legislatore ha espressamente disposto la parificazione della procura su foglio separato a quella in calce, regolando la validità della procura su foglio autonomo attraverso un ampliamento dei poteri certificatori del difensore e realizzando il requisito della "materiale congiunzione" su basi non solo materialmente fisiche.

Si può facilmente comprendere perché la motivazione del giudice milanese faccia ancora leva sul requisito "congiunzione materiale" costruendo un'analogia tra il metodo della "spillatura" e quello della procedura informatica dell'imbustamento degli atti e dei documenti offerti in deposito col ricorso e della successiva apposizione della firma digitale dell'avvocato sulla busta. Un'analogia, ad avviso di chi scrive, invocata in modo superfluo: meglio sarebbe stato, anche per dare rilievo alla forza innovativa della nuova disciplina del processo telematico, far leva sull'originalità e la specialità della disciplina dettata dall'art. 10 che non è affatto una mera utilizzazione di tecniche o di accorgimenti elaborati nel rito ordinario adattata alle esigenze tecniche del nuovo rito digitale. Invero, la firma digitale dell'avvocato, sia sull'atto, sia sulla busta che contiene anche la copia informatica della procura, funge da dichiarazione, più che sulla conformità, sull'esistenza di un valido potere di rappresentanza. Perché, come sostenuto in nota al paragrafo introduttivo, il comma 3 dell'art. 83 c.p.c. trova piena applicazione nell'ipotesi della procura originale rilasciata in formato digitale con firma digitale del soggetto che la conferisce, ed allegata ed imbustata insieme all'atto cui accede.

Nel futuro processo telematico, questa disposizione, specie in riferimento alla procura perderà ogni significato, proprio perché il meccanismo del PCT consentirà il riconoscimento iniziale dell'avvocato in riferimento ad una determinata causa, per la quale gli sia stato conferito mandato, e ciò al fine di consentirgli l'accesso al fascicolo d'ufficio tramite il sistema telematico senza necessità di dimostrare il possesso della procura. L'accesso ai documenti conservati nel *repository* dell'ufficio giudiziario potrà avvenire semplicemente con l'accesso alla rete interna della giustizia mediante il sistema di riconoscimento e autenticazione basato sulla firma digitale dell'avvocato a livello del Punto di accesso telematico, il c.d. Pda, senza dunque la necessità di dimostrare o esibire la procura.

Pertanto, in futuro non dovrebbero più leggersi sentenze anche della giurisprudenza di legittimità che per il conferimento della procura con atti diversi da quelli indicati all'art. 83, comma 3, c.p.c., affermano essere necessaria l'autenticazione notarile (34) o addirittura la nullità d'una procura apposta su un atto diverso da quelli elencati dall'art. 83 c.p.c. (35), in ciò per vero contrastata da buona parte della dottrina (36).

4. Conclusioni

La tecnologia informatica e gli strumenti telematici devono porsi come strumento utile al funzionamento della giustizia (37), non solo come meccanismi per rendere più veloci e sicure le attività processuali, ma soprattutto anche per evitare quei "bizantinismi" (38) ancora presenti nelle logiche legate ad un sistema processuale reso spurio da interpretazioni complesse e soffocate da applicazioni pratiche inefficaci.

Già subito dopo la legge del '97 e le prime pronunce del giudice di legittimità in tale materia, la dottrina (39) aveva avanzato con forza la proposta di sostituire l'attuale sistema del mandato "scritto e certificato nella firma dal difensore" col mandato "presunto" od anche semplicemente "orale" (40).

In sostanza, si attuerebbe un adeguamento della nostra disciplina a quella di altri Paesi, nonché al processo che si svolge innanzi alla Corte di giustizia della Comunità Europea per cui ai sensi dell'art. 38, n. 4, reg. proc. il difensore può semplicemente dimostrare con idoneo certificato di essere iscritto negli albi professionali di uno degli Stati membri e solo in caso di contestazione è tenuto a dare giustificazione dei suoi poteri (41).

Non vi è dubbio che l'art. 10 d.p.r. n. 123/2001 abbia attuato tale adeguamento. La tecnica informatica e l'ampliamento del potere certificatorio dell'avvocato ora consentono di esercitare l'ufficio procuratorio in forza della presunzione di conferimento della procura alle liti, senza che si renda necessaria l'esibizione immediata della procura ai fini della valida costituzione in giudizio, come auspicava una ormai lontana ma autorevole dottrina (42).

Note:

(34) Cass. 26 novembre 2004, n. 22285, cit.

(35) Cass. 1 aprile 1999, n. 3121, in *Mas. Giur. it.*, 1999.

(36) C. Mandrioli, *Diritto processuale civile*, I, Torino, 2007, 335; V. Andrioli, *Lezioni di diritto processuale civile*, 1973, 400; S. Satta, *Commentario al codice di procedura civile*, I, Milano, 1966, 282.

(37) R. Borruso, *Informatica, Internet e diritto*, in questa *Rivista*, 1, 2005, 7 ss., ha espresso la sua perplessità sull'atteggiamento ondivago del legislatore, talvolta propositivo, tal'altra frenante, di fronte ai fenomeni tecnologici, specie proprio in riferimento al processo telematico.

(38) F. Cipriani, *ult. op. cit.*, 3153.

(39) M. Acone, *ult. op. cit.*, 1171.

(40) Peralto il disegno di legge delega redatto dalla commissione ministeriale presieduta dal prof. G. Tarzia al punto n. 10, lett. d), prevedeva l'introduzione della "presunzione di esistenza della procura, in mancanza di contestazione o di esplicita richiesta di esibizione".

(41) In argomento si veda F. Cipriani - G. Costantino - A. Proto Pisani - G. Verde, *op. cit.*, 3445.

(42) L. Mortara, *Commentario del codice e delle leggi di procedura civile*, II, Milano, 1923, 755.

Procedimento civile

La comunicazione di cancelleria a mezzo e-mail

Cassazione civile, sez. Lavoro, 19 febbraio 2008, n. 4061 - Pres Sciarelli - Est. De Matteis - Rel. De Matteis - P.M. Fuzio R. (Conf.); Introvigne c. Inail - (Rigetta, App. Bolzano, 28 Aprile 2005)

Procedimento civile - Comunicazioni - In genere - Comunicazione di cancelleria - Comunicazione mediante posta elettronica all'indirizzo e-mail indicato dall'avvocato - Validità - Fondamento - Condizioni

(c.c. art. 1335; c.p.c. art. 136)

La comunicazione di cancelleria "ex" art. 136 c.p.c. ammette equipollenti basati su elementi volontaristici e sul conseguimento dello scopo: ne consegue, nel caso in cui un avvocato abbia aderito ad una convenzione tra l'ordine degli avvocati ed un ufficio giudiziario che preveda le comunicazioni via posta elettronica all'indirizzo e-mail indicato da ciascun legale, la validità della comunicazione di cancelleria effettuata al detto indirizzo a mezzo posta elettronica, ancorché priva di firma digitale, ove sia pervenuta alla cancelleria una risposta per ricevuta, data non in automatico.

...*Omissis*...

Svolgimento del processo

La questione di diritto oggetto del presente giudizio è se le comunicazioni di cancelleria ex 136 c.p.c., possano essere validamente effettuate attraverso e-mail con risposta di conferma, documentate dalla relativa stampa cartacea.

La causa è iniziata con ricorso del Sig. I.B. del 13 novembre 2002 avanti al giudice del lavoro per ottenere la condanna dell'Inail alla corresponsione di rendita per inabilità per infortunio sul lavoro subito il 29 giugno 2000. Dopo la costituzione dell'Inail, essendo stata l'udienza di assunzione delle prove orali rinviata per impedimento del giudice, il cancelliere ha comunicato la data della nuova udienza "per gli stessi incombenti" a mezzo di due e-mail, destinate all'indirizzo di posta elettronica dei difensori delle parti, con conferma della ricezione, secondo la procedura convenuta tra la Corte d'Appello di Trento ed il locale Consiglio dell'Ordine degli avvocati, all'indirizzo e-mail comunicato dallo stesso avvocato al Consiglio dell'Ordine e da questo alla Corte d'Appello. Non avendo la parte ricorrente intimato i propri testi, la causa veniva istruita con il solo teste di parte resistente e decisa con il rigetto della domanda.

L'appello dell'I. è stato respinto dalla Corte d'Appello di Trento, sezione distaccata di Bolzano, con sentenza 27/28 aprile 2005 n. 18, che ha altresì condannato l'appellante soccombente alle spese del grado.

Il giudice di appello ha preliminarmente individuato il fatto, qualificandolo pacifico: la comunicazione di cancelleria risulta pervenuta allo studio professionale del difensore di parte ricorrente in modalità elettronica e, con

la stessa modalità, è stata data risposta di ricezione, di che risulta conservata in atti la documentazione cartacea.

A tale fatto ha applicato i seguenti criteri decisori:

1. il principio di libertà delle forme con le quali la comunicazione disciplinata dall'art. 136 c.p.c., può essere effettuata;
2. il raggiungimento dello scopo della comunicazione, dimostrato sia dal messaggio di conferma, dato non in automatico, ma con il comando volontario "rispondi", sia dalla presenza del difensore all'udienza di assunzione delle prove;
3. la disciplina legislativa specifica sulle comunicazioni di cancelleria con il mezzo elettronico.

Analizzate le singole fonti normative (l. n. 59/1997, art. 15, comma 2, del d.lgs. n. 39/1993, art. 6, d.p.r. 13 febbraio 2001, n. 123, artt. 2 e 6), il giudice di appello ha distinto tra requisiti del documento informatico per i quali è richiesta la sottoscrizione con firma digitale, e comunicazione con biglietto di cancelleria, che non è un documento informatico ma una semplice modalità di trasmissione telematica, per la quale va seguita la disciplina appositamente prevista dal cit. d.p.r. n. 123/2001, art. 6, con distinzione già recepita dal d.p.r. n. 513/1997, art. 12. Ha infine rilevato che nella fattispecie in esame vi è addirittura un passaggio in più che garantisce la realizzazione dello scopo legale della procedura, e cioè una risposta non in automatico ma intenzionalmente generata dal computer destinatario a mezzo del tasto "rispondi" del programma di ricezione e scarico della corrispondenza elettronica.

Avverso tale sentenza ha proposto ricorso per Cassazione l'I., con unico articolato motivo, illustrato da memoria ex art. 378 c.p.c., e note d'udienza.

L'Istituto intimato si è costituito con controricorso, resistendo.

Motivi della decisione

Con il primo motivo il ricorrente, deducendo violazione e falsa applicazione del d.p.r. 13 febbraio 2001, n. 123, artt. 6 e 8; d.p.r. 28 dicembre 2000, n. 445, art. 25; d.p.r. 7 aprile 2003, n. 137;

D.lgs. 23 febbraio 2002, n. 10, ripropone l'argomento, già esaminato e respinto dalla sentenza impugnata, secondo cui anche la comunicazione di cancelleria ai sensi dell'art. 136 c.p.c., richiede la firma digitale.

Il motivo non è fondato.

La sentenza impugnata risulta corretta nel suo doppio percorso argomentativo, quello che trova fondamento nella disciplina codicistica, e quello basato sull'esegesi della legislazione speciale.

1. L'art. 136 c.p.c., nel testo vigente al tempo dei fatti di causa, disponeva: "1. Il cancelliere, con biglietto di cancelleria in carta non bollata, fa le comunicazioni che sono prescritte dalla legge o dal giudice al pubblico ministero, alle parti...; 2. Il biglietto è consegnato dal cancelliere al destinatario, che ne rilascia ricevuta, o notificato dall'ufficiale giudiziario". L'art. 45 disp. att. c.p.c., precisa poi che il biglietto si compone di due parti uguali, una delle quali deve essere consegnata al destinatario e l'altra deve essere conservata nel fascicolo d'ufficio. In questa parte che viene inserita nel fascicolo d'ufficio deve essere estesa la relazione di notificazione dell'ufficiale giudiziario o scritta nella ricevuta del destinatario.

Questa Corte ha già esaminato la questione di diritto se la comunicazione del provvedimento ad opera della cancelleria debba avere luogo nelle forme specificate dall'art. 136 c.p.c. e art. 45 disp. att. c.p.c., o possa viceversa avere rilievo anche la conoscenza del provvedimento acquisita per altra via. Ha statuito, con orientamento antico e costante, fatto proprio dalle Sezioni Unite, che si possono ammettere forme equipollenti a quelle stabilite dall'ordinamento (volte a garantire in via generale la conoscenza di un atto al fine dell'osservanza dei termini di decadenza relativi), ogni qual volta ci sia un'attività del cancelliere, sia assicurata la completa conoscenza della comunicazione da parte del destinatario, nonché la certezza della data (Cass. sez. un., 10 giugno 1998, n. 5761, in motivazione; per l'enunciazione dello stesso principio in *apicibus* Cass. 21 novembre 2006 n. 24742; Cass. 15 febbraio 2006 n. 3286). La declinazione in concreto di tali elementi essenziali risente della diversità delle fattispecie. La giurisprudenza di questa Corte ha ritenuto validi equipollenti: il "visto per presa visione" apposto dal procuratore o da suo incaricato sull'originale del biglietto di cancelleria predisposto per la comunicazione o sul provvedimento del giudice (Cass. 16 giugno 2004 n. 11319; Cass. 29 aprile 2002 n. 6221; Cass. 29 ottobre 1998 n. 10791; Cass. 12 settembre 1992 n. 10422); l'inserimento, ad opera del cancelliere, nel verbale d'udienza, del decreto di liquidazione del compenso al con-

sulente tecnico, e la verbalizzazione dell'impegno della parte a corrispondere la somma liquidata (Cass. 26 giugno 2006 n. 14737); la dichiarazione resa nella cancelleria di aver preso visione dell'atto e di rinunciare alla relativa comunicazione (Cass. 20 ottobre 2005 n. 20279). In tutte le fattispecie esaminate rileva un elemento volontaristico, e cioè l'accettazione da parte del procuratore nella forma equipollente, accettazione che tiene luogo nella sottoscrizione prevista dall'art. 45 disp. att. c.p.c. In altre fattispecie viene posto in rilievo il raggiungimento dello scopo della comunicazione, come in quella esaminata da Cass. 12 febbraio 2000 n. 2068, che ha ritenuto valido equipollente il rilascio al creditore, su sua richiesta, di copia autentica del decreto con il quale il giudice delegato aveva fissato l'udienza per la comparizione delle parti e stabilito il termine per la notifica del provvedimento al curatore, in quanto tutto ciò comporta la effettiva presa di conoscenza, da parte del creditore stesso, del decreto "de quo", ancorché non comunicato dal cancelliere a norma dell'art. 136 c.p.c., qualora risulti che l'atto abbia raggiunto il suo scopo per avere il creditore immediatamente utilizzato il detto decreto chiedendone la notificazione al curatore del fallimento.

Posto il principio volontaristico che precede, la comunicazione da parte dell'avvocato del proprio indirizzo e-mail all'Ordine, per la successiva comunicazione alla Corte d'Appello, secondo la procedura prevista dall'accordo tra la Corte d'Appello di Trento ed il Consiglio dell'Ordine di appartenenza, costituisce: a) adesione del professionista alla convenzione, b) consenso affinché la comunicazione di cancelleria gli sia effettuata con tale modalità; c) garanzia che all'indirizzo dato il messaggio di cancelleria sarà letto dall'avvocato stesso o da altra persona addetta allo studio (sulla nozione di destinatario ai fini dell'art. 136 c.p.c., e sulla sufficienza che la comunicazione pervenga a collaboratore del destinatario addetto allo studio: Cass. 25 settembre 2000 n. 12666, Cass. 14 aprile 1996 n. 332).

La risposta, non in automatico, di aver ricevuto la comunicazione garantisce la certezza richiesta dall'art. 136 c.p.c..

La procedura di comunicazione seguita risulta pertanto corretta sulla semplice base codicistica, e, con ogni evidenza, volta a realizzare l'obiettivo di cui all'art. 111 Cost., comma 2, inserito dalla Legge Costituzionale 23 novembre 1992 n. 2. 2. La procedura prevista da tale convenzione risulta corretta anche alla luce della legislazione speciale sul tema.

Come correttamente ricordato dalla sentenza impugnata, già la l. 15 marzo 1997, n. 59, art. 15, comma 2 (Delega al governo per la riforma della pubblica amministrazione), disponeva 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 trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge", rimandando poi per la determi-

nazione de "i criteri e le modalità di applicazione del presente comma" a specifici regolamenti; e il d.lgs. 12 febbraio 1993, n. 39, art. 6, menziona l'amministrazione della giustizia tra i soggetti pubblici destinati ad utilizzare i sistemi informativi automatizzati, sia pure con la riserva di particolari modalità di applicazione.

Il 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 è stato emanato con d.p.r. 13 febbraio 2001, n. 123, ed è il testo fondamentale che interessa la questione oggetto della presente causa.

Tre sono le norme principali che sorreggono la tesi della sentenza impugnata sulla distinzione tra documenti informatici a firma digitale e comunicazioni telematiche di cancelleria: l'art. 2:

"l'attività di trasmissione, comunicazione o notificazione, dei documenti informatici è effettuata per via telematica attraverso il sistema informatico civile, fatto salvo quanto stabilito dall'art. 6;

l'art. 4, comma 3: "Ove dal presente regolamento non è espressamente prevista la sottoscrizione del documento informatico con la firma digitale, questa è sostituita dall'indicazione del nominativo del soggetto procedente prodotta sul documento dal sistema automatizzato, a norma del d.lgs. 12 febbraio 1993, n. 39, art. 3, comma 2; l'art. 6: "Le comunicazioni con biglietto di cancelleria, nonché la notificazione degli atti, quest'ultima come documento informatico sottoscritto con firma digitale, possono essere eseguite per via telematica, oltre che attraverso il sistema informatico civile, anche all'indirizzo elettronico dichiarato ai sensi dell'art. 7".

È evidente la contrapposizione, contenuta nell'art. 6, tra notificazione degli atti effettuata con firma digitale attraverso il sistema informatico civile, e comunicazioni con biglietto di cancelleria eseguita all'indirizzo elettronico dichiarato ai sensi dell'art. 7, secondo il quale ai fini delle comunicazioni e delle notificazioni ai sensi dell'art. 6, l'indirizzo elettronico del difensore è unicamente quello comunicato dal medesimo al Consiglio dell'Ordine.

Altre norme del d.p.r. 13 febbraio 2001, n. 123, concorrono alla medesima conclusione: l'art. 3, commi 2 e 3, per i quali al sistema informatico civile possono accedere attivamente soltanto i difensori delle parti e gli ufficiali giudiziari, e non altri soggetti; le varie norme che, in attuazione dell'art. 4, comma 3 cit., precisano quali atti devono essere formati come documenti informatici sottoscritti con firma digitale (art. 6 per le notificazioni, art. 10 per la procura alle liti, art. 11 per l'iscrizione al ruolo, art. 15 per il deposito della relazione del C.T.U., art. 17 per la trasmissione della sentenza).

Infine la l. 28 dicembre 2005, n. 263, art. 2, comma 1, n. 1, lett. b, modificando leggermente la formula dall'art. 136 c.p.c., comma 2 ("Il biglietto è consegnato dal cancelliere al destinatario, che ne rilascia ricevuta, o è ri-

messo all'ufficiale giudiziario per la notifica"), evidenzia la distinzione di ruoli e di modalità di comunicazione tra il cancelliere e l'ufficiale giudiziario. Ed il terzo comma dell'art. 136, introdotto dalla Legge citata ("Le comunicazioni possono essere eseguite a mezzo telefax o a mezzo posta elettronica nel rispetto della normativa anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici teletrasmessi"), nel ribadire la distinzione tra documenti informatici e teletrasmessi, rinvia alla normativa regolamentare sopra citata.

Il carattere sostitutivo della procedura telematica rispetto a quella cartacea prevista dall'art. 136 c.p.c. e art. 145 disp. att. c.p.c.; la possibilità, ridotta ma effettiva, di malfunzionamento del sistema di trasmissione; la gravità delle conseguenze decadenziali, impongono di ritenere che sia necessaria la risposta manuale di ricevuta con il tasto "rispondi", e non sufficiente la risposta in automatico "letto" (per identica soluzione, limitatamente alla risposta "ok" del servizio di trasmissione via fax vedi Cass. 25 marzo 2003 n. 4319 e 3286/2006 cit.). Né argomenti in contrario sembra possano trarsi dallo *jus superveniens* costituito dal nuovo testo dell'art. 136 c.p.c., comma 3, perché questo rinvia alla normativa regolamentare sopra citata, la quale non disciplina il punto specifico in esame. Né alla materia processuale, specificamente disciplinata dal d.p.r. 13 febbraio 2001, n. 123, è applicabile il d.p.r. 10 novembre 1997, n. 513, art. 12 (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma della l. 15 marzo 1997, n. 59, art. 15, comma 2), per il quale il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

Poiché nel caso di specie il destinatario della comunicazione ha dato la risposta per ricevuta non in automatico, la comunicazione risulta validamente effettuata.

Si deve conclusivamente enunciare il seguente principio di diritto, in relazione alla fattispecie di causa: "È valida la comunicazione di cancelleria ex art. 136 c.p.c., effettuata per e-mail all'indirizzo elettronico comunicato dal difensore al proprio Consiglio dell'Ordine e da questi alla Corte d'Appello competente, a norma del d.p.r. 13 febbraio 2001, n. 123, artt. 2, 4, 6, del quale il destinatario ha dato risposta per ricevuta non in automatico, documentata dalla relativa stampa cartacea".

Con il secondo motivo il ricorrente deduce violazione e falsa applicazione degli artt. 253, 257 e 421 c.p.c.; omessa, insufficiente, contraddittoria motivazione. Censura la sentenza impugnata per non aver ammesso le domande all'unico teste e non avere delibato le richieste della difesa del ricorrente; e per non aver ammesso la consulenza medica sugli esiti dell'infortunio.

Il motivo è assorbito dal rigetto del primo motivo; peraltro esso è inammissibile, per difetto di autosufficienza, perché non specifica le circostanze su cui il teste avrebbe

dovuto testimoniare, al fine di consentire a questa Corte di apprezzarne la rilevanza.

Con il terzo motivo il ricorrente si duole della condanna alle spese del grado di appello, deducendo errata applicazione del d.l. 30 settembre 2003, n. 269, art. 42, comma 11; rileva che la corte territoriale non ha tenuto conto dei seguenti documenti, ritualmente prodotti: 1. della dichiarazione reddituale prodotta in primo grado; 2. dell'ulteriore dichiarazione reddituale prodotta ed allegata alle note difensive conclusionale del 7 aprile 2005

(documento 5), entrambe attestanti che il ricorrente poteva beneficiare della non soccombenza per le spese processuali. Anche questo motivo è inammissibile, perché non specifica il reddito dichiarato, che avrebbe consentito l'esenzione dalle spese processuali ai sensi del d.l. 30 settembre 2003, n. 269, art. 42, comma 11, convertito in l. 24 novembre 2003, n. 326.

Le spese processuali del presente giudizio vengono compensate.

... *Omissis*...

IL COMMENTO

di Francesco Buffa

Una questione previdenziale ha offerto alla Suprema Corte l'occasione di affrontare la questione relativa alla possibilità giuridica ed alla validità delle comunicazioni di cancelleria fatte mediante e-mail, con risposta di conferma documentata dalla relativa stampa cartacea.

1. La decisione della Suprema Corte

Nella sentenza in analisi, la Corte ha ritenuto valida la comunicazione di cancelleria ex art. 136 c.p.c. effettuata per *e-mail* all'indirizzo elettronico comunicato dal difensore al proprio consiglio dell'ordine e da questo alla corte d'appello competente, pur limitando l'affermazione del principio con riferimento al caso in cui il destinatario abbia dato risposta per ricevuta non in automatico, documentata dalla relativa stampa cartacea.

Più specificamente, la Corte è pervenuta a questa affermazione attraverso tre passaggi.

In primo luogo, la comunicazione di cancelleria ex art. 136 c.p.c. ammette equipollenti basati su elementi volontaristici (quali, come nella specie, la adesione alla convenzione tra ordine degli avvocati e ufficio giudiziario circa la comunicazione via posta elettronica all'indirizzo *e-mail* indicato dall'avvocato) o sul conseguimento dello scopo (nel caso realizzato dalla risposta data dal sistema informatico), e tra questi vi è anche la comunicazione a mezzo posta elettronica ai sensi del comma 3 della norma (introdotto dall'art. 2 della legge 263 del 2005).

In secondo luogo, la legislazione speciale sulla firma digitale (d.p.r. 123 del 2001) non impone la firma digitale per le comunicazioni di cancelleria, a differenza che per le notificazioni.

Infine, la presunzione di arrivo al destinatario della comunicazione telematicamente trasmessa (stabilita dall'art. 15 comma 2 d.p.r. n. 413/1997, poi confluito nel testo unico sulla documentazione amministrativa n.

445/00) non è applicabile alla materia processuale, ma nella specie ciò è irrilevante in quanto la comunicazione ha avuto una risposta per ricevuta data non in automatico.

Su ciascuno degli evidenziati punti possono essere formulate alcune considerazioni.

2. La convenzione per l'uso dell'*e-mail* nelle comunicazioni

Sul primo aspetto, l'intero sistema dell'uso delle tecnologie informatiche nel processo poggia su elementi volontaristici, che presuppongono l'adesione dei legali ad un sistema chiuso di telecomunicazioni.

Anche nel sistema del processo telematico, disciplinato dal d.p.r. n. 123/2001 e dal d.m. 14 ottobre 2004, infatti, la disciplina fa riferimento ad un sistema telematico chiuso.

Da un lato, le norme consentono la trasmissione, comunicazione o notificazione dei documenti informatici sottoscritti con firma digitale per via telematica, ma solo attraverso un sistema non accessibile da altri elaboratori non autorizzati: si tratta del "sistema informatico civile" (SICI), definito come il sottoinsieme delle risorse del dominio giustizia mediante il quale l'amministrazione della giustizia tratta il processo civile. Il sistema, come si è detto, non corre su internet né su altra rete pubblica aperta, ma è un sistema chiuso, ossia non aperto al pubblico; al sistema informatico civile, inoltre, a norma del comma 2 dell'art. 3 del citato regolamento 123/01, possono accedere soltanto i difensori delle parti e gli ufficiali giudiziari per le attività rispettivamente consentite dal regolamento. (1)

Nota:

(1) Sul processo civile telematico, in genere, la letteratura è abbastanza vasta: R. Borruso, *La legge, il giudice, il computer; un tema fondamentale dell'informatica giuridica*, in Aa.Vv. (a cura di D.A. Limone), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Milano, 1995, 1; S. Brescia - P. Liccardo, *Processo telematico*, in *Enc. giur. it.*, Roma, 2006; (segue)

In tale contesto, nella nomenclatura delle regole tecniche, l'avvocato è generalmente un "soggetto abilitato esterno privato", ossia un professionista - esterno all'amministrazione e rappresentante interessi di parti private - il quale è abilitato all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo previo accesso alle condizioni previste: il sistema, cioè, è accessibile solo dagli utenti autorizzati dal tribunale, come definiti in una *security policy* locale posta a fondamento dei *firewalls* di protezione del sistema. Dall'altro lato, a norma dell'art. 14 delle regole tecniche, come per gli altri soggetti abilitati esterni al SICI, l'accesso al SICI e la casella di posta elettronica si ottengono previa registrazione presso un punto di accesso, e dunque previa richiesta scritta (conservata dal punto d'accesso per almeno dieci anni); all'atto della registrazione, il punto di accesso acquisisce i dati prescritti e verifica l'identità del richiedente ed il relativo codice fiscale.

In terzo luogo, quanto al meccanismo di comunicazione telematica, i soggetti abilitati esterni, per utilizzare i servizi di trasmissione telematica dei documenti informatici, devono munirsi di un indirizzo elettronico e della relativa casella di posta elettronica forniti e gestiti dal punto di accesso, inoltrando apposita richiesta a questo all'atto della registrazione. Viene stabilito un principio di esclusività soggettivo ed oggettivo, secondo il quale da un lato ad ogni soggetto che interagisce per via telematica con il SICI corrisponde un solo indirizzo elettronico e, dall'altro lato, ogni indirizzo elettronico corrisponde ad una Casella di posta elettronica certificata per il processo telematico (CPECPT); infine, ogni CPECPT è abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale (art. 11). La CPECPT non è dunque una qualunque *mailbox*, ma quella avente i requisiti sopra detti, specificamente utilizzata per il processo telematico. Queste fin qui richiamate sono le regole previste in generale dall'ordinamento per il processo telematico.

Nel descritto contesto normativo, va ricordato peraltro che l'art. 2 l. 28 dicembre 2005, n. 263 (recante interventi correttivi alle modifiche in materia processuale civile nonché ulteriori modifiche al codice di procedura civile e alle relative disposizioni di attuazione) prevede che all'art. 170, comma 4, c.p.c. l'ultimo periodo è sostituito dai seguenti: «Il giudice può autorizzare per singoli atti, in qualunque stato e grado del giudizio, che lo scambio o la comunicazione di cui al presente comma possano avvenire anche a mezzo telefax o posta elettronica nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e teletrasmessi. La parte che vi procede in relazione ad un atto di impugnazione deve darne comunicazione alla cancelleria del giudice che ha emesso la sentenza impugnata. A tal fine il difensore indica nel primo scritto difensivo utile il numero di telefax o l'indirizzo di posta

elettronica presso cui dichiara di voler ricevere le comunicazioni».

La norma ha generalizzato la possibilità di uso della

Nota:

(segue nota 1)

S. Brescia, *La new economy del processo civile: sfida telematica per il ministero*, in *Diritto e giustizia*, 2000, 14, 37; M. Jacchia, *Funzione difensiva e burocrazia processuale, relazione al convegno. Il regolamento per la tenuta dei registri degli uffici giudiziari*, organizzato da Eurist, Roma, 9 giugno 2000, in atti del convegno; G. Briganti, *Il c.d. processo telematico: il decreto del ministro della Giustizia 13 febbraio 2001*, n. 123, in *www.diritto.it*; F. Buffa, *Al via il processo civile telematico: le nuove opportunità per gli avvocati*, in questa *Rivista*, 2005, 1, 9; F. Buffa, *Il processo civile telematico: la giustizia informatizzata*, Milano, 2002; F. Buffa, *L'apporto delle nuove tecnologie e dell'informatica nella gestione degli uffici dell'amministrazione della giustizia, relazione all'incontro di studi per magistrati sull'ordinamento giudiziario organizzato dal Consiglio Superiore della Magistratura in Frascati* (Roma), 28-30 giugno 2000, edita in *www.dirittoitalia.it*; G. Buonuono, *Processo telematico e firma digitale*, Milano, 2004; S. Caporusso, *Riforma del processo civile*, in *Nuove leggi civ. comm.*, 2006, 898; A. Contaldo - M. Gorga, *Le regole del processo civile telematico anche alla luce della più recente disciplina del SICI*, in questa *Rivista*, 1, 2008, 5; M. Delli Priscoli, *L'informatizzazione del processo civile nel distretto della Corte di Appello di Roma: sviluppi e prospettive*, in *Atti del V congresso internazionale Informatica ed attività giuridica*, 1993, 903; G. Di Benedetto, *L'informatica nel processo civile. Interpretazione e selezione dei dati*, Roma, 2001, 8; M. Fabri, *Tecnologie della giustizia*, Bologna, 2006; A. Graziani, *L'illusione processuale telematica*, in *Arch. Civ.*, 2006, 960; M. Iaselli, G.A. Cavaliere, *Il fascicolo informatico del processo telematico*, in *Inf. e dir.*, 2007, 1, 163; D. Intravaia, *Processo civile telematico: Disciplina normativa e infrastruttura tecnologica*, in M. Jori (a cura di), *Elementi di informatica giuridica*, Torino, 2006; G. Jacchia, *Il processo telematico*, (a cura di), Bologna, 2000; D.A. Limone, *Introduzione al Convegno Il processo telematico. Il regolamento per la tenuta dei registri degli uffici giudiziari*, organizzato da Eurist, Roma, 9 giugno 2000, in atti del convegno; M. Melica, *Le regole tecniche, relazione all'incontro nazionale degli sperimentatori del processo civile telematico*, Roma, 4 maggio 2004; C. Miele, *I provvedimenti del giudice e l'ausiliario informatico*, in *La riforma del processo civile, Quaderni del Consiglio Superiore della magistratura*, n. 75, 593; C. Miele, *Un sistema integrato per la gestione del lavoro del giudice e della cancelleria*, in *Atti del V congresso internazionale "Informatica ed attività giuridica"*, 1993, 1079; M. Morelli, *La seconda fase della digitalizzazione nella pubblica amministrazione tra utopia e realtà*, in *Nuova rass.*, 2005, 1123; P. Pacchioli - F. Pappalardo, *Il decreto ingiuntivo telematico con valore legale: l'esperienza del Tribunale di Milano*, in questa *Rivista*, 2007, 203; G. Riem - A. Sirotti Gaudenti, *La giustizia telematica e la procedura informatizzata*, Rimini, 2005; F. Rollerli, *I progetti per informatizzare l'amministrazione della giustizia*, in *Documenti Giustizia*, n. 11, 1995; F. Rollerli, *Informatica e amministrazione della Giustizia, lezione al Corso di perfezionamento in Diritto dell'Informatica*, diretto da D.A. Limone, organizzato dall'Università degli studi di Lecce, 3.6.00, in atti del corso, editi su cd-rom a cura della medesima Università, e in *www.studigiuridici.unile.it*; M. Delli Priscoli, *La gestione informatica del processo civile presso il Tribunale di Roma: risultati conseguiti*, in *Documenti Giustizia*, 1988, 5, 197; F. Sarzana di Sant'Ippolito, *Brevi considerazioni in margine al c.d. processo civile telematico*, in *Corr. Gur.*, 2001, 1242; A. Scarpulla, *La formazione informatica del personale giudiziario*, in *Aa.Vv.* (a cura di D.A. Limone), *Dalla giuritecnica all'informatica giuridica*. Studi dedicati a Vittorio Frosini, Milano, 1995, 301; Taddei Elmi G., *Il processo telematico*, (a cura di), Napoli, 2007; Torrice A., *Il decreto ingiuntivo telematico: innovazione tecnologica, normativa, sociale e organizzativa. L'esperienza del tribunale di Milano*, Roma, "Forum P.A. 2007", in http://www.forumpa.it/forum-pa2007/convegni/relazioni/1043_amelia_torrice.pdf; I. Tricomi, *Commento al d.p.r. n. 123/2001*, in *Guida al diritto*, 2001, 16, 105; A. Villecco, *Due facce di una stessa medaglia: il processo tradizionale ed il nuovo processo tecnologico*, in *Cyberspazio e diritto*, 2004; A. Villecco, voce *Processo telematico*, in *Dig. it, disc. priv., sez. civ.*, 2003; G. Xilo, *I sette laboratori a confronto: requisiti minimi per la sperimentazione e la carta dei servizi*, relazione all'incontro nazionale degli sperimentatori del processo civile telematico, Roma, 4 maggio 2004.

posta elettronica nelle comunicazioni rilevanti processualmente, senza fare specifico riferimento al SICI ed anzi prescindendo da questo.

Tornando al caso di specie, la comunicazione di cancelleria avveniva al di fuori del SICI e sulla base di un meccanismo fondato su una specifica convenzione fra ordine degli avvocati ed ufficio giudiziario.

Sul tema non si aggiunge altro, se non che, quale che sia il sistema normativo di riferimento, ricorre in ogni caso l'affidamento del sistema ad elementi volontaristici e ciò, secondo gli osservatori più acuti, è la vera causa del fallimento della riforma del processo telematico, posto che la non obbligatorietà dell'uso degli strumenti telematici di fatto pregiudica da anni l'attuazione della riforma del processo telematico e inibisce l'uso dei nuovi mezzi nelle concrete esperienze processuali, alimentando le resistenze e pigri mentali basate su tradizionali sistemi cartacei di scambio di dati.

3. Comunicazioni senza firma digitale

Venendo al secondo punto in rilievo della sentenza in epigrafe, la Suprema Corte introduce una distinzione tra notifiche e comunicazioni di cancelleria, ritenendo che solo per le notifiche sia prescritta la firma digitale.

Sul tema, il quadro normativo è il seguente.

Il regolamento sul processo telematico ha dettato una disciplina nuova delle (comunicazioni e) notificazioni, regolate in maniera diversa anche rispetto alla l. n. 183/1993 (che aveva disciplinato le notificazioni di atti e provvedimenti a mezzo fax (2)).

In particolare, l'art. 45 delle regole tecniche ha previsto che, ove non diversamente stabilito (cfr. art. 6, comma 1), l'attività di trasmissione per via telematica sia effettuata attraverso il sistema informatico civile. Nel sistema del regolamento, la notificazione telematica di documenti informatici tra difensori avviene, ove sussistono i presupposti di cui alla l. 21 gennaio 1994, n. 53, mediante inoltro del documento dal punto di accesso del mittente alla CPECPT del destinatario. A tale scopo il punto di accesso trasmette il messaggio con il documento da notificare al gestore centrale che, a sua volta, inoltra il messaggio ricevuto al punto di accesso di destinazione. Negli altri casi, le richieste dei difensori sono inoltrate all'UNEP per il tramite del punto di accesso del mittente e del gestore centrale, nel rispetto dei requisiti dei documenti informatici provenienti dall'esterno. La notificazione di documenti informatici da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione dall'ufficio giudiziario verso soggetti abilitati esterni, e dunque avviene mediante inoltro del documento dal gestore locale alla CPECPT del destinatario.

Il sistema informatico di gestione degli UNEP acquisisce i documenti informatici da notificare, procede alla loro notifica e li restituisce con la relata di notifica: eseguita la notifica, il sistema trasmette per via telematica, a chi ha richiesto il servizio, il documento informatico con la relata di notifica, costituita dalla ricevuta elet-

tronica, sottoscritta dall'ufficiale giudiziario con firma digitale. Nell'ipotesi di cui all'art. 6, comma 3, del regolamento n. 123/2001, l'ufficiale giudiziario provvede a notificare il duplicato del documento informatico, su supporto ottico non riscrivibile. La consegna del documento informatico alla CPECPT del soggetto abilitato esterno è assicurata dai punti di accesso mediante l'invio al mittente di una ricevuta di avvenuta consegna.

È contemplata peraltro dalla norma la possibilità che l'atto non possa essere notificato telematicamente al destinatario: ciò accade ad esempio ove il destinatario sia sprovvisto di mezzi informatici, o di indirizzo elettronico, ovvero quando la casella postale è già piena e rifiuti ulteriori messaggi, o rifiuti messaggi eccedenti la capacità di ricezione, ovvero ove l'indirizzo elettronico pur esistente non sia comunicato o dichiarato *ex art. 7* del regolamento. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, trae dall'atto ricevuto come documento informatico la copia su supporto cartaceo, ne attesta la conformità all'originale e provvede a notificare la copia stessa unitamente al duplicato del documento informatico, nei modi di cui agli artt. 138 e ss. del codice di procedura civile. Eseguita la notificazione, l'ufficiale giudiziario restituisce per via telematica l'atto notificato, munito della relazione della notificazione attestata dalla sua firma digitale.

L'ufficiale giudiziario, dunque, provvede alla notifica telematica all'indirizzo elettronico dichiarato dal destinatario al certificatore delle firme digitali ovvero al Consiglio dell'ordine degli avvocati (art. 6), e poi restituisce telematicamente l'atto notificato con relativa relata elettronica attestata dalla sua firma digitale.

Più in generale, il servizio di posta elettronica certificata restituisce al mittente una ricevuta di avvenuta consegna per ogni documento informatico reso disponibile al destinatario, cui è associata l'attestazione temporale di cui all'articolo 45.

In materia è poi intervenuto come noto l'art. 4 della l. n. 263/2005, che ha integrato l'articolo 3 della legge 21 gennaio 1994, n. 53, aggiungendo dopo il comma 3, un comma 3 *bis*, secondo il quale il notificante può anche servirsi delle procedure informatiche e, in tal caso, esegue la notificazione di atti in materia civile, amministrativa e stragiudiziale trasmettendoli per via telematica all'ufficio postale, sottoscritti con firma digitale, completi della relazione di notificazione e del numero di registro cronologico.

In entrambi i casi, di notificazioni e di comunicazioni, l'apposizione di firma digitale garantisce la provenienza dell'atto (dall'ufficio o dall'avvocato), e sembra necessaria oltre che utile allo scopo, scopo che ricorre in

Nota:

(2) Sulla prima applicazione delle tecnologie (telefax) alle notifiche, Turini L, *commento alla legge n. 183/93*, in *Nuove leggi civ. comm.*, 1994, 164; Loche M., *La teletrasmissione degli atti giudiziari*, in *Riv. Giur. Sarda*, 1993, 895.

modo analogo in entrambi i casi delle comunicazioni e notificazioni.

Peraltro, se nel caso delle notificazioni non sembrano configurabili equipollenti, nel caso delle comunicazioni di cancelleria può farsi riferimento alle norme che disciplinano l'uso dei sistemi informativi automatizzati da parte delle pubbliche amministrazioni, e consentono il documento elettronico sottoscritto con sottoscrizione elettronica diversa dalla firma digitale (ossia con criterio di imputazione diverso: è tale ad esempio, secondo alcuni la semplice e-mail (3)).

Facendo seguito al d.p.r. n. 513/997 ed al d.lgs. n. 445/2000 (testo unico della documentazione amministrativa), il d.lgs. n. 52/2005, recante il codice dell'amministrazione digitale prevede agli artt. 20, 21 e 22 in particolare che il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del codice ed alle regole tecniche, e che il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore e l'integrità del documento. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza, mentre il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'art. 2702 c.c.; in ogni caso, l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.

Quanto ai documenti informatici delle pubbliche amministrazioni, gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge, e che, nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate, sia il soggetto che ha effettuato l'operazione.

Sul punto, la deliberazione dell'Autorità informatica nella pubblica amministrazione (AIPA) del 23 novembre 2000, n. 51, recante regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, aveva aggiunto la distinzione tra i vari documenti dell'amministrazione in relazione alle forme della imputazione del documento ed alla rilevanza interna o esterna dello stesso.

La norma è confluita poi nel codice dell'amministrazione digitale di cui al d.lgs. n. 82/2005, che all'art. 34 prevede:

1) quanto ai documenti informatici di rilevanza esterna, che, ai fini della sottoscrizione, ove prevista, le pubbliche amministrazioni:

1a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati, individuati con d.p.c.m. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto;

1b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici;

2) quanto invece ai documenti informatici aventi rilevanza esclusivamente interna, ciascuna amministrazione può adottare, nella propria autonomia organizzativa per la loro formazione, gestione e sottoscrizione di, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 72 del codice.

In questo generale contesto, è intervenuto da ultimo la legge 14 maggio 2005, n. 80, recante conversione in legge, con modificazioni, del decreto-legge 14 marzo 2005, n. 35, c.d. decreto competitività (4).

Tale intervento normativo novella in più parti il codice di rito civile, prevedendo che il difensore indica nel primo scritto difensivo utile il numero di fax o l'indirizzo di posta elettronica presso cui dichiara di volere ricevere la comunicazione, e a tale indirizzo sono effettuate le comunicazioni da parte dell'ufficio, senza particolari formalità, ma "nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e teletrasmissioni" (5).

Note:

(3) Sul valore delle semplice e-mail, M. Farina, *Riflessioni sul valore legale dell'e-mail a seguito della pronuncia di alcuni decreti ingiuntivi basati esclusivamente sulla produzione di una e-mail*, in *Rass. Dir. civ.*, 2005, 615. Su alcuni aspetti penalistici, A. Luini, *I messaggi diffamatori a mezzo e-mail*, in *Riv. Pen.*, 2002, 533; G. Rognetta, *Presa di cognizione dell'e-mail con e senza involucro cifrato: i limiti della tutela penale*, in *Giur. Merito*, 2002, 1303.

(4) Sulla riforma del 2005, M. De Cristofaro, *Il nuovo processo civile "competitivo" secondo la l. n. 80/2005*, in *www.judicium.it*; F. Romano - M.A. Biasiotti, *Telematica e processo societario*, in *Inf. e diritto*, 2007, 1, 145; S. Caporusso, *Riforma del processo civile*, in *Nuove leggi civ. comm.*, 2006, 898; E. Sacchetti, *Avvocati obbligati a dare l'indirizzo e-mail*, in *Guida al diritto*, 2005, 22, 100.

(5) Sulle specifiche problematiche della trasmissione di atti processuali via e-mail, C. Mancuso, *Trasmissione degli atti processuali via fax o posta elettronica nel processo societario*, in *Giur. Mer.*, 2007, 382; Ciacci e Vari, *Forme alternative di notificazione: la notifica mediante strumenti informatici*, in *Riv. dir. comm. e dir. gen. obbl.*, 1994, I, 95; M. Cuniberti, *Posta elettronica e telefax: le nuove notificazioni e comunicazioni, il "documento informatico" e le "firme elettroniche"*, in *Giur. Merito*, 2007, 696; C. Mancuso, *Ancora* (segue)

4. Le presunzioni legali relative alla cognizione della comunicazione elettronica

Il terzo punto affermato dalla Suprema Corte nella sentenza in epigrafe riguarda invece, in un contesto che non ha visto l'applicazione della posta certificata (6), l'inapplicabilità della presunzione di arrivo della comunicazione di cui all'art. 15 comma 2 del decreto richiamato alla materia processuale. Qui bisogna intanto distinguere tra presunzione di arrivo e presunzione di conoscenza (7).

In proposito, l'art. 12 del d.p.r. n. 513/1997, il cui testo è stato trasfuso nell'art. 14 del testo unico sulla documentazione amministrativa (t.u.d.a.) dettato dal d.lgs. n. 445/2000, prevede che il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

Alcuni hanno ravvisato nella disposizione una norma sostitutiva dell'art. 1335 c.c. nelle comunicazioni elettroniche; in altri termini, l'affermazione del detto criterio altro non sarebbe che l'applicazione dei principi tradizionali in chiave evolutiva, attraverso l'estensione all'indirizzo e-mail dei principi e degli oneri applicati tradizionalmente in relazione alla cassetta delle lettere; l'indirizzo e-mail altro non sarebbe che una casella postale virtuale, con il correlato onere del titolare di controllare il contenuto della cassetta stessa, al pari di ogni altro titolare di cassetta postale fisica. In realtà, la norma dell'art. 14 t.u.d.a. può avere altra e preferibile interpretazione, in base alla quale nulla prevede della conoscenza del destinatario dell'atto pervenuto al suo indirizzo, per la quale conoscenza provvedono l'art. 1335 c.c. in linea generale e le disposizioni della direttiva sul commercio elettronico nelle fattispecie dalla stessa disciplinate: l'articolo 14 stabilisce solo la presunzione che il documento informatico trasmesso in via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. Quindi stabilisce una presunzione di ricezione, salvo prova contraria, del documento inviato all'indirizzo. Diversa è la norma da quella di cui all'art. 1335 c.c., che stabilisce, invece, la presunzione di conoscenza, cioè la presunzione che l'atto unilaterale recettizio giunto all'indirizzo del destinatario sia pervenuto a conoscenza dello stesso, salva la prova contraria (a contenuto vincolato) della impossibilità incolpevole di averne notizia. Si tratta secondo la dottrina di due presunzioni diverse: una è una presunzione - applicabile peraltro secondo alcuni ai soli documenti informatici sottoscritti con firma digitale, e non agli altri (che dovrebbero avere minori garanzie di sicurezza ed inalterabilità) - che il documento sia pervenuto all'indirizzo del destinatario in quanto trasmesso a questo telematicamente; l'altra, quella codificata, è la presunzione che l'atto, giunto all'indirizzo del destinatario, sia giunto altresì a conoscenza del soggetto.

Con riferimento poi alla previsione della presunzione di conoscenza di cui all'art. 1335 c.c., non vi è dubbio

che risulta difficile equiparare totalmente l'indirizzo elettronico alla casella postale tradizionale compiutamente, atteso che la casella elettronica di posta è ubicata in un luogo diverso da quello fisico ove è domiciliato il soggetto, è posta in luogo virtuale - che non coincide con la sede del *provider* ma con il *server* su cui si trova lo spazio di memoria con la *post-box* - fuori della sfera di controllo (fisico o tecnico) immediato del destinatario dell'atto, in relazione al quale la presa di conoscenza dell'atto pervenuto non può mai essere contestuale alla ricezione (a differenza della posta ordinaria) ma sempre solo successiva.

Inoltre, all'unicità dell'indirizzo postale del domicilio del soggetto può far riscontro l'esistenza di una pluralità di indirizzi elettronici, con la conseguenza che difficilmente può affermarsi l'onere del titolare di scaricare la posta da tutte le caselle possedute in tempi reali o nell'immediatezza dell'invio. Un siffatto onere, infatti, richiederebbe elementi ulteriori rispetto a quelli finora descritti.

La dottrina ha al riguardo precisato che solo in alcuni casi può configurarsi una presunzione di conoscenza *ex art.* 1335 c.c. in relazione all'indirizzo elettronico del destinatario, essendo tale soluzione imposta dalle norme (ad es. la direttiva sul commercio elettronico o il regolamento sul processo telematico), ovvero vi sia elezione di domicilio (cfr. art. 12 d.p.r. n. 513/1997, trasfuso nell'art. 14 t.u.d.a., il cui principio della dichiarazione dell'indirizzo elettronico può applicarsi in relazione all'art. 1335 c.c.), o usi negoziali.

In altri termini, il semplice possesso di un indirizzo e-mail non potrebbe ritenersi sufficiente per autorizzare notifiche e far scattare l'onere per il destinatario di scaricarsi la posta dal *server* del *provider*.

Note:

(segue nota 5)

sulla trasmissione degli atti processuali via fax o posta elettronica nel processo societario, in *Giur. Merito*, 2007, 1695; E. Senini, *Le notificazioni a mezzo fax e posta elettronica nel processo societario*, in *Le società*, 2006, 115; P. Frattino, *Regole operative per la posta elettronica certificata*, in *Forum fisc.*, 2006, 10, 35; A. Paladino, *Ricorsi per posta elettronica, serve la firma digitale per la piena validità*, in *Nuovo dir.*, 2005, 192; M. Giorgietti, *Le nuove norme sulle comunicazioni e notificazioni*, in *Riv.dir. proc.*, 2005, 701.

(6) Sulla posta elettronica certificata, M. Melica, *La posta elettronica certificata: funzionamento e applicazioni*, in *Inf. e diritto*, 2007, 271; A. Pelosi, *Il Codice dell'amministrazione digitale modifica il valore giuridico della posta elettronica certificata*, in *Contratti*, 2007, 255; G. Cammarota, *La disciplina della posta elettronica certificata*, in *Giorn. Dir. amm.*, 2005, 917; C. Rabazzi, *La posta elettronica certificata: le novità introdotte con il d.p.r. n. 68/2005*, in *Cyberspazio e dir.*, 2005, 229; D. Marongiu, *La trasmissione del documento informatico: il ruolo della posta elettronica certificata*, in *Inf. e diritto*, 2005, 135; C. Giurandella, E. Guarnaccia, *Il diritto pubblico dell'informatica nel d.lgs. n. 82/2005: rilievi critici*, in *Inf. e diritto*, 2005, 235; S. Giordano, *Pronto il d.p.r. sulla posta elettronica*, in *Dir. giustizia*, 2004, 16, 48.

(7) Su queste problematiche, F. Buffa, *Giurisdizione e ADR*, in *Aa.Vv.* (a cura di Bilotta), *Internet*, 2003; G. Finocchiaro, *Lex mercatoria e commercio elettronico - Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. e impr.*, 2001, 571; F. Fortinguerra, *Gli scambi telematici ed il consumatore*, Lecce, Quaderno n. 6 dell'ISUFI, 2006; N. Scannicchio, *La conclusione del contratto on-line nella direttiva europea sul commercio elettronico*, in A. Antonucci (a cura di), *E-commerce*, Milano, 2001, 95.

Per converso, potrebbe restrittivamente ammettersi tale forma di indirizzo del soggetto solo ove vi sia un uso professionale della posta elettronica: è infatti ragionevole ammettere un onere del destinatario di scaricare la posta dal *server* del *provider* tempestivamente solo ove l'uso della posta sia di tale entità tale da configurare una sorta di domiciliatazione del soggetto, come potrebbe ritenersi nei casi in cui il soggetto è in possesso di firma digitale, o abbia comunicato in qualsiasi modo il proprio indirizzo elettronico nell'ambito del rapporto sostanziale cui si riferisce l'atto giudiziario (o ad esempio sia l'unico indirizzo dato e l'unico punto di riferimento di un contraente telematico), o infine se vi siano usi tra le parti circa l'uso della posta elettronica per l'esecuzione contrattuale; in altri casi, sembra difficile far gravare un onere di conoscenza sul destinatario che di per sé non potrebbe assicurare (tenendo conto della non immediatezza del *download* della posta dalla casella) celebrità maggiore rispetto ai tempi offerti dai mezzi tradizionali di notifica.

Ciò spiega la previsione dell'art. 7 del d.p.r. n. 123/2001 (regolamento c.d. sul processo telematico), secondo il quale ai fini delle comunicazioni e delle notificazioni effettuate ai sensi dell'articolo 6, l'indirizzo elettronico del difensore è unicamente quello comunicato dal medesimo al Consiglio dell'ordine e da questi reso disponibile ai sensi del comma 3 dello stesso articolo. Per gli esperti e gli ausiliari del giudice l'indirizzo elettronico è quello comunicato dai medesimi ai propri ordini professionali o all'albo dei consulenti presso il tribunale. Per tutti i soggetti diversi da quelli indicati nel comma 1 l'indirizzo elettronico è quello dichiarato al certificatore della firma digitale al momento della richiesta di attivazione della procedura informatica di certificazione della firma digitale medesima, ove reso disponibile nel certificato.

Non tutti gli indirizzi sono quindi idonei, ma solo quelli comunicati; peraltro, il legislatore ha considerato che la richiesta di certificazione di una firma digitale, comunque, implica un uso professionale del computer e dei servizi di rete, onde la casella postale elettronica può essere anche il mezzo di trasmissione di atti a valenza processuale.

In ordine agli oneri delle parti di prendere cognizione del materiale ricevuto nella posta elettronica, va aggiunto inoltre che in materia ha inciso in parte la direttiva sul commercio elettronico (direttiva 00/31/CE), che all'art. 11 dispone che l'ordine e la ricevuta si considerano ricevuti quando le parti cui sono indirizzati hanno la possibilità di accedervi: in altri termini, la dichiarazione si potrà considerare accessibile solo dal momento in cui si trovi sul terminale di rete locale gestito direttamente dal destinatario, così ritenendo che sussista accessibilità del messaggio quando sia direttamente controllabile da quest'ultimo, tenendo a tal fine presente che accessibile tecnicamente il messaggio lo è già non appena giunto nella mail box presso il *server* del *provider*

(che peraltro il titolare della casella può consultare indifferentemente non solo da qualunque luogo con un portatile, ma anche da una qualunque postazione - pure altrui-, anche senza scaricare il relativo file nella memoria del computer).

5. La ricevuta

Fatte queste considerazioni di ordine generale, e tornati alla questione affrontata dalla sentenza, non si vede perché i principi della presunzione di ricezione e di quello distinto di presunzione di conoscenza non possano essere applicati alle comunicazioni processuali, visto che la ratio è basata sul funzionamento tecnico della comunicazione e sul potere di disposizione e controllo tendenzialmente esclusivo della casella di posta (elettronica o meno), e non sulla natura sostanziale o processuale dell'atto che resta del tutto irrilevante.

Piuttosto, tutto il discorso sarebbe stato assai più semplice osservando che la comunicazione di un atto, in forma non vietata dall'ordinamento che non impone forme particolari a pena di nullità, è valida ove, conseguendo il suo scopo, come avvenuto nel caso, raggiunga il destinatario, il quale abbia accusato ricevuta.

La distinzione ulteriore tra ricevuta in automatico o meno è errata invece sul piano tecnico e giuridico, perché la ricevuta predisposta in automatico ed automaticamente inviata è pur sempre attività riconducibile al titolare della risorsa informatica che così ha predisposto il sistema informatico, e rientra perciò nella sua sfera di controllo (e responsabilità).

Inoltre, sia o meno automatica la risposta per ricevuta, non vi è il problema ipotizzato dalla Corte della presunzione di arrivo del messaggio, quanto la certezza tecnica che lo stesso sia arrivato al destinatario sollecitando la risposta (in automatico o meno, poco importa).

Più problematico è se mai il riferimento alla documentazione probatoria delle ricevute, facendo la Corte riferimento alla stampa cartacea della stessa.

Sul punto, conclusivamente, va osservato che la prova è data dal file (e non dalla stampa) della comunicazione di ritorno, ossia da un documento informatico (comprensivo dei c.d. *headers* della *e-mail*), con tutto ciò che ne consegue in termini di valutazione della prova in giudizio, e, prima ancora, di modalità di produzione della stessa e di lettura dei dati ivi contenuti.

E qui si possono porre tanti problemi di paternità della comunicazione elettronica (su cui, in difetto di firma digitale della ricevuta di ritorno, rileveranno in prima battuta, gli *headers* del messaggio *e-mail*) e di inalterabilità della stessa (si pensi, ad esempio, alle problematiche di prova circa l'orario, esatto e certo, di invio e ricezione della comunicazione). La stampa cartacea potrà solo essere un primissimo indizio idoneo a radicare una fragile presunzione, suscettibile di venir meno in presenza di contestazioni, e ciò, ovviamente, anche se la ricevuta di ritorno sia data non in automatico.

Reati informatici

Per la configurabilità del reato di abusivo mantenimento nel sistema informatico è necessario che l'agente sia consapevole di agire *invito domino*

Tribunale di Nola 11 dicembre 2007, n. 488 - G.U.P. Rizzi Ulmo

Accesso e mantenimento nel sistema informatico protetto - Anagrafe tributaria - Dipendente dell'Agenzia delle Entrate - Elemento oggettivo - Natura delle informazioni captate - Irrilevanza - Elemento soggettivo - Consapevolezza della contraria volontà anche tacita del titolare del sistema - Necessità

(c.p. art. 615 ter)

Non commette il reato di cui all'art. 615 ter c.p., per esclusione dell'elemento soggettivo, l'impiegato dell'Agenzia delle Entrate che accede e si intrattiene nel sistema informatico per pochi secondi e per finalità diverse rispetto a quelle per cui vale la sua autorizzazione, in particolare per prendere visione di soli dati anagrafici di pubblica conoscenza e conoscibilità.

...omissis...

Motivi della decisione

All'esito della udienza preliminare osserva questo giudice quanto segue.

Il presente procedimento (trasmesso per competenza dalla Procura di Milano in relazione alle posizioni degli imputati C. e C.) rientra in una più ampia vicenda che ha interessato l'intero territorio nazionale, che è stata portata all'attenzione della magistratura da una denuncia del Vice - Ministro dell'Economia e delle Finanze V. che ha avuto ad oggetto una serie di interrogazioni all'anagrafe tributaria sul conto di R.P. e della consorte F.F. effettuate, per ragioni estranee al servizio, dagli stessi dipendenti dell'Agenzia delle Entrate nonché da militari della Guardia di Finanza. Per quel che interessa il presente procedimento, gli imputati R. C. ed A.C. sono dipendenti dell'Agenzia delle Entrate di: sul loro conto è emerso che la C. ha effettuato, il giorno 27 marzo 2006, due accessi all'anagrafe tributaria, uno alle ore 12:01 e 29 secondi, che ha riguardato esclusivamente i dati anagrafici di R.P. e consorte, e l'altro alle ore 12:01 e 48 secondi, che ha invece riguardato le dichiarazioni dei redditi dei predetti ("Unico" 2004); mentre il C. ha effettuato un unico accesso, il giorno 25 maggio 2006 alle ore 12:59 e 42 secondi, che ha riguardato solo i dati anagrafici di R.P. e consorte (su tali circostanze cfr. foglio 4 del fascicolo del P.M.).

La peculiarità della vicenda risiede nel fatto che i due predetti imputati, nella loro qualità di dipendenti dell'Agenzia delle Entrate, erano sì abilitati all'accesso alla banca dati dell'anagrafe tributaria, ma nel caso di specie hanno indiscutibilmente agito (come d'altronde da loro stesso ammesso in sede di interrogatorio) al di fuori dell'esercizio delle loro mansioni, non avendo in corso l'Agenzia delle Entrate di alcun tipo di accertamento nei confronti di R.P. e consorte (cfr., sul punto, le dichiarazioni rese in sede di sommarie informazioni dalla direttrice dell'Agenzia delle Entrate di, fogli 4 e ss del fascicolo del P.M.).

In punto di diritto va evidenziato che, come è stato autorevolmente sostenuto (cfr. Cass., sez. V, n. 1675/2000, Zara; Cass., sez. V, n. 12732/2000; Cass., sez. V, n. 44362/2003, Muscia; nella giurisprudenza di merito cfr. Tribunale di Bari, 18 dicembre 2006), il delitto previsto e punito dall'art. 615 ter c.p. si configura anche a carico di chi, pur essendo autorizzato all'accesso ad un sistema informatico per determinate finalità, utilizzi tale facoltà per finalità diverse rispetto a quelle per le quali vale la sua autorizzazione.

Invero, l'art. 615 ter c.p. punisce non solo chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (cfr. prima parte del comma 1 dell'art. 615 ter c.p.) - introduzione abusiva che è inconfigurabile in capo a colui che è autorizzato all'accesso

al sistema e che è quindi munito delle chiavi necessarie per superare le misure di protezione senza violarle, ma anche colui che, introdottosi lecitamente nel sistema, vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo (cfr. seconda parte del comma 1 dell'art. 615 *ter* c.p.): ebbene, il soggetto che sfrutta la sua possibilità di accesso al sistema per effettuare operazioni diverse rispetto a quelle per le quali è autorizzato tiene un comportamento che equivale al mantenersi nel sistema contro la volontà tacita di chi ha il diritto di escluderlo e che, pertanto, rientra nell'ipotesi prevista e punita dalla seconda parte del comma 1 dell'art. 615 *ter* c.p.

Pertanto, alla luce di tali principi, è configurabile l'elemento oggettivo del reato in contestazione, sotto forma di mantenimento nel sistema informatico contro la volontà tacita dell'amministrazione finanziaria, nei confronti di entrambi gli odierni imputati, che hanno acceduto all'anagrafe tributaria per conoscere dati relativi a R.P. e consorte senza che tale accesso fosse giustificato dall'esercizio delle loro funzioni, e quindi per finalità diverse da quelle per le quali erano autorizzati ad accedere all'anagrafe tributaria.

Tuttavia, ritiene questo giudice che da un punto di vista dell'elemento psicologico del reato occorra procedere ad una differenziazione tra la posizione della C., che ha acceduto sia ai dati anagrafici di R.P. e consorte sia anche alle loro dichiarazioni dei redditi ("Unico" 2004), e quella del C., che ha acceduto solo ai dati anagrafici dei predetti.

Questo giudice è ben consapevole del corretto orientamento giurisprudenziale secondo il quale la norma dell'art. 615 *ter* è posta a tutela del domicilio informatico in quanto tale, violando il quale è per ciò solo integrato il reato, irrilevante essendo la natura delle informazioni captate, se cioè riservate o meno (cfr. Cass., sez. V, n. 11689/2007, Cerbone; Cass., sez. VI, n. 3065/1999, De Vecchis): ed è, infatti, per tale motivo che si ritiene che nel caso di specie il delitto in esame sia sussistente da un punto di vista dell'elemento oggettivo anche in relazione al C..

Ad avviso di questo giudice, però, la circostanza che il C., legittimato ad accedere al sistema, vi si sia intrattenuto, presumibilmente per pochi secondi, non per prendere cognizione di dati sensibili quali le informazioni fiscali, bensì puramente e semplicemente per prendere visione di dati, quali quelli anagrafici, di pubblica conoscenza e conoscibilità e non sottoposti dall'ordinamento ad alcuna forma di tutela della riservatezza, porta a ritenere che egli non si sia nemmeno reso conto che vi potesse essere una tacita volontà contraria da parte dell'amministrazione finanziaria a che egli si mantenesse all'interno del sistema per consultare i dati anagrafici di R.P. e consorte. Ed è per tale ragione che, quanto meno ai sensi del comma 3 dell'art. 425 c.p.p., vada nei suoi confronti emessa sentenza di non luogo a procedere per mancanza del dolo del reato contestato, e quindi con la formula "perché il fatto non costituisce reato".

... *Omissis*...

IL COMMENTO

di Giovanni Garbagnati

La pronuncia che si annota mostra ancora una volta i limiti dell'interpretazione dominante, secondo cui il bene giuridico tutelato dall'art. 615 *ter* c.p. è il c.d. "domicilio informatico protetto" con conseguente irrilevanza, ai fini della configurabilità del reato, della natura, riservata o meno, delle informazioni captate. In ogni caso, per quanto riguarda le ipotesi di accesso ai sistemi informatici aziendali da parte dei dipendenti occorrerebbe che la Società (o l'Ente) titolare del sistema specificasse con chiarezza i limiti entro cui costoro sono autorizzati all'uso dell'elaboratore.

1. Il caso concreto: l'imputato prosciolto per la mancanza (presunta) del solo elemento soggettivo

Il pubblico dipendente che agendo al di fuori delle sue mansioni si è trattenuto per pochi secondi nel sistema informatico al quale è legittimato ad accedere per motivi di lavoro, al fine di prendere conoscenza di infor-

mazioni che non sono sottoposte dall'ordinamento ad alcuna forma di tutela della riservatezza, poteva presumibilmente ignorare l'esistenza di una tacita volontà contraria dell'Amministrazione di appartenenza. È questa in sintesi la ragione per cui il Giudice dell'udienza preliminare del Tribunale di Nola ha emesso una sentenza di non luogo a procedere "ai sensi del comma 3 dell'art. 425 c.p.p." (dunque per essere gli elementi a carico "insufficienti, contraddittori o comunque non idonei a sostenere l'accusa in giudizio") nei confronti di un impiegato dell'Agenzia delle Entrate cui era contestato il delitto *ex* art. 615 *ter* c.p. per avere questi, in una sola occasione, preso visione dei dati anagrafici di un noto uomo politico e della moglie del medesimo, in assenza di procedure di accertamento fiscale che giustificassero l'accesso da parte dell'imputato ai dati ad essi relativi (1).

Note:

(1) Nel medesimo procedimento penale era in verità imputato per l'identico reato anche un altro dipendente della stessa Agenzia delle Entrate
(segue)

La pronuncia in commento si segnala nello scarno panorama giurisprudenziale in tema di abusivo mantenimento in un sistema informatico protetto da misure di sicurezza perché affronta e risolve il caso sotto l'inedito profilo dell'elemento soggettivo del reato, ravvisando la (possibile) mancata consapevolezza in capo all'agente circa il carattere illecito della propria condotta nella occasionalità (un'unica interrogazione di brevissima durata) e nella tenuità della stessa (dettata verosimilmente da mera curiosità e riguardante soltanto "dati di pubblica conoscenza e conoscibilità").

Il giudice campano non si discosta invece dall'orientamento giurisprudenziale dominante per quanto attiene l'elemento oggettivo del reato, ritenuto nel caso concreto sussistente sul presupposto che, da un lato, il delitto in esame si può configurare anche a carico del soggetto che sfruttando la sua autorizzazione all'accesso all'elaboratore "utilizzi tale facoltà per finalità diverse rispetto a quelle per cui vale la sua autorizzazione" (2), e dall'altro che esso si perfeziona con la semplice violazione del c.d. domicilio informatico "irrilevante essendo la natura delle informazioni captate, se cioè riservate o meno" (3).

1.1 Buon senso e contraddittorietà della pronuncia di proscioglimento: i limiti strutturali di una decisione giusta

È da dire che la soluzione adottata dal G.U.P. di Nola, pur contraddistinta da ragionevolezza e buon senso, poggia su un percorso argomentativo che - per così dire - sconta la rigidità e le lacune dell'interpretazione accolta in punto di elemento oggettivo del reato, così che la ritenuta mancanza di dolo appare un *escamotage* usato per sfuggire ad una pronuncia di condanna (*rectius*: all'emissione del decreto di rinvio a giudizio) che sarebbe stata eccessiva rispetto alla ridotta offensività della condotta incriminata.

Peraltro, sembra in qualche modo contraddittorio sostenere l'applicabilità del principio secondo cui la mera intrusione abusiva nel domicilio informatico altrui costituisce una condotta penalmente rilevante quale che sia lo scopo dell'accesso o la natura delle informazioni (pubbliche o private) così ottenute dall'intruso, ed allo stesso tempo ipotizzare la mancata consapevolezza in capo all'agente circa la contraria volontà del titolare dello *ius excludendi*, sul presupposto che oggetto dell'acquisizione erano soltanto - come è precisato in sentenza - "dati di pubblica conoscenza e conoscibilità", quali quelli anagrafici dei due personaggi pubblici. Se si ritiene che l'ordinamento punisca il dipendente per qualsiasi uso estraneo alle esigenze lavorative del sistema informatico (protetto), pare difficile immaginare che questi mentre digita il nome di una famoso uomo politico al fine di apprenderne (per diletto) i dati anagrafici possa ritenere di avere il consenso del titolare del sistema o che, all'inverso, quest'ultimo abbia autorizzato i propri impiegati a curiosare nell'elaboratore per ciò che non attiene ai dati sensibili.

In realtà, al di là del condivisibile esito assolutorio

adottato nel caso concreto, la sentenza mette ancora una volta in evidenza come siano incerti (a causa della generica formulazione (4) e dell'ambigua collocazione editta di questa norma) i limiti applicativi dell'art. 615 *ter* c.p. e come per l'effetto siano intuibili i rischi di difformità interpretativa da parte delle Corti di merito, con possibile violazione del principio di offensività laddove si andassero a colpire con la sanzione penale condotte di infima pregnanza. Pare perciò opportuno, in sede di commento, verificare se sia corretta l'interpretazione data alla fattispecie in esame, ovvero si possa escludere o delimitare il reato di cui all'art. 615 *ter* c.p. in ragione della neutralità dell'accesso (non riguardante dati riservati) e/o della qualifica soggettiva dell'agente (dipendente autorizzato per ragioni di lavoro all'uso del sistema informatico). A tal fine occorre dapprima prendere in esame il bene giuridico oggetto di tutela e quindi definire l'ambito del "mantenimento" nel sistema informatico penalmente rilevante.

2. Il bene giuridico tutelato dall'art. 615 *ter* c.p.

È ben noto come la laconicità della norma *de qua* e l'improvvida, ma non casuale (5), scelta del legislatore

Note:

(segue nota 1)

(che qualche mese prima aveva effettuato due accessi "abusivi" all'anagrafe tributaria, aventi ad oggetto rispettivamente i dati anagrafici e la dichiarazione dei redditi degli stessi due personaggi pubblici), la cui posizione è stata opportunamente stralciata dal Giudice in considerazione dell'evidente diversità tra le condotte, avendo quest'ultimo preso visione anche di un dato sensibile, quale è la dichiarazione dei redditi.

(2) In questo senso, la prevalente giurisprudenza di legittimità: v. in particolare Cass., 19 dicembre 2001 n. 7041, Corrao, in *Guida al diritto*, 2002, 18, 72.

(3) Cfr., *ex multis*, Cass., sez. V, 7 novembre 2000 n. 1675, Zara e altri, in *Cass. pen.*, 2001, 3078; conf., Cass., sez. V, 14 ottobre 2003 n. 44362, P.M. in proc. Muscia, in *Cass. pen.*, 2005, 1580.

(4) Nella giurisprudenza di merito è stato efficacemente puntualizzato che "la ben laconica enucleazione degli elementi costitutivi del reato a fronte della "novità" nonché della rilevante complessità, anche tecnica, e vastità della materia che essa disciplina, determina indubbiamente ardui problemi interpretativi in fase di applicazione ai più vari e diversi casi concreti ad essa astrattamente riconducibili" (così, Trib. Gorizia, 19 febbraio 2003 n. 601, Merini, in *Riv. pen.*, 2003, 895). Alcuni Autori hanno osservato che la scelta del legislatore di inserire le nuove fattispecie penali all'interno delle partizioni già esistenti nel nostro Codice è stata una scelta coerente con la natura dell'intervento normativo, non trattandosi "di introdurre nuove fattispecie a tutela di nuovi beni giuridici quanto piuttosto di introdurre fattispecie relative a nuove forme di aggressione, cioè portate con modalità nuove a beni in larga parte già penalmente rilevanti e tutelati (...)" e con la particolarità della materia riguardante "essenzialmente le tecniche di commissione del reato nonché gli strumenti e gli oggetti materiali dell'azione, non l'oggetto giuridico". *Contra*, sulla necessità di distinguere tra norme che identificano nuove forme di aggressione a beni già oggetto di tutela penale e norme che definiscono oggetti, giuridici e materiali, parzialmente o talmente nuovi, R. Flor, *Sull'accesso abusivo ad un sistema informatico e telematico: il concetto di "domicilio informatico" e lo "ius excludendi alios"*, in *Dir. pen. proc.*, 2005, 86 e L. Picotti, voce *reati informatici*, in *Enc. dir.*, Milano, agg. 2000, VIII, 1 ss.

(5) La "Relazione al Disegno di legge n. 2773 poi divenuto legge 23 dicembre 1993 n. 547" (in www.penale.it/legislaz/rel_ddl_2773_XI) (segue)

di darne collocazione all'interno della sezione IV del libro II del *corpus* codicistico riservata ai "delitti contro l'inviolabilità del domicilio" abbia ingenerato un'accesa disputa su quale sia il bene giuridico tutelato dall'art. 615 *ter* c.p. e, di conseguenza, sul fatto se sia o meno configurabile il reato anche in assenza (come nel caso in esame) di captazione di dati riservati o di inceppamenti nel funzionamento del sistema informatico. Secondo il prevalente orientamento - che trae spunto dalla Relazione preliminare alla l. n. 547/1993 -, ormai recepito dalla Cassazione (e come si è detto seguito anche dal G.U.P. campano) (6), proprio l'ubicazione della norma dimostrerebbe che oggetto della tutela è il c.d. "domicilio informatico", inteso come "luogo in cui può estrinsecarsi la personalità individuale", il quale rappresenta (7) la trasposizione sul piano virtuale dello *ius excludendi alios*, ovvero del diritto del titolare di vietare a chicchessia l'accesso indesiderato dallo spazio informatico (protetto da misure di sicurezza) di sua pertinenza (8). A questa stregua, non rileverebbe mai ai fini della configurabilità del reato il carattere personale o meno delle informazioni contenute nel sistema, potendo anzi la tutela operare anche se l'elaboratore non contiene alcun dato (9).

Per quanto consolidata, questa tesi è oggetto di numerosi rilievi critici. È invero stato osservato che:

- da essa deriverebbe un'incongrua espansione dei concetti di domicilio e riservatezza personale (10);

- difficilmente i sistemi informatici possono essere ricondotti alla nozione (peraltro assai controversa) di domicilio rilevante per il diritto penale in quanto nella maggior parte essi sono totalmente privi di contenuti personalistici e privatistici (11);

- se il bene giuridico fosse lo "spazio privato virtuale" dell'elaboratore sarebbe viziata da irragionevolezza la scelta del legislatore di circoscriverne la tutela ai soli sistemi informatici protetti da misure di sicurezza (tanto più che l'art. 614 c.p. non opera distinzioni in questo senso) (12);

- la disposizione in esame si applica anche ai sistemi operanti nel settore pubblico, quali quelli indicati nell'aggravante di cui all'art. 615 *ter*, comma 3, c.p., ovvero "i sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico", che sono estranei alla nozione di domicilio ed alla proiezione spaziale della persona (13);

- l'operatività della norma in esame prescinde dalla circostanza che titolare del "domicilio informatico" sia una persona fisica o giuridica, mentre come è noto l'istituto di cui all'art. 614 c.p. si misura (prevalentemente) con il concetto di abitazione e privata dimora, "ossia con una dimensione funzionale del bene domicilio, incentrata sul rapporto persona - ambiente" (14).

Si è perciò osservato criticamente che seguendo l'impostazione in esame sorge il rischio che l'ordinamento - sanzionando anche l'intrusione non autorizzata in quanto tale - offra tipi di tutela meramente formali che

esporrebbero la norma a censura di incostituzionalità per violazione del principio di proporzionalità (15).

Note:

(segue nota 5)

leg.html) precisa che essa è invero dovuta al fatto che "i sistemi informatici e telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 c.p."

(6) Si veda diffusamente G. Corrias Lucente, *Brevi note in tema di accesso abusivo e frode informatica; uno strumento per la tutela penale dei servizi*, in *Dir. Inf.*, 2001, 492 ss., la quale analizza partitamente le "quattro tesi alternative sull'oggettività giuridica del reato di accesso abusivo"; N. Maiorano, *sub art. 615 ter*, in Lattanzi-Lupo, (a cura di), *Codice penale. Rassegna di giurisprudenza e di dottrina*, Milano, 2005, 578 ss.

(7) A. Cisterna, *Solo una misura di protezione calibrata dà luogo a violazioni di sistema criminali*, in *Guida al diritto*, 2008, 12, 80 sottolinea come da questa impostazione discenda una protezione che "privilegia non il contenuto o la natura dell'informazione, ma il locus che la contiene".

(8) R. Flor, *Identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 930.

(9) Secondo Cass., 4 ottobre 1999, Piersanti, in *Dir. Inf.*, 2001, 485, questa è la soluzione che meglio si attaglia alla lettera (perché la norma non opera distinzioni tra sistemi a seconda dei contenuti, ma soltanto delle misure di sicurezza) e allo scopo della legge, perché l'interpretazione contraria porterebbe all'esclusione dalla tutela di aspetti non secondari, quali per esempio quelli connessi ai profili economico-patrimoniali dei dati: "Con il riferimento al "domicilio informatico" sembra che il legislatore abbia voluto individuare il luogo fisico - come sito in cui può esplicarsi la personalità umana - nel quale è contenuto l'oggetto della tutela (qualsiasi tipo di dato e non i dati aventi ad oggetto particolari contenuti) per salvaguardarlo da qualsiasi tipo di intrusione (*ius excludendi alios*) indipendentemente dallo scopo che si propone l'autore dell'abuso".

(10) In questo senso, G. Corrias Lucente, *op. cit.*, 499. Sul punto v. altresì, L. Cuomo, *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, 2998 ss.; L. Cuomo-B. Izi, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cass. pen.*, 2002, 1018 ss.; D. Trentacapilli, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, in *Dir. pen. proc.*, 2002, 1280 ss.; A. Cisterna, *op. e loc. cit.*.

(11) F. Berghella-R. Blaiotta, *Diritto penale dell'informatica e beni giuridici tradizionali*, in *Cass. pen.*, 1995, 1463, 2330, che citano quale esempio "una banca di dati di giurisprudenza, di bibliografia, di articoli di stampa, di dati climatici, ecc."

(12) Secondo la Relazione preliminare alla l. n. 547/1993, *cit.*, ciò è dovuto al fatto che "dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'accesso e la permanenza nel sistema alle sole persone da lui autorizzate".

(13) In questo senso, C. Pecorella, *Il diritto penale dell'informatica*, Padova, 2000, 316.

(14) Così, Trib. Rovereto, 9 gennaio 2004 n. 343, L.T., in *Dir. pen. proc.* 2005, 81, secondo cui il "domicilio informatico", bene giuridico protetto dalla norma in commento, non può risolversi in una mera specificazione del domicilio tutelato dall'art. 614 c.p., ma ha la "dignità di un vero e proprio nuovo bene giuridico, che può indicarsi come riservatezza informatica e che, in concreto, si risolve nella indisturbata fruizione del sistema informatico o telematico". Si veda altresì R. Flor, *Sull'accesso abusivo ad un sistema informatico e telematico: il concetto di "domicilio informatico" e lo ius excludendi alios*, *ivi*, 87, per il quale il legislatore nel predisporre la norma sulla falsariga dell'art. 614 c.p. non ha tenuto in adeguata considerazione che l'elaboratore è l'ambiente in cui si manifesta la personalità soggettiva della persona.

(15) Così, F. Berghella-R. Blaiotta, *Diritto penale dell'informatica*, *cit.*, 2235.

Resta dunque da porsi l'interrogativo se sia (stata) veramente intenzione del legislatore offrire una protezione a così ampio spettro in tema di illecita intrusione nell'elaboratore altrui. Per quanto la risposta non sia univoca, l'analisi dell'ordito normativo svolta alla luce dei lavori parlamentari e dell'esperienza sovranazionale dovrebbe indurre l'interprete a circoscrivere (e non ad estendere) in questo settore l'area della tutela penale. Anzitutto nella Relazione preliminare alla legge n. 547/1993 si precisa che, nella scelta tra opzione penale ed amministrativa, si sono seguite indicazioni "ispirate ai principi di proporzionalità e di sussidiarietà, e rapportate al rango dell'interesse da tutelare ed al grado dell'offesa (principio di proporzionalità) nonché alla inevitabilità della sanzione penale, quale ultima *ratio* (principio di sussidiarietà)" (16).

È inoltre significativo che il legislatore italiano non abbia recepito (17) in alcuna norma la prescrizione contenuta nella "lista facoltativa" del Consiglio d'Europa (18) in tema di utilizzazione non autorizzata di un elaboratore (non protetto) (19), volta a sanzionare almeno le condotte poste in essere con l'intenzione o l'effetto di causare pregiudizio al titolare, al sistema o al suo funzionamento. Si avrebbe infatti il paradosso di un ordinamento che, da un lato, tutela in quanto tale l'inedito bene del "domicilio informatico protetto", luogo di proiezione della personalità umana, anche nell'ipotesi di utilizzo contro la tacita volontà contraria del titolare di un sistema informatico pubblico (protetto) che non contenga dati personali o riservati, e dall'altro lascia privo di protezione giuridica il titolare del sistema (in ipotesi contenente informazioni private) che sia utilizzato con l'effetto o l'intenzione di danneggiarlo, solo perché privo di misure di sicurezza (e ciò tanto più che l'art. 614 c.p. tutela il domicilio anche se questo non è dotato di protezioni).

Di pari rilievo è che sia la Convenzione di Budapest sulla criminalità informatica del novembre 2001, sia la Decisione Quadro del Consiglio d'Europa del 24 febbraio 2005 sullo stesso tema (20), nel prevedere l'ipotesi dell'"accesso illegale" ai sistemi di informazione segnalano la possibilità o l'opportunità di limitarne la applicazione ai soli casi gravi (Decisione CE) o alle ipotesi in cui la condotta è commessa con l'intenzione di ottenere dei dati informatici o con altro scopo fraudolento (Convenzione). È infine da aggiungere che neppure la legge di ratifica ed esecuzione della Convenzione di Budapest, finalmente in via di approvazione (21), pur prevedendo la rimodulazione o l'introduzione di nuove e più severe fattispecie nel nostro ordinamento in materia di criminalità informatica, è intervenuta sul tema degli "accessi abusivi" (22).

Pertanto, al di là delle difficoltà esegetiche sopra descritte in merito all'inquadramento del bene giuridico tutelato dall'art. 615 *ter* c.p. all'interno dell'impalpabile criterio del c.d. "domicilio informatico", appare che la rigorosa applicazione di quest'ultimo porterebbe a conse-

guenze di dubbia conformità con il quadro costituzionale e comunitario, estendendo l'area di tutela penale ben al di là delle intenzioni stesse del legislatore.

Se così è, occorre però individuare in quale altro modo possa venire individuato il bene tutelato dalla norma in esame. In dottrina vi è chi ritiene che esso consista nell'integrità dei dati e dei sistemi informatici (23);

Note:

(16) Rel. Prel., *cit.*, 3. In essa il Relatore afferma altresì che "in sostanza il sistema penale vigente richieda adattamenti ed integrazioni necessari perché fatti criminosi di rilevante incidenza sociale (...) ricevano finalmente una risposta punitiva".

(17) E ciò nonostante che nella Relazione Preliminare alla l. n. 547/1993 (pagg. 5 e 6) si facesse espressamente riferimento al tema dell'"uso di apparecchiature informatiche per fini personali", lamentando che non fosse ancora oggetto di tutela.

(18) È invero noto come, da un lato, l'art. 615 *ter* c.p. sia stato introdotto dall'art. 4 della legge 23 dicembre 1993 n. 547 sulla scorta della prescrizione di cui alla lett. e) - relativa all'"accesso non autorizzato (accesso senza diritto ad un sistema o ad una rete informatica mediante violazione delle regole di sicurezza)" - della "lista minima" della Raccomandazione R (89)9 adottata dal Consiglio dei Ministri del Consiglio d'Europa il 13 settembre 1989. È evidente che tra questa ipotesi e quella - inserita nella lista facoltativa - relativa all'uso del sistema o rete informatica (v. nota seguente) vi sia il discrimine che solo nel primo caso il sistema deve essere protetto da norme di sicurezza (diversamente la seconda fattispecie ne sarebbe stata assorbita).

(19) Relativa alla "utilizzazione senza diritto di un sistema o di una rete informatica effettuata: (a) accettando un rischio rilevante di causare un pregiudizio a colui che ha diritto di utilizzare il sistema o al suo funzionamento ovvero (b) con l'intenzione di creare un pregiudizio alla persona che ha diritto di utilizzare il sistema o il suo funzionamento, ovvero (c) causando in tal modo un pregiudizio alla persona che ha diritto di usare il sistema o arrecando un pregiudizio al sistema o al suo funzionamento" (Rel. prel., pag. 5).

(20) La Convenzione di Budapest di lotta alla criminalità informatica del 23 novembre 2001 prevede l'ipotesi di "illegal access" (art. 2, title 1, Sec. 1, Chapter II): "Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system". Analogamente, la decisione quadro 2005/222/GAI del Consiglio d'Europa del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione (in GUCE 16.3.05) prevede (art. 2) "Accesso illecito ai sistemi di informazione": «Ciascuno Stato membro adotta le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato, almeno per i casi gravi. Ciascuno Stato membro può decidere che i comportamenti di cui al paragrafo 1 siano punibili solo quando il reato è commesso violando una misura di sicurezza».

(21) Il Senato della Repubblica ha approvato il disegno di legge in data 27 febbraio 2008.

(22) Soltanto il nuovo art. 635 *quater* c.p. (in tema di danneggiamento di sistemi informatici o telematici) prevede la diversa ipotesi del danneggiamento mediante introduzione o trasmissione di dati, informazioni o programmi.

(23) Così M. Mantovani, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica al Diritto*, 1994, 12 ss. *Contra*, G. Corrias Lucente, *op. cit.*, 499, perché si tratta di un requisito non espressamente previsto dalla fattispecie incriminatrice. Conf. Trib. Gorizia, 19 febbraio 2003, n. 601, Merini, in *Riv. pen.*, 2003, 896, secondo cui la tutela della legge - premesso che non si riguarda solo i contenuti personalissimi dei

(segue)

chi nella riservatezza dei dati e dei programmi contenuti in un sistema informatico dal pericolo di aggressione da parte di terzi non autorizzati (24) (con la conseguenza che rimarrebbero al di fuori dell'area applicativa della norma *de qua* sia i sistemi privi di dati e misure di sicurezza, sia quelli che contengono soltanto dati o programmi di pubblico dominio); chi, ancora, nella indisturbata fruizione del sistema stesso (25). Conseguentemente, secondo queste diverse tesi il mero accesso *invito domino* al sistema informatico non sarebbe di per sé sufficiente ad integrare il delitto in esame, occorrendo a tal fine anche la messa in pericolo o la lesione dell'integrità dei dati e dei sistemi informatici, ovvero della riservatezza degli stessi ovvero ancora del funzionamento del sistema (26).

Certamente tali teorie (27), nella loro diversità, hanno in comune il pregio di circoscrivere l'ambito del reato in misura più ossequiosa rispetto al principio di offensività; nondimeno esse non appaiono in grado di fornire un'interpretazione che possa essere unanimemente accolta, in quanto - si pensi ad esempio al pur condivisibile orientamento che pone in primo piano il diritto alla riservatezza del titolare del sistema, ovvero a quello volto a tutelare la libera fruizione del dispositivo informatico - sono ricavabili soltanto implicitamente dal dato letterale della norma in esame. Occorrerebbe pertanto un intervento chiarificatore da parte del legislatore che introducesse espressamente un discrimine circa la natura delle informazioni captate attraverso l'illecita introduzione ovvero in ordine al tipo di sistemi oggetto di accesso abusivo, così da escludere la sfera di operatività del delitto *ex art. 615 ter c.p.* nelle ipotesi quali quella oggetto della pronuncia in commento, al di là (e prima ancora) di ogni accertamento (presuntivo) sulla consapevolezza di agire *invito domino*.

3. Le differenze soggettive in tema di mantenimento abusivo nel sistema informatico

Si è detto che il G.U.P. di Nola ha affermato nella pronuncia annotata che il soggetto attivo del reato di "mantenimento abusivo" di cui all'*art. 615 ter c.p.* può essere non solo l'*extraneus*, ma anche chi, autorizzato (stabilmente) all'uso del *computer*, abusando della sua posizione operi per scopi personali.

Per quanto la Cassazione ed i giudici di merito abbiano in prevalenza affrontato la questione della "permanenza *invito domino*" con riferimento ai terzi (in particolare, ai c.d. *hackers*) ed ai soggetti non organici all'Ente o alla società titolare del sistema che in via eccezionale e temporanea sono abilitati all'introduzione nell'elaboratore altrui (28), anche il tema del "dipendente" (di Società o Ente) che usa a fini *lato sensu* personali il sistema informatico aziendale è già noto alla giurisprudenza, la quale lo include tra i possibili soggetti attivi del delitto *ex art. 615 ter c.p.* Ad esempio, in una pronuncia che ha riguardato un caso per molti versi simile a quello in esame, la suprema Corte ha ravvisato il reato di accesso abusivo ad un sistema informatico a carico di un ufficia-

le di polizia giudiziaria che, pur essendo astrattamente abilitato ad accedere al Centro elettronico di documen-

Note:

(segue nota 23)

dati raccolti nei sistemi informatici protetti - estende perciò anche agli aspetti economico-patrimoniali dei dati.

(24) In questo senso, C. Pecorella, *sub art. 615 ter c.p.*, in G. Marinucci-E. Dolcini (a cura di), *Codice penale commentato*, Milano, 2006, 4323, la quale ritiene che la norma in commento si riferisca ai soli "sistemi informatici destinati alla raccolta di dati, dal momento che nessuna esigenza di tutela della riservatezza si pone di regola nei confronti di possibili intrusioni in sistemi informatici predisposti esclusivamente alla erogazione di beni o alla prestazioni di servizi". *Contra*, Cass., 4 ottobre 1999, Pier-santi, cit. (relativo alla condotta di alcuni dipendenti di una società di telefonia che erano riusciti fraudolentemente ad eludere il blocco del centralino per le chiamate internazionali, così - per motivi di lucro - introducendosi abusivamente in una linea telefonica) e R. Flor, *Sull'accesso abusivo ad un sistema informatico e telematico: il concetto di "domicilio informatico" e lo ius excludendi alios*, in *Dir. pen. proc.*, 2005, 92, secondo cui "quando il legislatore ha avuto intenzione di tutelare la *privacy* vi ha fatto riferimento espresso e inequivocabile". Anche G. Pica, *op. cit.*, 42, sostiene in senso critico che questa impostazione comporterebbe un sindacato di merito sulla qualità dei dati "sterile, odioso e opinabile", mentre F. Resta, *Banche di dati on line. I limiti della tutela penale* in *Giur. mer.* 2007, 370, sottolinea come lo spettro di tutela della fattispecie si estenda al di là della garanzia della segretezza delle informazioni e della inviolabilità del domicilio, stante l'assenza nella norma di alcun riferimento al carattere personale o privato dei dati contenuti nel sistema. Sul punto si vedano altresì Fondaroli, *La tutela penale dei beni informatici*, in *Diritto dell'informazione e dell'informatica*, 1996, 311, e Nunziata, *Il delitto di "accesso abusivo ad un sistema informatico o telematico"*, 1996, 48.

(25) F. Berghella-R. Blaiotta, *Diritto penale dell'informatica e beni giuridici tradizionali*, in *Cass. pen.*, 1995, 2331.

(26) Per S. Aterno, *Sull'accesso abusivo ad un sistema informatico e telematico*, in *Cass. pen.*, 2000, 2996, l'*art. 615 ter c.p.* avrebbe una duplice funzione incriminatrice: "una funzione autonoma, relativa alle condotte di indiscrezione e accesso a sistemi informatici e telematici, ed una funzione secondaria e sussidiaria delle residue ipotesi di introduzione non rientranti nelle norme del 1993 e, in particolare, dell'introduzione-furto di servizi informatici e telematici, che altrimenti resterebbe impunito", da cui ne discende secondo questo A. la qualificazione come reato di danno e non di pericolo, concretandosi nella effettiva lesione del diritto alla riservatezza dei dati memorizzati nei sistemi informatici. Sul fatto che il delitto di accesso abusivo ad un sistema informatico si perfezioni con la violazione del domicilio informatico, senza che sia necessario anche che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi un'effettiva lesione degli stessi, v. da ultimo, C. cass., 6.2.07 n. 11689, in *CED Cass.*, rv 236221.

(27) In senso critico rispetto alle tesi secondo cui oggetto della tutela sarebbero rispettivamente l'integrità del sistema o dei dati ovvero la loro riservatezza è G. Corrias Lucente, *op. e loc. cit.*. Questa A. (la quale ritiene che, in via di principio, "le conseguenze, realizzate o soltanto volute, ovvero la natura dei dati contenuti nel sistema e persino l'esistenza degli stessi non si pongono dunque come criterio discriminatorio dell'accesso abusivo penalmente rilevante", 500) sottolinea come la prima tesi finisca per introdurre un ulteriore requisito per la configurabilità del reato, non espressamente previsto dalla fattispecie incriminatrice ("la distruzione di dati e programmi costituisce una conseguenza che lo stesso legislatore segnala meramente occasionale, la cui realizzazione resta estranea all'oggettività e persino al dolo tipico della fattispecie semplice").

(28) Ad esempio il programmatore che, legittimato all'accesso per controllare la funzionalità di un programma informatico, si avvale dell'autorizzazione per copiare i dati da esso gestiti, oppure l'impiegato che, dovendo effettuare in via occasionale o temporanea un lavoro tramite il *computer* dell'Amministrazione contabile, ne approfitta per spiare le "buste paga" dei colleghi. Sul primo caso, v. Cass., sez. V, 7 novembre 2000, Zara, in *Cass. pen.*, 2002, 1017. In dottrina, v. C. Pecorella, *op. cit.*, 351.

tazione del Ministero dell'Interno, vi sia entrato "abusivamente", per un fine meramente privato, quale quello di verificare il possesso legittimo di armi da parte di un proprio vicino di casa" (29).

Si tratta ora di verificare la validità di questo assunto, alla luce delle perplessità manifestate da una parte autorevole della dottrina che ha ravvisato come l'art. 615 *ter* c.p. dia "apparentemente rilevanza solo agli abusi realizzati da *outsider*, ovvero da *insider* privi di qualsivoglia autorizzazione all'uso dell'elaboratore" (30). A questo fine occorre anzitutto brevemente rammentare che la configurabilità del reato in esame è subordinata:

– all'introduzione abusiva all'interno di un sistema informatico e, dunque, al superamento delle barriere (logiche o fisiche) che ostacolano l'interazione con l'elaboratore. Il carattere abusivo dell'accesso (31) attiene invero a tutti i casi in cui esso "non sia accompagnato dal consenso del titolare dello *ius excludendi*, né facoltizzato o imposto dalla presenza di un'altra causa di giustificazione";

– al mantenimento all'interno del sistema informatico contro la volontà espressa o tacita di chi ha il diritto di escluderlo (32). Questa fattispecie è "alternativa" (33) rispetto a quella della abusiva introduzione, presupponendo, al contrario, la legittimità dell'accesso da parte dell'agente, vuoi perché autorizzato vuoi perché casuale, alla quale segue l'illecito trattarsi *invito domino*;

– alla presenza di misure di sicurezza (34), necessaria non solo nell'ipotesi di introduzione abusiva, ma anche in quella di mantenimento illecito nel sistema informatico, tanto che, come si vedrà, la permanenza non autorizzata del dipendente nell'"area comune" del computer non è sotto questo profilo penalmente rilevante. Ciò è di particolare importanza, considerato che un sistema può contenere tanti "domicili informatici protetti" quante sono le persone che, in virtù della chiave d'accesso a ciascuna di esse attribuite, abbiano a disposizione uno spazio virtuale entro il quale memorizzare dati personali, interdetti a terzi (35).

Orbene, è da dire che in effetti il testo della disposizione in esame fa riferimento unicamente alle ipotesi di accesso abusivo al "sistema informatico" nel suo complesso (sempre che questo sia protetto da misure di sicurezza) e non già ad una parte soltanto "della sua memoria interna", con ciò oltre tutto differenziandosi dalle omologhe norme dei vari Paesi europei, germinate dalla medesima Raccomandazione comunitaria del 1989 (36). È evidente che ciò, quanto meno in astratto, consenta di operare una distinzione tra la posizione del soggetto esterno all'azienda (37), che si trovi ad

illecitamente nel sistema non sembra invece doversi fare rientrare l'ipotesi (su cui Cass., 14.10.03, p.m. in proc. Muscia, in *Foro it.*, 2004, II, 582) del titolare di un esercizio commerciale che, in concorso con un cliente, abbia utilizzato il terminale in sua dotazione per effettuare operazioni commerciali tramite una carta di credito contraffatta: le modalità della condotta attestano che questo consiste in un caso di vera e propria introduzione abusiva nel sistema informatico (lo stesso varrebbe per il dipendente che pur autorizzato usasse la *password* di un collega - al fine di non farsi riconoscere - per accedere al sistema).

(30) C. Pecorella, *Diritto penale dell'informatica*, cit., 342. Peraltro, come si dirà *infra*, questa A. ritiene che a determinate condizioni sia configurabile il reato *ex art.* 615 *ter* c.p. a carico del dipendente di società o Ente autorizzato all'uso del sistema informatico.

(31) In giurisprudenza è stato specificato che per l'abusività dell'accesso non è necessaria l'effrazione delle misure protettive purché la condotta dell'agente risulti rivestita da altri connotati (anche tra loro eterogenei) che la caratterizzano: in tal senso, Trib. Gorizia, 19 febbraio 2003 n. 601, Merini, in *Riv. Pen.*, 2003, 895, con nota di A. Tarlao, *Accesso abusivo e sistema informatico: natura delle norme di protezione*. Definisce l'ingresso "assolutamente abusivo" quando il titolare del diritto non abbia in alcun modo autorizzato o abbia revocato una precedente autorizzazione ad intramettersi nel sistema e "relativamente abusivo" quando l'ingresso avvenga da parte di persone che operino con finalità non condivise e al di fuori del contesto temporale per il quale sono state autorizzate dall'avente diritto, D. Lusitano, *In tema di accesso abusivo a sistemi informatici o telematici*, in *Giur. it.*, 1998, 1923.

(32) Qualifica come condotta commissiva, e non omissiva, l'ipotesi dell'abusivo mantenimento nel sistema, poiché "la struttura della norma è incentrata sul volontario mantenimento dell'accesso nonostante il divieto, espresso o tacito, del titolare" G. Pica, *Diritto penale delle tecnologie informatiche*, 1999, 41 s.. Si veda anche L. Cuomo, *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, 2998 ss., il quale afferma che "ciò che in realtà si punisce attraverso tale modalità di condotta è l'uso dell'elaboratore più che l'accesso ad esso".

(33) Secondo R. Flor, *Sull'accesso abusivo*, cit., 90, nota 28, non è ammissibile il concorso materiale tra le due condotte perché il mantenimento abusivo si configura solo se è stato effettuato un accesso, lecito o illecito, al sistema. In senso conforme, C. Pecorella, *op. cit.*, 348, la quale sostiene che la permanenza abusiva ha come presupposto che l'introduzione sia avvenuta per caso o comunque in modo lecito. *Contra*, G. Pica, *op. cit.*, 57 secondo cui il "mantenimento" nella maggior parte dei casi rappresenta il "naturale ulteriore sviluppo dell'introduzione abusiva".

(34) Secondo parte della giurisprudenza questo requisito avrebbe, peraltro, la sola funzione di specificare il dissenso da parte del titolare, per cui sarebbe irrilevante l'esistenza di meccanismi di protezione informatica laddove il dissenso del titolare del sistema sia noto all'agente. In questo senso, cfr. Cass., sez. V, 7 novembre 2000 n. 1675, Zara e altri, cit.; Trib. Gorizia 19 febbraio 2003, in *Riv. Pen.*, 2003, 891. In dottrina, conforme è D'Aiotti, *La tutela dei programmi e dei sistemi informatici*, in Boruso e altri, *Profili penali dell'informatica*, Milano, 1994, 72. Non è invece condivisibile G.i.p. Trib. Roma, 4 aprile 2000, G.C., in www.penale.it/page.asp?mode=1&IDpag=86, circa la presunta necessità che i mezzi di protezione non solo esistano, ma siano anche efficaci. Sul punto, v. altresì Trib. Milano, sez. III, 12 dicembre 2006, est. Mambiani, in *Giur. mer.*, 2007, 370, con nota di F. Resta, *Banche di dati on line. I limiti della tutela penale*.

(35) Così, R. Flor, *Identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. It. Dir. Proc. pen.*, 2007, 931, secondo cui titolare dello *ius excludendi* potrebbe essere anche un lavoratore dipendente o un collaboratore nei limiti del contratto di lavoro.

(36) Si veda C. Pecorella, *Il diritto penale dell'informatica*, Padova, 2000, 311 s., la quale cita tra gli altri l'art. 138 lett. a del codice olandese, l'art. 323-1 del nuovo codice penale francese e la Section I del Computer Misuse Act 1990, le cui disposizioni si incentrano direttamente sull'accesso abusivo ai dati ed ai programmi contenuti nel sistema informatico violato.

(37) Nessun dubbio sul fatto che l'*extraneus* che violi le misure di sicurezza e non sia autorizzato alla permanenza nel sistema informatico risponda (segue)

Note:

(29) Cass., sez. V, 19 dicembre 2001 n. 7041, Corrao, in *Guida al diritto*, 2002, 18, 72. Da notare che, a differenza del GUP di Nola, la Cassazione qualifica il fatto come "introduzione abusiva" e non come "mantenimento *invito domino*". Alla categoria del soggetto autorizzato che si mantiene

avere un contatto saltuario con l'elaboratore, e quella del dipendente che tale elaboratore sia tenuto ad utilizzare quotidianamente per lo svolgimento del proprio lavoro: soltanto nel primo caso infatti è ravvisabile una preclusione all'accesso al sistema informatico in quanto tale (superabile soltanto grazie all'estemporanea autorizzazione del titolare), mentre al dipendente è eventualmente vietato soltanto l'accesso a determinate funzioni o a particolari informazioni contenute all'interno di esso.

Tuttavia va notato che l'art. 615 *ter* c.p. (38) nella sostanza prevede due forme di tutela complementari, intendendo punire sia (nella prima parte del comma 1) le condotte di abusiva introduzione, sia (nella seconda parte dello stesso comma) quelle che, se non fossero avvenute per caso o sulla base di un'autorizzazione iniziale, avrebbero integrato gli estremi dell'"introduzione abusiva" in un sistema informatico protetto (39).

È dunque da ritenere - conformemente all'orientamento prevalente (40) - che il "dipendente" sarà penalmente responsabile unicamente allorché penetri indebitamente in zone riservate (cioè protette da autonome misure di sicurezza) (41), ovvero quando, una volta entrato nel sistema, compia operazioni di natura del tutto diversa da quelle per il compimento delle quali egli è autorizzato ad accedere ad esso (è il caso del soggetto incaricato dell'inserimento dati che scarichi dei *files* dall'*hard disk*). In nessuna delle due ipotesi, infatti, il dipendente potrebbe addurre a giustificazione del proprio accesso al sistema informatico protetto la legittimazione all'uso dello stesso: nel primo caso perché egli comunque non potrebbe accedere ai dati riservati (in quanto protetti) senza uno speciale codice d'accesso (42); nel secondo in quanto tali operazioni esulano qualitativamente dal rapporto di lavoro (43).

Non pare invero che da questa impostazione derivino più o meno pericolosi vuoti di tutela, (44) atteso che le condotte del dipendente estranee all'area di operatività della norma in esame (ad esempio perché poste in essere in un sistema privo di misure di sicurezza o relative a dati non riservati) potranno eventualmente rientrare, ricorrendone i presupposti, nelle fattispecie di peculato d'uso (art. 314 c.p.), abuso d'ufficio (art. 323 c.p.) (45), frode informatica (art. 640 *ter* c.p.) danneggiamento di sistemi informatici (art. 635 *bis* c.p.), intercettazioni di comunicazioni telematiche (art. 617 *quater* c.p.) o nelle nuove figure di reato in via di approvazione tramite la legge di conversione e ratifica della Convenzione di Budapest sulla cybercriminalità (es. artt. 635 *ter* e *quater* c.p.).

4. La consapevolezza della contraria volontà del titolare del sistema informatico

Quanto infine all'elemento soggettivo del reato di cui all'art. 615 *ter* c.p., sulla base del quale, nel caso in esame, l'imputato è stato prosciolto (avendo il giudice

Note:

(segue nota 37)

del reato di cui all'art. 615 *ter* c.p., sia nell'ipotesi di accesso "da lontano" (ovvero per via elettronica, è il caso dei c.d. pirati informatici), sia di introduzione "da vicino" (cioè a diretto contatto con l'elaboratore). Al terzo deve peraltro essere equiparato il dipendente che, pur autorizzato ad accedere al sistema informatico, utilizzi fraudolentemente la *password* di un collega o comunque forzi i codici di accesso.

(38) Si veda D. Trentacapilli, *Accesso abusivo ad un sistema informatico ed adeguatezza delle misure di protezione*, in *Dir. pen. proc.*, 2002, 1285, nt. 24.

(39) Secondo Cass., 7 novembre 2000, Zara, cit., la ragione per cui integra la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa, e quindi non rispetti le condizioni alle quali era subordinato l'accesso "è da rinvenire nell'analogia tra questa norma e la fattispecie della violazione di domicilio".

(40) F. Mucciarelli, *Commento all'art. 4 L. 23.12.1993 n. 547*, in *Leg. pen.*, 1996, 100; C. Pecorella, *op. e loc. ult. cit.*; R. Flor, *Sull'accesso abusivo*, cit., 90, il quale sottolinea che le misure di sicurezza, anche se inadeguate, devono essere percepibili e che legislatore italiano "non ha chiaramente accolto tutte le indicazioni del Consiglio d'Europa, ritenendo non dotato di sufficiente lesività il mero utilizzo non autorizzato di un elaboratore", non punendo neppure "il c.d. furto di tempo, derivante dall'uso indebito dell'elaboratore".

(41) Così, Cass., sez. VI, 27 ottobre 2004, n. 46509, in <http://www.penale.it/page.asp?mode=1&IDPag=174>, relativa anch'essa all'appropriazione da parte di un dipendente pubblico del computer dell'ufficio per finalità personali, secondo cui non è ravvisabile la condotta contestata laddove il sistema informatico nel quale l'imputato si inseriva abusivamente non risulti obiettivamente protetto da misure di sicurezza "essendo anzi tale sistema a disposizione dell'imputato in virtù delle mansioni affidategli per ragioni d'ufficio. Il fatto che [l'imputato] ne facesse un uso distorto a fini illeciti e personali, non sposta i termini della questione, mancando il presupposto della 'protezione speciale del sistema stesso. Da tale reato pertanto l'imputato deve essere assolto perché il fatto non sussiste". Di particolare rilievo è altresì Trib. Rovereto, cit., pag. 84, che ha assolto il soggetto che si era limitato ad accedere ad una parte del sistema informatico comune a tutti i dipendenti dell'impresa, cui era anch'egli autorizzato, ove per errore o per condotta illecita di terzi erano stati collocati dati riservati del titolare, che l'imputato aveva duplicato e scaricato. In ogni caso deve esservi la prova che l'agente sia effettivamente penetrato nella zona vietata, neutralizzando le misure di sicurezza, non essendo sufficiente ai fini della configurabilità del reato che abbia preso visione (o duplicato) dati personali trascinati da terzi per errore nell'area comune (v. C. cass., sez. V, 15.2.07 n. 6459, in CED Cass., rv 236049).

(42) M.A. Alma-c. Perroni *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997, 505. Si veda altresì Trib. Viterbo, sez. Montefiascone, 5 luglio 2005, in *Giur. mer.*, 2006, 2394, secondo cui, condivisibilmente, al fine di considerare abusivo l'accesso al sistema informatico non è sufficiente che l'operatore entri in un'area posta al di fuori della sua competenza, essendo necessaria la presenza di finalità diverse (cioè interessi personali o di terzi, cioè per interessi assolutamente estranei all'istituto o all'Ente di appartenenza, ovvero vi sia una specifica previsione normativa che faccia divieto all'operatore di un istituto bancario di accedere in un particolare settore: nella specie un operatore di un istituto bancario addetto all'area rischi era più volte entrato nell'area titoli).

(43) Fermo restando che, come illustrato *sub* par. 2, la configurabilità del reato è comunque subordinata al tipo di informazioni che il soggetto intendeva captare (o ha effettivamente captato).

(44) Secondo R. Flor, *Sull'accesso abusivo*, cit., 92, la presa di conoscenza o duplicazione di dati altrui può eventualmente venire in considerazione, sussistendone i presupposti, in relazione agli illeciti previsti dalla legge sulla tutela della *privacy*, che ha un distinto ambito di operatività.

(45) Per il caso del dipendente di un ente pubblico, che aveva patteggiato la pena per i reati ex artt. 314, 323 e 640 c.p. perché nell'orario di lavoro si era numerose volte collegato a siti internet non istituzionali, v. C. Sarzana di Sant'Ippolito, *L'accesso illecito alle banche dati ed ai sistemi infor-*

ritenuto che questi non avesse avuto probabilmente contezza della tacita volontà contraria dell'Agenzia delle Entrate, titolare del sistema, a che il primo curioso (sulle anagrafe tributaria) si può osservare quanto segue.

Dottrina e giurisprudenza ritengono che ai fini della configurabilità del delitto in esame, sia sufficiente il dolo generico (46), che consiste nella volontà di introdursi o mantenersi all'interno del sistema informatico, con la consapevolezza (rispettivamente) dell'abusività dell'accesso o della volontà contraria, sia pur tacita, del titolare del sistema (47). Secondo alcuni Autori sarebbero irrilevanti, sotto questo profilo, sia le finalità, lecite o illecite, perseguite dall'agente, sia "la natura dei dati contenuti nel sistema e persino l'esistenza degli stessi" (48). In realtà, con riferimento all'ipotesi del dipendente (o più in generale del soggetto autorizzato all'uso del sistema informatico) è da ritenere che proprio lo scopo dell'accesso, insieme ad altri elementi (49), serva a qualificare la natura abusiva dell'introduzione ovvero la consapevolezza in ordine al dissenso del titolare del sistema (50) (si pensi ad esempio al tecnico che, rilevato un *virus* nelle "cartelle" di uso comune, provveda a fare delle verifiche anche nelle "sottocartelle" personali).

Nell'ipotesi del "mantenimento nel sistema informatico" è peraltro necessario accertare sia l'esistenza della contraria volontà del titolare (che, per espresso disposto dell'art. 615 *ter*, comma 1, c.p., può essere anche tacita) sia la conoscenza di tale dissenso in capo all'agente e la sua volontà di permanere nel sistema *invito domino*. Al riguardo, è anzi opportuno sottolineare che il dissenso del titolare non può in ogni caso "essere desunto dalla sola presenza di misure di sicurezza (*password*, *i-code*) la cui rimozione sia indispensabile per accedere ai dati" (51), tanto più che nel caso del dipendente queste - pur esistenti - potrebbero anche non operare (52).

Al fine di evitare pericolosi equivoci, sarebbe anzi opportuno (o, meglio, necessario) che le società, gli enti e più in generale le strutture che utilizzino sistemi informatici condivisi indicassero con chiarezza - all'atto dell'assunzione o con circolari o regolamenti interni portati a conoscenza dei destinatari - l'area delle informazioni o delle attività precluse ai dipendenti, fermo naturalmente restando che per i dati sensibili dovrebbero *a contrario* essere specificate le condizioni alle quali i dipendenti possano eventualmente accedervi (53).

5. Considerazioni conclusive

Alla luce di quanto sin qui illustrato, non sembra pertanto condivisibile l'orientamento - sorto anche per effetto dell'"infelice formulazione" dell'art. 615 *ter* c.p. - circa l'assoluta irrilevanza, ai fini della configurabilità di questo reato, della natura (riservata o meno) delle informazioni captate all'interno del sistema informatico: si

tratta invece di un discrimine necessario per evitare possibili violazioni principio di offensività, ravvisabili lad-

Note:

matici pubblici: profili giuridici, in *Dir. inf.*, 2007, 276 ss.

(46) Cfr., per tutti, C. Pecorella, *sub art.* 615 *ter*, cit., 4329. V. però Trib. Torino, 4 dicembre 1997, Zara, in *Giur. It.*, 1998, 1923.

(47) Si è sopra detto che, ad esempio nel caso di *computer* aziendali, vi possono essere anche più titolari del sistemi, quanti sono le persone che all'interno di essi hanno un proprio spazio personale, munito di chiave di accesso. Sul punto v. R. Flor, *Identity theft e identity abuse*, cit., 931.

(48) G. Corrias Lucente, cit., 500. In senso conforme, v. F. Mucciarelli, *op. cit.*, 100. Come si è sopra illustrato, è però da ritenere che "la natura dei dati contenuti nel sistema" dovrebbe rilevare sotto il profilo del bene giuridico tutelato dall'art. 615 *ter* c.p.

(49) Con riferimento all'abusività dell'accesso è stato detto che occorre valutare "la natura e la finalità dell'accesso, l'idoneità dell'intervento a ledere o porre in pericolo gli obiettivi ai quali era strumentale la protezione del sistema e dei dati in esso residenti, nonché l'esistenza o meno per l'agente, tenuto conto delle di lui eventuali funzioni rivestite in seno all'organizzazione titolare del sistema protetto, di divieti o limiti a conoscere o a utilizzare i contenuti dell'area informatica visitata, che siano stati violati mediante la realizzata condotta", così Trib. Gorizia, 19 febbraio 2003 n. 601, Merini, in *Riv. Pen.*, 2003, 895 (caso in cui il reato è stato ritenuto insussistente perché la condotta era inidonea a ledere gli interessi protetti e poiché l'imputato aveva titolo a conoscere ed utilizzare i dati captati). Conforme è Trib. Bologna, 21 luglio 2005, C.F. e C.S., in *Giur. mer.*, 2006, 5, 246, secondo cui a questo scopo occorre considerare "la natura, le finalità e le modalità della condotta, volte ad aggirare lo *ius prohibendi* del titolare".

(50) Secondo R. Flor, *Sull'accesso abusivo*, cit., 90, se l'agente accede al sistema tramite la propria *password* visualizzando tranquillamente una specifica cartella (o *file*) situata in una parte comune del sistema, priva o apparentemente priva di misure protettive, non ha la percezione della possibile contraria volontà del titolare della cartella medesima o del sistema rispetto al proprio accesso, essendo indifferente la natura dei dati e delle informazioni ivi archiviate.

(51) Così, A. Cisterna, *op. cit.*, 79. In senso conforme, C. Pecorella, *op. ult. cit.*, 4328, che sottolinea come il dissenso dell'avente diritto sia un elemento costitutivo del fatto tipico, la cui assenza impedisce che si realizzi la fattispecie oggettiva del reato.

(52) Secondo Cass., 7 novembre 2000, Zara, cit., anche in mancanza di meccanismi di protezione informatica commette il reato la persona estranea all'organizzazione che acceda ai dati senza titolo o autorizzazione, essendo implicita, ma intuibile la volontà dell'avente diritto di escludere gli estranei.

(53) È da segnalare favorevolmente in questa direzione il Provvedimento del Garante della Privacy 1 marzo 2007 ("Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte di lavoratori. Linee Guida del Garante per posta elettronica e internet"), in *Dir. inf.*, 2007, 455 ss., diretto ai datori di lavoro, in cui si afferma che è opportuno che questi ultimi adottino un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente, che comprende tra l'altro "in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle, oppure ricorrendo a sistemi di webmail, indicando le modalità e l'arco temporale di utilizzo (ad es. fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro, punto 3.2 "linee Guida"), così come è opportuno che i medesimi appongano misure di sicurezza volte sia a ridurre usi impropri della navigazione via internet sia ad evitare controlli successivi sui lavoratori (punto 5.2 "principio di necessità"). In merito alle problematiche giuridiche relative all'uso delle apparecchiature informatiche da parte dei pubblici dipendenti, v. anche C. Sarzana di Sant'Ippolito, *L'accesso illecito alle banche dati ed ai sistemi informatici pubblici: profili giuridici*, in *Dir. inf.*, 2007, 276 ss.

dove si perseguissero condotte (quali quella oggetto della pronuncia *ex art. 425 c.p.p. in commento*) prive di rilievo sociale.

Sarebbe anzi auspicabile in questo settore l'intervento del legislatore, volto a selezionare con maggiore chiarezza i comportamenti di illecita intrusione nei sistemi informatici protetti (con particolare riguardo all'uso indebito del *computer* aziendale da parte dei lavoratori), sulla scia dell'orientamento restrittivo adottato negli ordinamenti comunitari, fermi restando gli eventuali profili di responsabilità amministrativa e disciplinare (54).

Note:

(54) La stessa opinione, con riferimento ad un'altra fattispecie incriminatrice, è espressa da C. Sarzana di Sant'Ippolito, *op. cit.*, 292, secondo cui "è da riesaminare l'inquadramento tradizionale dell'ipotesi di abuso nell'ambito penalistico per evitare soluzioni giurisprudenziali oggettivamente inique di fronte alla scarsa rilevanza della condotta" (l'A. propone infatti di depenalizzare le ipotesi non gravi di uso privato degli strumenti tecnologici di ogni tipo da parte dei pubblici dipendenti, prevedendo una sanzione amministrativa).

LIBRI



Collana: **Formulari ragionati**

Formulario del processo penale

Con schemi di dottrina e CD-Rom allegato

Di Fulvio Baldi, Ilaria Ciarniello e Simone Luerti

L'opera riporta in modo sistematico le **formule** relative ai più importanti **atti** del procedimento penale:

- le formule sono precedute da una **trattazione d'autore che inquadra ogni singolo istituto** e che consente di individuare con facilità e con la massima precisione all'interno del processo.
- per una più immediata contestualizzazione è previsto l'ulteriore ausilio, ove necessario, di appositi **schemi di dottrina**.
- il CD-ROM allegato contiene **297 formule** utilizzabili con qualunque sistema di

videoscrittura ed adattabili al caso specifico, e il testo del **Codice di procedura penale** aggiornato con la **L. 48/2008**, cd. "**Criminalità informatica**".

Ipsoa 2008, Euro 58,00

Per informazioni e acquisti

- **Servizio Informazioni Commerciali** (tel. 02.82476794 – fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- <http://ipshop.ipsoa.it>

Appalto

Procedura di gara e annotazione nel casellario informatico per la mancata dimostrazione del possesso dei requisiti dichiarati

T.A.R. LAZIO, ROMA, Sez. III, 1 aprile 2008, n. 2773 - Pres. Baccharini - Est. Sapone - Impresa Ingegnere Alberto Fagotti s. r. l. c. Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture ed Agenzia delle Entrate di Perugia e Comune di Castiglione del Lago (accoglie)

Appalti - Verifica a campione - Obbligo di comprovare i requisiti dichiarati in gara - Annotazione nel casellario informatico - Illegittimità - Violazione di legge - Necessità della preventiva adozione del provvedimento di esclusione

(d.lgs. 12 aprile 2006, n. 163; direttiva CEE 2004/17; direttiva CEE 2004/18; determinazione dell'Autorità per la Vigilanza sui Lavori Pubblici 6 maggio 2003; d.P.R. 25 gennaio 2000, n. 34)

Ai sensi dell'art. 48, comma 1, del d.lgs. n. 163/2006 il provvedimento di esclusione del concorrente dalla gara per mancanza dei requisiti di partecipazione alla stessa rappresenta il presupposto logico necessario per poter procedere all'escussione della cauzione provvisoria e alla successiva segnalazione del fatto all'Autorità per di Vigilanza. Ne consegue che è illegittima la sanzione accessoria dell'annotazione nel casellario informatico di un'impresa quando tale determinazione non sia preceduta da un provvedimento di esclusione del destinatario da un affidamento antecedente in specie perché non siano stati dimostrati i requisiti richiesti nel termine perentorio di dieci giorni dal ricevimento della comunicazione successiva al sorteggio preliminare.

Omissis...

Fatto

Con il proposto gravame la srl Impresa Ingegnere Alberto Fagotti ha impugnato l'annotazione nel casellario informatico, disposta dalla resistente autorità sulla base della segnalazione inviata dal Comune di Castiglione del Lago, in cui è stato fatto presente che in sede di accertamenti dei requisiti in capo alla società ricorrente, la quale aveva partecipato alla gara indetta dalla citata amministrazione comunale per l'affidamento dei lavori di realizzazione dell'intersezione viaria tra la S. S. 72 e Via F.lli Rosselli classificandosi al secondo posto della relativa graduatoria, è risultata a carico della stessa una violazione definitivamente accertata rispetto agli obblighi relativi al pagamento delle imposte e tasse, così come attestato dalla certificazione prot. 18856 del 16/2/2007 dell'Agenzia delle Entrate di Perugia.

Il ricorso è affidato al seguente ed articolato motivo di doglianza:

Violazione e falsa applicazione degli artt. 38 e 48 del

d.lgs. n. 163/2006 e della determinazione dell'Autorità per la Vigilanza sui Lavori Pubblici del 6 maggio 2003, nonché dell'art. 27 d.p.r. 25 gennaio 2000 n. 34. Eccesso di potere manifesto per assenza dei presupposti e difetto di istruttoria. Infondatezza e manifesta violazione del giusto procedimento.

Si sono costituite sia l'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture sia l'Agenzia delle Entrate di Perugia prospettando l'improcedibilità del proposto gravame e contestando nel merito la fondatezza delle dedotte doglianze.

Alla pubblica udienza del 5 marzo 2008 il ricorso è stato assunto in decisione.

Diritto

In via preliminare deve essere esaminata l'eccezione con cui le resistenti amministrazioni hanno prospettato l'improcedibilità del proposto gravame atteso che, come si evince dalla nota del 21 gennaio 2008 dell'intimata Autorità, versata agli atti, la suddetta Autorità ha provveduto alla cancellazione della contestata annotazione.

La sollevata eccezione non è suscettibile di favorevole esame in quanto la cancellazione ha efficacia *ex nunc*, e quindi in relazione al periodo antecedente la data in cui è stata effettuata, ben può ritenersi sussistente un interesse in capo all'odierna ricorrente ad ottenerne l'annullamento.

Nel merito risulta fondata la doglianza con cui è stata contestata la legittimità della gravata annotazione in quanto assunta sulla base della comunicazione della stazione appaltante ed in assenza della previa adozione da parte di quest'ultima di un provvedimento di esclusione.

Al riguardo è sufficiente richiamare l'art. 48 del d.lgs. n. 163/2006, il cui primo comma prevede che "Le stazioni appaltanti prima di procedere all'apertura delle buste delle offerte presentate, richiedono ad un numero di offerenti non inferiore al 10 per cento delle offerte presentate, arrotondato all'unità superiore, scelti con sorteggio pubblico, di comprovare, entro dieci giorni dalla data della richiesta medesima, il possesso dei requisiti di capacità economico-finanziaria e tecnico-organizzativa, eventualmente richiesti nel bando di gara, presentando la documentazione indicata in detto bando o nella lettera di invito.

Quando tale prova non sia fornita, ovvero non confermi le dichiarazioni contenute nella domanda di partecipazione o nell'offerta, le stazioni appaltanti procedono all'esclusione del concorrente dalla gara, all'escussione della relativa cauzione provvisoria e alla segnalazione del fatto all'Autorità per i provvedimenti di cui all'articolo 6 comma 11. L'Autorità dispone altresì la sospensione da uno a dodici mesi dalla partecipazione alle procedure di affidamento"

In tale contesto, quindi, nella fattispecie in esame è palese l'illegittimità dell'operato della stazione appaltante e di riflesso della resistente Autorità, atteso che è stata effettuata la contestata annotazione in assenza della previa adozione di un provvedimento di esclusione, che nella dinamica procedimentale di cui alla richiamata disposizione ne costituisce un presupposto essenziale.

Ciò premesso, il proposto gravame v'è accolto con assorbimento dell'altra doglianza dedotta.

Sussistono giusti motivi per compensare tra le parti le spese del presente giudizio.

...*Omissis*...

IL COMMENTO di Mattia Pani

L'annotazione nel casellario informatico da parte dell'Autorità per la vigilanza nei contratti pubblici rappresenta una sanzione particolarmente grave per le imprese. Per tale ragione, in considerazione delle conseguenze estreme cui può condurre non solo in termini di esclusione dalle gare ma anche di danno all'immagine, deve essere necessariamente preceduta da una motivata attività istruttoria che ne giustifichi l'adozione ed in mancanza della quale alcuna determinazione preclusiva potrà essere legittimamente disposta.

1. Il contesto di riferimento

Negli ultimi anni la materia dei contratti della pubblica amministrazione ha visto la definitiva affermazione dei principi introdotti dai Trattati istitutivi delle Comunità Europee grazie all'adozione delle Direttive comunitarie n. 17 e 18 del 2004 (1). Queste ultime, in particolare, hanno il grande pregio di aver imposto la ricerca del miglior contraente per le stazioni appaltanti grazie a una esaltazione del principio fondamentale della più ampia partecipazione (2) di ogni impresa alle pubbliche gare, come estrinsecazione dell'interesse collettivo alla libera concorrenza (3), il quale richiede per una sua corretta

applicazione una forte sinergia con gli innovativi strumenti elettronici e telematici (4).

Note:

(1) R. Garofili, M. A. Sandulli, *Il nuovo diritto degli appalti pubblici nella direttiva 2004/18/CE e nella legge comunitaria n. 62 del 2005*, Milano, 2006, 562; R. De Nictolis, *La riforma del codice appalti*, in *Urbanistica e Appalti*, 3, 2007, 270 e *Le novità normative in materia di contratti pubblici di lavori, servizi e forniture*, in *Urbanistica e Appalti*, 9, 2007, 1061.

(2) La finalità della normativa comunitaria è, dunque, quella di garantire analoghe condizioni di competizione e accesso in tutti gli stati membri. In questo modo si cerca di rendere concreta l'apertura dei mercati, prima ristretta alle sole imprese nazionali e ora rivolta a tutti gli operatori degli stati membri. In tal senso si veda C. Galtieri, *Appalti Pubblici di Servizi*, in *Aa.Vv.*, Milano, 2002, 5.

(3) Ad esempio l'art. 28 del Trattato consacra il principio della libera circolazione delle merci. La Corte di Costituzionale italiana, sentenza 23 novembre 2007, n. 401, nel pronunciarsi in ordine al ricorso proposto da cinque regioni per l'illegittimità del d.lgs. n. 163/2006, ha richiamato la straordinaria importanza di tutti i principi comunitari in particolare di libera circolazione, di libertà di stabilimento e di libera prestazione. Si tratta dei cardini dell'intera materia contrattuale che devono sempre trovare la massima applicazione. Nello stesso senso si veda pure la "Comunicazione interpretativa della Commissione", del 1° agosto 2006, relativa al diritto comunitario applicabile alle aggiudicazioni di appalti non o solo parzialmente disciplinate dalle direttive "appalti pubblici".

(4) In particolare, ex art. 97 della Costituzione, si realizza nel rispetto dei tradizionali principi di imparzialità, buon andamento e legittimità dell'a-

(segue)

In tale prospettiva numerose sono state le modalità pratico-applicative di tipo informatico (5) che hanno consentito una più ampia conoscibilità dei bandi, una migliore speditezza delle procedure di gara e della documentazione integrativa oltretutto un miglior perseguimento dell'interesse pubblico attraverso l'individuazione di offerte di gran lunga più convenienti per la stazione appaltante.

Il riferimento si pone, principalmente, alla pubblicazione in rete della *lex specialis* e degli atti preliminari di gara così da renderli accessibili a tutti in tempo reale e senza costi né per il privato né per l'amministrazione procedente (6); in secondo luogo, poi, il richiamo è rivolto a tutte quelle disposizioni programmatiche che consentono un risparmio dei termini di pubblicazione, di invio e di trasmissione delle offerte ogni qual volta si faccia ricorso alle applicazioni telematiche (7); infine, il ricorso allo straordinario strumento delle aste elettroniche e, più in generale, a tutte le modalità elettroniche di scelta del contraente (8) consente di ottenere condizioni di aggiudicazione assolutamente più convenienti per la pubblica amministrazione (9).

Quanto sopra, pur rappresentandone solo una piccola parte, giustifica l'eccezionale attenzione che il legislatore comunitario ha riservato all'applicazione dei più innovativi strumenti informatici nelle pubbliche gare. Tale tendenza evolutiva, peraltro, evidenzia rappresenta un forte segnale di cambiamento rispetto all'impostazione di fondo che era stata data in Italia attraverso gli storici principi fissati dal Regio decreto 18 novembre 1923, n. 2440 (10). Le recenti timide aperture introdotte dal d.p.r. n. 101/2002 hanno, quindi, rappresentato solo un trampolino di lancio all'ingresso delle applicazioni elettroniche in tutte le fasi della procedura di scelta del contraente inderogabilmente imposta dal diritto comunitario.

Si tratta di una profonda rivoluzione procedurale che, necessariamente, rientra nel più ampio disegno di riforma delle pubbliche amministrazioni che passa attraverso una loro completa digitalizzazione (11).

L'obiettivo è quello di coniugare gli storici principi di economicità, efficienza ed efficacia, quali veicoli del buon andamento (12), con i principi di imparzialità e di trasparenza che consentono di raggiungere il migliore risultato per la pubblica amministrazione solo ove sia garantito un elevato livello di concorrenzialità in applicazione del principio della più ampia partecipazione.

Di conseguenza, nell'ambito di una più generale esigenza di informatizzazione e automazione completa delle amministrazioni pubbliche si pone anche il ricorso alle nuove tecnologie (13) che, pur essendo finalizzate alla semplificazione dell'*iter* burocratico-amministrativo verso l'esterno, non possono sacrificare o mettere in discussione le storiche garanzie offerte dai principi di certezza procedimentale imposti dalla legge n. 241/1990 (14).

In sostanza la ragionevolezza, logicità, coerenza del-

l'operato della pubblica amministrazione devono sempre essere dimostrate attraverso lo svolgimento di un'adeguata attività istruttoria preliminare indipendentemente dallo strumento cartaceo o elettronico utilizzato.

Per tali ragioni la sentenza del Tribunale Amministrativo regionale del Lazio che forma oggetto della presente nota assume primaria importanza in quanto, pur riconoscendo la straordinaria rilevanza degli strumenti di consultazione telematica nelle pubbliche gare, al fine di garantire il buon andamento della procedura, richiede una doverosa armonizzazione con gli storici principi cardine del procedimento amministrativo.

Quanto sopra, inoltre, assume ancora maggiore rilievo ove si consideri che l'inserimento nella banca dati dell'Autorità per la vigilanza nei contratti pubblici di dati informativi di natura estremamente "sensibile" attra-

Note:

(segue nota 4)

zione amministrativa. Sul punto F. Caringella, *Manuale di diritto amministrativo*, Milano, 2006, 848. Sul pubblico interesse anche, G. Clemente di San Luca, *I nuovi confini dell'interesse pubblico*, Padova, 1999, 169.

(5) Si veda E. Giuffè, *Con internet tempi più snelli per le procedure degli appalti*, in *Edilizia e Territorio*, 17/2006, 16.

(6) Ad esempio art. 66 d.lgs. n. 163/2006.

(7) Ad esempio art. 70 d.lgs. n. 163/2006.

(8) Ad esempio art. 85 e art. 60 d.lgs. n. 163/2006. E. Guarnaccia, *Ricorso alle Aste Elettroniche*, in Aa.Vv., *Commento al codice dei contratti pubblici*, Napoli, 2006, 330, ed, ivi, del medesimo Autore, *Sistemi dinamici di acquisizione*, 261.

(9) In proposito si veda, pure, D. Marongiu, *L'identificazione informatica e la sottoscrizione digitale nelle gare telematiche: l'applicazione delle regole sostanziali in materia di appalti nel contesto informatizzato*, in questa Rivista, 1, 2008, 67.

(10) ... recante "Nuove disposizioni sull'amministrazione del patrimonio e sulla contabilità dello Stato" e dal Regio decreto 23 maggio 1924, n. 827, recante il "Regolamento per l'amministrazione del patrimonio e per la contabilità generale dello stato". L'importanza delle citate disposizioni è ben evidenziata in A. Cianflone e G. Giovannini, *L'appalto di opere pubbliche*, Milano, 2003.

(11) Tra tutte, per la sua importanza storica, si richiama T.A.R. Lombardia, Milano, sez. III, 3 marzo 2003, n. 2393, in *Urbanistica e Appalti*, 3, 2004, 356, e T.A.R. Lazio, sez. III, 8 marzo 2004, n. 2159 su www.lexitalia.it. In dottrina si veda, invece, P. Piras, *L'Amministrazione nell'era del diritto amministrativo elettronico*, in questa Rivista, 6, 2006, 550.

(12) Sullo storico principio del buon andamento esiste una copiosa dottrina, su tutti si veda A. M. Sandulli, *Manuale di diritto amministrativo*, Napoli, 1982, 516.

(13) Ad esempio, certamente notevoli potranno essere i vantaggi anche per le pubbliche amministrazioni grazie all'utilizzo del sistema di posta elettronica certificata, approvato dal Consiglio dei Ministri in via definitiva in data 28 gennaio 2005, n. 68. In materia A. Natalini, *La posta elettronica certificata*, in *Giornale di Diritto Amministrativo* 2004, n. 7, 715. In giurisprudenza si veda Cons. St., 5 marzo 2003, n. 1218, su www.lexitalia.it, che riconosce la possibilità di utilizzare lo strumento della posta elettronica per l'invio di offerte.

(14) Sul rapporto tra la legge 241 e l'attività contrattuale si veda F.A. Caputo, *La procedura di evidenza pubblica e le innovazioni della legge 241/1990*, in *I Contratti dello Stato e degli Enti Pubblici*, 2, 2005, 18 e F. Mastragostino, *La riforma del procedimento amministrativo e i contratti della P.A., considerazioni sull'art. 1, comma 1 bis, della legge n. 241/1990 e ss. mm.*, su www.lexitalia.it.

verso l'annotazione nel casellario informatico, rappresenta uno strumento potenzialmente capace di incidere negativamente sull'immagine, professionalità e credibilità delle imprese interessate.

La pronuncia appare, pertanto, significativamente rilevante ove si consideri che interviene anche nella complessa tematica della semplificazione amministrativa applicata alla procedura di scelta del contraente in specie grazie al richiamo voluto dall'art. 77 bis, del d.p.r. n. 445/2000 (15) che, opportunamente, chiarisce come le disposizioni in materia di semplificazione e autocertificazione si applicano anche al settore degli appalti pubblici (16).

2. L'art. 48 del d.lgs. n. 163/2006

Una delle difficoltà che le stazioni appaltanti hanno più spesso dovuto fronteggiare nel tempo è stata quella di garantire la regolare esecuzione delle prestazioni contrattualmente previste. Infatti, più volte in passato, i partecipanti alle gare si spingevano nella formulazione di offerte particolarmente vantaggiose ma che, a causa degli eccessi di ribasso, non erano poi in grado di eseguire in concreto. Si trattava, nella sostanza, di offerte fuori dalla loro portata che venivano formulate, pur senza avere alcun supporto pratico, nella speranza che la pubblica amministrazione (come spesso accaduto in passato), al palesarsi delle prime difficoltà esecutive, consentisse un'immediata rideterminazione degli oneri contrattuali (17). Questa situazione causava, però, l'effetto paradossale di avere un soggetto vincitore nella procedura di scelta del contraente che, dopo breve tempo dalla stipula del contratto, si rendeva inadempiente rispetto agli obblighi assunti con grave danno per la pubblica amministrazione.

La colposa frequenza con la quale le descritte situazioni si ripetevano nel tempo aveva consigliato una severa riflessione imponendo la necessità di un immediato intervento normativo tempestivamente recepito in specie dal diritto comunitario.

In questo modo l'attenzione si è concentrata non solo nella richiesta di adeguate garanzie di affidabilità e serietà delle imprese attraverso la prestazione di opportune clausole fidejussorie (ovvero attraverso l'apposizione di pegno) ma anche, in termini di prevenzione, per mezzo dell'introduzione di tutte quelle previsioni normative, che, in seguito all'approvazione del codice unico dei contratti della pubblica amministrazione, sono ora contenute nella Parte II, Titolo I, Capo II (18), ed, in particolare, nell'art. 48 (19).

Il ragionamento di fondo che ispira la descritta previsione normativa è quello di intervenire prima ancora dell'aggiudicazione (20) e già nella procedura di gara allo scopo di accertare la serietà (21), la affidabilità e la credibilità di soggetti partecipanti alle gare e, per l'effetto, per verificare la attendibilità delle offerte contestualmente proposte (22).

Se per un verso i procedimenti di semplificazione

voluti dalle riforme della seconda parte degli anni novanta (23) consentono che i requisiti richiesti per la partecipazione alla gara siano semplicemente dichiarati al momento di presentazione delle offerte (24), per altro verso, in applicazione dei sopra esposti motivi, risulta essere altrettanto ragionevole, di conseguenza, non solo procedere all'esame dei requisiti del soggetto vincitore dopo l'aggiudicazione ma anche richiedere a tutti i partecipanti, prima ancora dell'apertura delle buste, la verifica dei requisiti di capacità economico-finanziaria e tecnico organizzativa eventualmente richiesti nel bando di gara (25).

Note:

(15) Inserito dall'art. 15, legge n. 3/2003, meglio noto come collegato alla finanziaria 2003.

(16) In tal senso D. Spinelli, F. Petullà e M. A. Portaluri, *Le procedure telematiche negli appalti pubblici*, Milano, 2004, 133.

(17) In materia V. Lopilato, *Le clausole di rinegoziazione nei contratti ad evidenza pubblica*, in *Foro Amm. Tar*, 4, 2006, 1911.

(18) A. Bartolini, *I requisiti di capacità economica e finanziaria tra restrizioni della lex specialis e favor participationis*, in *Urbanistica e Appalti*, 8, 2007, 1032.

(19) L'art. 48 riproduce, senza sostanziali modifiche, il controllo a campione disciplinato dal comma 1 quater dell'art. 10 della legge Merloni n. 109/1994, come introdotto dall'art. 3 della legge n. 415/1998. In ogni caso la verifica non può riguardare i requisiti generali come chiarito dall'Autorità per la vigilanza sui lavori pubblici, determinazione 30 marzo 2000, n. 15/2000.

(20) L'obiettivo ricercato dal legislatore, in ossequio al principio costituzionale di buona amministrazione, è quello di consentire che l'offerta formulata dal concorrente sia seria e congrua al fine di evitare che la non sostenibilità dell'offerta medesima possa divenire fonte di gravi irregolarità nel corso di esecuzione del contratto a danno della pubblica amministrazione e, soprattutto, degli utenti finali.

(21) Il richiamo deve essere esteso anche alla moralità professionale. Sul punto M. Baldi, *Il previgente regime di esclusione per reati incidenti sulla moralità professionale negli appalti di lavori e servizi*, in *Urbanistica e Appalti*, 2, 2007, 234.

(22) È evidente, tuttavia, che le informazioni relative alla veridicità delle dichiarazioni sostitutive che le amministrazioni devono acquisire d'ufficio riguardano i requisiti di ordine generale già in possesso di altre amministrazioni perché contenute, ad esempio, nei registri dello stato civile, nei registri professionali ovvero in albi tenuti da altra pubblica amministrazione. Le informazioni relative alla capacità economico-finanziaria sono, invece, comprovabili prevalentemente attraverso la documentazione in possesso degli stessi interessati. Così D. Spinelli, F. Petullà e M. A. Portaluri, *Le procedure telematiche negli appalti pubblici*, cit., 137.

(23) Il riferimento è in primo luogo alle leggi di semplificazione amministrativa meglio note come "leggi Bassanini" e al d.p.r. n. 445/2000.

(24) Secondo il Consiglio di Stato, sez. V, sentenza 27 ottobre 2005, n. 6006, art. 77 bis d.p.r. n. 445/2000 prevede che le disposizioni in materia di documentazione amministrativa, fra le quali è riconducibile quella riguardante le dichiarazioni sostitutive, si applicano a tutti i casi in cui è prevista una certificazione. Ne consegue che le prescrizioni dei bandi e degli altri atti regolatori di gare, per la scelta del miglior contraente da parte delle pubbliche amministrazioni, vanno sempre intese nel senso che, anche se non si richiamano alla norma ora citata, si deve ammettere la certificazione semplificata e sostitutiva stabilita dal menzionato testo unico.

(25) Secondo il Consiglio di Stato, sez. V, sentenza 27 ottobre 2005, n. 6003, l'art. 10, comma 1 quater, l. n. 109/1994, contempla due momenti (segue)

È chiaro, peraltro, che l'esigenza di presentare la documentazione indicata nel bando di gara o nella lettera d'invito preventivamente non può ripercuotersi in danno del principio di speditezza e tempestività del procedimento amministrativo causando un eccessivo aggravio dell'*iter* della gara ad evidenza pubblica. Infatti, in questo modo si vedrebbero notevolmente estesi i tempi necessari alla scelta del contraente in grave pregiudizio per l'interesse pubblico.

Per temperare tra le diverse esigenze della pubblica amministrazione, allora, la verifica preliminare, come previsto dall'art. 48, non deve essere effettuata nei confronti di tutti i soggetti partecipanti alla gara ma a campione richiedendola solamente a un numero di offerenti non inferiore al dieci per cento delle offerte presentate arrotondato all'unità superiore.

In questo modo l'ottimale armonizzazione tra le inderogabili sequenze procedurali dell'evidenza pubblica e la credibilità delle offerte pare essere adeguatamente raggiunta senza pregiudizio né per la tempestività dell'operato della pubblica amministrazione né per il principio che impone l'onere di scelta del miglior contraente possibile.

Resta, pertanto, solo da garantire la trasparenza e imparzialità dell'operato della stazione appaltante in modo tale che l'individuazione del partecipante obbligato alla dimostrazione preventiva dei requisiti possa avvenire secondo regole certe ma senza che lo stesso possa essere stabilito anticipatamente rispetto alla proposizione delle offerte perché in questo modo ne risulterebbe certamente compromessa la finalità ispiratrice dell'istituto in commento.

Per tali ragioni, la norma, in maniera decisamente condivisibile, ha stabilito che l'individuazione del partecipante vincolato alla preventiva dimostrazione dei requisiti dovrà avvenire attraverso l'opportuna previsione di un apposito sorteggio pubblico tra tutti gli partecipanti e prima dell'apertura delle buste contenenti le offerte.

Tale strategia procedurale incide in modo determinante nei tempi di svolgimento della gara garantendone l'economicità, l'efficienza e l'efficacia.

Infatti, la seconda parte dell'art. 48, in termini assolutamente sanzionatori, prevede che ove non sia fornita la prova del possesso dei requisiti (26) di capacità economico-finanziaria e/o tecnico-organizzativa precedentemente dichiarati nella domanda o nell'offerta di partecipazione, la stazione appaltante è tenuta ad adottare un conseguente provvedimento di esclusione del contraente dalla gara (27) oltre all'escussione della relativa cauzione provvisoria (28).

Si tratta, come può facilmente essere intuito, di conseguenze piuttosto radicali che, in quanto tali, si propongono di avere, necessariamente, un effetto dissuasivo e ammonitorio nei confronti delle imprese interessate a partecipare (29), le quali, al fine di evitare gravose sanzioni, sono efficacemente indotte a presentare un'offerta solo se in possesso di tutti i richiesti requisiti ovvero, in

caso contrario, evitano di aggravare l'*iter* procedimentale di scelta del contraente.

Il disegno legislativo, però, si muove in una prospettiva più ampia in quanto, attraverso la sopra descritta previsione normativa di cui all'art. 48, interviene in una duplice direzione ove si consideri che le sanzioni per chi ha reso false dichiarazioni (30) non sono limitate alla sola gara in corso di svolgimento ma, ricorrendo a un'efficace sinergia nell'utilizzo degli strumenti telematici e informatici, grazie all'ausilio dell'Autorità per la vigilanza nei contratti pubblici, si estende in maniera più generalizzata anche con riferimento alle gare future.

Infatti, è posto a carico della stazione appaltante

Note:

(segue nota 1)

per la dimostrazione del possesso dei requisiti di capacità economico-finanziaria e tecnico-organizzativa, eventualmente stabiliti nel bando di gara. Il primo si concretizza in un momento antecedente all'aggiudicazione ed è quello relativo all'esame a campione su un decimo degli offerenti; tale controllo ha natura perentoria e deve essere effettuato entro dieci giorni dal ricevimento della richiesta, stante l'esigenza di celerità insita nel procedimento. Il secondo deve essere posto in essere dopo l'aggiudicazione e riguarda l'aggiudicatario e il concorrente che segue in graduatoria i quali dovranno dimostrare i soprarichiamati requisiti (se già non l'hanno fatto) entro un termine meramente sollecitatorio di dieci giorni. In tal senso, da ultimo, si veda anche T.A.R. Lazio, Roma, sez. I *quater*, sentenza 26 febbraio 2008, n. 1695.

(26) Se la prova non viene fornita o non vengano confermate la dichiarazioni rese in corso di gara, si applicano le sanzioni di cui al comma precedente in forza delle quali si procede alla determinazione della nuova soglia di anomalia e alla conseguente nuova aggiudicazione. In merito alle problematiche connesse al ricalcolo della suddetta soglia si veda l'interessante repertorio giurisprudenziale riportato da M. Greco, *La verifica dei requisiti generali e speciali nel nuovo codice dei contratti pubblici*, in *Appalti e Contratti*, 1, 2006, 39.

(27) È evidente che se la non veridicità riguarda l'aggiudicatario questi perde il diritto all'aggiudicazione.

(28) Secondo Cons. di St. sez. V, 28 giugno 2004, n. 4789, l'escussione della cauzione provvisoria ha la funzione di garantire la veridicità delle dichiarazioni fornite dalle imprese in sede di partecipazione alla gara in ordine al possesso dei requisiti prescritti dal bando o dalla lettera d'invito, così da assicurare l'affidabilità dell'offerta, il cui primo indice è rappresentato proprio dalla serietà e dalla correttezza del comportamento del concorrente.

(29) Secondo A. Cancrini, P. Piselli e V. Capuzza, *La nuova legge degli appalti pubblici*, Roma, 2006, 121, le misure sanzionatorie sono espressamente comminate soltanto a carico del concorrente la cui indebita partecipazione alla gara sia stata accertata secondo la procedura di verifica a campione dalla stessa disposizione puntualmente disciplinata. Perché la sanzione possa essere legittimamente irrogata è necessario, dunque, il positivo accertamento, nei modi e nei termini dalla norma prescritti, del fatto dalla stessa punito; restando così esclusa la possibilità di un esercizio sanzionatorio al di fuori dei limiti normativamente stabiliti (Cons. di St., sez. V, sentenza 12 maggio 2003, n. 2512).

(30) ...ovvero dichiarazioni non suscettibili di essere comprovate. La questione non è di poco conto stante l'ampiezza di materie che le suddette dichiarazioni possono investire. In merito F. De Nardi, *Legittimità della clausola del bando che impone ai concorrenti della gara d'appalto l'autocertificazione di iscrizioni relative a sentenze ex art. 444 cod. proc. Pen.*, in *Riv. Trim. App.*, 4, 2005, 1168. La regolarità contributiva, invece, non è mai autocertificabile e va dimostrata mediante presentazione del D.U.R.C., U. Montella, *Il codice dei contratti pubblici di lavori, forniture e servizi, Manuale operativo*, Rimini, 2007.

precedente un inderogabile obbligo di segnalazione alla citata Autorità la quale è, poi, tenuta all'adozione dei provvedimenti di cui all'art. 6, comma 11 del codice (31).

L'effetto strumentale, dunque, determina l'applicazione di un'ulteriore sanzione accessoria consistente nella sospensione da uno a dodici mesi dalla partecipazione alle procedure di affidamento.

Il mezzo utilizzato per rendere operativa l'efficacia di tale sanzione aggiuntiva è il Casellario informatico sul quale sono registrate le annotazioni riguardanti le imprese responsabili di accertate mancanze in altre precedenti gare.

La severità della normativa ha un prorompente effetto dissuasivo che, però, per la rigidità della sua formula applicativa richiede che la previsione codicistica venga applicata con criterio e rigore ma senza discrezionalità alcuna da parte dell'Autorità che, in caso contrario, si troverebbe a causare un ingiusto pregiudizio alle imprese in conseguenza di un'illegittima annotazione.

È proprio in quest'ottica allora che la sentenza del Tribunale Amministrativo del Lazio assume peculiare rilievo in quanto, pur senza mettere minimamente in discussione l'efficacia e la rilevanza degli strumenti elettronici, richiede inderogabilmente che gli stessi siano applicati nel rispetto delle sequenze procedurali fissate non solo dalla legge n. 241/1990 in generale ma anche dal codice degli appalti in particolare (32).

3. L'Autorità per la vigilanza nei contratti pubblici e l'esclusione dalla gara

Le innovazioni succedutesi in materia telematica e informatica nell'ultimo decennio hanno influenzato profondamente la materia degli appalti come conseguenza di quel più generale percorso volto a favorire l'informatizzazione della pubblica amministrazione anche in questo settore.

In particolare, in poco tempo è emerso il *favor* delle stazioni appaltanti per gli strumenti informatici e telematici grazie alla loro straordinaria semplicità applicativa e alla eccezionale conoscibilità in concreto del dato elettronico trasmesso.

A poco a poco, pertanto, le conquiste tecnologiche sono diventate un importante elemento di supporto per le pubbliche amministrazioni per il regolare e il proficuo svolgimento delle procedure di gara.

L'insostituibile sinergia voluta dal legislatore comunitario tra l'informatica e la procedura di scelta del contraente si riversa in tutte le numerose fasi di cui si compone la gara ad evidenza pubblica e passa, ora, anche per il tramite della Autorità per la vigilanza dei contratti pubblici efficacemente chiamata a svolgere un'importante attività di sostegno e di supporto per le stazioni appaltanti (33).

Il riferimento ai dati normativi richiamati nei precedenti paragrafi dimostra che il ruolo della citata Autorità è notevolmente cresciuto avendo il suo operato

un'incidenza immediata e diretta non più solo nei lavori pubblici ma anche nella materia delle forniture e dei servizi. In sostanza la sua presenza diventa un elemento di ausilio fondamentale e indispensabile in tutte le fasi della procedura di gara pubblica in un'ottica di ricerca del miglior contraente possibile.

Quanto sopra ha trovato concreta ed immediata attuazione anche nel caso di specie in cui l'applicazione pratica del principio del buon andamento di cui all'art. 97 della costituzione impone alla pubblica amministrazione l'onere di fornire servizi innovativi agli utenti anche attraverso l'utilizzo dei più recenti dispositivi elettronici.

In particolare, nelle procedure di scelta del contraente per mezzo degli strumenti telematici diventa possibile fornire in tempo reale alle stazioni appaltanti informazioni relative ad eventuali irregolarità riscontrate nei confronti delle imprese partecipanti alle procedure di affidamento promosse attraverso le pubbliche gare.

Tutto ciò comporta una conoscibilità più ampia e tempestiva delle caratteristiche dei potenziali contraenti che, però, non può mettere in discussione la veridicità, la attendibilità e la fondatezza del dato elettronico.

Per tali ragioni, come correttamente ha fatto rilevare il Tribunale Amministrativo del Lazio, anche l'annotazione nel casellario informatico, in considerazione delle conseguenze estreme cui può condurre non solo in termini di esclusione dalle gare ma anche per effetto di un potenziale danno all'immagine, deve essere necessariamente pre-

Note:

(31) In applicazione di tale disposizione "con provvedimento dell'Autorità, i soggetti ai quali è richiesto di fornire gli elementi di cui al comma 9 sono sottoposti alla sanzione amministrativa pecuniaria fino a euro 25.822 se rifiutano od omettono, senza giustificato motivo, di fornire le informazioni o di esibire i documenti, ovvero alla sanzione amministrativa pecuniaria fino a euro 51.545 se forniscono informazioni od esibiscono documenti non veritieri. Le stesse sanzioni si applicano agli operatori economici che non ottemperano alla richiesta della stazione appaltante o dell'ente aggiudicatore di comprovare il possesso dei requisiti di partecipazione alla procedura di affidamento, nonché agli operatori economici che forniscono dati o documenti non veritieri, circa il possesso dei requisiti di qualificazione, alle stazioni appaltanti o agli enti aggiudicatori o agli organismi di attestazione".

(32) Giova ricordare che nel testo originariamente approvato dalle Camere il 14 novembre 2005 era prevista una formulazione parzialmente diversa della norma che comportava, sostanzialmente, l'eliminazione del controllo a campione e la previsione di una mera facoltà di controllo, in qualunque momento della gara, da parte della stazione appaltante, su tutti o alcuni dei candidati o concorrenti, nonché l'obbligo di controllo su aggiudicatario e secondo classificato. Sul punto si veda G. Caudullo, *Controllo sul possesso dei requisiti*, in Aa.Vv., *Il Codice dei Contratti Pubblici*, Napoli, 2006, 197.

(33) L'Autorità vigila sui contratti pubblici, anche di interesse regionale, di lavori, servizi e forniture nei settori ordinari e nei settori speciali, nonché, nei limiti stabiliti dal d.lgs. n. 163/2006, sui contratti pubblici di lavori, servizi e forniture esclusi al fine di garantire l'osservanza dei principi di correttezza e trasparenza delle procedure di scelta del contraente e di economica ed efficiente esecuzione dei contratti, nonché il rispetto delle regole della concorrenza nelle singole procedure di gara. I compiti, le funzioni, i poteri e gli obblighi dell'Autorità sono diffusamente elencati nell'art. 6 del codice dei contratti.

ceduta da una motivata attività istruttoria che ne giustifichi l'adozione da parte dell'Autorità per la vigilanza.

La particolarità della procedura impone, così come disposto dall'art. 48, comma 1, del d.lgs. n. 163/2006, che la gravità delle violazioni accertate trovi adeguato effetto nell'adozione di un provvedimento di esclusione da una precedente procedura di scelta del contraente in mancanza del quale alcuna annotazione potrà essere legittimamente disposta.

Si tratta, del resto, di un'operazione estremamente "sensibile" stante la delicatezza dei dati trattati in specie quando, attraverso la pubblicazione sul *web* (34), sia consentita un'immediata, rapida e più ampia conoscenza delle caratteristiche dei potenziali offerenti con evidenti riflessi in termini di buon andamento nell'individuazione del miglior contraente possibile (35).

In questa prospettiva il valore giuridico della sentenza in commento è duplice in quanto con essa non solo la pubblica amministrazione inizia a porsi al passo coi tempi ma in maniera decisamente significativa il Tribunale Amministrativo dimostra che l'applicazione ragionevole e legittima degli atti amministrativi prescinde dalla loro natura informatica o tradizionale.

Ciò comporta che, come correttamente osservato dai giudici capitolini, anche l'annotazione nel casellario informatico deve avvenire, stante la delicatezza degli interessi in gioco, nel rigoroso rispetto delle scansioni logico-procedimentali fissate dalla normativa di riferimento, tanto più quando le stesse dovessero apparire evidentemente logiche e razionali.

Il principio di fondo è molto semplice in quanto, pur ricorrendo agli strumenti telematici, si cerca di agevolare la pubblica amministrazione nell'individuazione del miglior contraente ma senza che da ciò possa derivare danno alcuno per gli operatori del mercato, com'è avvenuto nel caso della sentenza in commento.

Infatti, l'aver inserito nel casellario informatico il nominativo di un'azienda senza che alcun precedente provvedimento di esclusione dalla gara le fosse stato previamente comminato, rappresenta non solo una palese violazione di legge rispetto al dato letterale della norma fissato dall'art. 48 del codice degli appalti ma appare anche illogico e irrazionale. Del resto se la funzione dell'annotazione è quella di rendere evidente e conoscibile alle stazioni appaltanti l'anomalia commessa in precedenti procedure di affidamento da imprese scarsamente affidabili per le false dichiarazioni rese, la segnalazione deve inderogabilmente emergere da dati concreti e comprovabili stante la gravità degli effetti irreparabili che ne discendono.

Ciò comporta che in mancanza di un provvedimento di esclusione dalla gara nessuna contestazione risulta essere imputabile al concorrente che, dunque, non potrà neppure essere segnalato all'Autorità ai fini dell'eventuale inserimento nel casellario informatico mancando di fatto le ragioni di fondo che ne giustificano l'annotazione.

A differenza del passato i giudici si trovano non a dover valutare le censure di un privato ricorrente che abbia partecipato a una pubblica gara quanto piuttosto a dover valutare l'illegittimità di una ingiusta iscrizione sulle banche dati telematiche con tutte le conseguenze in termini di danno che possono scaturirne in concreto non solo con riferimento a una singola gara ma anche per gli evidenti riflessi lesivi dell'immagine e della credibilità dell'impresa.

Proprio per tale motivo, in modo decisamente condivisibile, la sentenza in commento ha respinto anche l'eccezione con cui le amministrazioni resistenti avevano prospettato una supposta improcedibilità del ricorso stante la cancellazione della contestata annotazione. Infatti, la cancellazione ha efficacia solo ed esclusivamente a partire dal momento in cui è disposta senza che la stessa possa avere efficacia sanante per la dannosa annotazione effettuata in relazione al periodo antecedente la data in cui è stata effettuata.

Tutto ciò comporta che l'interesse del ricorrente può ritenersi adeguatamente tutelato non solo per effetto della cancellazione, in quanto essa dispone i suoi effetti solo per il futuro, ma anche nel momento in cui si proceda ad accertare l'illegittimità della pregressa annotazione dal momento che tale sentenza di accertamento evidenzia l'ingiustizia commessa e rappresenta il presupposto logico necessario per richiedere un eventuale risarcimento del danno (36) ove se ne dimostri l'effettiva consistenza.

Note:

(34) L'Autorità per la vigilanza sui lavori pubblici con il comunicato del 28 giugno 2007, su www.autoritalavoripubblici.it, ha disposto che dal 4 agosto successivo l'accesso alle annotazioni fosse riservato esclusivamente alle stazioni appaltanti e alle SOA. Ciò ha comportato che non è più stato possibile consultare tali informazioni senza le credenziali richieste (*user id* e *password*) per l'accesso alla sezione riservata delle annotazioni. A partire da tale data le stazioni appaltanti all'atto della consultazione riservata sono tenute a specificare di volta in volta il motivo dell'accesso ad ogni specifica annotazione e ciascun accesso sarà registrato nei *log* del sistema. Restano, invece, liberamente accessibili le informazioni relative alle attestazioni di qualificazione.

(35) L'obiettivo posto dal legislatore comunitario, secondo il *considerando* n. 13, direttiva n. 18/2004, è quello di realizzare, tramite il ricorso a un mercato aperto in ogni tempo, un ventaglio particolarmente ampio di offerte grazie ai mezzi elettronici utilizzati e, quindi, di assicurare un impiego ottimale delle finanze pubbliche mediante un'ampia concorrenza.

(36) Sul risarcimento del danno F. Iacovone, *Fine della disputa: vanno ai Tar le domande di risarcimento*, in *Edilizia e Territorio*, 17, 2006, 103 e C. Papetti, *Risarcimento del danno da attività provvedimentoale: nuove frontiere sostanziali e processuali* (nota a T.A.R. Marche, 16 maggio 2006, n. 321), in *Foro Amm. Tar*, 5, 2006, 2026.

Processo civile

Formulario commentato con Cd-Rom

Tutte le formule relative ai procedimenti speciali del processo civile: il procedimento di **ingiunzione**, il **procedimento per convalida di sfratto**, i procedimenti **cautelari** e **possessori**, i procedimenti in materia di **famiglia** e di **stato delle persone**, la **copia** e la **collazione di atti pubblici**, i procedimenti relativi all'**apertura delle successioni**, lo **scioglimento di comunioni**, il processo di **liberazione degli immobili dalle ipoteche** e l'**arbitrato**.



Le formule sono corredate da un ampio e utile commento d'autore.

STRUTTURA:

Ogni articolo di riferimento è strutturato in quattro "moduli": un **inquadramento funzionale** che rappresenta un commento d'autore, sintetico ma completo, con suggerimenti e indicazioni di carattere pratico; un breve paragrafo che suggerisce gli **errori da evitare**, ossia cosa non si deve fare affinché la **formula** sia corretta; la formula in senso stretto; una **rassegna della giurisprudenza** più significativa, di legittimità e di merito, articolata nelle medesime voci dell'inquadramento funzionale.

Autori:

AA.VV.

A cura di:

C. Consolo e V. Mariconda

pagg. 1.760, € 130,00

Avvocati civilisti

Praticanti

Scuole di specializzazione
forense

Si, desidero acquistare il volume:

(00081333) **"Processo civile - Formulario commentato"** a € 130,00

Cognome e Nome Azienda/Studio _____

Via _____ C.a.p. _____ Città _____

Tel. _____ Fax _____ Cod. cliente _____

(3003) Pagherò con bollettino postale sul c.c. n° 583203, intestato a WKI S.r.l. - Gestione incassi

Addebitare l'importo di € _____ sulla mia carta di credito

[] Mastercard (16 cifre) [] American Express (15 cifre) [] VISA (16 cifre) [] Diner's (14 cifre)

n° _____ Data di scadenza _____

Nome e indirizzo intestatario carta di credito _____

Diritto di recesso. Clausola di ripensamento ai sensi dell'art. 5 D.Lgs. n. 185/1999. Decorsi 10 giorni lavorativi dalla data di ricevimento del bene da parte del cliente senza che questi abbia comunicato con raccomandata A.R. inviata a Wolters Kluwer Italia S.r.l. Milano/Assago (o mediante e-mail, telegramma, telex o facsimile confermati con raccomandata A.R. nelle 48 ore successive), la propria volontà di recesso, la proposta si intenderà impegnativa e vincolante per il cliente medesimo. In caso di recesso da parte del cliente, entro lo stesso termine (10 giorni lavorativi dal ricevimento) il bene dovrà essere restituito per posta a Wolters Kluwer Italia S.r.l., Milano/Assago, Strada 1-Pal. F6, 20090 Assago (MI). Le spese di spedizione saranno a carico di Wolters Kluwer Italia S.r.l.

Compili e invii subito
il coupon in busta chiusa a
Ipsoa Editore, Str. 1, Pal.F6,
20090, Milanofiori/Assago
oppure via fax allo
02 82476403,
Servizio Informazioni
Commerciali Ipsoa
tel. 02 82476794
oppure rivolgersi
all'**Agenzia Ipsoa** di zona

www.ipsoa.it

IPSOA
Gruppo Wolters Kluwer

Ai sensi dell'art. 13 del D.Lgs. n. 30.6.2003 n. 196. La informiamo che i Suoi dati sono conservati nel data base informatico del titolare del trattamento, Wolters Kluwer Italia S.r.l. Responsabile del trattamento: Ufficio MID. L'elenco aggiornato di tutti i responsabili del trattamento potrà essere richiesto per iscritto all'Ufficio MID presso la sede della società. I Suoi dati saranno utilizzati dalla nostra società, da enti e società esterne ad essa collegati, nonché da soggetti terzi, titolari autonomi del trattamento, solo per l'invio di materiale amministrativo-contabile, commerciale e promozionale. Ai sensi dell'art. 7 del citato D.Lgs., Lei ha diritto di conoscere, aggiornare, rettificare, cancellare i Suoi dati, nonché di esercitare tutti i restanti diritti ivi previsti, mediante comunicazione scritta a Wolters Kluwer Italia S.r.l., Ufficio MID, Milano/Assago, Strada 1-Palazzo F6, 20090 Assago (MI).

Appalto

La posta elettronica: una complessa qualificazione tra prassi, giurisprudenza e legge

T.A.R. PUGLIA, LECCE, sez. I, 21 febbraio 2008, n. 562 - Pres. Ravalli - Est. Viola - Officine meccaniche e ferroviarie del Salento (O.M.F.E.S.A.) s.r.l. c. Trenitalia S.p.A.

Appalti - Messaggio di posta elettronica che costituisce conclusione tacita del contratto - Revoca della procedura di gara - Contraddittorietà tra atto di revoca e precedente comunicazione via mail - illegittimità

(d.lgs. 12 aprile 2006, n. 163; d.lgs. 7 marzo 2005, n. 82)

L'invio di un messaggio di posta elettronica all'impresa aggiudicataria provvisoria, con cui si affidano i lavori appaltati, dà luogo al perfezionamento tacito del contratto, e assume il valore sostanziale di aggiudicazione definitiva. Il successivo atto di revoca con cui la stazione appaltante dichiara di non voler esternalizzare l'attività appaltata, e di valutare negativamente il Piano della qualità dell'aggiudicataria, è illegittimo.

...Omissis...

Fatto

Con nota UTRMP:SM/332 prot. n. 493 del 22.5.2006, Trenitalia s.p.a. indicava una procedura negoziata ai sensi dell'art. 15, 3° comma del d.lgs. 158 del 1995 per l'affidamento della «manutenzione ciclica di ROC per n. 10 carrozze Z1 con l'opzione per ulteriori cinque, per un importo complessivo presunto di € 540.000,00»; la ricorrente partecipava alla procedura presentando un'offerta che prevedeva un ribasso complessivo del 13,21% (derivante dal ribasso del 12,21% già contenuto nella domanda di partecipazione alla procedura e dall'ulteriore ribasso dell'1% offerto con la successiva nota del 2.8.2006).

In data 28 agosto 2006, Trenitalia s.p.a. comunicava alla ricorrente l'accettazione provvisoria dell'offerta in questione, sulla base della proposta migliorativa del 2.8.2006 e invitava la stessa a procedere agli adempimenti previsti dall'art. 8 delle Condizioni generali di contratto per gli appalti delle forniture del Gruppo FS. (esibizioni delle certificazioni idonee a dimostrare la presenza dei requisiti di ordine morale e di idoneità previsti dalla normativa; certificazioni antimafia; prestazione delle garanzie previste dall'art. 10 delle citate condizioni generali di contratto; presentazione ed approvazione del Piano di Gestione della Fornitura) e necessari per l'aggiudicazione definitiva del contratto.

In data 31 ottobre 2006, la ricorrente riceveva, per e-mail, una comunicazione che individuava le dieci carrozze oggetto di manutenzione e preannunciava l'arrivo delle stesse, in diversi scaglioni, in un periodo intercorrente tra il 3 e il 24 novembre 2006.

Con provvedimento 27.11.2006 prot. DOT/LC.PIMC 324 06 IP RG, Trenitalia s.p.a. comunicava però alla ricorrente l'annullamento della gara a procedura negoziata UTRMP:SM/332 prot. n. 493 del 22.5.2006, sulla base della seguente motivazione: «per sopperire al fermo di veicoli Z1 di I classe già scaduti ma necessari nella nuova programmazione di treni IC, la manutenzione ciclica di ROC di cui alla gara in oggetto, tenuto anche conto dei fermi previsti per la loro effettuazione c/o l'IP, è stata pianificata nelle OMC di Trenitalia ove è già in corso di svolgimento....(pertanto) non risulta più necessario dare corso all'affidamento a terzi della manutenzione dei suddetti rotabili».

Il provvedimento di annullamento era impugnato dalla ricorrente per: 1) violazione dell'art. 8 delle condizioni generali di contratto per gli appalti di forniture delle società del gruppo FS e delle norme in materia di procedimento di gara; 2) falsa ed erronea presupposizione, violazione dei principi in materia di formazione dei contratti nelle procedure di gara; 3) violazione artt. 7 e 8 l. 241 del 1990; 4) violazione dell'art. 21 *nonies* della l. 241 del 1990; 5) violazione dell'art. 21 *quinquies* della l. 241 del 1990; 6) violazione dell'art. 79 del d.lgs. n. 163 del 2006; con il ricorso la ricorrente chiedeva altresì l'accertamento dell'avvenuta formazione del contratto in questione e il risarcimento dei danni derivanti dal provvedimento di annullamento dell'aggiudicazione del contratto.

Si costituiva Trenitalia s.p.a., controdeducendo sul merito del ricorso e formulando eccezione preliminare di difetto di giurisdizione.

Alla camera di Consiglio del 7 marzo 2007, la Sezione accoglieva, con l'ordinanza n. 227/07, l'istanza cautelare

presentata da parte ricorrente, «ai fini del congruo e compiuto esame dei presupposti della revoca della gara come precisati in motivazione».

Con provvedimento 5.4.2007 DTAI/LCC.PIC 0159 RG, Trenitalia s.p.a. riesaminava l'intera fattispecie, a seguito dell'ordinanza cautelare della Sezione e confermava la revoca della procedura di gara in questione, sulla base di una motivazione più articolata; in particolare, la motivazione apposta al nuovo provvedimento di revoca confermava la necessità di "internalizzare" la manutenzione già affidata alla ricorrente a seguito di «una significativa e non prevedibile carenza di disponibilità di vetture di I classe della tipologia a 200 km/h (Z1 e Gran Comfort) ... determinato da ritardi nella restituzione all'esercizio delle carrozze della suddetta tipologia comprese in progetti di ristrutturazione in corso» ed aggiungeva ulteriori considerazioni desunte dal Piano della Qualità della prestazione presentato dalla ricorrente (che avrebbe prospettato modalità di restituzione delle carrozze oggetto di manutenzione e di realizzazione dell'intervento, tali da non garantire il rispetto dei tempi di effettuazione dell'intervento).

Il nuovo provvedimento di revoca era impugnato dalla ricorrente, con motivi aggiunti regolarmente notificati e depositati in data 19 maggio 2007, per: 1) illegittimità derivata; 2) illegittimità propria, violazione art. 1 e 21 *quinquies* l. 241 del 1990, inottemperanza all'ordinanza del T.A.R. Lecce n. 227 del 2007, violazione dell'art. 8 delle condizioni generali di contratto per gli appalti di forniture delle società del gruppo FS e delle norme in materia di procedimento di gara; 3) falsa ed erronea valutazione degli elementi di fatto e di diritto, violazione dell'art. 21 *quinquies* della legge n. 241 del 1990, eccesso di potere, inottemperanza all'ordinanza del T.A.R. Lecce n. 227 del 2007.

Alla camera di Consiglio del 13 giugno 2007, la Sezione accoglieva, con l'ordinanza n. 538/07, l'istanza cautelare presentata da parte ricorrente, dichiarando l'obbligo di Trenitalia s.p.a. di procedere all'esecuzione del contratto di appalto; con ordinanza 13 luglio 2007 n. 3727/07, la VI Sezione del Consiglio di Stato annullava però il pronunciamento cautelare della Sezione e rigettava l'istanza cautelare proposta in primo grado.

All'udienza del 23 gennaio 2008 il ricorso passava quindi in decisione.

Diritto

...*Omissis*...

Venendo all'esame del merito del ricorso, deve poi rilevarsi come l'impugnazione originaria, proposta con riferimento al primo provvedimento di annullamento dell'aggiudicazione (in particolare, si tratta dell'atto 27.11.2006 prot. DOT/LC.PIMC 324 06 IP RG) adottato da Trenitalia s.p.a. debba essere dichiarata improcedibile per sopravvenuto difetto di interesse; a seguito della concessione della tutela cautelare da parte della Sezione (T.A.R. Puglia Lecce sez. I, ord. 7.3.2007 n.

227/07), la resistente ha infatti riesaminato la problematica, emanando un nuovo provvedimento di revoca dell'aggiudicazione che sostituisce completamente il precedente atto di autotutela e che è stato impugnato dalla ricorrente con i motivi aggiunti depositati in data 19 maggio 2007.

La decisione dei motivi aggiunti richiede poi una preliminare ricostruzione delle vicende relative alla formazione del contratto in questione.

La lettera di invito UTRMPSM/332 prot. n. 493 del 22.5.2006, conteneva una disciplina della formazione del contratto che riproduceva sostanzialmente i contenuti dell'art. 8 delle Condizioni generali di contratto per gli appalti delle forniture del Gruppo FS.; in particolare, la lettera di invito prevedeva un fase di aggiudicazione articolata sui seguenti principi:

1. una prima fase, in cui la Stazione appaltante comunicava al partecipante l'«accettazione provvisoria dell'offerta» (in termini più decisamente pubblicitari, potremmo dire l'aggiudicazione provvisoria della procedura);
2. una successiva fase in cui l'aggiudicatario provvisorio era onerato del deposito delle certificazioni necessarie per la definitiva conclusione del contratto e del cd. Piano della Qualità della prestazione;
3. una terza fase in cui la Stazione appaltante, dopo la verifica positiva in ordine al possesso dei requisiti per la stipulazione del contratto, comunicava all'interessato l'«accettazione definitiva dell'offerta» (la cd. aggiudicazione definitiva);
4. in ogni caso, la conclusione del contratto non era sottoposta all'obbligo di riproduzione delle dichiarazioni delle parti in unico atto pubblico, essendo possibile la formalizzazione del contratto «con la forma di corrispondenza commerciale» (vale a dire, mediante scambio di proposta e accettazione, anche non contestuali) e, soprattutto, intendendosi concluso il contratto «con il ricevimento da parte del concorrente migliore offerente della comunicazione scritta dell'intervenuta aggiudicazione definitiva».

In un primo momento, il procedimento di formazione del contratto previsto dalla lettera di invito era seguito da Trenitalia s.p.a.; la nota 28 agosto 2006, DA. UTA. RGR 332 prot. n. 724 recava, infatti, la comunicazione dell'aggiudicazione provvisoria della procedura ed invitava la ricorrente all'esibizione della documentazione necessaria per l'aggiudicazione definitiva, espressamente subordinata alla definizione del subprocedimento di verifica del possesso dei requisiti necessari per la positiva conclusione della procedura previsto dalla lettera di invito e dall'art. 8 delle condizioni generali di contratto per gli appalti delle forniture del Gruppo FS.

Successivamente e quando ormai la ricorrente aveva proceduto al deposito della documentazione richiesta con la nota di aggiudicazione provvisoria, Trenitalia s.p.a. si allontanava dallo schema procedurale previsto dalla lettera di invito; piuttosto che comunicare alla ricorrente l'aggiudicazione definitiva della procedura

d'appalto, la resistente inviava infatti alla ricorrente, in data 31 ottobre 2006, una e-mail che individuava già precisamente, attraverso il numero di matricola, le dieci carrozze oggetto di manutenzione e preannunciava l'arrivo delle stesse, in diversi scaglioni, in un periodo intercorrente tra il 3 e il 24 novembre 2006.

A questo proposito, la Sezione non può mancare di rilevare come la citata e-mail (mai disconosciuta dalla difesa della resistente e quindi da considerarsi imputabile a Trenitalia s.p.a.), presupponga la positiva conclusione delle verifiche previste dalla lettera di invito e, quindi, assuma il valore sostanziale dell'esternazione della positiva volontà della Stazione appaltante in ordine all'accettazione definitiva della proposta contrattuale della ricorrente.

Del resto, si tratta solo di applicare i tradizionali principi in materia di conclusione "tacita" del contratto (mediante compimento di un atto successivo, come l'individuazione delle carrozze oggetto di manutenzione, che presuppone ed estrinseca all'esterno la volontà della parte di concludere il contratto) ad una fattispecie in cui, per espressa previsione della lettera di invito, era possibile la conclusione del contratto con la forma della corrispondenza commerciale e non era quindi necessaria la consacrazione delle volontà negoziali in unico atto produttivo.

A decorrere dalla ricezione dell'e-mail del 31 ottobre 2006, il contratto tra Trenitalia s.p.a. e la resistente era pertanto da ritenersi definitivamente perfezionato, non essendo più possibili tardivi "ripensamenti" della Stazione appaltante che dovevano trovare espressione all'interno di una fase ormai definitivamente conclusa con l'invio alla O.M.F.E.S.A. di una comunicazione che presupponeva (ed estrinsecava tacitamente) la conclusione definitiva del contratto.

Venendo alla legittimità del provvedimento di revoca impugnato con i motivi aggiunti depositati in data 19 maggio 2007, la Sezione deve rilevare come, anche aderendo alla tesi che ritiene possibile procedere all'annullamento in sede di autotutela della delibere di aggiudicazione dopo la formazione del vincolo negoziale (in questo senso, si veda Consiglio Stato, sez. IV, 31 ottobre 2006, n. 6456), l'esercizio del potere di autotutela da parte di Trenitalia s.p.a. nella fattispecie concreta sia certamente viziato sotto il profilo della legittimità.

La resistente pone a base della revoca da ultimo intervenuta due circostanze giustificative, costituite:

1) dalla impreveduta necessità di "internalizzare" la manutenzione già affidata alla ricorrente, a seguito di una «significativa e non prevedibile carenza di disponibilità di vetture di I classe della tipologia a 200 km/h (Z1 e Gran Comfort) ... determinata da ritardi nella restituzione all'esercizio delle carrozze della suddetta tipologia comprese in progetti di ristrutturazione in corso»;

2) da una sostanziale valutazione negativa del Piano della Qualità della prestazione presentato dalla ricorrente che avrebbe evidenziato due aspetti problematici (il luo-

go di restituzione delle carrozze oggetto di manutenzione e la tempistica di lavorazione) tali da non rendere credibile il rispetto dei tempi fissati per la piena operatività delle carrozze revisionate.

A questo proposito, la Sezione non può mancare di rilevare come la citata e-mail del 31 ottobre 2006 permetta di risolvere agevolmente le due problematiche.

In primo luogo, deve infatti rilevarsi come la documentazione depositata in giudizio dalla difesa della resistente Trenitalia s.p.a. non abbia dimostrato l'unico fatto rilevante nella presente fattispecie, costituito dall'avvenuta "internalizzazione" della manutenzione delle carrozze precisamente individuate (tramite numero di matricola) nella e-mail del 31 ottobre 2006 (che ha quindi integrato il contenuto contrattuale, individuando precisamente le carrozze oggetto di manutenzione e i tempi di consegna) e non di altre carrozze che nulla hanno a che vedere con la presente vicenda; in altre parole, il fatto che Trenitalia s.p.a. abbia operato un massiccio ricorso all'internalizzazione della manutenzione nel periodo in riferimento non può esplicitare effetti su una vicenda che riguarda alcune carrozze precisamente individuate e rispetto alle quali manca del tutto la prova che la manutenzione sia stata effettuata negli stabilimenti della resistente o sia stata comunque effettuata.

Anche per quello che riguarda la valutazione del Piano della Qualità della prestazione presentato dalla ricorrente, quanto sopra argomentato in ordine al momento di conclusione del contratto (riportato alla ricezione della e-mail del 31 ottobre 2006) permette di rilevare come si tratti di valutazioni che dovevano trovare espressione nella fase precedente l'aggiudicazione definitiva e quindi di problematiche che non possono essere più ridiscusse, una volta che il contratto si sia definitivamente perfezionato, anche se in forma tacita.

In definitiva, i motivi aggiunti depositati in data 16 maggio 2007 devono essere accolti e deve essere disposto l'annullamento del provvedimento 5.4.2007 DTAI/LCC.PIC 0159 RG con il quale Trenitalia s.p.a. ha revocato la gara a procedura negoziata, indetta con la lettera-invito UTRMP.SM/332 prot. n. 493 del 22.5.2006 e definitivamente aggiudicata alla ricorrente. L'annullamento della delibera di revoca ripristina sotto ogni aspetto il vincolo negoziale esistente tra le parti a seguito della definitiva conclusione del contratto in questione e permette quindi la piena soddisfazione dell'interesse della ricorrente per effetto dell'adempimento contrattuale o della proposizione degli ordinari strumenti avverso l'inadempimento contrattuale; del resto, l'azione risarcitoria dedotta in giudizio, in quanto attinente ad un vincolo contrattuale ormai perfezionato tra le parti, non rientrerebbe comunque nella giurisdizione del Giudice amministrativo ma dell'A.G.O. (in questo senso, Consiglio Stato, sez. V, 14 giugno 2004, n. 3819) e la stessa ricorrente non prospetta alcun danno (come, ad es., il danno da ritardo nell'esecuzione della prestazione) indipendente dall'interesse "finale" ad eseguire la presta-

zione che è inglobato nel vincolo contrattuale e deve quindi seguirne le sorti, sia per quello che riguarda la giurisdizione, sia per quello che riguarda le modalità di tutela.

Le spese di giudizio devono essere poste a carico della resistente e liquidate, in mancanza di nota spese, in complessivi € 4.000,00 (quattromila).

...Omissis...

IL COMMENTO

di Daniele Marongiu

Il ruolo della posta elettronica semplice ha un peso differente nella prassi, dove è il mezzo telematico più adoperato, e nella legislazione, dove assume un ruolo secondario rispetto a strumenti più avanzati sotto il profilo delle garanzie, come la posta elettronica certificata e la firma elettronica qualificata. La giurisprudenza si inserisce nella distanza fra questi due diversi approcci all'uso dell'e-mail in ambito amministrativo, mostrando una tendenza a riconoscere il valore che essa ha nella pratica comune.

1. La posta elettronica: lo scarto tra l'uso comune e la legislazione

La posta elettronica rappresenta oggi, nell'universo dell'amministrazione digitale, uno strumento che più di altri permette di cogliere l'esistenza di un *gap* tra la prassi e la normazione. L'e-mail infatti costituisce, da un lato, il mezzo più usato nelle comunicazioni elettroniche tra l'Amministrazione e i cittadini, ma risulta essere, nello stesso tempo, uno strumento poco incentivato dalla legge, nella quale emerge la preferenza per sistemi di comunicazione che siano più "robusti" dal punto di vista delle garanzie, sistemi che tuttavia non possono essere ancora considerati, oggi, di uso comune.

La ragione di ciò è connessa al fatto che l'e-mail (semplice) si è diffusa spontaneamente - dapprima nelle comunicazioni tra privati, ma successivamente anche in ambito amministrativo - come mezzo efficace che, pur non accorpando certezze formali circa la provenienza e l'inalterabilità dei dati trasmessi, può essere accettato in un regime di ragionevole fiducia tra gli interlocutori (1). Quando il Legislatore, intervenendo in tale contesto, ha disciplinato le comunicazioni telematiche in ambito amministrativo, ha sì ammesso in linea generale l'uso della comune posta elettronica (nell'articolo 45 e nel primo comma dell'articolo 47 del decreto legislativo 7 marzo 2005, n. 82), tuttavia ha previsto che in determinate circostanze, in cui occorre un livello più elevato di certezza, si debba ricorrere al sistema rafforzato della posta elettronica certificata, o alla sottoscrizione del messaggio inviato via mail con procedure di firma elettronica qualificata (2).

Ciò è evidente, in particolare, nella formulazione dell'articolo 47 del decreto 82 che, al terzo comma, quando elenca le condizioni di validità delle trasmissioni telematiche tra uffici nell'ambito del procedimento amministrativo, esclude che in tale circostanza possa avere valore una semplice mail (3). Con riferimento particolare all'ambito specifico delle procedure d'appalto, si registra una conferma della preferenza del Legislatore per strumenti più garantistici, dal punto di vista formale, della comune posta elettronica: il decreto legislativo 12 aprile 2006, n. 163 (il Codice dei contratti pubblici), infatti, al quinto comma dell'articolo 77, prevede l'uso della posta elettronica certificata come unico sistema di scambio telematico tra le stazioni appaltanti e gli operatori economici che partecipano alle procedure di gara (4).

Ovviamente non è qui in discussione la validità intrinseca della posta elettronica certificata e della firma digitale; si sta tuttavia ravvisando, nella ricerca di uno sguardo pragmatico, l'esistenza di una difficoltà nell'adottare a pieno regime tali strumenti (5).

Note:

(1) Cfr. G. Arena, *Certezze pubbliche e semplificazione amministrativa*, in G. Arena, M. Bombardelli, M.P. Guerra, A. Masucci, *La documentazione amministrativa*, Rimini, 2001, 21. L'Autore afferma che esiste "una sorta di economia delle certezze, che induce ad esigere in determinate circostanze un grado più alto di sicurezza, mentre in altre occasioni è sufficiente fermarsi ad un livello inferiore. E non sarebbe economicamente conveniente utilizzare strumenti di certezza particolarmente raffinati (e quindi costosi da confezionare) quando basta una probabilità minore di certezza". A nostro avviso, l'ampio uso della posta elettronica si colloca certamente in questo minimo grado di certezza formale, in cui l'esistenza di un sufficiente grado di fiducia tra mittente e destinatario, e normalmente la disponibilità di canali di comunicazione paralleli, induce a non investire in strumenti che offrano garanzie più elevate.

(2) Su queste norme cfr. il commento di S. Mistichelli in E. Carloni (a cura di), *Codice dell'amministrazione digitale*, Rimini, 2005, 260.

(3) Altrettanto evidente è il caso previsto dall'articolo 65, che nel contemplare le modalità di invio telematico delle istanze non include l'ipotesi del messaggio mandato per posta elettronica.

(4) Su questa disposizione cfr. E. Guarnaccia, *Regole applicabili alle comunicazioni*, commento all'art. 77 del Decreto Legislativo 12 aprile 2006, n. 163, in C. Giurandella (a cura di), *Il Codice dei Contratti Pubblici*, Napoli, 2007, 317.

(5) Si può osservare, peraltro, che proprio l'ipotesi nella quale la legge incentiva l'uso dell'e-mail, ossia gli scambi documentali tra amministrazioni, (segue)

Si può dunque osservare come l'articolo 45 del Codice dell'amministrazione digitale, in questo contesto, assuma sostanzialmente il ruolo di una "norma-ponte" fra la prassi e la legislazione di dettaglio. Da un lato, infatti, l'inserimento nel decreto 82 di detta disposizione, che riconosce in via di principio l'uso della posta elettronica semplice, ha costituito, in qualche modo, un passaggio obbligato per il Legislatore, al fine di non bloccare il più diffuso canale di comunicazione telematica tra uffici e cittadini (6). Dall'altro lato, la portata di tale articolo appare sensibilmente ridimensionata dal tenore delle disposizioni successive, che sono improntate su una preferenza per lo strumento della posta elettronica certificata (7).

Dalla lettura combinata delle norme del decreto 82 deriva, pertanto, che l'uso della posta elettronica semplice è previsto limitatamente ai documenti inviati dai privati verso la Pubblica Amministrazione (8) (come stabilisce l'articolo 45), o ai rapporti interamministrativi (come dispone l'articolo 47 al primo comma) (9), comunque al di fuori del procedimento amministrativo. Viceversa, nessuna norma del Codice contempla (e ancor meno incentiva) l'uso della posta elettronica semplice per l'invio di atti o comunicazioni formali dall'Amministrazione verso i privati in ambito procedimentale (10); al contrario, dalla lettura dell'articolo 6 del decreto 82 appare pacifico che nel flusso "Amministrazione-cittadino" lo strumento naturale debba essere individuato nella posta elettronica certificata.

2. Il caso di specie: il "peso" di una mail nel procedimento di gara

La controversia che ha dato luogo alla sentenza che qui commentiamo costituisce un esempio chiaro dell'esistenza di questo scarto tra prassi e legislazione intorno all'uso della posta elettronica, e la sua analisi è utile per comprendere quale sia la posizione della giurisprudenza al riguardo: in che misura essa tenda a salvare, con pragmatismo, l'elasticità della prassi, o quanto sia invece propensa a sposare, con maggiore rigidità, il taglio più formalistico della legge.

Nel caso specifico su cui verte la decisione del T.A.R. Puglia, accade che, durante l'iter di una gara pubblica che procede secondo i canoni formali, interviene un messaggio di posta elettronica inviato dalla stazione appaltante all'azienda vincitrice. Tale e-mail si colloca dopo l'atto di aggiudicazione provvisoria, ma prima che si sia avuto un provvedimento di aggiudicazione definitiva; essa contiene una richiesta, precisa e circostanziata, di inizio dei lavori appaltati. Poiché l'ente appaltante ha successivamente disposto, in via di autotutela, la revoca della gara, adducendo motivazioni che appaiono in contrasto con il testo della mail, la controversia verte, sostanzialmente, sul valore formale del messaggio di posta elettronica nella sequenza degli atti procedurali, ossia sulla sua capacità di condizionare le fasi successive della gara.

Il giudice, nell'accogliere il ricorso, qualifica la mail come atto pienamente idoneo ad esprimere la volontà di conclusione del contratto e ne deduce che, a seguito della sua trasmissione, l'aggiudicazione definitiva possa considerarsi tacitamente avvenuta. Il Tar dichiara dunque illegittimo il successivo atto di revoca della gara, in virtù del fatto che, se la stazione appaltante avesse ravvisato la necessità di non esternalizzare *in toto* l'attività oggetto della selezione, e se avesse valutato negativamente il Piano della qualità dell'aggiudicataria provvisoria (così motiva infatti l'atto di ritiro), non avrebbe già espresso la manifestazione di volontà volta alla conclusione positiva del contratto, di cui la mail è stata veicolo (11).

Note:

(segue nota 5)

è quella in relazione alla quale la dottrina ritiene che la posta elettronica sia il mezzo meno indicato, in quanto, nei rapporti tra uffici, lo scambio di informazioni dovrebbe avvenire tramite accesso diretto alle banche dati. Cfr. in questo senso G. Duni, *I "viaggi telematici" dell'atto informatico. Note sul procedimento informatico*, in *Quaderni del DAE*, 2003, pubblicato in rete all'URL www.cesda.it/quadernidae, e A. Masucci, *Informatica pubblica*, voce del *Dizionario di diritto pubblico*, Milano, 2006, IV, 3120.

(6)Cfr. E. De Giovanni, *Il codice delle amministrazioni digitali e il procedimento amministrativo elettronico*, in P. Piras (a cura di), *Incontri sull'attività amministrativa e il procedimento*, Torino, 2006, p. 81, ove, in riferimento all'articolo 45 del Codice dell'amministrazione digitale, afferma che esso "è una norma basata sull'esperienza e sulla fiducia perché, a rigore, si potrebbe dire che (...) la trasmissione di un'e-mail può non essere sicura. (...) Questo dunque per una ragione di "correttezza" di rapporti tra pubblica amministrazione e cittadini e anche per un fine di semplificazione dell'azione amministrativa".

(7)Sull'articolo 45 del Codice, e sulla sua lettura in contrapposizione alle norme successive che prevedono sistemi di garanzia più rigidi e formalizzati, cfr. G. Duni, *L'amministrazione digitale*, Milano, 2008, 36 ss. L'Autore esordisce nella sua analisi osservando che "L'art. 45 d.lgs. 82 del 2005 contiene una disciplina di una liberalità tale da suscitare qualche timore anche nelle persone più disponibili alla semplificazione".

(8)Circa tale osservazione cfr. A. Pelosi, *Il Codice dell'amministrazione digitale modifica il valore giuridico della posta elettronica, commento al D.Lgs. 7 marzo 2005*, n. 82, in *I contratti*, 2007, 261.

(9)Con riferimento al primo comma dell'articolo 47 del Codice dell'amministrazione digitale, occorre ravvisare che il Consiglio di Stato, in sede di parere obbligatorio sulla bozza del decreto (il n. 11995 del 7 febbraio 2005), aveva manifestato perplessità sulla validità della formulazione normativa, esprimendosi in questi termini: "Al comma 1 occorre chiarire il significato della formula secondo cui le comunicazioni avvengono «di norma» mediante l'utilizzo della posta elettronica, precisando il parametro che consente all'amministrazione di derogare a tale precetto (es. ragioni tecniche, organizzative o di sicurezza)".

(10)Si osservi che anche la direttiva del Ministro per l'innovazione e le tecnologie del 27 novembre 2003 intitolata "Impiego della posta elettronica nelle pubbliche amministrazioni", che continua a rappresentare tuttora uno degli atti di massima apertura all'uso della mail in ambito istituzionale, contiene le due limitazioni osservate nelle norme del decreto n. 82 del 2005: la posta elettronica è incentivata nei rapporti tra amministrazioni, e al di fuori del procedimento amministrativo.

(11)Poiché, peraltro, nella gara oggetto di giudizio si era espressamente previsto, in sede di lettera d'invito, che la conclusione del contratto potesse avvenire tacitamente mediante scambio di corrispondenza, appare evidente che il fulcro su cui ruota la sentenza non sia la mancanza di un atto contestuale di perfezionamento del contratto, bensì l'ammissibilità della forma elettronica, mediante e-mail semplice (cioè non certificata, e

(segue)

In definitiva, dunque, il tribunale amministrativo considera il messaggio di posta elettronica come atto chiaramente valido e inserito a pieno titolo nella sequenza degli atti della gara, e non come semplice comunicazione informale. In relazione a ciò è possibile formulare alcune riflessioni.

3. Considerazioni sul ruolo della giurisprudenza nella qualificazione della posta elettronica in ambito procedimentale

Dapprima, occorre comprendere quale sia l'iter logico che consente al giudice di accreditare il pieno valore formale della comunicazione inviata per posta elettronica.

In riferimento a ciò, si può osservare innanzitutto che nella decisione del T.A.R. non si menzionano le norme di legge su cui sarebbe fondata la validità giuridica della mail. L'unica esplicitazione di un ragionamento che il giudice presenta come pacifico è data dal fatto che la mail è considerata valida in quanto "mai disconosciuta" dall'ente appaltante, e quindi ad esso imputabile.

L'idea della semplice condizione del mancato riconoscimento come presupposto per la validità dell'atto richiama, implicitamente, il contenuto dell'articolo 2702 del Codice Civile, ove si stabilisce - come è noto - che "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione". Tale accostamento presuppone l'individuazione di una forma di sottoscrizione del messaggio inviato, e in questo senso la decisione in commento si può collegare a quel filone giurisprudenziale che considera la procedura di validazione dell'e-mail (l'inserimento della *user-id* e della *password* dell'utente) come una tipologia di firma elettronica non qualificata, rendendo così applicabile alla posta elettronica il comma 1 bis dell'articolo 20 e il primo comma dell'articolo 21 del Codice dell'amministrazione digitale. Il giudice, insomma, secondo questo orientamento, potrebbe valutare di volta in volta le "caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità" dell'e-mail, e verificare se, in relazione al contesto specifico, essa possa costituire un documento "sottoscritto" (12).

Il dato che scaturisce dalla lettura della sentenza, comunque, non è tanto di carattere formale, quanto di ordine sostanziale.

Certamente dalla decisione emerge che, nello scarto tra una prassi elastica e una normazione rigida, il giudice tende, in modo deciso, a suffragare la validità della prassi o, più correttamente, a fare in modo che la pratica comune (l'uso diffuso della semplice e-mail) sia "salvata" da un'interpretazione estensiva della normativa vigente.

Il giudice, dunque, con la sentenza in commento e con decisioni simili, copre un ampio vuoto normativo, uno spazio che corrisponde alla distanza che si crea, nell'amministrazione digitale, tra la realtà degli uffici e il quadro legislativo. Si tratta di un *vacuum* che il Legisla-

tore avrebbe potuto colmare nel momento in cui ha emanato il Codice dell'amministrazione digitale (13), in quanto nel 2005 si era già posto, in più controversie, il problema del "destino" della posta elettronica non certificata. L'estensore del decreto 82 avrebbe potuto inserire una formulazione espressa che sarebbe potuta andare in due direzioni opposte: assimilare esplicitamente l'e-mail, *ex lege*, alla firma elettronica semplice, oppure negare espressamente tale qualificazione della posta elettronica; in ogni caso avrebbe sciolto un dubbio che ancora genera dibattiti e alimenta il contenzioso. Così tuttavia non è avvenuto, e questa è la ragione per la quale si sta progressivamente accrescendo il ruolo della giurisprudenza nella valutazione di fattispecie concrete difficilmente qualificabili negli schemi della normativa vigente.

Note:

(segue nota 11)

sprovvisa di sottoscrizione digitale), nell'invio della comunicazione all'impresa aggiudicataria.

(12) Sulla formazione di tale giurisprudenza, cfr. A. Pelosi, *Il Codice dell'amministrazione digitale modifica il valore giuridico della posta elettronica*, cit., 261; M. Lupano, *Natura dell'e-mail, sua efficacia probatoria nella normativa vigente e nel d. lgs. 7.3.2005, n. 82*, nota a Trib. Mondovì, decreto ingiuntivo, 7 giugno 2004, in *La nuova giurisprudenza civile commentata*, 2005, I, 936 ss.; M. Cuniberti, *Posta elettronica e telefax: le nuove notificazioni e comunicazioni, il «documento informatico» e le «firme elettroniche»*, in *Giurisprudenza di merito*, 2007, 700, il quale cita Trib. Bari, sez. IV, 2 giugno 2005 (ord.). Cfr. infine P. Giacalone, *La normativa sul governo elettronico*, Milano, 2007, 243, che cita, oltre al decreto ingiuntivo del tribunale di Mondovì già menzionato, i decreti ingiuntivi del tribunale di Bari del 20 gennaio 2004, n. 89, e del tribunale di Cuneo del 15 dicembre 2003, n. 848.

(13) Con riferimento alle carenze del Codice dell'amministrazione digitale nella parte in cui disciplina il valore probatorio del documento sottoscritto con firma elettronica, cfr. M. Lupano, *Natura dell'e-mail*, cit., 941.

Osservatorio della giurisprudenza italiana

a cura di Iacopo Pietro Gimino e Francesco di Giommo

■ Tutela della riservatezza e *files sharing*

PREVALE IL DIRITTO ALLA RISERVATEZZA SULLE NECESSITÀ DI REPRESSIONE DELLE VIOLAZIONI AL DIRITTO D'AUTORE

Tribunale Roma, Sez. IX, ord., 17 marzo 2008 - Giud. Muscolo

Non può essere disposta la *discovery* sui dati personali degli utenti di un servizio di *files sharing* laddove sia assunta la commissione di un illecito civile, necessitando - ai fini della legittimità della misura - la commissione di un fatto di reato.

Con la sentenza in commento il Tribunale di Roma è tornato sulla questione del conflitto tra tutela dei dati personali e repressione degli illeciti riguardanti lo scambio *on-line* di materiale protetto da diritto d'autore. La parte ricorrente proponeva una domanda, da essa qualificata come domanda di *discovery* in via cautelare, il cui *petitum* era costituito dalle informazioni sui dati di consumatori utenti del servizio informatico e utilizzatori dei programmi di *file sharing*, e la *causa petendi* dalla lesione dei diritti di proprietà intellettuale sulle opere scambiate gratuitamente in rete, asseritamente fondata sugli artt. 8.3 della direttiva CE 2001/29 (sulla armonizzazione di taluni aspetti del diritto di autore e dei diritti connessi nella società della informazione), sugli artt. 8, 9 e 11 della direttiva CE 2004/48 (c.d. direttiva *enforcement*) e sugli artt. 156 e 156 *bis* e 156 *ter* l. n. 633/1941 sul diritto di autore. La medesima parte argomentava la possibilità giuridica della propria domanda sul presupposto di una serie di "errori" del legislatore storico, postulando, quanto all'art. 8.3 della dir 2001/29, che nel testo italiano l'uso del termine "inibitoria" invece di quello "ingiunzione" sarebbe frutto di un errore di traduzione e, circa l'art. 156 *bis* e 156 *ter*, che la mancata menzione, tra i destinatari dell'ordine, dei terzi in possesso delle informazioni, costituirebbe una omissione materiale in sede di recepimento della dir. 2004/48.

Il Tribunale di Roma, qualificata la azione proposta quale istanza di *discovery* delle informazioni sulla rete di distribuzione di servizi di *file-sharing* diretta al *provider* del servizio informatico, ne ha rinvenuto il fondamento negli artt. 156 *bis* e 156 *ter* L.d.A. Così qualificata la domanda - osserva il Tribunale - la questione della sua ammissibilità sotto il profilo della strumentalità deve rap-

portarsi non ad una azione di merito, bensì al processo in cui utilizzare le prove raccolte con la *discovery*, e a questo proposito deve rilevarsi che l'art. 156 *ter* menziona espressamente anche il processo cautelare, in piena attuazione dell'art. 24 Cost., che, nella interpretazione più recente, tutela parimenti il diritto di azione ordinaria e di azione cautelare. Questione centrale è quella della ammissibilità della *discovery* in via preventiva rispetto al processo (di merito o cautelare) da instaurare, che il Tribunale risolve positivamente, con una interpretazione estensiva delle citate norme sulla *discovery*, che la ammettano anche come misura di istruzione preventiva, per assicurarsi anticipatamente una prova altrimenti a rischio di assunzione. Quanto al merito della domanda proposta e cioè, alla questione dell'uso della *discovery* per la comunicazione di dati personali, il giudice romano richiama quanto già statuito dalla Corte di Giustizia. Questa ha affermato che: "il diritto comunitario richiede che detti Stati, in occasione della trasposizione di tali direttive, abbiano cura di fondarsi su una interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Inoltre in sede di attuazione delle misure di recepimento delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su una interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come ad esempio, il principio di proporzionalità". Sulla scorta di tale rilievo il Tribunale ha affermato che il legislatore nazionale, attuando tutte le direttive in materia, ha effettuato la scelta di limitare le deroghe alle norme protettive della riservatezza al caso di illeciti penali, senza estenderle al caso di illeciti civili; scelta compatibile con il diritto comunitario come interpretato dalla Corte di Giustizia. Sicché, in conclusione, rigettando il ricorso - nell'ordinanza in rassegna - si afferma che l'esecuzione dell'ordine di *discovery* si risolverebbe in una comunicazione dei dati personali dei consumatori senza alcun consenso di coloro che operano sulla rete sulla presunzione di anonimato. La misura violerebbe, pertanto, il diritto alla riservatezza dei medesimi.

Nota:

(*) Il testo integrale delle disposizioni illustrate è pubblicato sul sito www.ipsoc.it/drittodellinternet.

■ E-government**EQUIVALENZA DEI DOCUMENTI AMMINISTRATIVI INFORMATICI**

Consiglio di Stato, 18 marzo 2008, n. 1127 - Cons. Rel. Taormina

L'archivio informatico di una P.A. deve essere considerato alla stregua di un registro (costituito da materiale non cartaceo) tenuto da un soggetto pubblico.

Con un unico motivo di ricorso la ricorrente chiede la revocazione della sentenza resa, ai sensi dell'art. 395, n. 3), c.p.c. (revocazione straordinaria) per aver reperito - dopo la pubblicazione della decisione - documenti decisivi, non prodotti nel giudizio concluso per cause non ad essa imputabili. Tale documento (rinvenuto il 7.10.2006) consiste in un "documento informatico INPS". Le circostanze, cristallizzate nel predetto documento informatico, dimostrerebbero - a parere del ricorrente - l'irregolarità contributiva della aggiudicatrice la gara d'appalto, in contrasto con quanto accertato con la sentenza, di cui si chiede la revocazione.

Ai fini della presente rassegna, ciò che interessa rilevare è la qualificazione data sotto il profilo della natura della predetta certificazione INPS, della quale si vorrebbe dimostrare la ideologica falsità. Ritiene il Collegio indubbio che essa abbia natura e portata fidefaciente, in armonia con quanto afferma la costante giurisprudenza penalistica di legittimità, secondo cui l'estratto conto contributivo rilasciato dall'INPS è atto pubblico e non certificato amministrativo. Ricorre pertanto il delitto di falso in atto pubblico qualora il dipendente INPS determini l'alterazione dei dati contenuti nel supporto informatico creando una falsa posizione contributiva relativa ad un soggetto assicurato. (Cass. pen., sez. V, 19 febbraio 2003, n. 15774). Ed ancora l'archivio informatico di una P.A. deve essere considerato alla stregua di un registro (costituito da materiale non cartaceo) tenuto da un soggetto pubblico, con la conseguenza che la condotta del pubblico ufficiale che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici di pertinenza della P.A., confezioni un falso atto informatico destinato a rimanere nella memoria dell'elaboratore, integra una falsità in atto pubblico, a seconda dei casi, materiale o ideologica (art. 476 e 479 c.p.), ininfluyente peraltro restando la circostanza che non sia stato stampato alcun documento cartaceo (Cass. pen., sez. V, 18 giugno 2001, n. 32812).

■ Documento informatico**LEGITTIMA L'ESCLUSIONE DALLA GARA D'APPALTO IN IPOTESI DI DOCUMENTAZIONE INFORMATICA PRIVA DI FIRMA DIGITALE**

T.A.R. Napoli, sez. I, 8 febbraio 2008, n. 664

Nell'ambito d'una gara d'appalto deve escludersi che un documento informatico privo di firma digitale o equipollente possa sostituire sul piano formale un documento cartaceo con sottoscrizione olografa.

Nel giudizio in oggetto il T.A.R. è tornato sulla questione del deposito di documenti di gara su supporto informatico. Rilevano in proposito i giudici che, del disciplinare di gara, era espressamente prevista l'esclusione nel caso di presentazione dei documenti componenti l'offerta tecnica privi della sottoscrizione di tutte le imprese partecipanti ad un costituendo raggruppamento. Si afferma inoltre che tale adempimento, conforme alla comune prassi nelle gare pubbliche, implica un minimo onere di diligenza da parte dei partecipanti alla procedura e risponde ad un rilevante interesse della stazione appaltante di evitare ogni possibilità di contestazione in ordine al contenuto impegnativo delle offerte tecniche presentate dalle concorrenti. Questa esigenza assume particolare evidenza e rilevanza nel caso di offerte presentate da costituendi raggruppamenti di imprese, poiché prima della loro costituzione la capogruppo designata non ha alcun potere di esprimere la volontà delle future mandanti (cfr. Cons. St., sez. IV, 11 aprile 2007, n. 1653); per cui l'assunzione di un impegno negoziale con la sottoscrizione non può essere surrogata da altri fatti conclusivi, quali la genuinità e la sicura provenienza del plico. Ciò premesso il Collegio afferma che per quanto riguarda la produzione della anzidetta documentazione anche su supporto informatico, non risultando nella specie l'apposizione di firma elettronica digitale (nel rispetto delle regole tecniche dettate dal d.lgs. n. 82/2005), è da escludere che questo strumento possa sostituire sul piano formale un documento cartaceo con sottoscrizione olografa.

E-MAIL E REATO DI FALSO IN ATTO PUBBLICO

Tribunale di Brescia, 11 marzo 2008, n. 348 - G.u.p. Benini

L'assenza di sottoscrizione informatica e pertanto, di esatta individuazione dell'organo da cui l'atto promana non consentono di qualificare il messaggio di posta elettronica privo dei requisiti di cui sopra alla stregua di atto pubblico.

Il Tribunale si è pronunciato sulla configurabilità del reato di cui agli artt. 476 e 479 c.p. nel caso di un pubblico ufficiale - Maresciallo Capo in servizio presso il locale Nucleo Operativo del Comando Provinciale dei Carabinieri, il quale, avendo accesso, per ragioni d'ufficio, al programma per l'invio della posta elettronica installato in uno dei p.c. presenti negli uffici del predetto Nucleo Operativo, nell'esercizio delle sue funzioni formava e inviava alla Stazione dei Carabinieri di Dello una falsa e-mail, contenente la richiesta di informazioni anagrafiche.

Nell'escludere la sussistenza dell'ipotizzato reato il giudice ha affermato che è indispensabile, ai fini della configurazio-

ne del delitto di falso in atto pubblico, la riconoscibilità dell'autore dell'atto; cosa che si ottiene normalmente con la sottoscrizione. È certo vero - si legge nella motivazione - che la sottoscrizione vergata a mano può essere sostituita da stampiglie personali, laddove la legge non richieda l'autografia come garanzia formale per l'individuazione dell'autore. Va però sottolineato che il messaggio di posta elettronica (non certificato ai sensi del d.p.r. 11 febbraio 2005, n. 68, e privo di firma digitale a crittografia asimmetrica ai sensi

del d.lgs. 7 marzo 2005, n. 82) non può fornire alcuna certezza circa la propria provenienza o sull'identità dell'apparente sottoscrittore, bastando intervenire sul programma di posta elettronica perché chi riceve il messaggio lo veda come se fosse inviato da diverso indirizzo.

L'assenza di sottoscrizione e di esatta individuazione dell'organo da cui l'atto promana non consentono di qualificare il messaggio di posta elettronica privo dei requisiti di cui sopra alla stregua di atto pubblico.

RIVISTE



Il Lavoro nella giurisprudenza

Mensile di giurisprudenza e dottrina

Direzione scientifica: Franco Carinci, Michele Miscione

Periodicità: mensile

Il mensile che informa con puntualità sulle novità giurisprudenziali in tema di rapporto di lavoro, previdenza sociale, prevenzione infortuni e igiene del lavoro, processo del lavoro. Accanto a qualificati articoli di dottrina, contiene numerose rubriche dedicate alla giurisprudenza della Corte di Cassazione e alla magistratura di merito; le sentenze più significative e innovative sono pubblicate integralmente e commentate autorevolmente.

Il **servizio online**, compreso nel prezzo e riservato esclusivamente agli abbonati è

consultabile all'indirizzo **www.ipsoa.it/il-lavoronellagiurisprudenza** e permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 200,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 – fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- **www.ipsoa.it**

Osservatorio di diritto internazionale ed europeo

a cura di Giovanni Maria Riccio, Guido Scorza e Giovanni Ziccardi

■ Contraffazione di marchio, concorrenza sleale, link commerciali

Tribunal de Grande Instance de Lyon, 13 marzo 2008

Google è responsabile di contraffazione di marchio e concorrenza sleale qualora, nell'ambito del proprio servizio Adwords, consenta l'associazione di un altrui marchio registrato ad un link sponsorizzato relativo ad un sito attraverso il quale vengano erogati servizi analoghi a quelli contraddistinti dal marchio contraffatto .

La decisione del Tribunale di Lione che si annota affronta, ancora una volta, l'annosa questione della responsabilità di Google nell'ipotesi in cui un cliente del proprio servizio promozionale Adwords, usi detto servizio per associare un altrui marchio registrato al *link* al proprio sito internet attraverso il quale siano erogati servizi analoghi a quelli contraddistinti dal marchio registrato.

Nel caso di specie una società operante nel settore dei micropagamenti per via telefonica, utilizzando il servizio Adwords di Google, aveva fatto sì che ogni qualvolta un utente avesse "lanciato" una ricerca attraverso Google utilizzando quale parola chiave il marchio del concorrente, il motore di ricerca gli restituisse tra i "link sponsorizzati" anche quello alla propria pagina web.

Google, nel costituirsi in giudizio, aveva tra l'altro dedotto la propria impossibilità di verificare se le parole scelte dai propri clienti corrispondessero a marchi registrati.

Tale eccezione, tuttavia, secondo i giudici non poteva ritenersi sufficiente a consentire alla società titolare del celebre motore di ricerca di sottrarsi alle proprie responsabilità.

L'associazione tra il marchio contraffatto ed il *link* al sito internet del contraffattore, infatti, costituisca oggetto specifico del contratto intercorso tra quest'ultimo e Google (France).

■ Proprietà industriale, utilizzo di marchio notorio su Ebay

Tribunal de Grande instance de Paris, 18 marzo 2008

Configura una violazione dei diritti di privativa del titolare del marchio l'utilizzo di segni corrispondenti ad un marchio notorio per la commercializzazione su E-bay di beni diversi ancorché correlati ai prodotti o servizi

contraddistinti da detto marchio.

Il Tribunale di Parigi nella decisione che si annota ha condannato un utente della piattaforma di aste telematiche Ebay per violazione dei diritti di privativa industriale della SFR - Société Française du Radiotéléphone per aver posto in vendita 3 modelli di lettera-tipo da utilizzarsi per la risoluzione dei contratti di abbonamento con la citata compagnia di telecomunicazioni.

Secondo i giudici del Tribunale di Parigi, infatti, pur non integrando l'utilizzo di tale marchio una fattispecie di contraffazione, esso costituisce, comunque, una violazione dei diritti di privativa industriale della SFR.

L'utente, infatti, ben avrebbe potuto commercializzare le proprie lettere-tipo senza utilizzare il citato marchio che ha, evidentemente, scelto di usare all'unico fine di accrescere la visibilità della propria offerta commerciale, sfruttando così indebitamente la notorietà dell'altrui segno distintivo.

■ Condizioni generali di contratto

Michele Mazur v. eBay Inc., Hot Jewelry Auctions.com d/b/a Jewelry Overstock Auctions and Paramount Auctions, et al., No. C 07-03967 MHP (N.D. Ca., March 4, 2008)

Le condizioni generali di contratto di abbonamento ad un sito di aste on-line non può contenere clausole che siano eccessivamente gravose per l'abbonato.

Una corte federale statunitense ha stabilito che le clausole di risoluzione delle controversie contenute nelle condizioni generali di contratto di un sito che effettua aste on-line (Hot Jewelry Auctions.com) sono inefficaci nei confronti dell'utente che ritiene di aver subito una lesione dall'asta alla quale ha partecipato.

Nel caso di specie, tali condizioni prevedevano che le parti avrebbero dovuto risolvere le loro controversie dinanzi ad un collegio arbitrale, senza poter essere difesi da legali e senza poter ricorrere a testimoni. Per questo motivo, la corte ha ritenuto che l'attore potesse adire l'autorità giudiziaria. Allo stesso modo, la Corte ha consentito che l'attore po-

Nota:

(*) Il testo integrale delle disposizioni illustrate è pubblicato sul sito www.ipsoc.it/dirittoellinternet.

tesse citare in giudizio la società E-Bay che, nel suo servizio di aste "live!", ospitava l'altra società convenuta. Tuttavia, è interessante osservare che la corte ha ritenuto che E-Bay non potesse essere corresponsabile per le violazioni relative all'asta, ma esclusivamente perché aveva garantito la professionalità del gestore dell'asta.

■ Contratto concluso da minori

A.V., et al. v. iParadigms, Limited Liability Company
Civ. Act. No. 07-0293 (E.D. Va., March 11, 2008)

Un dipendente non può visionare materiale pornografico durante l'orario di ufficio. In questo caso, grava sul datore di lavoro l'obbligo di adottare misure idonee ad evitare che il proprio dipendente, che scarica fotografie che ritraggono minori coinvolti in atti sessuali, compia atti che possano ledere i diritti dei terzi.

Una corte statunitense ha statuito è valido il contratto nel quale un minore clicca sull'icona "accetta" che appare al termine delle condizioni generali di contratto.

Nel caso di specie, alcuni studenti delle scuole superiori hanno utilizzato il sito "turnitin", specializzato nel reperire materiale plagiato. Per adoperare tale servizio, i minorenni hanno dovuto caricare alcuni loro scritti (si trattava di compiti per la scuola) all'interno di un database contenente i testi da comparare, per evidenziare eventuali plagii. Gli studenti, citando il sito, chiedevano che fosse dichiarata la violazione del diritto d'autore che gli stessi pretendevano di vantare sui loro compiti.

La corte, però, ha rigettato la domanda, affermando che gli stessi erano vincolati alle condizioni contrattuali, dal momento che avevano comunque ottenuto dei benefici dall'utilizzo del sito. Peraltro, a giudizio della corte, non vi sarebbe violazione del copyright, dal momento che gli studenti avevano acconsentito ad un'utilizzazione libera (coperta dalla *doctrine* del *fair use*) dei materiali in questione.

RIVISTE

Il Diritto industriale

Tutta l'informazione su marchi, brevetti, concorrenza, diritto d'autore e internet

Direttore scientifico: Giorgio Floridia

Periodicità: bimestrale



La rivista che dal 2003 diventa **bimestrale**, per essere sempre più tempestiva, propone un intervento sistematico sulle principali novità normative - nazionali e comunitarie - e giurisprudenziali in materia di marchi, brevetti, concorrenza sleale, antitrust, pubblicità e diritto d'autore. Dà conto, inoltre, di proposte di legge, regolamenti e direttive. Nella sezione Giurisprudenza sono riportate, con note e commenti, le decisioni della Corte di giustizia CE, della Corte Costituzionale, della Corte di Cassazione, dei giudici di merito e della Commissione dei ricorsi, i provvedimenti dell'Autorità garante della concorrenza e del mercato

e le pronunce del Giuri di Autodisciplina pubblicitaria.

Il servizio online, riservato esclusivamente agli abbonati e consultabile all'indirizzo www.ipsoa.it/ildirittoindustriale, permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 140,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 - fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- www.ipsoa.it

Le nuove procedure di captazione

Il sistema unico nazionale d'intercettazione tra contenimento della spesa e regole processuali

di Alberto Cisterna

Le tensioni nei rapporti tra apparati di giustizia e pubblica opinione non di rado si incentrano sull'uso delle intercettazioni e sui costi che esse comportano. Le spese che l'amministrazione sopporta per le prestazioni rese dai gestori di telefonia e per il noleggio presso privati degli apparati di intercettazione ha indotto il Parlamento a prevedere nella legge finanziaria 2008 la costituzione, a cura del Ministero della giustizia, di "un sistema unico nazionale, articolato su base distrettuale di corte d'appello, delle intercettazioni telefoniche, ambientali e altre forme di comunicazione informatica o telematica disposte o autorizzate dall'autorità giudiziaria". L'obiettivo è quello di contrarre le spese per il noleggio degli apparati e di pattuire con i gestori telefonici una riduzione delle somme per l'allaccio agli impianti. Deve escludersi che l'autorità ministeriale possa disporre la costituzione di un "centro unico d'intercettazione", poiché la disposizione legislativa consente l'implementazione di una rete di servizio volta principalmente a ridurre il numero dei fornitori di apparati e i connessi costi di noleggio, con l'intento di arginare le spese di giustizia per le intercettazioni e di contrarre gli ambiti di autonomia negoziale di ciascun ufficio di procura nei noleggi.

1. Fenomenologia della crisi

Le tensioni che oramai da oltre un decennio attraversano il rapporto tra apparati di giustizia e pubblica opinione non di rado si incentrano sull'utilizzazione delle intercettazioni a fini investigativi. L'intrusione che il mezzo di prova realizza nella vita quotidiana dei cittadini, in uno con la controversa interpretazione del contenuto letterale delle conversazioni, provoca polemiche per lo più destinate a reclamare un irrigidimento delle procedure di captazione sia in relazione alla loro durata che alle ipotesi delittuose consentite. Esiste, accanto a un'argomentazione per così dire *in iure* che reclama una più cogente protezione della *privacy*, un altro genere di rilievi che enfatizza i costi, davvero molto elevati, del sistema di intercettazione nel nostro paese e denuncia l'incidenza finanziaria della bulimia captativa (1). La denuncia delle spese che l'amministrazione sopporta per le prestazioni rese dai gestori di telefonia e per il noleggio presso privati degli apparati di intercettazione costituisce un'efficace argomentazione per assecondare la crisi di fiducia della pubblica opinione verso questo delicato strumento investigativo. Nella «Relazione annuale sullo stato della giustizia in Italia» presentata il 16 gennaio 2008 dal Ministro della giustizia è dato leggere: «nel solo anno 2006, realizzando un'accorta circolazione delle informazioni tra i diversi uffici deputati alla stipulazione dei contratti, abbiamo portato la spesa per in-

tercettazioni telefoniche da 308 a 229 milioni di euro, malgrado l'incremento dei bersagli intercettati di oltre 11.000 unità, con un risparmio netto di quasi 80 milioni, in termini percentuali pari al 25%. Abbiamo ereditato una posizione debitoria al 31 dicembre 2006 di oltre 219 milioni di euro, e la presentiamo oggi al Paese con un'esposizione di poco più di 143 milioni di euro, in riduzione del 34% in quota percentuale, e di quasi 76 milioni in cifra assoluta». Com'è dato a tutta prima constatare si tratta di cifre che incidono significativamente sul bilancio del dicastero e che hanno determinato il consolidarsi di un'esposizione debitoria verso i fornitori delle prestazioni connesse all'esecuzione delle

Note:

(1) Il consolidarsi di prassi intercettative a largo spettro è questione che, invero, non affligge in esclusiva il nostro Paese, come da qualche parte viene strumentalmente fatto intendere, ma che - anche a seguito delle attività terroristiche dell'11 settembre 2001 - ha investito anche altri ordinamenti cfr. sul punto E. Falletti, *La lotta al terrorismo e la violazione della sfera privata individuale: il caso delle intercettazioni abusive di massa. Commento a United States District Court Eastern District of Michigan Southern Division, August 17th 2006, American Civil Liberties Union and Others v. National Security Agency and Others, Case No.06-CV-10204 - Hon. Anna Diggs Taylor*, in questa Rivista, 2007, 50. In dottrina P. Ferrua, *Privacy e riservatezza nella riforma delle intercettazioni*, in *Studi sul processo penale*, III, Torino, 1997, 119 e da ultimo, S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

attività captative talmente elevata da indurre il Parlamento con la legge n. 27 dicembre 2006, n. 296 (finanziaria 2007) a statuire che «non sono soggetti ad esecuzione forzata i fondi destinati al pagamento di spese per servizi e forniture aventi finalità giudiziaria o penitenziaria, nonché gli emolumenti di qualsiasi tipo dovuti al personale amministrato dal Ministero della giustizia e dalla Presidenza del Consiglio dei Ministri, accreditati mediante aperture di credito in favore dei funzionari delegati degli uffici centrali e periferici del Ministero della giustizia, degli uffici giudiziari e della Direzione nazionale antimafia e della Presidenza del Consiglio dei ministri» (art. 1 comma 1348). Attualmente risultano dovuti ai soli gestori delle reti telefoniche e telematiche decine di milioni di euro per attività di intercettazione disposte dagli uffici di procura e contabilizzati a carico del Ministero della giustizia secondo un meccanismo di imputazione delle cosiddette spese di giustizia che, prima o poi, dovrà essere seriamente riformato. Non può infatti ulteriormente tollerarsi che le sedi giudiziarie conducano indagini a costo illimitato e che l'amministrazione centrale del dicastero copra le spese a rendicontazione, senza alcun serio budget preventivo.

2. Le novità della l. 24 dicembre 2007 n. 244

La legge finanziaria 2008 (art. 2, commi 82 e 83) segna un punto di svolta, giacché per la prima volta si abbandona la via degli interventi di *moral suasion* sugli operatori giudiziari, attuati in parte anche attraverso accessi ispettivi di natura contabile volti a contenere i tetti di spesa, e si tenta di realizzare un ulteriore contenimento dei costi agendo su un duplice versante: a) da un lato attraverso la costituzione di «un sistema unico nazionale, articolato su base distrettuale di corte d'appello, delle intercettazioni telefoniche, ambientali e altre forme di comunicazione informatica o telematica disposte o autorizzate dall'autorità giudiziaria»; b) dall'altro mediante l'adozione dei provvedimenti di cui dall'art. 96 del Codice delle comunicazioni e relativi al tariffario delle prestazioni obbligatorie cui sono tenuti gli operatori telefonici e telematici per esigenze di sicurezza e di giustizia.

L'obiettivo più immediato, quindi, è quello di contrarre le spese per il noleggio degli apparati (allo stato nebulizzato in decine di micro-mercati operanti presso ciascuna procura e gestiti talvolta da singoli magistrati) e di pattuire con i gestori telefonici e delle reti telematiche una riduzione delle somme corrisposte per ciascun allaccio agli impianti, sia pure nella difficile condizione che vede il Ministero della giustizia esposto finanziariamente, come detto, per decine di milioni di euro nei confronti della società telefoniche. D'altronde, per tale ultimo profilo, l'art. 2 comma 82 sembra recare, con scarsa convinzione, una mera esortazione ad adottare le determinazioni tariffarie già previste dal Codice delle comunicazioni, omettendo qualsivoglia prescrizione circa modalità o scadenze ulteriori. Insomma il tutto resta rimesso alla buona volontà dei contraenti di trovare una soluzione

che determini una contrazione dei corrispettivi dovuti agli operatori privati.

Decisamente più innovativa appare la previsione, recata sempre dalla l. n. 244/2007, di un «sistema unico nazionale, articolato su base distrettuale di corte d'appello». In questo caso il legislatore ha avuto cura di indicare lo *start-up* («Il Ministero della giustizia provvede entro il 31 gennaio 2008 ad avviare la realizzazione») e sebbene al momento non si registrino iniziative degne di nota, v'è da sottolineare che la disposizione lascia il dicastero sostanzialmente arbitro di determinarsi circa l'opzione tecnologica idonea a implementare il sistema.

Si tratta, tuttavia, di accertare se il ventaglio delle soluzioni a disposizione dell'autorità amministrativa possa includere la costituzione di un «centro unico d'intercettazione» - per come si è da taluno paventato evocando il rischio di scenari massivi di controllo - ovvero se la disposizione legislativa si limiti a consentire la costituzione di una rete di servizio volta principalmente a ridurre il numero dei fornitori di apparati e i connessi costi di noleggio.

A sostegno di un assetto, per così dire, meno invasivo dell'azione ministeriale può sicuramente dedursi la circostanza che la norma trovi la propria collocazione sistematica all'interno della legge di bilancio. La *sedes materiae* sta a indicare che intento prioritario dell'intervento normativo è quello di arginare le spese di giustizia sul versante delle intercettazioni armonizzando le attività di noleggio degli apparati e contraendo gli ambiti di autonomia negoziale di ciascun ufficio di procura e, spesso, di singoli magistrati. In coerenza con siffatto orientamento legislativo possono svolgersi talune precisazioni.

3. Il controllo della spesa per le intercettazioni

In primo luogo un argomento a sostegno si rinviene nell'art. 2, comma 83, della legge finanziaria 2008 laddove si prevede che «il Ministero della giustizia, di concerto con il Ministero dell'economia e delle finanze, procede al monitoraggio dei costi complessivi delle attività di intercettazione disposte dall'autorità giudiziaria». Si trattava di assegnare un apprezzabile coefficiente di concretezza all'esigenza primaria che ha ispirato la previsione del «sistema unico», ossia il contenimento delle spese di gestione, e a tal fine si è introdotto un meccanismo di verifica degli esborsi, destinato a funzionare in forme supplementari e di più ampio raggio rispetto alle consuete ispezioni contabili e amministrative. Par evidente che l'infrastruttura di sistema destinata a essere approntata dal Ministero, pur nel rispetto assoluto del segreto investigativo, dovrà offrire *real time* alla cabina di regia centrale un quadro aggiornato delle spese sostenute per le intercettazioni. Ovviamente si tratterà di una mera indicazione quantitativa, concernente il numero dei «bersagli» intercettati dal singolo ufficio di procura in un certo arco temporale, posto che i costi unitari dell'attività saranno prefissati in sede ministeriale con esclusione di prassi, non sempre trasparenti, di pattuizione dei prezzi dei noleggi tra ditte

private e singoli magistrati. In particolare il riferimento ai «costi complessivi delle attività di intercettazione» rende palese che la verifica contabile non verrà effettuata esclusivamente sulla base della fatturazione proveniente dagli operatori di telefonia fissa e mobile, ma aggregando a essa i dati di spesa riguardanti le ditte di noleggio e la loro penetrazione sui mercati circondariali e distrettuali. Attualmente si registra una presenza “a macchia di leopardo” delle società private addette all’installazione dei *device* di captazione che non sembra rispondere ad alcuna razionalità commerciale, ma appare piuttosto il frutto di una contrattazione affidata a gare estremamente circoscritte e alla fine risolte *intuitu personae*. La previsione di una procedura centralizzata di monitoraggio e l’elaborazione di parametri per l’elaborazione dei dati di spesa dovrebbe consentire un’immediata rilevazione di qualsivoglia anomalia nella conduzione degli affidamenti presso i singoli uffici di procura e, soprattutto, realizzare il contenimento di operazioni di *dumping* tariffario volte a escludere la concorrenza di altre società. La delicatezza delle informazioni messe a disposizione delle ditte che curano l’installazione e il noleggio degli apparati di intercettazione dovrebbe indurre a estrema attenzione nella scelta del contraente e evitare pratiche commerciali non in linea con rigorosi canoni deontologici. Occorre subito precisare che questa proiezione organizzativa verso un controllo efficace e penetrante non solo dei costi delle attività captative, ma finanche delle sottese prassi negoziali non costituisce un’assoluta novità nel panorama della scorsa legislatura. Com’è noto la Camera dei deputati il 17 aprile 2007 aveva approvato a larga maggioranza il disegno di legge di riforma delle intercettazioni telefoniche e ambientali, con un pacchetto di disposizioni destinato a rimaneggiare in profondità il codice di procedura penale e a creare un parallelo sistema di controllo e sanzione. L’iter legislativo, si ricorderà, si è interrotto per effetto delle aspre polemiche che hanno riguardato le disposizioni penali in tema di divulgazione del testo delle intercettazioni sugli organi di stampa. Comunque il ddl n. 1512, all’art. 20, aveva predisposto un protocollo di verifiche contabili più articolato, stabilendo l’interpolazione di un’art. 90 *bis* disp.att. c.p.p. («Spese di gestione e di amministrazione in materia di intercettazioni telefoniche e ambientali») per effetto del quale «entro il 31 marzo di ogni anno, ciascun procuratore della Repubblica trasmette al Ministro della giustizia una relazione sulle spese di gestione e di amministrazione avente ad oggetto le intercettazioni telefoniche e ambientali effettuate nell’anno precedente. Ai fini del controllo sulla gestione amministrativa ... la relazione è trasmessa dal Ministro della giustizia al procuratore generale della Corte dei conti».

Il sistema previsto dalla finanziaria 2008, una volta andato a regime, surroga la relazione annuale prevista dal d.l. n. 1512 con una più efficace, immediata conoscenza dei costi delle intercettazioni monitorate che il dicastero consegue attraverso la struttura unica; il che - sarebbe

sciocco negarlo - realizzerà un indiscutibile effetto dissuasivo su protocolli investigativi orientati verso l’utilizzo indiscriminato delle captazioni quale principale, se non esclusivo, mezzo d’indagine.

4. Il sistema unico nazionale

Una conferma di siffatta, non troppo obliqua, *intentio legis* di agire in vista di una contrazione finanziaria e operativa dello strumento intercettativo può rinvenirsi nell’art. 9 del ddl n. 1512 che recava le nuove «Disposizioni in materia di intercettazioni telefoniche e ambientali e di pubblicità degli atti di indagine». Il progetto prevedeva che «le operazioni di registrazione sono compiute per mezzo degli impianti installati e custoditi nei centri di intercettazione telefonica istituiti presso le procure generali o presso le procure della Repubblica della sede del distretto di corte di appello. Le operazioni di ascolto delle conversazioni intercettate sono compiute mediante impianti installati nei punti di ascolto istituiti presso la competente procura della Repubblica ovvero, previa autorizzazione del pubblico ministero, presso i servizi di polizia giudiziaria delegati per le indagini» (art. 268 comma 3). Inoltre il comma 2 del citato art. 9 stabiliva che «al fine di garantire la concreta rispondenza degli apparati di registrazione e ascolto installati presso le procure della Repubblica alle finalità e alle previsioni della presente legge, il Ministro della giustizia ... definisce le procedure e le specifiche tecniche degli apparati, indicando l’ente che deve provvedere alla loro omologazione». Dall’esame delle cennate disposizioni - secondo cui l’attività captativa doveva essere modulata sotto il profilo infrastrutturale su base distrettuale - si evince che il «sistema unico nazionale» previsto dalla finanziaria 2008 non intende sostituire l’architettura del ddl n. 1512, ma piuttosto anticiparne taluni segmenti con meri intenti di contenimento della spesa. In base al progetto già in discussione innanzi alle Camere, infatti, le operazioni di registrazione dovevano essere eseguite presso «centri di intercettazione telefonica istituiti presso le procure generali o presso le procure della Repubblica della sede del distretto di corte di appello», mentre le attività di ascolto potevano essere “remotizzate” verso le procure ordinarie o gli uffici di polizia delegati. D’altronde il richiamo alle intercettazioni ambientali recato dall’art. 2 comma 82 della finanziaria 2008, e assente nel disposto dell’art. 9 del ddl n. 1512, convalida la conclusione che il «sistema unico» appena approvato non assume ad oggetto della disciplina i luoghi della registrazione e dell’ascolto per i quali - in attesa di un nuovo avvio dell’iter parlamentare di riforma - deve farsi richiamo al disposto vigente dell’art. 268 c.p.p. Resta a questo punto da verificare quali possano essere i requisiti architetture del sistema voluto dal Parlamento con la l. n. 244/2007.

5. I luoghi dell’intercettazione

A prima lettura la mancata incidenza dell’art. 2 comma 82 sui luoghi che il codice di rito individua come inde-

rogabilmente (art. 271) deputati all'esecuzione delle captazioni, potrebbe trovare conferma nell'assenza di qualsivoglia abrogazione espressa o successione tacita di norme processuali (2), per effetto della palese diversità tra oggetto della disciplina finanziaria e codicistica (3). Tuttavia può essere utile chiarire se la disposizione appena approvata, una volta a regime il sistema unico, sia comunque idonea a incidere sul contenuto di provvedimenti giurisdizionali in tema di intercettazione (4). La prima domanda che può legittimamente formularsi è se la costituzione, a cura del Ministero della giustizia, di una struttura di servizio per l'esecuzione delle captazioni a norma della l. n. 244/2007 obblighi o meno il pubblico ministero ad avvalersene nel momento in cui, ai sensi dell'art. 267 comma 3, rilascia il decreto che indica le modalità delle operazioni.

Non si tratta naturalmente di prendere in esame i profili di responsabilità disciplinare o contabile derivanti da una discordanza, quanto prefigurare l'eventuale incidenza di questa distonia sulla validità del provvedimento. Il principio di tassatività che, com'è noto, governa la materia dell'inutilizzabilità ex art. 191 c.p.p. (5) esclude che la violazione circa il *quomodo* delle operazioni indicato dall'art. 2 comma 82 possa intaccare la validità delle intercettazioni. A meno che il Ministero della giustizia non curi di allocare presso gli uffici di procura tipologie uniche di apparati capaci di escludere l'insufficienza o l'inidoneità che abilitano il pubblico ministero a disporre il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria ovvero il noleggio presso privati (art. 268 comma 3 e 3 bis): in questo caso sarebbe agevole censurare l'utilizzabilità delle intercettazioni ex art. 271 (6).

La questione flette verso i profili *de facto* esaminati in precedenza che riguardano le modalità con cui si vorrà organizzare la "cabina di regia" introdotta dalla finanziaria 2008. Del sistema, come abbiamo visto, sono indicati taluni connotati: dovrà essere «unico», «nazionale», «articolato su base distrettuale di corte d'appello» e dovrà riguardare tutte le «intercettazioni telefoniche, ambientali e altre forme di comunicazione informatica o telematica disposte o autorizzate dall'autorità giudiziaria»

Note:

(2) Cfr. sul punto O. Mazza, *La norma processuale nel tempo*, Milano, 1999.

(3) La questione della localizzazione degli impianti di intercettazione conserva, com'è noto, il suo assoluto rilievo processuale per effetto del combinato disposto degli artt. 268 comma 3 e 271 c.p.p. e della connessa sanzione di inutilizzabilità. Benché da più parti si sia posta in discussione la ragionevolezza, anche costituzionale (cfr. Corte costituzionale, ordinanza 19 luglio 2000 n. 304, in *Cass. pen.*, 2001, 19; ordinanza 17 luglio 2001 n. 259, in *Cass. pen.*, 2001, 3320; ordinanza 5 luglio 2004 n. 209, inedita), di un'opzione privilegiata in favore dell'allestimento *infra moenia* degli impianti di intercettazione, non può dubitarsi della necessità di garantire che le attività d'indagine tecnica si svolgano sotto la materiale vigilanza del magistrato che le dispone e, quindi, di assicurare la presenza delle strutture di captazione negli uffici di giustizia.

Si legge nella relazione di accompagnamento al disegno di legge n. 1099

presentato dal Ministro di Grazia e Giustizia (Gonella) che diede luogo alla prima riforma della materia delle intercettazioni: «il progresso dell'elettronica e della tecnica della miniaturizzazione ha reso possibile la creazione di microapparecchi trasmettenti capaci di controllare a distanza l'intimità e la riservatezza delle persone, in particolare con il fraudolento ascolto e la registrazione delle private conversazioni sia *inter praesentes* che telefoniche» in V. Di Ciolo - P. Di Muccio, *L'intercettazione telefonica e il diritto alla riservatezza*, Milano, 1974, 125. Invero l'esame dei lavori parlamentari che anticiparono l'approvazione della legge 8 aprile 1974 n. 78 rivela l'esistenza di diverse valutazioni espresse sul punto della localizzazione degli impianti dai relatori al disegno di legge n. 1099 al Senato ed alla Camera. Il sen. Martinazzoli nell'illustrare l'originaria disposizione del disegno di legge, di seguito modificata, annotava: «Non si è creduto di accogliere la proposta di dotare gli uffici delle procure della Repubblica delle apparecchiature necessarie al controllo telefonico... proprio al fine di non rendere eccessivamente facile l'uso di questo rischioso mezzo di prova». L'on. Castelli, relatore del disegno alla Camera di deputati, traghettò invece il consenso parlamentare verso la soluzione di privilegiare, per l'esecuzione delle operazioni, gli impianti installati presso gli uffici giudiziari inquirenti «giacché ritenne che la soluzione adottata dal Senato (ovvero dell'esecuzione esclusivamente presso gli impianti di servizio pubblico) fosse, in certi casi tecnicamente impossibile ovvero compromettesse gravemente la segretezza dell'operazione. Propose pertanto di prevedere la possibilità di svolgere tale attività anche presso appositi locali delle Procure della Repubblica» così in V. Di Ciolo - P. Di Muccio, *op.cit.*, 46 e 61. Per un'ampia disamina delle deviazioni riscontrate in quegli anni a causa della costituzione di vere e proprie «centrali d'ascolto» presso taluni comandi di polizia, sottratte ad ogni controllo da parte dell'autorità giudiziaria cfr. V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, 328; A. Mittone, *La legge sulle intercettazioni telefoniche*, in *Biblioteca delle libertà*, 1974, n. 49-50, 159. E, ancora, si vedano le preoccupazioni espresse dalla Corte costituzionale nella nota sentenza 4 aprile 1973 n. 34, laddove a presidio della norma costituzionale di parametro (ossia l'art. 15) si auspicavano «garanzie che attengono alla predisposizione anche materiale dei servizi tecnici necessari per le intercettazioni telefoniche, in modo che l'autorità giudiziaria possa esercitare anche di fatto il controllo necessario ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione».

(4) La disposizione, in linea di continuità con quanto avvenuto attraverso l'approvazione della legge 20 novembre 2006, n. 271 (sul punto A. Gaito, *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime*, in *Osservatorio del processo penale*, 2007, n. 1, settembre-ottobre, 1), marca la tendenza più recente a trasferire pericolosamente fuori dal codice di procedura penale, disposizioni aventi una evidente connotazione processuale. In proposito, sia pure con riferimento ad altro corpus di disposizioni, cfr. S. Lorusso, *Il processo penale italiano tra micro-sistemi e codificazione*, in *Dir.pen. proc.*, 2007, 425.

(5) Cfr. F. Ruggieri, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001. E anche A. Camon, *Le intercettazioni nel processo penale*, Milano 1996; L. Filippi, *L'intercettazione di comunicazioni*, Milano, 1997; P. Balducci, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, 2002. Riferisce della previsione dell'art. 268 comma 3 come un'ipotesi di «inutilizzabilità rafforzata» A. Bargi, *Procedimento probatorio e giusto processo*, Napoli, 1990, 254.

(6) Poche altre questioni, al pari di questa, registrano il cadenzato succedersi di interventi delle Sezioni unite, tutti evocati invero al fine di disciplinare la sorte delle captazioni nel caso in cui il pubblico ministero non abbia correttamente adempiuto agli obblighi di motivazione prescritti per eseguire *extra moenia* le operazioni di intercettazione, ossia in luoghi diversi dalla procura della Repubblica cfr. Cassazione sezioni unite, 21 settembre 2000, Primavera, in *Dir.pen. proc.*, 2001, 621; sezioni unite, 31 ottobre 2001, Policastro e altri, in *Guida al dir.*, 2004, 6, 54; sezioni unite, 2 novembre 2003, Gatto, in *Guida al dir.*, 2004, 6, 49; sezioni unite, 17 novembre 2004, Esposito, in *Arch.n. proc.pen.*, 2005, 193; sezioni unite, 24 gennaio 2006, Campenni, in *Guida al dir.*, 2006, 5, 79 e, da ultimo, sezioni unite, 12 luglio 2007, Agunche e altri, in *Guida al dir.*, 2007, 37, 69. Sul punto di recente F. Giunchedi, *Norma e prassi in tema di motivazione dei decreti di autorizzazione delle intercettazioni*, in *Osservatorio del processo penale*, 2007, n. 1 (settembre-ottobre), 12.

(ivi incluse quelle richieste dai servizi di sicurezza ex art. 4 della legge 31 luglio 2005 n. 155 per come modificato dalla legge 3 agosto 2007 n. 124).

Il termine «unico» pretende senza meno che l'architettura del sistema preveda l'utilizzazione di apparati e modalità di acquisizione/trasferimento dei flussi vocali e digitali rispondenti a un medesimo standard tecnico e economico. Questo potrebbe comportare la stipula a livello ministeriale di un contratto cumulativo di noleggio degli impianti da mettere a disposizione degli uffici di procura con la previsione di adeguati obblighi di *upgrading* dei requisiti tecnologici e di idonei centri di assistenza e manutenzione.

Parimenti il connotato di «nazionale» sta a esigere che lo stesso dovrà indistintamente riguardare tutti gli uffici di procura sul territorio del paese (ossia 165) sia pure al fine di consentire le sole procedure di ascolto delle intercettazioni. Ossia dovrà consentire alla procure circondariali (non distrettuali) di avvalersi dei propri impianti, ove disponibili, affinché non incorrano nella sanzione di inutilizzabilità comminata dall'art. 271 c.p.p. Salvo che tali impianti, con provvedimento ministeriale, non siano disattivati e estromessi dalla rete telefonica e telematica di trasmissione delle captazioni, determinando le

condizioni di insufficienza e inidoneità prescritte dall'art. 268, comma 3 c.p.p.

Infine l'articolazione del sistema «su base distrettuale di corte d'appello» sta a indicare che l'apparato strumentale dovrà prevedere centri distrettuali di registrazione con «remotizzazione» dell'ascolto presso gli uffici giudiziari periferici o di polizia, organizzati in modo tale da precludere qualsivoglia conoscenza dei dati esteriori (numero, utente, sito web ect.) o del contenuto delle comunicazioni intercettate a soggetti diversi dal pubblico ministero procedente e dalla polizia giudiziaria delegata. È probabilmente il distretto la dimensione strutturale più conveniente per organizzare la distribuzione degli apparati di intercettazione noleggiati e per procedere a una quantificazione immediata dei costi delle attività tecniche. Potrebbe essere così emulato il percorso della procura di Bolzano, unico ufficio inquirente che pubblica ogni anno un bilancio sociale del servizio reso ai cittadini regolarmente certificato ISO 9001; da tale atto è possibile trarre indicazioni su i risultati conseguiti e i costi sostenuti: ad esempio dalla relazione per l'anno 2006 (edita sul sito www.procura.bz.it) si evincono spese per intercettazioni pari a € 300.261,41 di cui € 172.364,80 per noleggio attrezzature.

LIBRI



Collana Diritto e processo penale oggi
diretta da F. P. Palazzo e G. Spangher

Il procedimento per decreto penale
di Pasquale Ventura

Il volume propone una lettura approfondita e completa del **procedimento speciale** chiamato «procedimento per decreto».

In particolare esamina i **presupposti** di tale procedimento; la **richiesta del p.m.**; la fase della **decisione**; il **decreto penale** in sé considerato; l'**opposizione al decreto** stesso e il **giudizio** conseguente all'opposizione, anche in relazione agli altri procedimenti speciali.

IPSOA 2008
PREZZO: € 34,00

Per informazioni:

- **Servizio Informazioni Commerciali:**
www.ipsoa.it/servizioclienti
E-mail: info.commerciali@wki.it
Tel. 02/82476794 - Fax 02.82476403
- **Agenzia Ipsoa di zona**
(www.ipsoa.it/agenzie)
- **www.ipsoshop.ipsoa.it**

Servizi finanziari

L'informazione del consumatore nella commercializzazione a distanza di servizi finanziari

di Valerio Sangiovanni

Il D.Lgs. n. 221/2007 modifica il codice del consumo inserendo una sezione IV bis dedicata alla commercializzazione a distanza di servizi finanziari. Alcuni aspetti meritano particolare approfondimento: la tempistica, le modalità e il contenuto dell'informazione del consumatore.

1. Introduzione

Il recente D.Lgs. n. 221/2007 ha apportato alcune modifiche al codice del consumo (1).

In particolare l'art. 9 D.Lgs. n. 221 del 2007 introduce i nuovi articoli da 67 bis a 67 vices bis, con i quali il codice del consumo si arricchisce di una nuova sezione IV bis (2) dedicata alla commercializzazione a distanza di servizi finanziari ai consumatori (3). Si tratta di una sezione corposa, in quanto gli articoli che - sotto questo profilo - vanno a incrementare il codice del consumo sono ben 21.

L'origine delle disposizioni degli artt. 67 bis ss. c.cons. è il diritto comunitario. Le corrispondenti norme sono state difatti introdotte nel diritto italiano, per la prima volta, in attuazione della direttiva n. 65/2002 (4).

La sezione IV bis c.cons. non contiene disposizioni nuove per l'ordinamento italiano. Le relative norme erano difatti contenute, fino alla recente trasposizione nel codice del consumo, nel D.Lgs. n. 190/2005 (5). L'art. 21 D.Lgs. n. 221/2007 abroga però il D.Lgs. n. 190/2005 e le disposizioni che erano contenute in quest'ultimo decreto sono state inserite negli artt. 67 bis ss. c.cons.

2. La nozione di "commercializzazione a distanza di servizi finanziari ai consumatori"

È utile iniziare l'analisi dallo stesso titolo della sezione IV bis, avente a oggetto la "commercializzazione a distanza di servizi finanziari ai consumatori". Bisogna esaminare le nozioni di: 1) servizio finanziario; 2) consumatore; 3) commercializzazione a distanza.

Per "servizio finanziario" si intende "qualsiasi servizio di natura bancaria, creditizia, di pagamento, di investimento, di assicurazione o di previdenza individuale" (art. 67 ter comma 1 lett. b) c.cons.). La nozione di servizio finanziario è dunque particolarmente ampia e va ben al di là dei singoli elementi che ne costituiscono il fondamento: "bancario", "creditizio", "di pagamento", "di investimento", "di assicurazione", di "previdenza individuale".

Questa definizione di servizio finanziario vale ai fini della sezione IV bis c.cons. Essa deve convivere: a) con eventuali altre definizioni contenute in altre parti del codice del consumo; b) con eventuali altre definizioni contenute in altri testi normativi.

Note:

(1) D.Lgs. 23 ottobre 2007, n. 221, in G.U. n. 278 del 29 novembre 2007.

(2) Il capo I del titolo III della parte III c.cons. è rubricato "particolari modalità di conclusione del contratto" e si divide nelle seguenti sezioni: sezione I (contratti negoziati fuori dei locali commerciali; artt. 45-49); sezione II (contratti a distanza; artt. 50-61); sezione III (disposizioni comuni; artt. 62-63); sezione IV (diritto di recesso; artt. 64-67); sezione IV bis (commercializzazione a distanza di servizi finanziari ai consumatori; artt. 67 bis-67 vices bis).

(3) In materia di commercializzazione a distanza di servizi finanziari cfr., fra gli altri, G. Alpa, *Commercializzazione a distanza di servizi finanziari ai consumatori*, in *I Contratti*, 2005, 1173 s.; P. Balzarini, *Attuazione della direttiva sulla vendita a distanza di servizi finanziari*, in *Riv. soc.*, 2005, 1177 s.; G. De Cristofaro, *Contratti aventi ad oggetto "servizi finanziari" stipulati a distanza e tutela dei consumatori: il d.legisl. 19 agosto 2005, n. 190, di recepimento della direttiva 2002/65/CE (prima parte)*, in *Studium iuris*, 2006, 265 ss.; G. De Cristofaro, *Contratti aventi ad oggetto "servizi finanziari" stipulati a distanza e tutela dei consumatori: il D.Lgs. 19 agosto 2005, n. 190, di recepimento della direttiva 2002/65/CE (seconda parte)*, in *Studium iuris*, 2006, 385 ss.; U. Draetta, *La protezione dei consumatori e i servizi finanziari forniti a distanza: la legge italiana di attuazione della direttiva comunitaria*, in *Dir. comm. int.*, 2005, 465 ss.; M. Giurgiola, *La direttiva 2002/65/CE sulla commercializzazione a distanza di servizi finanziari: l'epilogo di una lunga attesa*, in *Le Società*, 2003, 103 ss.; M.-T. Paracampo, *La direttiva 2002/65/CE sulla commercializzazione a distanza di servizi finanziari e la tutela del consumatore*, in *Nuova giur. civ. comm.*, 2003, II, 382 ss.; L. Pontiroli, *La disciplina del pagamento nella vendita a distanza dei servizi finanziari: prime considerazioni*, in *Banca borsa tit. cred.*, 2006, I, 678 ss.; A. Torelli, *Contratti a distanza e tutela del consumatore. La nuova disciplina nella commercializzazione dei servizi finanziari*, in *Nuove leggi civ. comm.*, 2006, 621 ss.

(4) Direttiva 2002/65/CE del Parlamento europeo e del Consiglio del 23 settembre 2002 concernente la commercializzazione a distanza di servizi finanziari ai consumatori e che modifica la direttiva 90/619/CEE del Consiglio e le direttive 97/7/CE e 98/27/CE, in G.U.C.E. n. L 271 del 9 ottobre 2002.

(5) D.Lgs. 19 agosto 2005, n. 190, in G.U. n. 221 del 22 settembre 2005. Attuazione della direttiva 2002/65/CE relativa alla commercializzazione a distanza di servizi finanziari ai consumatori.

Sotto il primo profilo bisogna porre attenzione all'art. 3 c.cons., il quale è rubricato "definizioni". Qui si trovano le definizioni di "consumatore o utente", "associazioni dei consumatori e degli utenti", "professionista", "produttore", "prodotto" e "codice". Non si rinviene dunque, nell'art. 3 c.cons., una definizione di servizio finanziario. La definizione di servizio finanziario va però conciliata anche con le eventuali altre definizioni previste in altri testi normativi. Ad esempio, si pensi all'art. 1 comma 5 D.Lgs. n. 58/1998 il quale contiene la definizione di "servizio e attività di investimento": "per servizi e attività di investimento si intendono i seguenti, quando hanno per oggetto strumenti finanziari: a) negoziazione per conto proprio; b) esecuzione di ordini per conto dei clienti; c) sottoscrizione e/o collocamento con assunzione a fermo ovvero con assunzione di garanzia nei confronti dell'emittente; c bis) collocamento senza assunzione a fermo né assunzione di garanzia nei confronti dell'emittente; d) gestione di portafogli; e) ricezione e trasmissione di ordini; f) consulenza in materia di investimenti; g) gestione di sistemi multilaterali di negoziazione". Il servizio finanziario è peraltro nozione di ampiezza maggiore rispetto a quella di servizio d'investimento, comprendendo ad esempio anche i servizi di natura bancaria e creditizia.

La seconda espressione di cui il legislatore si avvale nella rubrica della sezione IV bis è quella di consumatore. Per "consumatore" si intende qualunque soggetto di cui all'art. 3 comma 1 lett. a) c.cons. (art. 67 ter comma 1 lett. d) c.cons.). Secondo questa disposizione di carattere generale (nel senso di valevole per tutto il codice del consumo) "consumatore" o utente è "la persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta" (art. 3 comma 1 lett. a) c.cons.) (6).

La nuova sezione IV bis c.cons. disciplina la "commercializzazione a distanza". Il codice del consumo non contiene però la definizione di "commercializzazione a distanza", bensì solo quella di "contratto a distanza". Bisogna rilevare che "commercializzazione" è un'espressione non diffusa nella terminologia classica del diritto civile italiano. In alternativa si sarebbe potuto usare il termine "vendita". Si è tuttavia ritenuta tale espressione inadeguata rispetto ai servizi, per i quali è più appropriato parlare di "erogazione" o di "prestazione" che di "vendita", termine che si attaglia invece meglio alla cessione di beni (7).

Nel codice del consumo si rinviene due definizioni di contratto a distanza, una dettata nel contesto dei servizi finanziari e una di carattere generale. Nel contesto dei servizi finanziari per "contratto a distanza" si intende "qualunque contratto avente per oggetto servizi finanziari, concluso tra un fornitore e un consumatore ai sensi dell'art. 50, comma 1, lettera a)" (art. 67 ter comma 1 lett. a) c.cons.). In generale per contratto a distanza si intende "il contratto avente per oggetto beni o servizi stipulato tra un professionista e un consumatore nell'ambi-

to di un sistema di vendita o di prestazione di servizi a distanza organizzato dal professionista che, per tale contratto, impiega esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto, compresa la conclusione del contratto stesso" (art. 50 comma 1 lett. a) c.cons.). L'art. 67 ter comma 1 lett. a) c.cons. richiama l'art. 50 comma 1 lett. a) c.cons. Per il resto la sezione relativa ai contratti a distanza (artt. 50-61 c.cons.) non si applica ai contratti a distanza relativi ai servizi finanziari di cui agli artt. 67 bis ss. c.cons. (art. 51 lett. a) c.cons.).

La definizione di contratto a distanza si caratterizza per l'elemento della "organizzazione". Deve cioè sussistere un sistema di vendita o di prestazione di servizi a distanza "organizzato". Questo elemento vale a escludere dalla definizione di contratto a distanza il contratto concluso occasionalmente (8). Manca peraltro, nell'art. 50 comma 1 lett. a) c.cons., una definizione di "sistema (di vendita o di prestazione di servizi a distanza) organizzato", per cui potrebbe risultare - nella prassi - non facile distinguere fra prestazione organizzata e prestazione occasionale. Bisogna tuttavia rilevare che il testo del considerando n. 18 della direttiva n. 65/2002 fa riferimento a una occasionalità "stretta". Da questo dato testuale si può ricavare che anche un minimo di organizzazione basta a elevare il fornitore a soggetto cui è applicabile la direttiva. Un'interpretazione del genere favorisce la tutela dei consumatori.

Altro elemento caratterizzante il contratto a distanza è la "esclusività" delle tecniche di comunicazione a distanza. Tale esclusività, come risulta dal considerando n. 15 della direttiva n. 65/2002 (9), riguarda sia la fase della negoziazione sia la fase della conclusione del contratto. Se si verificano degli incontri di persona fra le parti, ciò - in linea di principio - esclude la natura di contratto a distanza. È stata però suggerita un'interpretazione non eccessivamente rigida. Il criterio discrezionale che viene proposto è quello della natura dell'incontro fisico che avviene fra le persone (10). Se questo incontro ha carat-

Note:

(6) Per una critica alla limitazione della nozione di consumatore alle sole persone fisiche cfr. P. Fiorio, *Offerte a distanza e fuori sede tra testo unico della finanza, nuovo regolamento intermediari e codice del consumo*, in www.ilcaso.it, 14 ss.

(7) Cfr. F. Mastroianni, M.P. Serra, *La commercializzazione a distanza di prodotti finanziari: la direttiva 23 settembre 2002 n. 65 e il decreto legislativo di attuazione 19 agosto 2005 n. 190*, in questa Rivista, 1, 2006, 84.

(8) In questo senso si esprime il considerando n. 18 della direttiva n. 65/2002, secondo cui "riferendosi a un sistema di prestazioni di servizi organizzato dal fornitore di servizi finanziari, la presente direttiva mira a escludere dal proprio campo di applicazione le prestazioni di servizi effettuate su base strettamente occasionale e al di fuori di una struttura commerciale avente l'obiettivo di concludere contratti a distanza".

(9) Il considerando n. 15 della direttiva n. 65/2002 prevede che i contratti a distanza sono "quelli in cui l'offerta, la negoziazione e la conclusione sono effettuate a distanza".

(10) Cfr. G. Artale, *Commento al d.lgs. n. 190/2005*, in AA.VV., *Codice del consumo*, a cura di V. Cuffaro, Milano, 2006, 838 s.

tere occasionale e, soprattutto, se non consente di chiarire tutti gli aspetti del rapporto contrattuale, allora esso potrebbe essere ritenuto non sufficiente a far venir meno la natura "a distanza" dell'operazione e la conseguente tutela di cui gode il consumatore.

3. L'informazione dei consumatori in generale

Alcuni articoli della nuova sezione IV bis sono dedicati all'informazione del consumatore.

L'informazione costituisce un elemento importante per la tutela del consumatore (11). I soggetti attivi sul mercato non godono tutti dello stesso livello informativo. Esistono asimmetrie che tendono ad avvantaggiare il contraente forte a scapito del contraente debole. Più la materia è tecnica e complessa, maggiori tendono a essere le asimmetrie informative. I settori assicurativo, bancario e finanziario ne costituiscono un significativo esempio. I regolatori cercano di ridurre queste asimmetrie. La finalità ultima è quella di realizzare mercati più efficienti, fondati su una ragionevole fiducia dei contraenti deboli nei confronti dei contraenti forti. Nel settore dei contratti a distanza, l'informazione assume ancora maggiore importanza, in quanto manca il contatto personale.

Della importanza dell'informazione per la tutela del consumatore è consapevole anzitutto il legislatore europeo, il quale prevede che la Comunità contribuisce a promuovere il diritto dei consumatori all'informazione (art. 153 del Trattato che istituisce la Comunità europea). Più specificamente nel contesto della direttiva n. 65/2002 i considerando nn. 21 (12) e 23 (13) sottolineano l'importanza dell'informazione.

Attesa l'importanza dell'informazione per la tutela del consumatore, essa viene prevista e regolata in diversi passaggi del codice del consumo. La prima disposizione che si deve menzionare è l'art. 2 c.cons., il quale elenca fra i diritti fondamentali dei consumatori il diritto a un'adeguata informazione (art. 2 comma 2 lett. c) c.cons.). Il codice del consumo prevede poi che "sicurezza, composizione e qualità dei prodotti e dei servizi costituiscono contenuto essenziale degli obblighi informativi" (art. 5 comma 2 c.cons.). La legge specifica inoltre che "le informazioni al consumatore, da chiunque provengano, devono essere adeguate alla tecnica di comunicazione impiegata ed espresse in modo chiaro e comprensibile, tenuto anche conto delle modalità di conclusione del contratto o delle caratteristiche del settore, tali da assicurare la consapevolezza del consumatore" (art. 5 comma 3 c.cons.).

Rispetto ad altri settori, nella materia dei servizi finanziari le informazioni sono di centrale rilevanza per una ragione aggiuntiva. Dati e notizie servono non solo per il corretto instaurarsi del rapporto contrattuale fra fornitore e consumatore (funzione "privatistica"). Le informazioni sono utili anche per assicurare il buon funzionamento dei mercati finanziari (funzione "pubblicitica"). Esse consentono che vengano effettuate consapevoli

scelte d'investimento e rafforzano dunque la fiducia dei consumatori nell'efficienza dei mercati. La direttiva n. 39/2004, recentemente attuata nel diritto italiano, dedica ampio spazio agli obblighi informativi delle imprese d'investimento (14).

Passando all'esame del testo della legge, questa stabilisce anzitutto che "nella fase delle trattative e comunque prima che il consumatore sia vincolato da un contratto a distanza o da un'offerta, gli sono fornite le informazioni riguardanti: a) il fornitore; b) il servizio finanziario; c) il

Note:

(11) Recentemente in materia di tutela del consumatore nel contesto del commercio elettronico cfr. G. Cassano, *Condizioni generali di contratto e tutela del consumatore nell'era di Internet*, in questa Rivista, 1, 2007, 5 ss. V. inoltre AA.VV., *Commercio elettronico e tutela del consumatore*, a cura di G. Cassano, Milano, 2003; G. Cassano, I.P. Cimino, *Contratto via Internet e tutela della parte debole*, in *I Contratti*, 2002, 869 ss.

(12) Il considerando n. 21 della direttiva n. 65/2002 prevede: "l'impiego di tecniche di comunicazione a distanza non dovrebbe portare a una diminuzione indebita dell'informazione fornita al consumatore. Per assicurare la trasparenza la presente direttiva fissa requisiti volti a garantire un livello adeguato di informazione del consumatore sia prima che dopo la conclusione del contratto. Il consumatore dovrebbe ricevere, prima della conclusione di un contratto, le informazioni preliminari necessarie al fine di poter valutare opportunamente il servizio finanziario propostogli e quindi scegliere con cognizione di causa. Il fornitore dovrebbe espressamente indicare per quanto tempo la sua offerta eventuale rimane immutata".

(13) Il considerando n. 23 della direttiva n. 65/2002 stabilisce: "per garantire una protezione ottimale del consumatore, è importante che egli sia sufficientemente informato sulle disposizioni della presente direttiva ed eventualmente sui codici di condotta esistenti in questo settore, e che disponga di un diritto di recesso".

(14) Direttiva 2004/39/CE del Parlamento europeo e del Consiglio del 21 aprile 2004 relativa ai mercati degli strumenti finanziari e che modifica le direttive 85/611/CEE e 93/6/CEE del Consiglio e la direttiva 2000/12/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 93/22/CEE del Consiglio, in G.U.C.E. n. L 145 del 30 aprile 2004. Sugli obblighi d'informazione delle imprese d'investimento nella direttiva MIFID cfr. E. Girino, *L'informazione nel sistema MiFID: dalla trasparenza monodirezionale alla biunivocità dei flussi*, in *Amm. & Fin.*, 2008, 48 ss.; V. Sangiovanni, *Gli obblighi informativi delle imprese di investimento nella più recente normativa comunitaria*, in *Dir. com. scambi int.*, 2007, 363 ss. A vario titolo sulla MIFID e sulla sua attuazione v. poi F. Bruno, A. Rozzi, *Il destino dell'operatore qualificato alla luce della MiFID*, in *Le Società*, 2007, 277 ss.; C. Comporti, *I conflitti di interesse nella disciplina comunitaria dei servizi finanziari*, in *Dir. banca merc. fin.*, 2005, I, 593 ss.; F. Durante, *Verso una diversa gradazione della tutela degli investitori (ed un diverso ruolo della Consob): dal diritto giurisprudenziale al recepimento delle misure "di secondo livello" della Mifid*, in *www.judicium.it*; L. Frumento, *La valutazione di adeguatezza e di appropriatezza delle operazioni di investimento nella Direttiva Mifid*, in *I Contratti*, 2007, 583 ss.; E. Girino, *MiFID: fra rivoluzione e trasparenza*, in *Amm. & Fin.*, 2007, 29 ss.; F. Recine, *La direttiva relativa ai mercati degli strumenti finanziari (MIFID): nuove regole sulla cooperazione tra le autorità di vigilanza*, in *Dir. banca merc. fin.*, 2006, I, 303 ss.; A.A. Rinaldi, *Il decreto Mifid e i regolamenti attuativi: principali cambiamenti*, in *Le Società*, 2008, 12 ss.; V. Sangiovanni, *Informazioni e comunicazioni pubblicitarie nella nuova disciplina dell'intermediazione finanziaria dopo l'attuazione della direttiva MIFID*, in corso di pubblicazione in *Giur. it.*, 2008; V. Sangiovanni, *La nuova disciplina dei contratti di investimento dopo l'attuazione della MIFID*, in *I Contratti*, 2008, 173 ss.; V. Sangiovanni, *Operazione inadeguata dell'intermediario finanziario fra nullità del contratto e risarcimento del danno alla luce della direttiva MIFID*, in *I Contratti*, 2007, 243 ss.; S. Scotti Camuzzi, *I conflitti di interessi fra intermediari finanziari e clienti nella direttiva MIFID*, in *Banca borsa tit. cred.*, 2007, I, 121 ss.

contratto a distanza; d) il ricorso” (art 67 *quater* comma 1 c.cons.).

Dall’art. 67 *quater* comma 1 c.cons. si evince anzitutto che le informazioni vanno fornite nel corso delle trattative e prima che il contratto si concluda. Al riguardo è appropriato parlare di informazione “precontrattuale”. L’informazione deve precedere la conclusione del contratto in quanto essa è funzionale all’espressione di un consenso consapevole. Il consumatore può prestare il proprio consenso con cognizione di causa solo se è stato adeguatamente informato. Attesa la presenza di asimmetrie informative, soprattutto in settori a carattere particolarmente tecnico come i servizi finanziari, il contraente debole deve essere da subito adeguatamente informato da parte del contraente forte. Se il consumatore non è informato in modo appropriato, aumenta il rischio della conclusione di un contratto che non soddisfa i suoi reali bisogni. La scelta sbagliata di concludere un contratto comporta non pochi costi (15). Innanzitutto non si realizzano i benefici che erano attesi dall’operazione contrattuale. In secondo luogo il tempo sprecato può aver fatto perdere occasioni contrattuali che altrimenti sarebbero state sfruttate. Inoltre si sono affrontati inutilmente dei costi in connessione con la conclusione del contratto, anche se bisognerebbe dire che - nel caso di conclusione a distanza - tali costi normalmente non sono elevati. Infine può capitare che si debbano affrontare delle spese per rimuovere gli effetti del contratto.

Il legislatore prevede, nella disposizione in esame, due possibili momenti per la comunicazione delle informazioni. Le informazioni devono essere fornite: 1) nella fase delle trattative, 2) oppure, comunque, prima che il consumatore sia vincolato.

Idealmente dunque le informazioni vanno fornite nel corso delle trattative, in modo che il consumatore abbia la possibilità di negoziare le clausole del contratto. Nella prassi bisogna però rilevare che il testo contrattuale è normalmente predisposto dal fornitore, cosicché è difficile che si possa realizzare una negoziazione vera e propria (16).

La norma consente però che le informazioni vengano messe a disposizione anche dopo le trattative (o indipendentemente dalla trattative, nel caso in cui queste non vi siano del tutto), e segnatamente nell’imminenza della conclusione del contratto. Questa possibilità è stata criticata sulla base dell’assunto che la tutela del consumatore verrebbe, in tal modo, ridotta (17). L’osservazione è corretta, ma deve tenere conto del fatto che nel caso di commercializzazione a distanza di servizi finanziari i margini di negoziazione del contenuto del contratto sono minimi (se non del tutto assenti). Si può allora affermare che la funzione centrale dell’informazione precontrattuale è quella di garantire l’alternativa secca fra “conclusione” oppure “non conclusione” dell’accordo. Sotto questo profilo è tendenzialmente sufficiente che le informazioni vengano fornite prima della possibile conclusione del contratto.

Certo, idealmente, dati e notizie andrebbero forniti molto prima della conclusione del contratto, lasciando così al consumatore tutto il tempo necessario per le sue opportune riflessioni. Nella pratica, tuttavia, non è facile stabilire quale sia il lasso di tempo necessario per assicurare una scelta consapevole del consumatore. Tale periodo di tempo varia a seconda di quelle che sono le caratteristiche del servizio offerto e le qualità personali dell’utente. Nel caso di servizi finanziari complessi può essere necessario parecchio tempo per comprendere appieno tutti gli elementi dell’offerta.

Infine, per giustificare la possibilità della dazione d’informazioni nell’imminenza del contratto, bisogna riflettere sul fatto che il consumatore - anche laddove avesse concluso il contratto in maniera “affrettata” - gode comunque di un diritto di recesso ai sensi dell’art. 67 *duodecies* c.cons. (entro un termine di 14 giorni senza penali e senza dover indicare il motivo). Nel complesso, dunque, anche se le informazioni vengono date solo nell’imminenza della conclusione del contratto, il consumatore appare sufficientemente tutelato.

Vi è poi il problema di capire quando un contratto a distanza si possa considerare concluso. La problematica è rilevante anche perché dalla conclusione del contratto decorre, di norma, il termine per esercitare il diritto di recesso ai sensi dell’art. 67 *duodecies* c.cons. La questione non è precisata dal legislatore e in tema si confrontano essenzialmente due tesi (18). Secondo una prima opinione, il momento rilevante è quello in cui il fornitore riceve l’ordine del consumatore. Secondo una seconda opinione, la conclusione del contratto avverrebbe in un momento successivo, quando il fornitore conferma al consumatore di avere ricevuto l’ordine. La prima tesi pare essere più convincente. Il legislatore prevede difatti da quando decorre il termine per l’esercizio del diritto di recesso e stabilisce che esso decorre “dalla data della conclusione del contratto, tranne nel caso delle assicurazioni sulla vita, per le quali il termine comincia a decorrere dal momento in cui al consumatore è comunicato che il contratto è stato concluso” (art. 67 *duodecies* comma 3 lett. a) c.cons.). Da questa disposizione si evince che, di norma, una comunicazione del fornitore che il contratto è stato concluso non è necessaria. Solo nel caso di assicurazioni sulla vita tale comunicazione è richiesta. Di regola il contratto si conclude in un momento anteriore. Il legislatore, dopo avere enunciato la tempistica della dazione d’informazioni, elenca le categorie d’informazioni da fornirsi, che vengono specificate nei quattro arti-

Note:

(15) P. Longhini, *Servizi finanziari telematici*, Milano, 2006, 181.

(16) Più in generale si può osservare che, nel caso di offerte indirizzate a una massa di persone, le trattative tendono a essere inesistenti. In questo senso P. Longhini, *op. cit.*, 181.

(17) Cfr. F. Totaro, *Commento al d.lgs. n. 190/2005*, in AA.VV., *Codice del consumo*, a cura di V. Cuffaro, Milano, 2006, 845.

(18) Cfr. F. Totaro, *op. cit.*, 845.

coli successivi (art. 67 *quinquies*, 67 *sexies*, 67 *septies* e 67 *octies* c.cons.). Il livello di dettaglio cui giunge il legislatore è stato criticato in dottrina (19). Per quanto la legge cerchi di essere specifica, non è difatti possibile individuare a priori tutte le possibili informazioni che possono assumere rilevanza per il consumatore. La necessità del ricorso a clausole generali, nel determinare esattamente quali informazioni vanno fornite, rimane dunque ferma.

La legge stabilisce che le informazioni, “il cui fine commerciale deve risultare in maniera inequivocabile, sono fornite in modo chiaro e comprensibile con qualunque mezzo adeguato alla tecnica di comunicazione a distanza utilizzata, tenendo debitamente conto in particolare dei doveri di correttezza e buona fede nella fase precontrattuale” (art. 67 *quater* comma 2 c.cons.). L'analisi di questa disposizione consente di enucleare tre regole cui si devono attenere i fornitori.

La prima regola che si evince da questa disposizione è la necessità di enunciare la finalità della dazione d'informazioni. Il consumatore deve essere consapevole che il fine delle stesse è commerciale. Questo non significa, peraltro, che le informazioni possano essere incomplete oppure contrarie a verità.

La seconda regola cui devono attenersi i fornitori, ai sensi della disposizione in esame, è che le informazioni devono essere fornite in modo “chiaro” e “comprensibile”. I termini chiarezza e comprensibilità sono peraltro, probabilmente, da intendersi come sinonimi e indicano la necessità che le informazioni sia immediatamente capibili da un destinatario medio. Al riguardo non rileva il mezzo con cui dati e notizie vengono comunicati. Mancano però, nella disposizione, alcune specificazioni che - per la loro importanza - si dovrebbero considerare come ovvie: non si dice cioè che l'informazione deve essere completa e veritiera. La tutela del consumatore sarebbe pressoché azzerata se il fornitore fosse legittimato a fornire informazioni incomplete o inveritiere. Stante il silenzio della norma in merito a questo punto specifico, la necessità di completezza e verità si desume dal richiamo operato a correttezza e buona fede.

La terza regola cui si devono attenere i fornitori e che risulta dalla disposizione in esame è il rispetto dei doveri di correttezza e buona fede. In questo modo viene effettuato un richiamo, anche se non esplicito, all'art. 1337 c.c., secondo cui “le parti, nello svolgimento delle trattative e nella formazione del contratto, devono comportarsi secondo buona fede”. Ma l'art. 1337 c.c. trova in ogni caso applicazione ai contratti a distanza aventi a oggetto servizi finanziari. In questo senso milita l'art. 38 c.cons. che fa salve le disposizioni del codice civile in funzione integrativa. Il richiamo a correttezza e buona fede nell'art. 67 *quater* comma 2 c.cons. sembrerebbe dunque essere ridondante.

Correttezza e buona fede implicano, in prima istanza, di comunicare alla controparte tutte le informazioni rilevanti che si hanno a disposizione (*requisito della comple-*

tezza). Gli artt. 67 *quinquies*, 67 *sexies*, 67 *septies* e 67 *octies* c.cons. non fanno altro che specificare, nel particolare contesto della commercializzazione a distanza di servizi finanziari, quali siano questi obblighi informativi derivanti da correttezza e buona fede. Potrebbe verificarsi il caso in cui la fornitura di tutte le informazioni richieste da tali articoli di legge non basti. Certo, la lettura di queste disposizioni evidenzia come si tratti di un catalogo dettagliato ed è difficile pensare che, operando nel rispetto di esso, possano essere omessi dati e notizie rilevanti. Il legislatore si preoccupa però della sostanza delle cose e non del dato formale. Può cioè accadere che anche l'adempimento formalmente corretto di quanto richiesto dalle disposizioni menzionate non sia sufficiente a realizzare un'informativa secondo correttezza e buona fede. Questi principi potrebbero esigere di fornire informazioni ulteriori. Oppure potrebbero imporre di dare maggior peso ai dati e alle notizie che sono effettivamente rilevanti per la scelta del consumatore rispetto ad altre informazioni d'importanza secondaria.

I principi di correttezza e buona fede implicano, in seconda istanza, di non comunicare alla controparte informazioni contrarie a verità (*requisito della verità*).

È stato rilevato che l'art. 67 *quater* c.cons. omette di disciplinare le informazioni che devono essere fornite al consumatore dopo la conclusione del contratto (20). Tanto è vero che la disposizione è rubricata “informazione del consumatore *prima* della conclusione del contratto a distanza”. Le informazioni da rendersi prima della conclusione del contratto tendono a essere più importanti delle informazioni da rendersi in pendenza del rapporto contrattuale. Difatti l'informativa precontrattuale serve a determinare l'espressione del consenso del consumatore sotto due profili. In primo luogo il consumatore può decidere se concludere o meno il contratto. In secondo luogo il consumatore può (almeno teoricamente), una volta ricevute le opportune informazioni, negoziare le condizioni contrattuali. Pur essendo, per queste ragioni, certamente più importanti le informazioni che precedono la conclusione del contratto, non si può tuttavia negare che - anche in pendenza di contratto - un'adeguata informazione del consumatore può rivelarsi importante.

L'osservazione per cui il legislatore ha ommesso di disciplinare l'informazione durante il rapporto contrattuale conosce, fra l'altro, una parziale eccezione nell'art. 67 *bis* comma 2 alinea 3 c.cons.

Tale rilievo deve inoltre fare i conti con la circostanza che la disciplina dettagliata dettata dagli artt. 67 *bis* ss. c.cons. non fa venire meno l'applicazione dei principi generali. L'art. 38 c.cons. prevede che, per quanto non

Note:

(19) V. Cuffaro, *Dopo il codice del consumo: la disciplina della commercializzazione a distanza di servizi finanziari*, in *Contr. impr.*, 2007, 273 ss.

(20) F. Totaro, *op. cit.*, 848 s.

previsto dal codice del consumo, “ai contratti conclusi tra il consumatore ed il professionista si applicano le disposizioni del codice civile”. L’art. 38 c.cons. sancisce così l’applicazione in via integrativa del codice civile. Ora: fra le disposizioni del codice civile va annoverato l’art. 1375 c.c., secondo cui “il contratto deve essere eseguito secondo buona fede”. Dall’applicazione di questa disposizione deriva che il fornitore, anche durante lo svolgimento della relazione contrattuale (e non solo prima della conclusione del contratto), è tenuto a fornire informazioni al consumatore. Certo, non vi sono previsioni dettagliate come quelle degli artt. 67 *quinquies*, 67 *sexies*, 67 *septies* e 67 *octies* c.cons. in merito ai contenuti dell’informazione, ma - ciò nonostante - il fornitore che ometta informazioni ragionevolmente rilevanti in pendenza di contratto può essere ritenuto responsabile nei confronti del cliente.

È condivisibile, in linea di principio, l’auspicio di una regolamentazione della questione dell’informativa in pendenza di contratto su base volontaria da parte degli operatori di settore (21). Tuttavia, anche in mancanza d’iniziativa del genere, il consumatore trova - ad avviso di chi scrive - sufficiente tutela nel codice civile.

La disposizione in commento continua occupandosi di profili di legge applicabile. Si prevede difatti che “le informazioni relativi agli obblighi contrattuali, da comunicare al consumatore nella fase precontrattuale, devono essere conformi agli obblighi contrattuali imposti dalla legge applicabile al contratto a distanza anche qualora la tecnica di comunicazione impiegata sia quella elettronica” (art. 67 *quater* comma 3 c.cons.). La legge stabilisce inoltre che “se il fornitore ha sede in uno Stato non appartenente all’Unione europea, le informazioni di cui al comma 3 devono essere conformi agli obblighi contrattuali imposti dalla legge italiana qualora il contratto sia concluso” (art. 67 *quater* comma 4 c.cons.).

Dal punto di vista del diritto internazionale privato italiano, in materia contrattuale - in linea di principio - spetta alle parti determinare la legge applicabile al contratto. L’art. 57 l. n. 218/1995 rinvia alla Convenzione di Roma del 19 giugno 1980 sulla legge applicabile alle obbligazioni contrattuali. Il principio è che il contratto è regolato dalla legge scelta dalle parti (art. 3 comma 1 Convenzione di Roma). Nel contratto può così essere pattuita l’applicazione del diritto italiano oppure del diritto di un altro Paese. Per i contratti conclusi dai consumatori si prevede tuttavia una disciplina speciale: “in deroga all’articolo 3, la scelta ad opera delle parti della legge applicabile non può aver per risultato di privare il consumatore della protezione garantitagli dalle disposizioni imperative della legge del paese nel quale risiede abitualmente” (art. 5 comma 2 Convenzione di Roma). Il legislatore è preoccupato che la legge applicabile al contratto sulla base della scelta delle parti offra meno garanzie di quelle attribuite dal diritto del luogo in cui il consumatore risiede abitualmente. La norma che impo-

ne di tenere conto delle disposizioni imperative dei singoli Paesi può però avere l’effetto pratico di rendere più difficile l’attività transfrontaliera dei fornitori (22). Si immagini il caso di un fornitore che vuole vendere servizi finanziari in diversi Paesi dell’Unione europea. In questo caso non sarà sufficiente conformarsi alle disposizioni di legge del Paese del fornitore, ma occorrerà tenere conto delle norme imperative dei singoli Paesi in cui risiedono i destinatari dei servizi.

4. Il contenuto delle informazioni da fornirsi ai consumatori

I successivi articoli della sezione IV *bis* si occupano di definire le informazioni che vanno fornite ai consumatori. Un primo gruppo d’informazioni attiene al fornitore (art. 67 *quinquies* c.cons.).

La legge prevede anzitutto che vanno indicate “l’identità del fornitore e la sua attività principale, l’indirizzo geografico al quale il fornitore è stabilito e qualsiasi altro indirizzo geografico rilevante nei rapporti tra consumatore e fornitore” (art. 67 *quinquies* lett. a) c.cons.). Le informazioni sul fornitore servono a identificare la controparte contrattuale del consumatore. Tre sono gli elementi che vanno comunicati. In primo luogo bisogna indicare l’identità del fornitore. In secondo luogo occorre indicare l’attività principale del fornitore. In terzo luogo va indicato l’indirizzo geografico. L’indirizzo geografico va tenuto distinto da un eventuale indirizzo di posta elettronica. Non è dunque sufficiente comunicare che il fornitore è raggiungibile a un certo indirizzo di posta elettronica, ma bisogna dare un recapito geografico, al fine di garantire - in caso di necessità - una migliore raggiungibilità.

Bisogna anche indicare “l’identità del rappresentante del fornitore stabilito in Italia e l’indirizzo geografico rilevante nei rapporti tra consumatore e rappresentante, quando tale rappresentante esista” (art. 67 *quinquies* lett. b) c.cons.). Questa disposizione prende atto del fatto che il fornitore potrebbe non essere presente direttamente in Italia, ma avervi solo un rappresentante. Se non vi è tale rappresentante, non sarà necessaria alcuna indicazione. Se invece vi è un rappresentante, bisogna indicarne identità e indirizzo geografico.

La legge prevede poi che occorre indicare, “se il consumatore ha relazioni commerciali con un professionista diverso dal fornitore, l’identità del professionista, la veste in cui agisce nei confronti del consumatore nonché l’indirizzo geografico rilevante nei rapporti tra consumatore e professionista” (art. 67 *quinquies* lett. c) c.cons.). Nell’ipotesi in cui fra fornitore e consumatore si frapponga, a qualsiasi titolo, un professionista, bisogna fornire al consumatore adeguate informazioni su ta-

Note:

(21) F. Totaro, *op. cit.*, 849.

(22) Cfr. F. Totaro, *op. cit.*, 848.

le professionista: identità, veste in cui agisce e indirizzo geografico.

In aggiunta il legislatore impone la seguente indicazione: “se il fornitore è iscritto in un registro commerciale o in un pubblico registro analogo, il registro di commercio in cui il fornitore è iscritto e il numero di registrazione o un elemento equivalente per identificarlo nel registro” (art. 67 *quinquies* lett. d) c.cons.). Anche questi elementi servono per la pronta e corretta identificazione del fornitore.

Infine l'art. 67 *quinquies* c.cons. si chiude con la statuizione della necessità d'indicare, “qualora l'attività del fornitore sia soggetta ad autorizzazione, gli estremi della competente autorità di controllo” (art. 67 *quinquies* lett. e) c.cons.). Questa indicazione può risultare utile nel caso in cui si vogliono presentare reclami o ricorsi.

L'art. 67 *quinquies* c.cons. (informazioni relative al fornitore) non esaurisce le informazioni che devono essere date al consumatore. Un secondo gruppo d'informazioni che devono essere necessariamente fornite è quello relativo al servizio finanziario (art. 67 *sexies* c.cons.).

Anzitutto la legge impone una descrizione delle principali caratteristiche del servizio finanziario (art. 67 *sexies* lett. a) c.cons.). In questo modo il consumatore viene messo nelle condizioni di conoscere gli elementi essenziali che caratterizzano il servizio che va a comprare.

In secondo luogo va indicato “il prezzo totale che il consumatore dovrà corrispondere al fornitore per il servizio finanziario, compresi tutti i relativi oneri, commissioni e spese e tutte le imposte versate tramite il fornitore o, se non è possibile indicare il prezzo esatto, la base di calcolo del prezzo, che consenta al consumatore di verificare quest'ultimo” (art. 67 *sexies* lett. b) c.cons.). Il prezzo del servizio finanziario costituisce uno degli elementi fondamentali di decisione del consumatore. È importante che tale prezzo sia indicato nella sua complessità, per evitare sorprese in capo al contraente debole. Alcune volte non è possibile indicare il prezzo totale esatto. In questi casi la legge consente d'indicare la base di calcolo del prezzo. Tuttavia il legislatore effettua una specificazione importante: la base di calcolo deve consentire di verificare il prezzo. Ne deriva che la base di calcolo deve essere presentata e strutturata in modo tale che un destinatario medio sia in grado, senza particolari difficoltà, di determinare l'esatto ammontare del prezzo totale dovuto.

Occorre poi, “se del caso, un avviso indicante che il servizio finanziario è in rapporto con strumenti che implicano particolari rischi dovuti a loro specifiche caratteristiche o alle operazioni da effettuare, o il cui prezzo dipenda dalle fluttuazioni dei mercati finanziari su cui il fornitore non esercita alcuna influenza, e che i risultati ottenuti in passato non costituiscono elementi indicativi riguardo ai risultati futuri” (art. 67 *sexies* lett. c) c.cons.).

Al riguardo bisogna rilevare che non tutti i servizi finanziari implicano lo stesso livello di rischio. Esistono alcuni servizi particolarmente rischiosi e il consumatore de-

ve esserne reso edotto. Buona parte della giurisprudenza che si è sviluppata negli ultimi anni sui casi Argentina, Cirio e Parmalat è stata determinata dalla violazione dei doveri informativi degli intermediari finanziari (23).

Nota:

(23) Gli interventi dottrinali in materia di responsabilità di banche e intermediari finanziari sono talmente numerosi che è difficile elencarli tutti in una nota. Anzitutto cfr., per la sua attualità, la monografia di M. Pellegrini, *Le controversie in materia bancaria e finanziaria*, Padova, 2007. La sentenza più importante pronunciata al riguardo è Cass., 19 dicembre 2007, n. 26725, in *I Contratti*, 2008, 221 ss., con nota di V. Sangiovanni. V. inoltre fra i molti contributi, a titolo esemplificativo, A. Barenghi, *Disciplina dell'intermediazione finanziaria e nullità degli ordini di acquisto (in mancanza del contratto-quadro): una ratio decidendi e troppi obiter dicta*, in *Giur. mer.*, 2007, 59 ss.; E. Battelli, *L'adempimento contrattuale dell'intermediario finanziario*, in *I Contratti*, 2006, 465 ss.; M. Bombelli, M. Iato, *Obbligazioni Argentina e Cirio: responsabilità dell'istituto bancario intermediario*, in *Giur. mer.*, 2006, 1403 ss.; V. Bulfaro, *La responsabilità contrattuale dell'intermediario per violazione del dovere di informazione*, in *Nuova giur. civ. comm.*, 2007, I, 1092 ss.; I.A. Caggiano, *I doveri d'informazione dell'intermediario finanziario nella formazione ed esecuzione del contratto. Violazione e rimedi*, in *Dir. giur.*, 2006, 453 ss.; D. Cesiano, *La prestazione dei servizi di investimento e la tutela degli investitori: nota a sentenza del Tribunale di Napoli 21 febbraio 2007*, in www.dirittobancario.it; G. Cottino, *La responsabilità degli intermediari finanziari. Ancora qualche divagazione sul tema*, in *Giur. it.*, 2006, 1633 ss.; G. De Nova, *La responsabilità dell'operatore finanziario per esercizio di attività pericolosa*, in *I Contratti*, 2005, 709 ss.; E.A. Emiliozzi, *Vendita alla clientela retail di titoli prima dell'emissione ed omessa acquisizione da parte dell'intermediario dell'offering circular*, in *Giur. it.*, 2007, 1673 ss.; P. Fiorio, *La non adeguatezza delle operazioni di investimento*, in www.ilcaso.it; F. Galgano, *I contratti di investimento e gli ordini dell'investitore all'intermediario*, in *Contr. impr.*, 2005, 889 ss.; A.M. Mancini, *La tutela del risparmiatore nel mercato finanziario tra culpa in contrahendo e vizi del consenso*, in *Rass. dir. civ.*, 2007, 51 ss.; V. Mariconda, *Regole di comportamento nella trattativa e nullità dei contratti: la criticabile ordinanza di rimessione della questione alle sezioni unite*, in *Corr. giur.*, 2007, 635 ss.; G. Meruzzi, *La responsabilità precontrattuale tra regola di validità e regola di condotta*, in *Contr. impr.*, 2006, 944 ss.; S. Panzini, *Violazione dei doveri d'informazione da parte degli intermediari finanziari tra culpa in contrahendo e responsabilità professionale*, in *Contr. impr.*, 2007, 982 ss.; L. Picardi, *Nuovi sviluppi giurisprudenziali in tema di responsabilità degli intermediari*, in *Dir. giur.*, 2007, 192 ss.; A. Pisapia, *Responsabilità degli intermediari finanziari e negoziazione in strumenti finanziari “derivati”*, in *Le Società*, 2007, 711 ss.; V. Roppo, G. Afferni, *Dai contratti finanziari al contratto in genere: punti fermi della Cassazione su nullità virtuale e responsabilità precontrattuale*, in *Danno resp.*, 2006, 25 ss.; V. Sangiovanni, *Acquisto di obbligazioni e risoluzione del contratto*, in *I Contratti*, 2008, 5 ss.; V. Sangiovanni, *Contratti derivati e dichiarazione del rappresentante legale*, in *Corr. mer.*, 2008, 41 ss.; V. Sangiovanni, *Contratto di swap e nozione di operatore qualificato*, in *I Contratti*, 2007, 1093 ss.; V. Sangiovanni, *Contratto di negoziazione, forma convenzionale e nullità per inosservanza di forma*, in *I Contratti*, 2007, 778 ss.; V. Sangiovanni, *Emissioni di obbligazioni e scandali finanziari fra diritto internazionale privato e diritto comunitario*, in *Le Società*, 2007, 547 ss.; V. Sangiovanni, *Finanzskandale (Argentinien, Cirio und Parmalat) und die Haftung der Anlagevermittler in der neuesten italienischen Rechtsprechung*, in *BKR (Zeitschrift für Bank- und Kapitalmarktrecht)*, 2006, 476 ss.; V. Sangiovanni, *La violazione delle regole di condotta dell'intermediario finanziario fra responsabilità precontrattuale e contrattuale*, in *I Contratti*, 2006, 1133 ss.; V. Sangiovanni, *La responsabilità dell'intermediario finanziario nel diritto austriaco sullo sfondo del diritto comunitario e un suggerimento al legislatore italiano*, in *Danno resp.*, 2006, 1182 ss.; V. Sangiovanni, *Inadeguatezza della operazione finanziaria, risoluzione del contratto per inadempimento e risarcimento del danno*, in *Corr. giur.*, 2006, 1569 ss.; V. Sangiovanni, *Circolazione dei prodotti finanziari e responsabilità degli investitori professionali: il nuovo art. 100 bis TUF*, in *Le Società*, 2006, 1355 ss.; V. Sangiovanni, *La nullità del contratto di gestione di portafogli di investimento per difetto di forma*, in *I Contratti*, 2006, 966 ss.; V. Sangiovanni, *Sollecitazione all'investimento, nullità del contratto e frode alla* (segue)

Uno degli obblighi violati più frequentemente è quello di comunicare al cliente tutti i rischi che il compimento dell'operazione comporta. È evidente l'importanza che ha per il consumatore essere informato sui rischi derivanti dal servizio finanziario che acquista. Il fornitore potrebbe essere tentato di tacere tali rischi al fine di vendere più facilmente il suo prodotto e di trarne il relativo guadagno (24). Il legislatore non accetta però una pratica del genere, in quanto connotata da scorrettezza e indicativa di un indebito sfruttamento delle asimmetrie informative a vantaggio del contraente forte.

Vi è da chiedersi quali siano le conseguenze di un'omissione dell'informativa sui rischi. Al riguardo si deve ritenere che, almeno in certi casi, l'omissione possa essere stata determinante del consenso. Il fatto che vengano taciuti dei rischi può cagionare un errore in capo al consumatore, il quale conclude così un contratto che - altrimenti - non avrebbe concluso. Il rimedio ipotizzabile è, allora, l'annullamento del contratto (25).

Le informazioni relative al servizio finanziario riguardano inoltre "l'indicazione dell'eventuale esistenza di altre imposte e costi non versati tramite il fornitore o non fatturati da quest'ultimo" (art. 67 *sexies* lett. d) c.cons.). Questa lettera va letta insieme alla lett. b). Imposte e costi possono essere pagati direttamente dal fornitore e allora vanno a formare il prezzo totale. Può peraltro capitare che vi siano imposte e costi non pagati direttamente dal fornitore, e che - dunque - dovranno essere pagati dal consumatore. La legge esige che di tali imposte e costi il consumatore venga reso edotto.

Bisogna poi indicare qualsiasi limite del periodo entro il quale sono valide le informazioni fornite (art. 67 *sexies* lett. e) c.cons.). Le informazioni non necessariamente hanno validità illimitata nel tempo. Il fornitore potrebbe così, dopo un certo periodo di tempo, affermare che la dichiarazioni precedentemente rilasciate si devono ritenere superate. Per evitare un esito del genere, la legge impone al fornitore d'indicare l'eventuale periodo di validità delle informazioni.

Le informazioni relative al servizio finanziario riguardano anche "le modalità di pagamento e di esecuzione, nonché le caratteristiche essenziali delle condizioni di sicurezza delle operazioni di pagamento da effettuarsi nell'ambito dei contratti a distanza" (art. 67 *sexies* lett. f) c.cons.). Nei contratti a distanza il pagamento dei servizi forniti presenta caratteristiche diverse rispetto all'acquisto di servizi in relazione ai quali i contraenti si incontrano. La legge impone allora di specificare le modalità di pagamento. Questa disposizione va letta in connessione con il successivo art. 67 *quater decies* comma 1 c.cons., che fissa le modalità di pagamento (con carta di credito, di debito o con altri strumenti).

La legge prevede che le informazioni relative al servizio finanziario riguardano anche "qualsiasi costo specifico aggiuntivo per il consumatore relativo all'utilizzazione della tecnica di comunicazione a distanza, se addebitato" (art. 67 *sexies* lett. g) c.cons.). Questa disposizione va let-

ta in collegamento alle altre norme che disciplinano l'informativa sui costi. L'idea di fondo è che il consumatore deve essere pienamente informato in via anticipata di tutti i costi che dovrà affrontare, al fine di subire cattive sorprese.

Nel contesto della commercializzazione a distanza di servizi finanziari ai consumatori vi è poi un terzo articolo in materia d'informazioni, il quale impone di dare informazioni sul contratto a distanza (art. 67 *septies* c.cons.).

Le informazioni riguardano anzitutto "l'esistenza o la mancanza del diritto di recesso conformemente all'art. 67 *duodecies* e, se tale diritto esiste, la durata e le modalità d'esercizio, comprese le informazioni relative all'importo che il consumatore può essere tenuto a versare ai sensi dell'art. 67 *terdecies*, comma 1, nonché alle conseguenze derivanti dal mancato esercizio di tale diritto" (art. 67 *septies* lett. a) c.cons.). Il consumatore è privo, in alcuni casi, del diritto di recesso, come stabilisce l'art. 67 *duodecies* comma 5 c.cons. e di ciò deve essere informato. Utili sono anche le informazioni relative a durata e modalità di esercizio di tale diritto. Con riferimento alla durata, si potrà - ad esempio - prevedere una durata superiore a quella di 14 giorni fissata come minimo dall'art. 67 *duodecies* comma 1 c.cons. Nella prassi è peraltro improbabile che il fornitore sia disponibile a concedere un vantaggio del genere al consumatore.

Le informazioni sul contratto a distanza riguardano poi "le informazioni relative agli eventuali diritti delle parti, secondo i termini del contratto a distanza, di mettere fine allo stesso prima della scadenza o unilateralmente,

Note:

(segue nota 23)

legge, in *Giur. mer.*, 2006, 1389 ss.; V. Sangiovanni, *La responsabilità precontrattuale dell'intermediario finanziario nel diritto inglese*, in *Le Società*, 2006, 1173 ss.; V. Sangiovanni, *Scandali finanziari: profili di responsabilità dell'intermediario*, in *Danno resp.*, 2006, 874 ss.; V. Sangiovanni, *La responsabilità dell'intermediario nel caso Cirio e la recente legge per la tutela del risparmio*, in *I Contratti*, 2006, 686 ss.; V. Sangiovanni, *La nullità del contratto per inosservanza di forma nel caso delle obbligazioni argentine*, in *Com. mer.*, 2006, 737 ss.; V. Sangiovanni, *La responsabilità dell'intermediario nel caso Parmalat e la recentissima legge per la tutela del risparmio*, in *Le Società*, 2006, 605 ss.; M. Ticozzi, *Violazione di obblighi informativi e sanzioni: un problema non solo degli intermediari finanziari*, in *I Contratti*, 2007, 363 ss.; R. Viglione, *La tutela dell'investitore retail nel nuovo art. 100-bis T.U.F.*, in *Studium iuris*, 2007, 779 ss.; S.A. Vignolo, *Le regole di condotta degli intermediari finanziari al vaglio della giurisprudenza ligure e nazionale*, in *Nuova giur. lig.*, 2007, 42.

(24) Sulla possibile reticenza dell'intermediario nel contesto dei servizi d'investimento cfr. il contributo di R. Vigo, *La reticenza dell'intermediario nei contratti relativi alla prestazione dei servizi d'investimento*, in *Banca borsa tit. cred.*, 2005, I, 665 ss.

(25) È utile ricordare che, in altra sede, il codice del consumo si occupa di possibili omissioni ingannevoli. Il riferimento è all'art. 22 comma 1 c.cons. secondo cui "è considerata ingannevole una pratica commerciale che nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, nonché dei limiti del mezzo di comunicazione impiegato, omette informazioni rilevanti di cui il consumatore medio ha bisogno in tale contesto per prendere una decisione consapevole di natura commerciale e induce o è idonea ad indurre in tal modo il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".

comprese le penali eventualmente stabilite dal contratto in tali casi” (art. 67 *septies* lett. c). Questa disposizione impone d’indicare i casi in cui il contratto può essere terminato prima della scadenza oppure unilateralmente. Si tratta di ipotesi distinte da quella del recesso, oggetto di una speciale disciplina nell’art. 67 *duodecies* c.cons. La disposizione qui in esame consente di prevedere delle penali, che devono essere indicate. L’indicazione delle penali serve a evitare effetti-sorpresa in capo al consumatore. Si noti invece che, per il caso di esercizio del diritto di recesso, è vietato prevedere delle penali, come statuisce l’art. 67 *duodecies* comma 1 c.cons.

Bisogna anche dare informazioni riguardanti “le istruzioni pratiche per l’esercizio del diritto di recesso, comprendenti tra l’altro il mezzo, inclusa in ogni caso la lettera raccomandata con avviso di ricevimento, e l’indirizzo a cui deve essere inviata la comunicazione di recesso” (art. 67 *septies* lett. d) c.cons.). Il legislatore è consapevole che - ai fini di un’adeguata tutela del consumatore - non è sufficiente riconoscere in maniera astratta il diritto di recesso, così come si limita a fare l’art. 67 *duodecies* c.cons. Occorre invece dare concretezza a tale diritto. Il consumatore deve pertanto essere informato sulle istruzioni pratiche per l’esercizio del diritto di recesso. Vanno specificate le modalità con cui il diritto di recesso deve essere esercitato; ma, in ogni caso, deve essere garantita la possibilità di utilizzare lo strumento della lettera raccomandata.

Si rinviengono poi nel testo dell’art. 67 *septies* c.cons. tre lettere dedicate ai profili internazionali della materia. In merito al contratto a distanza bisogna anche indicare “lo Stato membro o gli Stati membri sulla cui legislazione il fornitore si basa per instaurare rapporti con il consumatore prima della conclusione del contratto a distanza” (art. 67 *septies* lett. e) c.cons.). Inoltre va indicata “qualsiasi clausola contrattuale sulla legislazione applicabile al contratto a distanza e sul foro competente” (art. 67 *septies* lett. f) c.cons.). Infine occorre specificare “la lingua o le lingue in cui sono comunicate le condizioni contrattuali e le informazioni preliminari di cui al presente articolo, nonché la lingua o le lingue in cui il fornitore, con l’accordo del consumatore, si impegna a comunicare per la durata del contratto a distanza” (art. 67 *septies* lett. g) c.cons.). Legislazione applicabile e foro competente sono due circostanze di grande rilevanza per il consumatore. La legge applicabile determina la disciplina dei rapporti intercorrenti fra le parti. Il foro competente assume rilevanza in caso di controversie fra i contraenti. Diritto applicabile e foro competente potrebbero essere diversi da quelli italiani. Considerato poi che il fornitore può essere straniero, occorre una specificazione in merito alla lingua di comunicazione. Può trattarsi di una lingua diversa dall’italiano, a condizione che vi sia il consenso del consumatore.

Un intero articolo è dedicato alle informazioni relative al ricorso (art. 67 *octies* c.cons.). La legge prevede che “le informazioni relative al ricorso riguardano l’esistenza o la mancanza di procedure extragiudiziali di reclamo e di ricorso accessibili al consumatore che è parte del contrat-

to a distanza e, ove tali procedura esistano, le modalità che consentono al consumatore di avvalersene” (art. 67 *octies* c.cons.) (26). Al fine di dare una reale opportunità al consumatore di far valere reclami o ricorsi deve, anzitutto, essergli comunicata la loro esistenza. In secondo luogo occorre un’indicazione delle modalità con cui il consumatore può avvalersi di tali rimedi. Meccanismi di soluzione extragiudiziale delle controversie dovrebbero garantire una soluzione veloce e poco costosa delle liti. Le procedure extragiudiziali potrebbero essere particolarmente utili nel caso di controversie a carattere internazionale (27).

L’art. 67 *novies* c.cons. si occupa di dettare una disciplina particolare per una modalità speciale di comunicazione delle informazioni: le comunicazioni mediante telefonia vocale. La comunicazione per via telefonica richiede una disciplina particolare per alcune ragioni. Anzitutto il telefono, diversamente da altre tecniche di comunicazione a distanza, consente un contatto immediato e personale fra fornitore e consumatore, il quale potrebbe essere sorpreso dalla telefonata ricevuta. In secondo luogo, il consumatore potrebbe avere difficoltà ad opporsi allo stesso fatto di ricevere telefonate indesiderate.

La legge prevede anzitutto che in caso di comunicazioni mediante telefonia vocale “l’identità del fornitore e il fine commerciale della chiamata avviata dal fornitore sono dichiarati in maniera inequivoca all’inizio di qualsiasi conversazione con il consumatore” (art. 67 *novies* comma 1 lett. a) c.cons.). Deve anzitutto essere dichiarata l’identità del fornitore. Il consumatore viene a sapere, in questo modo, con quale soggetto ha a che fare. Inoltre la legge impone un’immediata chiarificazione sul fine commerciale della telefonata. Si vuole così evitare un effetto-sorpresa del consumatore. Si vuole in particolare evitare che la volontà di chi riceve la telefonata possa, in qualche modo, essere manipolata da un abile telefonista. La disposizione in esame non si applica invece quando è il consumatore a contattare il fornitore, poiché in questi casi si presume che il consumatore conosca l’identità del fornitore e sappia che il fornitore cercherà di vendergli dei servizi.

La legge stabilisce poi che, in caso di comunicazioni mediante telefonia vocale, “devono essere fornite, previo

Note:

(26) Il considerando n. 27 della direttiva n. 65/2002 prevede che “per tutelare i consumatori occorre prevedere procedure appropriate ed efficaci di reclamo e di ricorso negli Stati membri onde disciplinare le eventuali controversie tra fornitori e consumatori utilizzando, se del caso, le procedure esistenti”.

(27) Il considerando n. 28 della direttiva n. 65/2002 recita “gli Stati membri dovrebbero incitare gli organismi pubblici o privati preposti alla composizione stragiudiziale delle controversie a cooperare nella risoluzione delle controversie transfrontaliere. Questa cooperazione potrebbe in particolare mirare a consentire al consumatore di sottoporre agli organi extragiudiziali stabiliti nello Stato membro in cui risiede i reclami relativi ai fornitori stabiliti in altri Stati membri. L’istituzione della rete FIN-NET offre un’ulteriore assistenza ai consumatori che si avvalgono di servizi transfrontalieri”.

consenso del consumatore, solo le informazioni seguenti: 1) l'identità della persona in contatto con il consumatore e il suo rapporto con il fornitore; 2) una descrizione delle principali caratteristiche del servizio finanziario; 3) il prezzo totale che il consumatore dovrà corrispondere al fornitore per il servizio finanziario, comprese tutte le imposte versate tramite il fornitore o, se non è possibile indicare il prezzo esatto, la base di calcolo del prezzo, che consenta al consumatore di verificare quest'ultimo; 4) l'indicazione dell'eventuale esistenza di altre imposte e/o costi non versati tramite il fornitore o non fatturati da quest'ultimo; 5) l'esistenza o la mancanza del diritto di recesso conformemente all'art. 67 *duodecies* e, se tale diritto esiste, la durata e le modalità di esercizio, comprese le informazioni relative all'importo che il consumatore può essere tenuto a versare ai sensi dell'art. 67 *terdecies*, comma 1" (art. 67 *novies* comma 1 lett. b) c.cons.).

La prima osservazione da fare in relazione a questa disposizione è che la legge prevede la necessità del consenso del consumatore. Se questi, conosciuto il fine commerciale della telefonata, non è interessato alla continuazione del colloquio, la telefonata deve terminare. La disposizione in esame fissa non tanto un livello minimo, bensì un quantitativo massimo d'informazioni che devono essere date. Fra le tante informazioni identificate in via generale dagli artt. 67 *quinquies* ss. c.cons., il legislatore ne seleziona alcune soltanto che vanno fornite per telefono. Nel caso di comunicazioni mediante telefonia vocale, il legislatore ritiene inopportuno che vengano fornite tante informazioni. Probabilmente la *ratio* della disposizione è quella di evitare che il consumatore possa essere tratto in errore da un quantitativo eccessivo d'informazioni trasmesse per via orale. Inoltre bisogna tenere presenti le difficoltà di comunicare per telefono, in un breve lasso di tempo, molti dati e notizie.

In questa ottica va letto l'art. 67 *novies* comma 2 c.cons. secondo cui "il fornitore comunica al consumatore che altre informazioni sono disponibili su richiesta e ne precisa la natura. Il fornitore comunica in ogni caso le informazioni complete quando adempie ai propri obblighi ai sensi dell'art. 67 *undecies*". In caso di comunicazioni telefoniche il legislatore consente dunque la dazione immediata di (relativamente) poche informazioni, a condizione che il fornitore enunci che altre informazioni sono ottenibili su richiesta. In ogni caso il consumatore riceve tutte le informazioni dovute in adempimento dell'art. 67 *undecies* c.cons.

L'art. 67 *decies* c.cons. disciplina i requisiti aggiuntivi in materia d'informazioni.

Si prevede che "oltre alle informazioni di cui agli articoli 67 *quater*, 67 *quinquies*, 67 *sexies*, 67 *septies* e 67 *octies* sono applicabili le disposizioni più rigorose previste dalla normative di settore che disciplina l'offerta del servizio o del prodotto interessato" (art. 67 *decies* comma 1 c.cons.) (28). Questa disposizione è di grande importanza, in quanto sancisce la concorrenza - con le norme che si sono appena esaminate - di tutte le regole di settore

che dovessero essere più rigorose. Vi è dunque una duplice serie di disposizioni che trova applicazione alle informazioni: 1) quelle degli artt. 67 *quater* ss. c.cons.; 2) quelle di settore più rigorose.

L'art. 67 *undecies* c.cons. impone la comunicazione delle condizioni contrattuali e delle informazioni preliminari. La legge prevede che "il fornitore comunica al consumatore tutte le condizioni contrattuali, nonché le informazioni di cui agli articoli 67 *quater*, 67 *quinquies*, 67 *sexies*, 67 *octies*, 67 *novies* e 67 *decies*, su supporto cartaceo o su un altro supporto durevole, disponibile e accessibile per il consumatore in tempo utile, prima che lo stesso sia vincolato da un contratto a distanza o da un'offerta" (art. 67 *undecies* comma 1 c.cons.).

Questa disposizione fissa alcune importanti regole.

La prima di esse riguarda le modalità con cui le informazioni vanno fornite. Il fornitore deve utilizzare un supporto cartaceo oppure un altro supporto durevole. È esclusa dunque la comunicazione in forma meramente orale delle informazioni. La forma scritta o comunque la necessità dell'utilizzo di un supporto durevole consente una fissazione delle condizioni contrattuali e delle informazioni a futura memoria. In qualsiasi momento il consumatore può avere così accesso a condizioni e informazioni e verificarne il contenuto.

In secondo luogo la norma in esame fissa la tempistica della comunicazione d'informazioni. Esse vanno date prima che il consumatore sia vincolato da un contratto, in modo che questi possa riflettere sulle condizioni contrattuali proposte e sulle informazioni comunicate. La ragione di questa disposizione è che sono le condizioni e le informazioni provenienti dal fornitore a consentire al consumatore di assumere una decisione appropriata. Se esse vengono comunicate dopo la conclusione del contratto, non sono di giovamento per la parte debole del rapporto. Per quanto riguarda la tempistica della dazione d'informazioni il legislatore preferisce però non fissare un termine preciso, ma si avvale dell'espressione "in tempo utile". Questa scelta appare sensata se si considera che il lasso di tempo che deve ragionevolmente trascorrere fra la dazione d'informazioni e la conclusione del contratto dipende da numerose circostanze, che variano a seconda del caso concreto. Bisognerà tenere conto, ad esempio, della complessità del servizio proposto e del conseguente tecnicismo delle condizioni contrattuali e delle informazioni da fornirsi (29). Maggiore è tale complessità, mag-

Nota:

(28) Il considerando n. 22 della direttiva n. 65/2002 stabilisce che "le informazioni elencate nella presente direttiva comprendono informazioni di natura generale relative a tutti i tipi di servizi finanziari. Gli altri requisiti in materia di informazioni relative ad un determinato servizio, quali la copertura di una polizza assicurativa, non sono precisati unicamente nella presente direttiva. Le informazioni di questo tipo dovrebbero essere fornite in conformità, ove del caso, della pertinente normativa comunitaria o della pertinente legislazione nazionale, adottata conformemente al diritto comunitario".

(29) Cfr. P. Longhini, *op. cit.*, 185.

giore dovrebbe essere il tempo lasciato a disposizione del consumatore per effettuare una scelta consapevole.

La legge continua stabilendo che “il fornitore ottempera all’obbligo di cui al comma 1 subito dopo la conclusione del contratto a distanza, se quest’ultimo è stato concluso su richiesta del consumatore utilizzando una tecnica di comunicazione a distanza che non consente di trasmettere le condizioni contrattuali né le informazioni ai sensi del comma 1” (art. 67 *undecies* comma 2 c.cons.). Con questa disposizione il legislatore fa eccezione al principio di cui al comma 1 secondo il quale condizioni contrattuali e informazioni vanno date prima della conclusione del contratto. Si tratta peraltro di un’eccezione che opera in presenza di due presupposti del tutto particolari. La prima condizione è che il contratto sia stato concluso su richiesta del consumatore. È dunque questi, per così dire, a “pretendere” la conclusione del contratto. La seconda condizione fissata dalla norma in esame è la presenza di una situazione d’impossibilità di comunicazione prima della conclusione del contratto. A fronte di un’impossibilità di trasmissione immediata di condizioni e informazioni e di una richiesta del consumatore, l’interesse a una veloce conclusione del contratto prevale rispetto all’esigenza di un’approfondita informativa. La disposizione è per certi versi sorprendente in quanto consente la conclusione di un contratto in una situazione di carenza d’informazioni. Bisogna tuttavia tenere presente

che la parte debole del rapporto contrattuale trova tutela nel diritto di recesso, il cui termine decorre dalla data in cui il consumatore riceve le condizioni contrattuali e le informazioni ai sensi dell’art. 67 *duodecies* comma 3 lett. b) c.cons. Ne consegue che è vero che il consumatore può concludere un contratto senza conoscerne i dettagli, ma è altrettanto vero che egli può - una volta preso conoscenza di condizioni contrattuali e informazioni - recedere dallo stesso. Nel complesso, dunque, il consumatore appare sufficientemente tutelato.

La legge stabilisce infine che “in qualsiasi momento del rapporto contrattuale il consumatore, se lo richiede, ha il diritto di ricevere le condizioni contrattuali su supporto cartaceo” (art. 67 *undecies* comma 3 c.cons.). Nell’ipotesi in cui le condizioni contrattuali vengano messe a disposizione solo su supporto durevole (e non su supporto cartaceo), il consumatore ha diritto di ottenerle anche su supporto cartaceo. Questo obbligo del fornitore sussiste non solo prima della conclusione del contratto, ma durante tutto il rapporto contrattuale. Se il consumatore non riesce più a reperire le condizioni contrattuali, può sempre rivolgersi al fornitore, il quale è tenuto a comunicargliele. Il fornitore dispone di norma di una struttura organizzativa migliore e, per questa ragione, gli viene addossato l’onere - su richiesta della controparte - di fornire alla parte debole del rapporto le condizioni su supporto cartaceo.

RIVISTE

Famiglia e diritto

Rivista mensile di dottrina e giurisprudenza

Direzione scientifica: Piero Schlesinger

Comitato scientifico: Giacomo Caliendo, Vincenzo Carbone, Massimo Dogliotti, Michele Sesta, Ferruccio Tommaseo, Mario Trimarchi

Periodicità: mensile

La Rivista offre un panorama completo del diritto di famiglia esaminato alla luce dell’**evoluzione giurisprudenziale** e delle **novità legislative**. Tutte le sentenze più innovative della giurisprudenza di legittimità e di merito trovano ampio spazio e sono corredate da **commenti autorevoli**.

La selezione dei provvedimenti mira a privilegiare questioni nuove nonché opzioni interpretative originali, così da fornire all’operatore spunti da utilizzare nel lavoro quotidiano. Grande attenzione è dedicata ai profili processuali in materia.

La Rivista, che da sempre ha dato spazio ai **profili internazionalistici** del diritto di famiglia, offre ora ai lettori un’apposita **rubrica quadrimestrale: “Panorama sovranazionale”**. La rubrica prenderà in considerazione il diritto internazionale privato, il diritto internazionale e il diritto comunitario.

Il **servizio online**, compreso nel prezzo e riservato esclusivamente agli abbonati è consultabile all’indirizzo **www.dottrinaediritto.it**. Il servizio oltre ad integrare e completare l’informazione offerta dalla rivista cartacea, consente di consultare in anteprima e prelevare l’ultimo numero di “Famiglia e diritto”.

Abbonamento annuale € 175,00

Per informazioni

- **Servizio Informazioni Commerciali**
(tel. 02.82476794 – fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- **<http://ipsoshop.ipsoa.it>**

Casellario giudiziale

Le regole tecniche del nuovo casellario giudiziario telematico

di Alfonso Contaldo e Michele Gorga

Il sistema amministrativo della giustizia da un'ulteriore accelerata verso quella rivoluzione informatica che fino a pochi anni fa sembrava solo annunciata. Con l'adozione della normativa tecnica sul Casellario giudiziario telematico si aprono nuovi orizzonti e si ravviva il dibattito sul diritto alla privacy nella comunicazione e quindi anche alla sicurezza degli impianti e delle reti attraverso cui tale informazione transita. Il Casellario giudiziario, quello dei carichi pendenti e delle sanzioni per gli illeciti amministrativi offrirà *on-line* una completa mappa del soggetto che entra in contatto con il sistema giustizia e pone la necessità di nuove politiche di sicurezza e di tutela dei soggetti coinvolti.

1. La documentazione nella giustizia penale e per il casellario giudiziale

Il sistema amministrativo, soprattutto della giustizia, com'è noto oramai tendenzialmente è rivolto a fare un grande impiego dell'informatica anche per poter fornire una facile reperibilità di quanto richiesto nell'ottica di buon andamento gestionale nell'amministrazione della giustizia (1). Una delle prime realizzazioni di cooperazione applicativa tra rami della P.A., anche alla luce delle disposizioni sul protocollo informatico e sulla gestione dei flussi documentali, nonché sulla firma digitale, è stata quella disciplinata dal D.M. 27 marzo 2000 n. 264 relativa al "regolamento per la tenuta dei registri presso gli uffici giudiziari" (2). La disciplina dettata da questo decreto attiene a quattro problematiche differenti e vale a dire: la problematica relativa all'individuazione dell'insieme dei registri, tenuti a cura delle cancellerie o delle segreterie presso gli uffici giudiziari, ovvero dei registri previsti dai codici, da leggi speciali o dai regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'amministrazione della giustizia; la tenuta dei registri ed, in particolare, la loro formazione, conservazione, custodia ed esibizione; gli atti formati o comunicati dalle cancellerie o dagli uffici giudiziari; l'accesso ai registri.

I registri sottoposti alla disciplina del regolamento sono indicati all'art. 13 il quale distingue tra registri da tenersi presso: *a)* il tribunale (comma 1); *b)* le sezioni distaccate dei tribunali (comma 3); *c)* la Corte d'Appello (comma 4); *d)* la Corte di Cassazione (comma 5); *e)* il Giudice di Pace (comma 6). Tali registri sono tenuti "su base annuale ed in modo da garantire l'integrità, la completezza, la disponibilità e la riservatezza di iscrizioni ed annotazioni nonché l'identificazione del soggetto" che vi accede in forma informatizzata. Secondo le regole procedurali, emanate in ossequio alle esigenze relative alla

integrità fisica e logica dei dati, con d. M. G. (sulla tipologia dei dati stessi da inserire negli atti e nei registri) nonché ai sensi del d.P.R. 28 ottobre 1994 n. 748 i dati contenuti nei registri, memorizzati su uno o più supporti informatici, sono poi aggregati in un sistema, il quale deve consentire "la estrazione dei dati secondo la natura delle controversie, la sezione, il giudice, il nome delle parti, lo stato della causa, l'udienza ed ogni altro tipo di dato eventualmente richiesto dalle disposizioni che regolano la tenuta dei registri e la loro individuazione". Una volta disciplinata la tenuta dei registri, il d. M. in esame si è preoccupato di organizzare l'accesso alle infor-

Note:

(1) Sul punto ci si permette di rinviare a A. Contaldo, M. Gorga, *E-law. Le professioni legali, la digitalizzazione delle informazioni giuridiche e il processo telematico*, Soveria Mannelli, CZ, 2006, 122 ss.; Idem, *Le regole del processo civile telematico anche alla luce della più recente disciplina del SICI*, in questa Rivista, 2008, n. 1, 14 ss.

(2) Sul punto vedi M. Cammarata, *Giustizia: il fascicolo informatico*, in www.interlex.it; C. Mattioli, *Il processo telematico*, in www.foroeuropeo.it; G. Briganti, *Il cd. processo telematico*, in www.foroeuropeo.it; S. Niger, *Il processo telematico: speranze e prospettive*, in www.diritto.it; inoltre vedi al riguardo P. Liccardo, *Introduzione al processo civile telematico*, in *Riv. trim. dir. proc. civ.*, 2000, 1165 ss.; F. Carpi, *Processo civile e telematica: riflessioni di un profano*, in *Il processo telematico. Nuovi ruoli e nuove tecnologie per un moderno processo civile*, a cura di M. Jacchia, Bologna, 2000, 110 ss.; F. Sarzana di Sant'Ippolito, *Brevi considerazioni in margine al cd. processo telematico*, in *Corr. Giur.*, 2001, 832 ss.; F. Sorrentino, *Il cosiddetto "processo telematico"*, in *Fisco*, 2001, 1871 ss.; S. Fadda, *L'uso di strumenti di informatici e telematici nel processo civile*, in *Diritto delle nuove tecnologie informatiche e dell'internet*, a cura di G. Cassano, Milano, 2001, 1507 ss.; V. Ruggeri, *Il processo civile telematico. Breve guida al D.M. 13 febbraio 2001*, n. 123, Torino, 2001, spec. 63 ss.; V. Vigoriti, *E-commerce e tutela giurisdizionale*, in *Nuova giur. civ. comm.*, 2002, n. 1-2, pt. 2, 20 ss.; F. Buffa, *Il processo telematico. La gestione informatica*, Milano, 2002, 72 ss.; G. Riem, *Il processo civile telematico. Le nuove frontiere del processo alla luce del D.P.R. 123/2001*, Napoli, 2001, spec. 31 ss.; G. Buonomo, *Processo telematico e firma digitale*, Milano, 2004, 72 ss.; P. Moro, *L'informatica forense. Verità e metodo*, Cinisello Balsamo (MI), 2006, 96 ss.

mazioni ivi contenute (3). L'accesso alle informazioni, il rilascio di copie, di estratti o certificati è disciplinato secondo quattro differenti livelli, e la disciplina è comune sia ai registri che agli atti ivi contenuti. Per quanto attiene all'accesso questo è effettuato, da parte degli utenti esterni, direttamente dall'interessato o tramite l'ufficio depositario o per via telematica, previa identificazione di colui che agisce (art. 11 comma 1). Gli utenti interni, invece, possono accedere ai registri per effettuare operazioni di immissione, cancellazione, variazione ed esibizione solo se autorizzati dal dirigente amministrativo dell'ufficio ed il sistema informatico conserva, per ogni attività espletata, l'identificazione di colui che effettua l'operazione e della relativa indicazione della data e dell'ora.

Le regole procedurali, di cui all'art. 1 comma 1 lett. f) del decreto, relativamente ai registri informatizzati tenuti a cura delle cancellerie e delle segreterie, presso gli uffici giudiziari, ovvero ai registri previsti da codici, leggi speciali o da regolamenti, comunque connessi all'espletamento delle funzioni e dei servizi svolti dall'amministrazione della Giustizia, sono esplicitate dal D.M. 24 maggio 2001 del Ministro della Giustizia (4). L'art. 1 offre la definizione dei concetti di sistema informativo (comma 1), di sistema informativo di edificio (comma 2) e di sistema informativo dell'ufficio (comma 3). È previsto che il sistema informativo è costituito dall'insieme delle risorse umane, delle regole organizzative, delle risorse *hardware* e *software* (applicazione e dati), dei locali e della documentazione (sia in formato cartaceo, sia elettronico) che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti i registri informatizzati degli uffici. Per sistema informativo occorre intendere l'insieme costituito dalle risorse condivise, specificato nel secondo comma dell'art. 1 lett. f), g) e h) dalle relative quote di personale, che gestisce e utilizza il sistema, e dall'infrastruttura logistica. Il terzo comma dell'art. 1 dell'Allegato, definisce il sistema informativo dell'ufficio come l'insieme delle componenti "dedicate esclusivamente all'ufficio" e specificate dalle lett. c), d) ed e) del comma 2". Il sistema informativo, inoltre, ai sensi dell'art. 2, deve rendere disponibili agli utenti le informazioni ed i servizi compatibilmente ai livelli di servizio prestabiliti, assicurare l'integrità delle informazioni e dei servizi medesimi, i quali possono essere creati, modificati o cancellati solo dalle persone autorizzate e secondo le modalità predefinite, infine deve garantire l'autenticità dei dati ed il controllo degli accessi (5).

L'art. 5 dell'Allegato classifica gli utenti del sistema in due categorie: gli utenti interni e gli utenti esterni. L'insieme degli utenti interni è costituito dal personale dell'ufficio abilitato all'accesso al sistema informativo, i quali hanno l'obbligo di operare i comportamenti previsti per gli utenti e quelli previsti dal manuale per l'utente, stilato dall'amministratore di sistema (le cui funzioni sono disciplinate dall'art. 4) sulla base delle regole di cui

allo stesso Allegato e del piano di sicurezza, redatto dal responsabile della tenuta dei Registri (e cioè dal dirigente amministrativo dell'ufficio) assieme all'amministratore di sistema stesso.

L'art. 8 regola la materia degli accessi, richiamando la procedura di autenticazione definita dall'art. 5 D.M. n. 264 del 2000 che, rispetto alle risorse del sistema informatico, "consente di ottenere uno specifico insieme di privilegi di accesso e di utilizzo", poiché attraverso la procedura di autenticazione si individua un insieme di gruppi di utenti di modo che ad ogni gruppo corrisponda "uno e un solo" profilo (utente) ed a ciascun utente possono essere assegnati "uno o più" profili. I gruppi di utenti sono individuabili a livello di sistema, a livello di *database management system* ed a livello applicativo. A livello di sistema, per il disposto del comma 3 dell'art. 8, deve essere definito almeno un gruppo di utenze per il Responsabile della tenuta dei registri, per l'amministrazione di sistema, per gli utenti interni ed "in corrispondenza di ciascun gruppo", è definito un profilo tale da assegnare a ciascun utente, appartenente al gruppo, solo ed esclusivamente i privilegi di accesso e utilizzo strettamente necessari per l'espletamento delle attività di propria competenza. Per ciascun *database*, invece, è definito sia un gruppo di amministratori di sistema sia un gruppo di utenti a livello di *database management system*; anche a questi è assegnato un profilo che attribuisce i privilegi di accesso e di utilizzo strettamente necessari per l'espletamento delle sole attività di propria competenza. Per ciascun applicativo, infine, è definito almeno un gruppo per ciascuna delle diverse tipologie di utenza previste da ogni specifico *software*, disciplinati dai successivi artt. 12, 13, 18, 19 (6). La prima di queste norme dispone che presso ogni Ufficio giudiziario è possibile installare ed utilizzare esclusivamente il *software* commerciale, di rilevanza nazionale o realizzato a livello locale. Il *software*, installato solo ed esclusivamente a partire da supporti fisici originali o dei quali sia nota e sicura la provenienza, nel caso in cui sia *software* commerciale può essere messo in utilizzo solo se munito di una licenza d'uso idonea. Se, invece, l'applicativo è di rilevanza nazionale deve essere rilasciato dall'Ufficio del Responsabile per i sistemi informativi automatizzati del Ministero della Giustizia (URSIA), che ne certifica la conformità ai sensi dell'art. 3 D.M. 27 marzo 2000 n. 264, mentre gli applicativi realizzati nell'ambito di iniziative locali devono essere

Note:

(3) Vedi al riguardo F. Buffa, *Il processo telematico. La gestione informatica*, cit., 82 ss.

(4) Vedi al riguardo P. Liccardo, *Introduzione al processo civile telematico*, cit., 1172 ss.; F. Sarzana di Sant'Ippolito, *Brevi considerazioni in margine al cd. processo telematico*, cit., 835 ss.

(5) Vedi al riguardo F. Sorrentino, *Il cd. "processo telematico"*, cit., 1871 ss.; F. Buffa, *Il processo telematico. La gestione informatica*, cit., 94 ss.

(6) Sul punto vedi A. Piraino, *Brevi note critiche sulle modalità di attuazione della riforma*, in www.giustiziasicilia.it

conformi alle “presenti regole procedurali” (art. 18). È da notare, ancora, che per il disposto del secondo comma dell’art. 19 delle regole procedurali in questione, se gli applicativi utilizzati rientrano nella categoria di *software* di rilevanza nazionale o realizzati nell’ambito di iniziative locali, devono essere sviluppati da società dotate di certificato di qualità EN ISO 9001, relativo ai servizi di sviluppo di prodotti *software* (CPV 77207721-7723) (7).

L’area di intervento “Giustizia penale” costituisce una delle maggiori aree dedicate all’informatizzazione della Giustizia italiana. Allo stato, nell’area penale, si è garantita la presenza, all’interno di ogni ufficio giudiziario, di un’applicazione per la gestione dei registri basata su un’architettura *client/server*. A dire il vero, tale obiettivo non è tuttavia sufficientemente integrato con altre applicazioni appartenenti agli altri e diversi settori di attività (esecuzione penale, misure cautelari etc.), i quali gestiscono i dati secondo un formato proprietario, vale a dire non condivisibile con altri *software*, rendendo non attuabile lo scambio dei dati, da un sistema informatico all’altro, se non attraverso un’apposita applicazione che consenta la traduzione del formato.

In generale, comunque, si assiste a situazioni di informatizzazione consolidate che oggi necessitano di soli interventi di gestione e manutenzione, diffusione o estensione applicativa. È questo il caso del Sistema di Gestione dei Registri Penali, del Sistema Informativo della Direzione Nazionale Antimafia e delle Direzioni Distrettuali Antimafia, nonché del Sistema Informativo per la Magistratura di Sorveglianza. A tali progetti, di lungo corso e risalenti alla prima pianificazione in materia, si aggiungono iniziative nuove o in uno stato iniziale di realizzazione che si ispirano, non più ad una filosofia di automazione di un singolo processo o servizio, ma di razionalizzazione ed integrazione di soluzioni applicative.

Per quanto riguarda il Sistema Integrato Area Penale (SIAP), occorre evidenziare come questo si proponga di realizzare un unico ed integrato sistema informativo al servizio di tutta l’area penale. La finalità del progetto SIAP è quella di dar vita ad un “sistema cooperativo tra i vari processi di servizio inseriti nell’area penale”, cooperazione che si espliciterà nel veicolare le informazioni che, ottenute in *output* da un sistema, costituiscono l’*input* di altri sistemi informativi. Il progetto consentirà il trasferimento delle informazioni tra sistemi informatici eterogenei, cercando di mascherare all’utente finale, che pure ne manterrà il pieno controllo, il passaggio delle informazioni da e verso quegli uffici i quali, disponendo di altri sistemi informativi, manipolano informazioni riguardanti lo stesso incartamento.

Per il raggiungimento di tali risultati si sono utilizzate le architetture di cooperazione applicativa predisposte anche dal CNIPA per la R.U.P.A. ed alla base anche della *ratio* del SPC (8). Oltretutto, ed allo stato, all’interno di ogni ufficio è presente un’applicazione strutturata sulle specifiche esigenze dello stesso, con un’architettura, nel-

la maggior parte dei casi, di tipo *client/server*. Poiché tali applicazioni gestiscono i dati in un formato proprietario, non condivisibile con altre applicazioni, si è reso necessario realizzare interfacce duali di comunicazione tra coppie di applicazioni, anche se tale soluzione, sebbene efficace per la risoluzione di un problema specifico, è strettamente vincolata sia al formato dei dati utilizzati dalle applicazioni, che all’evoluzione di queste ultime.

Visti i progetti dell’Area Penale coinvolti, e, quindi, la quantità degli Uffici interessati ed il numero di applicazioni tra loro diverse, si è adottata la soluzione strutturale del *work flow management system* e cioè di un’architettura “scalabile” e capace di adattarsi nel tempo ai mutamenti tecnologici e legislativi.

Inoltre, attraverso lo studio di fattibilità del progetto in esame, si è principalmente tenuto conto del rapporto tra fase di cognizione e fase di esecuzione, determinando nuovamente i requisiti del sistema Re.Ge. ed avviando l’interazione con il sistema informativo della Corte di Cassazione, garantendo così la totale circolarità dei dati fino all’irrevocabilità della sentenza, presupposto necessario per l’avvio della fase di esecuzione. Contemporaneamente, dallo studio è derivata anche una rideterminazione delle specifiche necessarie alla completa integrazione tra il sistema Re.Ge. e quello del casellario nonché con quello dell’Amministrazione Penitenziaria al fine di pervenire alla totale eliminazione dei trasferimenti di informazioni su supporto cartaceo.

In ultimo, l’analisi degli aspetti informativi e informatici connessi allo svolgimento dei processi, e delle procedure di natura amministrativa di supporto alla fase dell’esecuzione penale, ha permesso di individuare l’organo di naturale focalizzazione di tutte le problematiche giurisdizionali ed informative, relative alle fasi di cognizione ed esecuzione, nella Procura Generale. Il livello distrettuale rappresenterà, quindi, il momento principale di cooperazione tra i sistemi degli Uffici giudiziari coinvolti nella fase dell’esecuzione e costituirà l’interfaccia per lo scambio dei dati verso i sistemi nazionali, con particolare riferimento al Casellario Giudiziario ed al *datawarehouse* con finalità statistiche.

Il progetto “*Polis penale*” (9) è, invece, un progetto fina-

Note:

(7) Sul rapporto fra tecnologia e diritto anche con riguardo alle fonti del diritto vedi dapprima V. Frosini, *Il giurista e le tecnologie dell’informazione*, Roma, 1998, 75 ss.; per le implicazioni internazionalistiche K. Intven, L. Zomar, J. Howard, *Internet telephony. Ther regulatory issues*, in *Comm/Ent. Hastings Communications*, 1999, 12 ss.; vedi inoltre G. Alpa, *Premessa*, in *I problemi giuridici di Internet*, a cura di E. Tosi, Milano, 1999, I ed., 12 ss.

(8) Sul punto ci si permette di rinviare a A. Contaldo, *La rete unitaria per la Pubblica Amministrazione e per gli enti pubblici territoriali*, in A. Contaldo, F. Dainotti, *Diritto e tecnologie delle reti di informazione*, Napoli, 2005, 169 ss.

(9) Sul Punto vedi A. Contaldo, M. Gorga, *E-Law*, cit., 132 ss., laddove si evince come l’applicativo “*Polis penale*”, in quanto sistema informatico di supporto alla gestione del processo, è costituito, dal punto di vista delle proprie componenti strutturali, da più sottosistemi i quali assistono

(segue)

lizzato alla realizzazione di una banca dati della giurisprudenza dei giudici di merito in materia penale e, principalmente, al supporto dell'attività di stesura, classificazione, archiviazione, ricerca delle sentenze anche in maniera innovativa.

2. Le regole tecniche del nuovo sistema del casellario giudiziario telematico

Il nuovo sistema del casellario giudiziario telematico così come ridisegnato in forza delle disposizioni di legge vigenti in materia, soltanto con il decreto del Ministero Giustizia del 25 gennaio 2007 (pubblicato in G.U. il giorno 08 febbraio 2007) ha visto l'emanazione delle nuove regole tecniche per il suo funzionamento. Occorre, però, subito precisare che le funzioni del nuovo sistema, la cui gestione è demandata all'ufficio centrale, sono definite come di «supporto alla base di tutte le procedure per le attività degli e tra gli uffici coinvolti concernenti l'iscrizione, l'eliminazione, lo scambio, la trasmissione, la conservazione dei dati e i servizi certificativi, anche nei rapporti con l'utenza che si uniforma ai principi indicati all'art. 41 del T.U.». In forza di predetta disposizione è stato conseguentemente previsto che il sistema deve raccogliere e conservare in una banca dati centralizzata sia l'insieme dei dati del casellario giudiziale e del casellario dei carichi pendenti, con la previsione che debbono essere trattati separatamente i dati relativi ai minorenni, sia l'insieme dei dati relativi all'anagrafe delle sanzioni amministrative dipendenti da reato, che l'anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato.

È stato, poi, previsto che detti dati, raccolti e memorizzati nella banca dati centralizzata siano protetti mediante l'utilizzo di tecniche di cifratura. Il sistema è stato poi abilitato a conservare, ai soli fini statistici ed in modo anonimo, i dati eliminati, per le attività di supporto che siano demandate all'ufficio centrale. Il nuovo sistema, quindi del casellario giudiziario telematico nella sua architettura e struttura logistica funzionale è stato articolato su due siti: a) il c.d. polo primario con sede in Roma; b) il c.d. polo secondario con sede in Napoli. I due poli, su cui sono installate tutte le funzioni e le strutture delle banche dati del sistema, sono speculari a livello di struttura e sono allineati in modalità asincrona, tramite un si-

Nota:

(segue nota 9)

gli utenti nelle seguenti attività: produzioni dei documenti giudiziari ("sottosistema di produzione"); attività di classificazione delle sentenze e caratterizzazione delle stesse per le successive ricerche ("sottosistema di classificazione"); gestione degli adempimenti relativi alla pubblicazione della sentenza quali quelli di cancelleria, elaborazione e stampa dei registri obbligatori e produzione di lettere di avviso delle parti ("sottosistema di pubblicazione"); ricerca e consultazione della pubblicazione giuridica ("sottosistema di consultazione"); gestione delle funzioni di ausilio tecnico ("sottosistema di amministrazione"); produzione di elaborati statistici ("sottosistema di statistica"). Inoltre, gli utenti del sistema possono usufruire dell'assistenza di un modulo logico dedicato alla sicurezza e trasversale rispetto dei vari sottosistemi, di modo che sia assicurata la riservatezza,

l'autenticità e l'integrità dei dati. Il Piano triennale 1999-2001 di informatizzazione della Giustizia individuava già quale soluzione ottimale quella di realizzare un prodotto su tre livelli: applicazione, protocollo e database.

Il livello applicativo è individuato nella realizzazione propria dell'applicativo "Polis penale"; il livello di protocollo di comunicazione è costituito dall'interfaccia, che rende indipendente il prodotto dal Data Base Management System, mentre il livello database si identifica nella realizzazione della base di dati e nella scelta del DBMS.

Dal punto di vista della struttura di dati servente, è possibile classificare i flussi di informazioni in due gruppi di dati e, cioè, quelli prodotti dallo stesso sistema Polis e quelli acquisitivi del sistema di Gestione dei Registri Penali (Re. Ge.). Il database "Polis Penale" sarà collegato con la base di dati Re.Ge. al fine di avere disponibili anche le sue informazioni, senza la necessità di replicare i dati contenutivi.

Sulla base del Sistema Informativo per la Direzione Nazionale Antimafia (SIDNA) e del Sistema Informativo Distrettuale Antimafia (SIDDA), il progetto risponde all'esigenza di costruire una banca dati in cui far confluire le informazioni concernenti i processi di criminalità organizzata, attraverso la realizzazione di un'infrastruttura telematica di collegamento tra gli uffici centrali della DNA e quelli territoriali della DDA e l'implementazione di strumenti che consentano sia il trattamento di atti di indagine, nel loro formato originario, sia l'archiviazione delle singole informazioni in essi contenute, definendo delle relazioni che ne consentano una ricerca tempestiva. Le funzioni di coordinamento, di analisi e di studio assegnate alla DNA fanno sì che tale organismo debba svolgere azioni sia di tipo tattico che di tipo strategico. Le azioni tattiche sono svolte dal DNA quando essa, dal confronto dei dati pervenuti dalle diverse Procure Distrettuali, che svolgono indagini contro gli stessi individui, ne informa i vari magistrati inquirenti favorendone lo scambio di dati; svolge, invece, azioni strategiche quando, raccolte e aggregate un insieme di informazioni elementari, di cui ritiene fondamentale la conseguenza, ne ricava "situazioni, tendenze e valutazioni che potranno servire ad orientare, nel medio o nel lungo periodo, le modalità operative della criminalità organizzata", le cui linee d'azione consentono la strutturazione del database tattico e di quello strategico.

Nel suo insieme il sistema informativo DNA-DDA si prefigge una pluralità di obiettivi: ex multis, facilitare la composizione e la catalogazione degli atti e dei documenti; consentire lo scambio di informazioni con l'esterno; creare un patrimonio storico di conoscenza indipendente dalla memoria del singolo giudice e disponibile dalla pluralità degli inquirenti interessati all'analisi ed alla valutazione dei fenomeni criminali; integrare i dati gestiti dai diversi sistemi informatici, che automatizzano le diverse fasi delle attività penali (registri, archivi documentali, automazione d'ufficio), e uniformare sul territorio gli strumenti e le metodologie di lavoro usate.

Nell'Area di intervento Giustizia Penale si colloca il progetto "Sistemi di archiviazione documentale", il quale si prefigge lo scopo di dar seguito ad una diffusione capillare di sistemi per la gestione elettronica dei documenti nell'ambito dell'amministrazione della giustizia. Inoltre nel D.P.R. 28 dicembre 2000 n. 445(10), per quanto riguarda l'archiviazione documentale, si richiede alle singole P.A. di formulare un piano per il recupero del supporto informatico, archivi attualmente in formato cartaceo.

Gli obiettivi perseguiti dal progetto in esame sono legati, da un lato, alla realizzazione di un adeguato supporto tecnologico e, dall'altro, al fattore organizzativo: specificatamente attraverso l'attuazione del progetto "Sistemi di archiviazione documentale" si dovrà giungere: a) alla razionalizzazione e semplificazione di tutte le operazioni connesse alla classificazione ed all'archiviazione dei fascicoli processuali; b) all'ottimizzazione della gestione, della ricerca e della diffusione delle informazioni contenute nei fascicoli processuali, con l'intento di renderle fruibili a tutti gli interessati utilizzando anche infrastrutture di rete geografica; c) maggior controllo della consistenza degli archivi al fine di una tempestiva attivazione delle procedure di scarto, una volta trascorsi i tempi previsti dalla legge per la conservazione degli atti; d) all'introduzione di una struttura informatica e di nuove modalità di gestione degli atti che favoriscano la revisione dei processi di trattamento dei documenti che compongono il fascicolo processuale; e) alla possibilità di incrementare il patrimonio informativo degli addetti del settore, realizzando integrazioni e automatismi di ricerca tra le informazioni gestite dagli applicativi, dedicati al dibattito; f) alla possibilità di incrementare i documenti in formato elettronico compresi nei fascicoli.

stema di replica che è stato progettato per assicurare la protezione dei dati e l'indipendenza dei due poli. Questa scelta strutturale consente sia il bilanciamento del carico di lavoro tra i due poli stessi, attraverso una soluzione che prevede la suddivisione degli accessi sul sistema in funzione del tipo di utente che si connette, sia la continuità dei servizi erogati dal sistema, in relazione ai diversi scenari di indisponibilità eventuale di uno dei due poli del sistema. Questa caratteristica non è tuttavia la sola del nuovo sistema del casella giudiziario telematico in quanto già dai primi articoli, e segnatamente dall'art. 2, viene in rilievo un'altra fondamentale distinzione introdotta, sicuramente caratterizzante rispetto al sistema precedente, laddove nel nuovo sistema, viene fatta la fondamentale distinzione tra «casellario giudiziale» definito come l'insieme dei dati relativi a provvedimenti giudiziari e amministrativi riferiti a soggetti determinati, e «casellario dei carichi pendenti» inteso come l'insieme dei dati relativi a provvedimenti giudiziari riferiti a soggetti determinati che hanno la qualità di imputato. Pur mantenendosi, quindi, il *nomen juris* di «casellario» la funzione essenziali dei due tipi di registrazioni, la prima a certificazione delle condanne subite dal soggetto, definibile, quindi come pregiudicato, la seconda, per i soggetti che, invece, tale qualità non rivestono per essere semplicemente «imputati» diviene rilevante sotto il profilo dell'immediata percettibilità della sfera delle attività del soggetto sottoposto ad indagine con la conseguente possibilità, per l'amministrazione della giustizia, che è sempre tenuta ad uniformare la propria attività al principio costituzionale del buon andamento, di essere in grado di attuare tutte quelle misure necessarie in ordine ad ogni attività, amministrativa, di esecuzione, penitenziaria ecc., di sua competenza nell'ambito dell'amministrazione della giustizia. L'immediata è totale certificazione che la nuova impostazione del casellario giudiziario telematico offre, è quindi anche la possibilità dell'immediata percezione dei dati sensibili, trova ulteriore sviluppo, poi, nella previsione di una nuova ed ulteriore sorta di registrazione definita nel decreto «anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato». Quest'ultimi sono stati concepiti come l'insieme dei dati relativi a provvedimenti giudiziari riferiti agli enti con personalità giuridica e alle società ed associazioni anche prive di personalità giuridica, cui è stato contestato l'illecito amministrativo dipendente da reato. Proseguendo nell'analisi del provvedimento è da osservare che lo stesso definisce il «sistema» come l'insieme informativo automatizzato del casellario giudiziale, del casellario dei carichi pendenti, dell'anagrafe delle sanzioni amministrative dipendenti da reato, dell'anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato. Nel decreto è poi definito il «codice identificativo» che è il codice fiscale del soggetto che deve essere registrato in una delle voci del casellario giudiziario telematico. Nel decreto è poi confermata la natura della Rete Unitaria della Giustizia (RUG) quale infrastruttura

telematica che interconnette tra loro i sistemi informatici interni al Dominio Giustizia e dove si intende per sistema forte i sistemi informatici interni al Dominio Giustizia da cui sono generati i dati per l'iscrizione, l'aggiornamento e l'eliminazione dei provvedimenti nelle stesse banche dati centralizzate. È proprio nell'ambito delle banche dati che si innesta, poi, la previsione dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento della «Centrale di Allarme Interbancaria» (archivio CAI) quale segmento ASP «Archivio Sanzioni Penali», istituito presso la Banca d'Italia. In merito è previsto all'art 17 del d.M.G. un collegamento telematico proprio tra il sistema del casellario e la Banca d'Italia per la trasmissione di tutti i dati in possesso del Ministro della giustizia all'ufficio centrale all'archivio CAI - segmento ASP - della Banca d'Italia. Identicamente è previsto che anche i dati relativi alla pena accessoria del divieto di emettere assegni bancari e postali, e quelli relativi alla durata e alla data di scadenza della stessa, debbono essere iscritti nel sistema. Ancora è previsto che lo stesso sistema provveda, sulla base di una procedura automatizzata, alla trasmissione all'archivio CAI anche delle sanzioni amministrative pecuniarie e accessorie, applicate a norma dell'art. 24 della legge 24 novembre 1981, n. 689. Com'è facile intuire il nuovo sistema del casellario giudiziario telematico offre quindi una copertura totale in ordine all'immediata identificazione del soggetto iscritto che è quindi, nel nuovo sistema telematico, non solo più iscritto in relazione alle condanne riportate, ma anche in ordine al carico pendente quale indiziato di reato ed ancora in ordine al carico pendente degli illeciti amministrativi dipendenti da reato, delle sanzioni amministrative pecuniarie e accessorie ai sensi della legge 24 novembre 1981, n. 689. Inoltre, ed ancora, per tutto quanto attiene alle pene accessorie, alla situazione in ordine agli assegni bancari e postali e alle carte di pagamento, alla sua posizione presso la centrale allarme interbancaria nonché al tempo del divieto di emettere assegni bancari e postali. Una mappa, quindi, totale del soggetto sottoposto a procedimento sarà immediatamente disponibilità all'A.G.O., con possibilità, per la stessa A.G. di avere in tempo reale la situazione aggiornata, *on-line* del soggetto e quindi fino all'emissione del provvedimento giurisdizionale, sarà sempre possibile avere la mappa aggiornata al momento della posizione del soggetto e del suo debito rispetto alla pretesa punitiva esercitata dallo Stato.

3. Le politiche di sicurezza del casellario giudiziario telematico

Ai sensi dell'art. 4 del d.M.G. sul sistema sono implementate le politiche di sicurezza volte a salvaguardare la riservatezza delle informazioni allo scopo di ridurre al minimo il rischio di accessi, volontari o involontari, non autorizzati. Inoltre sono adottate misure per preservare l'integrità delle informazioni e il rischio di cancellazioni o modifiche a seguito di interventi di soggetti non auto-

rizzati o del verificarsi di fenomeni non controllabili (quali il deteriorarsi dei supporti di memorizzazione, il degrado dei dati trasmessi su canali rumorosi, i guasti degli apparati, i problemi ai sistemi di distribuzione dell'energia, gli incendi, gli allagamenti, etc.). Sono state, poi, previste adeguate procedure di recupero delle informazioni (piani di *back-up*, etc.) per salvaguardare l'esattezza, l'accessibilità e la disponibilità delle informazioni e delle risorse del sistema e a tal fine l'ufficio centrale adotta un documento programmatico per la sicurezza in conformità con le indicazioni contenute nel decreto legislativo 30 giugno 2003, n. 196. In detto documento è previsto che sia specificata la politica di sicurezza proposta e che in ogni caso l'ufficio centrale adotti idonee politiche e procedure per il salvataggio (*back-up*) dei dati, che deve avvenire con frequenza almeno settimanale, nonché un piano di *disaster recovery* in cui siano analizzate le situazioni di emergenza ovvero gli scenari di indisponibilità del sistema ed il relativo impatto sui servizi erogati (10). Ai sensi del successivo art. 5, presso l'Ufficio centrale è attivato l'ufficio del responsabile che è il punto unico di interazione a livello nazionale tra il sistema ed i soggetti abilitati il quale provvede, in conformità alle disposizioni impartite dal dirigente dell'ufficio centrale, sulle richieste di attivazione, modifica e revoca dell'accesso al sistema, nel rispetto dei profili di utenza predeterminati dall'amministrazione nella fase di definizione delle politiche di sicurezza. Per la trasmissione telematica dei dati e di qualsiasi altro messaggio è utilizzata l'infrastruttura tecnologica messa a disposizione dalla RUG. Per la comunicazione con enti esterni al "Dominio Giustizia" è utilizzata l'infrastruttura tecnologica resa disponibile dalla Direzione generale per i Sistemi informativi automatizzati del Ministero della giustizia. Ai sensi dell'art. 6, poi, l'accesso al sistema degli utenti, nei limiti delle competenze e delle responsabilità assegnate dal T.U. e nel rispetto delle norme di sicurezza e di protezione dei dati personali, è subordinato all'espletamento di una procedura atta a consentirne l'identificazione e la registrazione da parte del sistema. Gli uffici locali, gli uffici iscrizione, gli uffici che esercitano la giurisdizione penale e quelli del pubblico ministero ai fini dell'acquisizione diretta dei certificati di cui agli artt. 21 e 30 del T.U., comunicano preliminarmente all'ufficio centrale il nominativo di un referente (11), che assume la responsabilità della gestione degli accessi al sistema, con riferimento a tutte le utenze assegnate all'ufficio. Per quanto attiene all'accesso l'art. 7 prevede che l'ufficio centrale provvede senza ritardo in merito a ciascuna domanda di registrazione. In caso di accoglimento della domanda, per ciascuna delle utenze richieste all'interno della domanda e nel rispetto delle procedure di sicurezza in vigore, l'ufficio centrale ha cura di registrare i parametri identificativi e di definire i parametri di accesso, in termini di «Nome Utente» e «Parola Chiave», nonché di trasmettere al referente indicato sulla domanda, in busta chiusa sigillata, i parametri di accesso. Inoltre attiva l'utenza sul

sistema a seguito di conferma dell'avvenuta corretta ricezione della busta. In caso di rigetto della domanda, invece, l'ufficio centrale ne comunica le motivazioni al referente indicato sulla domanda stessa. La gestione delle utenze avviene poi tramite un registro delle utenze abilitate all'accesso al sistema, gestito dall'ufficio del responsabile centrale dell'accesso al sistema.

In particolare quest'ultimo registro contiene informazioni riguardo al nome e cognome, il luogo e la data di nascita, il codice fiscale. Le credenziali di autenticazione sono il nome utente, la parola chiave, protetta con tecniche di cifratura, e l'ufficio. Quest'ultimo si identifica in base alla tipologia e alla sede, nonché alla data ed all'ora di creazione dell'utenza ed alla data ed all'ora dell'ultima variazione. L'identificazione dei soggetti abilitati all'accesso al sistema è basata, infine, sull'abbinamento di credenziale di autenticazione - ufficio. Per quanto attiene alle modalità di accesso al sistema prevede l'art. 9 del decreto cit., che il sistema provvede all'autenticazione informatica dei soggetti abilitati ed attiva i corrispondenti livelli di visibilità e operatività sulla base dei profili di autorizzazione. Il sistema obbliga l'utente alla modifica della propria parola chiave in occasione del suo primo accesso. In fase di autenticazione, il sistema permette all'utente di effettuare tre tentativi di inserimento del nome utente e della parola chiave prevedendo che dopo il terzo tentativo di accesso fallito, il sistema disabilita l'utenza. In quest'ultima ipotesi l'utente contatta l'ufficio del responsabile centrale dell'accesso al sistema il quale provvede al controllo delle credenziali del richiedente ed eventualmente al ripristino, ricorrendone i presupposti, dell'utenza stessa. Invece l'utente che abbia dimenticato la propria parola chiave deve contattare l'ufficio del responsabile centrale dell'accesso al sistema il quale provvede al controllo delle credenziali e all'assegnazione di una nuova parola chiave che è modificata almeno ogni trenta giorni. Se l'utente non accede al servizio per un periodo superiore a tre mesi, il sistema disabilita l'utenza. In tal caso l'utente rinnova la richiesta di registrazione con le modalità di cui all'art. 6, comma 4 di cui abbiamo appena detto sopra. Le credenziali di autenticazione possono consistere anche in un dispositivo di autenticazione in possesso ed uso esclusivo dell'utente del sistema, eventualmente associato ad un codice identificativo o ad una parola chiave, oppure in una caratteristica biometrica dell'incaricato (12), eventualmente associata ad un codice identificativo o ad una parola chiave. L'utilizzo delle credenziali di autenticazioni di cui al

Note:

(11) Sul punto vedi G. Corasaniti, *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 221 ss.; ci si permette altresì di rinviare a A. Contaldo, *La sicurezza della rete: lineamenti giuridici su un'innovazione tecnologica al servizio della P.A.*, in *Riv. amm. Rep. it.*, 2003, 812 ss.

(12) La registrazione avviene in base ad un modulo che può essere richiesto all'ufficio centrale o acquisito per via telematica dal sistema o dal sito web del casellario. Il modulo di registrazione, compilato in tutte le sue parti e firmato dal referente è inoltrato all'ufficio centrale.

comma 7 è disciplinato, in conformità alla normativa vigente, con provvedimento del Direttore della Direzione generale della Giustizia penale, adottato d'intesa con il Direttore della Direzione generale dei Sistemi informativi automatizzati del Ministero della Giustizia. Il Controllo e la verifica degli accessi e delle operazioni svolte è disciplinato dall'art. 10 secondo il quale l'ufficio centrale, nel rispetto delle procedure di sicurezza in vigore, cura la registrazione dei dati necessari a garantire innanzitutto la tracciabilità dei collegamenti telematici attuati tra il sistema ed i sistemi informatici interessati, sia interni che esterni al dominio giustizia. Inoltre lo stesso cura l'identificazione di tutti gli utenti che interagiscono con il sistema, ivi compresi gli utenti tecnici, eventualmente appartenenti a ditte esterne incaricate della conduzione e/o manutenzione del sistema. Per le finalità di cui appena detto sono istituiti registri informatizzati volti a consentire agli uffici, attraverso l'utilizzo di appositi strumenti di controllo, il costante monitoraggio dei soggetti che compiono le attività di acquisizione dei dati, della data e della tipologia delle stesse (cd. registro delle attività) dei certificati e delle visure che consente agli uffici, attraverso l'utilizzo di appositi strumenti di controllo, il costante monitoraggio dei soggetti che compiono le attività di certificazione e visura dei dati.

L'integrità di detti registri è verificata dall'ufficio centrale con frequenza almeno mensile mentre per quanto attiene ai contenuti i registri sono conservati per un periodo di dieci anni.

Ai sensi dell'art. 11 gli utenti appartenenti agli uffici non giudiziari abilitati al rilascio di certificati, devono essere in possesso della firma digitale. I provvedimenti in materia di grazia sono iscritti nel sistema dall'ufficio centrale dove sono anche iscritti i provvedimenti amministrativi di espulsione e i provvedimenti giudiziari che decidono il ricorso avverso gli stessi. Nello stesso sistema sono iscritti per estratto anche le decisioni definitive adottate dalla Corte europea dei diritti dell'uomo nei confronti dello Stato italiano, concernenti i provvedimenti giudiziari ed amministrativi definitivi delle autorità nazionali già iscritti. Ai sensi dell'art. 14 del decreto in esame l'ufficio iscrive nel sistema i provvedimenti utilizzando tecnologie informatiche volte ad impedire l'inserimento di dati non pertinenti o errati (*warning*). Terminata l'iscrizione l'ufficio procede alla validazione dei dati relativi al provvedimento che ha iscritto per estratto nel sistema con conseguente non modificabilità dei dati iscritti che possono essere utilizzati ai fini certificativi. Il provvedimento iscritto risulta nella fase denominata «in lavorazione» finché non è completata la procedura di verifica e di validazione. In tale fase è visibile all'autorità giudiziaria, nonché agli uffici iscrizione, ai soli fini del completamento della iscrizione stessa. Una volta validati i dati gli stessi possono essere modificati solo a seguito di svalidazione da parte dell'ufficio iscrizione e solo se ne viene indicata la relativa motivazione. Il sistema autorizza la modifica del dato anagrafico da parte dell'ufficio

iscrizione o dell'ufficio locale solo se tra le iscrizioni presenti a carico del soggetto riscontra almeno un provvedimento iscritto dall'ufficio e comunque previa operazione di svalidazione. La modifica del dato anagrafico comporta la creazione di un nuovo soggetto e il trasferimento a suo carico dei provvedimenti svalidati o che risultino in lavorazione. Con l'operazione di validazione il sistema attiva la procedura denominata «determinazione delle date di menzionabilità» che applicando le norme stabilite nel T.U., determina, a livello di soggetto, di provvedimento, di reato e di pena accessoria il termine fino al quale il dato è riportato nelle diverse tipologie di certificati ovvero il giorno in cui verrà eliminato dal sistema. L'ufficio iscrizione se nel provvedimento riscontra dati mancanti o incompleti, lo segnala all'autorità competente alla correzione, e in particolare, al giudice penale ai sensi dell'art. 130 c.p.p., al giudice civile o amministrativo ai sensi dell'art. 288, secondo comma, del codice di procedura civile, all'autorità amministrativa che ha emesso il provvedimento. Per l'art. 15 l'ufficio iscrizione che procede all'iscrizione di un provvedimento giudiziario collegato ad altro provvedimento, ove riscontri la mancata iscrizione del provvedimento giudiziario da collegare, provvede: a) ad inserire un provvedimento denominato provvisorio; b) a sollecitare, senza ritardo, l'ufficio iscrizione competente; c) a validare il provvedimento di sua pertinenza una volta pervenuta la comunicazione dell'avvenuto inserimento del provvedimento mancante.

L'ufficio iscrizione competente provvede, senza ritardo e comunque entro e non oltre dieci giorni dal ricevimento del relativo sollecito, ad iscrivere il provvedimento mancante ovvero a comunicare per via telematica all'ufficio iscrizione che ha effettuato il sollecito i motivi del rifiuto dell'iscrizione, ed inoltre, giornalmente, attraverso apposita funzione resa disponibile dal sistema, l'esistenza di comunicazioni o solleciti ai fini degli adempimenti previsti. Provvede, inoltre, al costante monitoraggio del corretto svolgimento della procedura prevista. Ai sensi dell'art. 16 nel caso di correzione di errore materiale relativo a un provvedimento già iscritto l'ufficio presso l'autorità giudiziaria che ha emesso il provvedimento di correzione dell'errore materiale ne cura l'iscrizione nel sistema e ne trasmette l'estratto all'ufficio che ha iscritto il provvedimento oggetto della correzione, affinché proceda alla rettifica dei dati la cui rettifica è preceduta dalla svalidazione del provvedimento che è consentita solo a seguito dell'inserimento dei motivi per cui si svalida.

4. Il Regime transitorio previsto per l'attuazione del casellario giudiziario telematico

In via transitoria, ex art. 18, in attesa della realizzazione delle funzioni di interconnessione telematica con i sistemi fonte, i provvedimenti sono iscritti nel sistema dall'ufficio iscrizione competente, per via telematica,

mediante funzioni di immissione dei dati. Competente per l'iscrizione dei provvedimenti, esclusi quelli di competenza dell'ufficio centrale, è l'ufficio presso l'A.G.O. che ha emesso la sentenza divenuta irrevocabile, il decreto penale divenuto esecutivo, il provvedimento che sia eseguibile anche durante il termine per proporre impugnazione o l'ordinanza, divenuta irrevocabile, con la quale sia stato dichiarato inammissibile l'appello.

Gli uffici iscrizione presso le autorità giudiziarie militari e quelli del giudice di pace non connessi alla RUG trasmettano, senza ritardo, l'estratto del provvedimento da iscrivere all'ufficio locale nel cui ambito territoriale è nata la persona cui è riferita l'iscrizione. Gli uffici iscrizione presso i tribunali di sorveglianza trasmettano, senza ritardo, l'estratto del provvedimento da iscrivere all'ufficio locale nel cui ambito territoriale è nata la persona cui è riferita l'iscrizione. L'estratto del provvedimento da iscrivere è trasmesso all'ufficio locale presso il Tribunale di Roma, per le persone nate all'estero, o delle quali non è stato accertato il luogo di nascita nel territorio dello Stato. In attesa della realizzazione del nuovo sistema informativo della Corte di cassazione, e delle relative funzioni di interconnessione telematica con gli altri sistemi fonte e con il casellario, la competenza per l'iscrizione del provvedimento divenuto irrevocabile a seguito della pronuncia della Corte di cassazione è individuata secondo le modalità finora osservate. Sino alla completa operatività della trasmissione telematica delle informazioni i Comuni continuano a comunicare l'avvenuta morte delle persone all'ufficio locale, nel cui ambito territoriale le persone sono nate. Per le persone nate all'estero, o delle quali non si è potuto accertare il luogo di nascita nel territorio dello Stato, l'ufficio locale competente è quello presso il Tribunale di Roma. Pervenuta la comunicazione dell'avvenuta morte, l'ufficio locale competente inserisce nel sistema i dati relativi al decesso. Il dato anagrafico è eliminato definitivamente dal sistema decorsi cinque anni dalla data dell'avvenuto decesso o comunque al compimento dell'ottantesimo anno di età. In via transitoria i certificati in materia di casellario giudiziale e di anagrafe delle sanzioni amministrative dipendenti da reato sono rilasciati dai soli uffici locali, ai quali sono affidati in materia di casellario giudiziale il rilascio dei certificati richiesti dall'interessato e dal difensore, quali quelli per uso elettorale limitatamente agli uffici che esercitano la giurisdizione penale e di quelli del pubblico ministero non collegati alla RUG. In materia di anagrafe delle sanzioni amministrative dipendenti da reato spetta sempre all'ufficio locale il rilascio dei certificati richiesti dall'ente interessato e i certificati richiesti limitatamente agli uffici che esercitano la giurisdizione penale e di quelli del pubblico ministero non collegati alla RUG. La persona o l'ente interessato ha diritto, in questi casi, di ottenere i certificati senza motivare la richiesta. I certificati sono prodotti attraverso la stampa delle iscrizioni estratte di-

rettamente dal sistema al nome di un determinato soggetto o ente e sottoscritte dal responsabile del servizio designato in ciascun ufficio giudiziario dal dirigente. La richiesta è redatta in forma scritta e conservata agli atti dell'ufficio per anni cinque. L'identità dell'interessato è verificata mediante esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero una delega sottoscritta, e la presentata unitamente a copia fotostatica, non autenticata, di un documento di riconoscimento dell'interessato. Se l'interessato è un ente, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

Ai sensi dell'art. 30 la consultazione del sistema da parte delle amministrazioni pubbliche e dei gestori di pubblici servizi è effettuata, per via telematica a fronte di richieste specifiche e puntuali, mediante tempestiva attestazione o certificazione. Nel caso di cambiamento delle generalità di un collaboratore di giustizia, continuano ad essere applicate le modalità finora osservate che prevedono, a seguito di comunicazione del servizio centrale di protezione e con modalità idonee a garantire la segretezza delle informazioni, l'iscrizione nel sistema a cura dell'ufficio locale di Roma delle risultanze del casellario giudiziale, riferendole alle nuove generalità. Dalla data di efficacia del decreto in esame risulta, poi, essere espressamente abrogato il decreto dirigenziale 1° aprile 2003 pubblicato sul Bollettino ufficiale del Ministero della giustizia n. 8 del 30 aprile 2003.

5. Conclusioni

L'innovazione tecnologica del Casellario giudiziario telematico comporta, come abbiamo visto, tutta una serie di chiarimenti, particolarmente sotto il profilo della sua coincidenza o meno con la sfera della cd. libertà informatica (13): ciò comportando inevitabilmente l'affrontare un'altra delle questioni da tempo oggetto di discussione, concernente la configurabilità di un diritto alla *privacy* nella comunicazione e quindi anche grazie alla sicurezza degli impianti e delle reti attraverso cui tale informazione transita (14). Discorso, questo, rispetto al quale si evidenziano poi posizioni opposte in merito alla domanda sul se l'attività di informazione e di comunicazione con i nuovi media possa o meno essere inquadrata

Note:

(13) Ci si permette di rinviare ancora a A. Contaldo, *Biometrie e documenti di viaggio: problematiche giuridiche*, in *Amm.it.*, 2007, n. 2, 212 ss.

(14) Per una prima disamina della problematica sulla cd. libertà informatica vedi S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, spec. 32 ss.; V. Frosini, *La libertà informatica: l'Europa senza l'Italia*, in *Infom. Dir.*, 1986, n. 2, 12 ss.; Idem, *Informatica, diritto e società*, Milano, 1992, 19 ss.; L. Serrotti, *Libertà di informazione e libertà informatica: La tutela della riservatezza*, in *Infom. Dir.*, 1996, 12 ss.; E. Giannantonio, *Manuale di diritto dell'informatica*, Padova, II ed., 1998, 32 ss.; A. Bevere, A. Cerri, *Il diritto di informazione e i diritti della persona*, in *Teoria prat. dir.*, 1998, 42 ss.

nella tutela costituzionale dell'art. 15 Cost., oltreché beninteso in quella ex art. 97 Cost.

È sembrato che l'inquadramento costituzionale della materia si articoli anche sul caposaldo dell'art. 15, anche se non dobbiamo trascurare ambiti di tutela altresì dell'art. 21 Cost. (15). Il primo, riferito a quella che potremmo definire la comunicazione interpersonale, in analogia alla tradizionale libertà di corrispondenza privata (*e-mail*); il secondo, riferibile, invece, alla manifestazione del pensiero con destinatario indeterminato (notizie *open source*). Tutto ciò tenuto, peraltro, conto del fatto che, nella dimensione dell'interattività, la distinzione appena delineata tende sempre più a scomparire, al punto che uno stesso tipo di comunicazione presenta talvolta i caratteri di entrambe le libertà.

Tanto premesso, e tralasciando di affrontare il problema dell'esatta individuazione caso per caso della linea di confine tra la libertà informatica ed i due diritti, conviene innanzitutto osservare che, relativamente alla comunicazione interpersonale, lo sviluppo di Internet, pur avendo moltiplicato le potenzialità esplicative della relativa libertà, sembra implicare un indebolimento sotto il profilo della segretezza da garantire al contenuto della stessa. Indebolimento assunto a conferma dell'idea secondo la quale l'accento andrebbe posto sulla volontà del soggetto comunicante in quanto "non è la comunicazione che diviene riservata solo laddove vi sia segretezza in senso tecnico, bensì è piuttosto la pretesa di segretezza che diviene possibile solo in presenza di una comunicazione riservata, ossia rivolta ad una cerchia delimitata di destinatari infungibili" (16).

Bisogna evidenziare che con le comunicazioni elettroniche e telematiche trova una chiara esplicitazione quel fenomeno di convergenza multimediale del quale si sono poste in luce le conseguenze sotto il profilo delle interferenze tra il progresso raggiunto nel settore delle comunicazioni a distanza e la dimensione delle situazioni giuridiche soggettive costituzionalmente rilevanti.

Tuttavia, un approccio che si limitasse agli aspetti di diritto interno sarebbe certamente insufficiente a cogliere la complessità dell'ambito delle esigenze amministrative della giustizia, che, per sua natura, comporta il superamento dei confini nazionali e dai continenti fisici (*cyberspazio*) (17).

E che vi sia un rapporto di stretta continuità e derivazione tra i due aspetti viene confermato proprio dall'Unione europea in diversi atti ufficiali, nei quali è stato sottolineato come i servizi di interesse generale si pongono "al centro del modello europeo di società", in quanto sono riferiti ad un insieme di valori comuni a tutti i nostri Stati e che fanno l'originalità dell'Europa. Inoltre la disciplina della sicurezza delle reti, come si è visto, ha avuto negli anni una disciplina episodica ed incerta, e non solo in Italia. Ancora oggi non è possibi-

le concludere che il quadro normativo sia completo. Il sempre vivo dibattito imprenditoriale, politico e giuridico sulla disciplina in vigore, poi, dimostra con forza che le disposizioni in esame certo non rispondono in modo perfetto non solo alle esigenze normative degli Stati. Le normative più recenti la prendono in considerazione, anche se ricordano che il Legislatore dovrà "rifare a breve i conti" anche con le rapidissime mutazioni tecnologiche in atto.

Note:

(15) Ci si permette di rinviare a A. Contaldo, *Trasmissione del documento informatico nella P.A. contenente dati personali anche alla luce delle problematiche della sicurezza delle reti e dei risvolti connessi alle intercettazioni nelle comunicazioni*, in *Giur. merito*, 2003, 756 ss.

(16) Vedi A. Valastro, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale*, Milano, 2001, 123 ss.; vedi altresì P. Costanza, *Profili costituzionali delle telecomunicazioni*, in *La disciplina giuridica delle telecomunicazioni*, a cura di G. Bonelli, S. Cassese, Milano, 1999, 8 ss.; R. Perez, *Telecomunicazioni e concorrenza*, Milano, 2002, 112 ss.

(17) Vedi A. Valastro, *op. supra cit.*, 172.

(18) Vedi al riguardo le analisi di T. Ballarino, *Internet nel mondo della legge*, Padova, 1999, 121 ss.

Sicurezza informatica

Phishing: strategie operative dell'inganno

di Monia Fantini

Il phishing è una forma di inganno ormai divenuta quotidiana. Nella sua forma più comune, si avvale di messaggi fraudolenti che, sfruttando tecniche di ingegneria sociale, mirano a catturare l'attenzione del destinatario inducendolo a dire sì alle richieste in esso contenute. Il fenomeno è oggi uno degli argomenti più discussi nel campo della sicurezza informatica. Capire perché ancora oggi il phishing rappresenti una seria minaccia, significa soprattutto capire cosa effettivamente spinge l'utente a dar seguito a queste e-mail spesso a dir poco strane, ovvero perché le ritiene credibili.

1. Il Phishing in sintesi

Seppur la storia dei furti d'identità possa considerarsi vecchia come il mondo, negli ultimi anni, tali furti hanno sicuramente trovato un nuovo alleato in *internet*, dove si stanno trasformando, in una nuova, lucrosa industria del crimine a rischi relativamente bassi e guadagni decisamente interessanti (1).

Il termine "*phishing*", che deriva dall'unione dei termini inglesi "*phreaking*" (tecnica usata negli anni '70 per effettuare telefonate senza pagare) e "*ishing*" (pescare), sta ad indicare una forma di furto di identità, nata ufficialmente a metà degli anni '90, che mira ad ottenere dati personali e credenziali di *account* finanziari, allo scopo di frodare gli utenti coinvolti.

Dalle sue origini ad oggi, il *modus operandi* ha subito un'evoluzione ed un affinamento sempre maggiori. Oggi è possibile carpire i dati personali dell'utente in vari modi (2), ma nella sua forma più comune, il *phishing* si avvale di un messaggio *e-mail* dall'aspetto ufficiale, in apparenza proveniente da un istituto di credito o una società che fornisce servizi a mezzo *internet* (3). Nel testo del capzioso messaggio, i truffatori generalmente rappresentano talune improcrastinabili esigenze di sicurezza che si traducono nell'invito perentorio a recarsi presso il sito indicato nel *link* al fine di inserire e/o modificare i codici d'accesso personali relativi ai propri conti *on-line*. Non appena viene visualizzato il sito relativo a questo *link*, nel *computer* dell'utente viene visualizzata una pagina *web* in tutto e per tutto identica a quella del proprio istituto di credito. L'incauto correntista che abbocca all'esca, inserisce i codici relativi al proprio *account on line*, i *phishers* sono in grado di recuperare queste informazioni e derubando così l'"identità digitale" bancaria dell'utente ne alleggeriscono consistentemente i conti.

2. Quadro normativo interessato

Nell'ordinamento italiano non esiste una norma incriminatrice specifica per il *phishing*. Sussistono, tuttavia,

diverse norme (4) nel cui alveo sembrano potersi ricondurre, ad una prima ricognizione, le condotte finora illustrate, così come del resto è stato messo in evidenza da molteplici commentatori (5).

Innanzitutto, scrivere una *e-mail* dal contenuto mendace, per trarre in inganno il destinatario, è una "Falsificazione di comunicazione telematica" (art 617 *sexies* c.p.). L'*e-mail* fraudolenta contiene un collegamento ipertestuale ingannatorio (artifici o raggiri) che rimanda verso un sito clone dell'originario (induzione in errore) e nel quale vengono sottratti i codici d'accesso della vittima utilizzati successivamente per sottrarre il denaro (ingiusto profitto ed altrui danno). Cosicché, con quest'ultima azione si perfeziona il reato di "Truffa" (art. 640 c.p.). A volte nell'*e-mail* è presente anche il consiglio di recarsi nel sito del proprio istituto di credito, prospettando rischi di truffe o altri accessi ai dati personali non consentiti (ingenerando nella persona offesa il timore di un pericolo immaginario). In quest'ultimo caso, ci sono gli estremi che integrano l'ipotesi di un'aggravante.

Successivamente alla raccolta dei dati personali della vittima, il *phisher* pone in essere un trattamento di tali dati in violazione del disposto dell'art. 11 decreto legislativo 30 giugno 2003, n. 196 ed in seguito con la condot-

Note:

(1) Per lo stato dell'arte nel nostro Paese v. G. Costabile e F. Cajani "Phishing e cybericiclaggio: lo "stato dell'arte" nel panorama italiano" in *Consumatori, Diritti e Mercato*, 3, 2006 - Argomenti, 67.

(2) Per i dati complessivi sul fenomeno si rimanda al sito dell'Anti-Phishing Working Group, all'URL: <http://www.antiphishing.org>

(3) Si veda, per esempio, Paypal o Ebay.

(4) F. Cajani, "Profili penali del Phishing" *Cass. pen.*, Vol. 47, n. 6, 2007, 2294-2306.

(5) S. Fratellone, "Phishing, fenomenologia e profili penali: dalla nuova frode telematica al cyber-riciclaggio" all'URL: http://www.globaltrust.it/documents/press/phishing/EnTrustAvv_FrattallonePhishing08Set05.pdf, marzo 2008; L. Bovino, all'URL: "Phishing: aspetti legali" all'URL: <http://www.anti-phishing.it/phishing/phishing.aspetti.legali.php>, marzo 2008

ta di trarne profitto, nel momento in cui il denaro viene sottratto, il *phisher* realizza un ulteriore illecito penale: "Trattamento illecito di dati" (art. 167 d.lgs. n. 196/2003).

L'accesso all'*account* della vittima senza aver nessun titolo ed eludendo le misure di autenticazione e identificazione predisposte per garantire la tutela dei dati in esso contenuti, si caratterizza come "Accesso abusivo in un sistema informatico o telematico" (art. 615 *ter* c.p.).

Il *phisher* carpendo i dati d'accesso della vittima, li utilizza nei rispettivi *account* intervenendo nei sistemi informatici, ad esempio dell'istituto di credito, senza aver alcun titolo (senza diritto, con qualsiasi modalità). In questa fattispecie, il reato di "Frode informatica" (art. 640 *ter* c.p.) è commesso contro l'istituto di credito colpendo il suo sistema informatico.

Infine, le somme illecitamente trafugate tramite il *phishing* vengono fatte circolare attraverso molteplici conti correnti ed i titolari dei conti vengono in questo modo coinvolti in un'attività illecita di "Riciclaggio" (art. 648 bis c.p.).

3. L'importanza del fattore umano

Il fenomeno, che allo stesso tempo, sorprende e preoccupa per la sua stessa semplicità, rappresenta oggi uno degli argomenti più discussi nel campo della sicurezza informatica.

Rispetto all'analisi delle varie modalità tecniche di cui questo crimine si avvale, quella degli elementi relazionali costitutivi viene spesso posta in secondo piano. Ciascun elemento gioca sempre un ruolo nel tenere unito un sistema.

Gli elementi fondanti in questo caso sono: da una parte gli utenti che abboccano all'esca, dall'altra l'astuto truffatore.

a) L'anello debole della sicurezza

La sicurezza non è mai stata solo un problema di tecnologia. A capo dei sistemi, *software* e programmi vari c'è sempre la figura umana, che con tutte le sue sfaccettature e vulnerabilità rappresenta il vero anello debole della catena.

Poiché non è solo qualcosa di reale, ma anche una sensazione "... un modo di sentire, un *feeling*, che non si basa sulla probabilità e sui calcoli matematici ma sulle nostre reazioni psicologiche ai rischi ed alle misure di protezione" (6) troppo spesso capita di non fare una valutazione corretta della gravità di un pericolo.

Parte di ciò può essere addebitata al fatto che le persone generalmente: hanno la convinzione della propria non vulnerabilità (sindrome del "a me non può accadere"), tendono implicitamente a dare fiducia agli altri per una loro propensione ed in base ad esperienze precedenti, hanno una naturale attitudine ad aiutare chi chiede loro di farlo, tendono a sottostimare il pieno valore delle loro informazioni personali non prendendo in considerazione le conseguenze delle loro azioni.

La mancanza di indizi reali che abbiamo imparato ad utilizzare nel mondo fisico per capire frodi ed inganni, fa sì che i nostri giudizi di credibilità nei confronti di questo tipo di trappole *on-line*, siano facilmente esposti ad errori.

Il *phishing* rappresenta il tipico "errore di credulità": l'errore che interviene quando si mostra una fiducia incondizionata verso una fonte che si giudica credibile anche quando non lo è.

Se è vero però che le fonti più sono "credibili" più hanno la capacità di persuadere (Howland e Weiss, 1951) è altrettanto vero che, oltre alle caratteristiche intrinseche e connaturate della fonte comunicativa, importanti sono anche: "gli occhi di chi guarda". Siamo tutti potenziali vittime del *phishing*.

Un famoso psicologo legale, il Professor Clive Hollin dell'Università di Leicester afferma: "Date le giuste condizioni in termini di capacità di persuasione della comunicazione e la combinazione critica di fattori personali e circostanziali, la maggior parte delle persone potrebbe essere vulnerabile a informazioni fallaci. Ciò è vero sia per gli utenti di computer esperti che inesperti: mentre l'ingenuità potrebbe essere una spiegazione parziale, anche gli utenti più sofisticati possono essere tratti in inganno e diventare suggestionabili da messaggi illusori." (7)

Questo perché, come Robert Cialdini (8) sostiene, "seppur a differenza di qualunque specie animale, l'uomo ha una capacità di elaborazione dell'informazione superiore, talvolta sembra rinunciare ad un più elaborato e lungo processo decisionale per sostituirlo con una più automatica e primitiva risposta basata su un solo elemento o su dati comunque parziali. Automatismi tanto più probabili quanto più siamo in condizioni di fretta, stress, incertezza, indifferenza, distrazione o affaticamento".

La vera fortuna dei *phishers*, è proprio la capacità, tramite tecniche comunemente conosciute come di "ingegneria sociale", di oltrepassare le barriere mentali dell'utente facendo leva su questa tendenza a ricorrere a "scorciatoie mentali", schemi automatici d'azione, sfruttati singolarmente o in combinazione tra loro per farci acconsentire alle loro richieste.

b) L'arte dell'attaccante: l'ingegneria sociale

Un mestiere quello della persona astuta sicuramente antico nella sostanza.

Note:

(6) Cit. in B. Schneider, "Psicologia della sicurezza" (traduzione di Agatino Grillo) all'URL: <http://www.agatinogrillo.it>, 2007

(7) v. art. "Una nuova ricerca rivela i giochi psicologici utilizzati dai truffatori cibernetici per sfruttare la natura umana al fine di ottenere soldi e informazioni personali" consultabile all'URL: http://www.idome.com/flash-news/pagina.phtml?_id_articolo=11664-Mcafee-svela-la-guerra-psicologica-dei-cybercriminali.html

(8) R. Cialdini., *Le Armi Della Persuasione. Come e perché si finisce col dire di sì*, Firenze, 1995 (ed. Orig: Influence. The Psychology Of Persuasion)

La possibilità dell'inganno è infatti insita nella natura umana.

Ottenere quello che si vuole dagli altri, può essere perseguito in due modi: mediante la persuasione, oppure mediante una manipolazione prevaricatrice (9).

La Persuasione sfrutta le leve intrinseche al soggetto e la sua stessa volontà per realizzare un obiettivo in qualche modo comune, o quantomeno il soggetto lo percepisce e lo accetta come proprio, ed in tal senso può essere definita etica.

La Manipolazione invece non rispettando la comune etica (la volontà del soggetto viene posta in secondo piano) non esita a ricorrere ad una serie di metodi e tecniche in grado di influenzare il modo in cui una persona pensa, sente ed agisce.

La chiave del successo risiede quindi nella sua sottigliezza, astuzia, nel modo in cui promuove la "illusione di controllo".

Si tratta quindi di inganno, plagio, per questo la parola viene utilizzata per lo più in senso dispregiativo: chi manipola lo fa generalmente per strumentalizzare qualcuno ai propri fini.

Il termine "Social Engineering", in italiano "Ingegneria Sociale", sta appunto ad indicare la pratica dell'ottenere con l'inganno, informazioni riservate da ignari individui di cui si è abilmente guadagnata la fiducia (10).

Il nome serve proprio a far capire il lavoro metodico di preparazione che si cela dietro a questa tecnica dove, l'arte della persuasione si combina con quella del raggirare e dove l'attacco stesso non è che una piccola parte anche se la più evidente. L'utente crede quindi di prendere decisioni autonome quando in realtà è stato influenzato a disinsediare la mente critica e la capacità di prendere decisioni indipendenti (11).

L'applicazione maggiore di questo tipo di tecniche è oggi proprio nel *phishing*.

In linea generale, il riferimento teorico può essere rintracciato nelle sei "tendenze base della natura umana" coinvolte nel "dire di sì", individuale da Cialdini.

L'ossequio all'"autorevolezza", che spinge a fare qualunque cosa richieda uno sconosciuto che si presenti come fonte autorevole.

La simpatia, indotta da chi finge di essere inesperto e di avere bisogno di aiuto.

La reciprocità o l'istinto a ricambiare chi ci fa un favore (vero o presunto).

La coerenza con le posizioni prese, che può essere messa davanti alla sicurezza.

La riprova sociale, ovvero l'istinto a collaborare coi colleghi

La reazione alla scarsità, che può spingere a rivelare informazioni importanti pur di entrare in possesso, per esempio, di un antivirus contro un presunto pericolosissimo nuovo virus.

4. Esperimento

Nella prevenzione psicologica, finalizzata allo sviluppo

di una cultura della sicurezza informatica, è di estremo interesse l'analisi della percezione di un dato crimine.

Conoscere come gli utenti interpretino un fenomeno, o una situazione di rischio, dà sicuramente un valido contributo nell'indirizzare le strategie di intervento.

Al fine di analizzare il fattore umano nell'ambito della più diffusa frode *on-line* è stata effettuata una ricerca sperimentale, denominata "*Phishing (In)Credibility*" che ha preso in considerazione l'effettiva conoscenza del fenomeno e soprattutto il tipo di elaborazione a cui maggiormente ricorrono gli utenti per esprimere il loro giudizio di credibilità o meno nei confronti di queste *e-mail* esca.

4.1. I soggetti

L'indagine è stata condotta su un campione di 30 soggetti di età compresa tra i 20-40 anni, poiché si è assunto che in tale fascia di età l'uso di servizi *on-line* e quindi la conseguente possibilità di essere vittime del *phishing* possa essere maggiore.

I soggetti sono stati assegnati casualmente (tramite tavola *random*) a due condizioni di ricerca: un gruppo di controllo ed uno sperimentale, entrambi di 15 ciascuno.

4.2. Il questionario

Il questionario, a cui sono stati sottoposti, somministrato attraverso posta elettronica, viene loro presentato come studio di sensibilizzazione al fenomeno del *phishing* da parte del Master di II livello in scienze forensi (Criminologia-Investigazione-Security-Intelligence) dell'Università La Sapienza di Roma e si compone esclusivamente di domande chiuse, ovvero domande che limitano le risposte dei soggetti ad alternative prefissate.

Tali domande sono sicuramente più facili da codificare ed analizzare e permettono insieme all'anonimato di cui si avvale il test, una maggiore disponibilità da parte dei soggetti poiché richiedono meno tempo ed energia rispetto a quelle aperte.

Al fine di evitare eventuali errori di comprensione delle domande o di compilazione delle risposte, il soggetto viene invitato a leggere prima di iniziare il test, un'alquanto sommaria descrizione del crimine in questione, e le indicazioni di compilazione provviste di esempio chiarificatore. La descrizione in realtà, ha principalmente l'intento di sottolineare l'utilizzo di *e-mail* fraudolente.

4.3. Procedura sperimentale

Al gruppo di controllo viene richiesto di visionare cinque coppie di messaggi di posta elettronica più o meno

Note:

(9) V.M. Borella "Comunicare persuadere convincere. Come ottenere dagli altri quello che si vuole con le tecniche di programmazione neurolinguistica", III ed., 2002.

(10) K. Mitnick "The art of reception", 2002.

(11) A. Violetti - Presidente Associazione Informatici Professionisti "Importanza strategica del "fattore umano nella sicurezza informatica" ICT security day 2007

simili tra loro (una coppia per pagina) e di indicare, in un'apposita tabella, se secondo loro siano veri (V) o falsi (F), scegliendo anche tra quattro indicatori suggeriti (fonte, linguaggio, contenuto e grafica) quello su cui maggiormente si sono affidati per esprimere tale giudizio. In realtà i messaggi sono tutti falsi, messaggi di *phishing* già da tempo in circolazione, utilizzati per presentare e descrivere il fenomeno in rete. Viene inoltre chiesto loro prima di effettuare il test di rispondere semplicemente con un SI o con un NO alla seguente domanda: "Aveva già avuto informazioni sul *Phishing*?"

Il trattamento (manipolazione) a cui verrà sottoposto il gruppo sperimentale consiste invece in un'indicazione in cui si suggerisce che, nell'ambito di ogni coppia, solo uno è sicuramente un messaggio falso (di *phishing*), mentre l'altro probabilmente non lo è.

Un suggerimento quindi non del tutto veritiero che comunque non rappresentando un'istruzione da seguire, lascia al soggetto la possibilità di fidarsi o meno.

Il percepire la fonte del suggerimento come autorevole può avere sicuramente un notevole impatto in tale tipo di scelta e, questo effetto "autorità", di cui spesso si avvalgono tali truffatori, è stato perseguito in questo caso, dal presentarmi (o essere presentata) come persona sicuramente competente in quanto psicologa/criminologa impegnata in un progetto "Anti-*Phishing*" e come fonte affidabile, poiché il questionario riproduce il logo dell'Università La Sapienza e soprattutto il nome del Master in scienze forensi.

4.4. Tipo di analisi e risultati

Lo strumento permette di rispondere a tre tipi di domande sul *phishing*.

Si conosce?

Analizzando il numero di risposte Si e No alla domanda posta prima del questionario, misura a livello quantitativo, l'effettivo raggio di azione delle ormai numerose campagne di prevenzione e sensibilizzazione già in atto nello specifico campione.

Malgrado diverse organizzazioni forniscano continuamente report attraverso i quali conoscere le caratteristiche e le dinamiche dei crimini *on-line*, poco meno della metà dei soggetti (40%) sottoposti al test ha affermato di non conoscere ancora quello che può essere considerato uno dei maggiori problemi di oggi connessi all'utilizzo di Internet. Il risultato sorprende soprattutto considerando che di *phishing* ormai se ne parla in ogni dove, tramite svariati canali comunicativi.

Quanto si conosce?

Poiché si tratta di tutti messaggi falsi, è possibile avere una stima di quanto si riesca ad essere ingannati, affidandosi all'"errore di credulità", commesso dai soggetti ovvero al numero di volte che rispondono V quando in realtà si tratta di tutti F. Seppur più della metà dei soggetti (60%) ha dichiarato di aver già avuto modo di ri-

cevere informazioni su questo tipo di truffa, in totale ben 98 messaggi su 300 non sono stati riconosciuti come messaggi di *phishing*.

Interessante notare che, di questi 98 errori, ben 64 sono commessi proprio da soggetti che affermano già di aver avuto modo di "conoscere" il fenomeno!

Inoltre, confrontando gli errori commessi dai due gruppi separatamente è stato possibile evidenziare l'effettivo potere delle tecniche di ingegneria sociale di influenzare tali giudizi di credibilità.

Si è evidenziata una differenza tra i due gruppi statisticamente significativa al livello di probabilità 1%, (12) il che significa che si ha il 99% di probabilità che la manipolazione psicologica a cui sono stati sottoposti i soggetti del gruppo sperimentale abbia avuto effetto.

Come si riconosce?

Tra i quattro indicatori suggeriti: fonte e contenuto, rappresentano elementi caratteristici in genere di un tipo di elaborazione più attenta e profonda, mentre l'affidarsi prevalentemente all'aspetto della grafica intesa come un buon *look* professionale da parte del mittente del messaggio e ad un linguaggio più o meno consona, risulta tipico di un'elaborazione di tipo superficiale.

Dall'analisi delle frequenze degli indicatori scelti dai soggetti per basare i loro giudizi di credibilità o meno dei messaggi, è emerso che 190 valutazioni su 300 si sono affidate ad aspetti secondari.

Si potrebbe quindi affermare che la credibilità superficiale, che nasce da un'analisi semplice (quel tipo di analisi che sta dietro al proverbio "è l'abito che fa il monaco") sia quindi di particolare interesse per i messaggi presentati.

Nello specifico, per quanto concerne la grafica, sicuramente è da sempre l'aspetto più curato dai *phishers*, soprattutto considerando che per la maggior parte questi messaggi simulano come mittente una istituzione finanziaria o commerciale.

In considerazione di ciò, verrebbe da supporre che tale aspetto, magari scelto in alternativa alla fonte autorevole (rappresentata per lo più da banche), possa aver influito più nella scelta di un giudizio positivo di credibilità che in uno negativo.

Ma se la grafica rappresenta un punto di forza, punto debole di questi messaggi in circolazione è da sempre stato il linguaggio. Per la maggior parte infatti, trattandosi di messaggi tradotti automaticamente da programmi appositi a seconda del Paese in cui li si voglia far circolare, presentano veri e propri "orrori" ortografici.

Le 137 valutazioni sulle 300 complessive basate su di

Nota:

(12) Il test statistico utilizzato è stato il Chi 2. L'ipotesi nulla (H0) postula come inesistenti (nulle, pari a zero) le differenze fra le risposte errate date dai due gruppi (H0: GCv=GSv). L'ipotesi alternativa (H1) suppone invece che ci siano differenze significative al livello di probabilità scelto. Si è ottenuto $X^2 = 7.334$; GL = 1; Significatività: $p = .01$

esso, si suppone quindi siano state utili principalmente per esprimere un giudizio di non credibilità. Purtroppo però il consiglio di leggere attentamente può oggi non servire più in quanto il fenomeno ha preso piede anche nel nostro Paese e un linguaggio che prima lasciava molto a desiderare, risulta oggi sicuramente più adeguato.

Ciò che comunque stupisce di più è però che, i messaggi presentati hanno tutti contenuti a dir poco paradossali, aspetto questo che da solo avrebbe dovuto bastare ad evidenziarne la natura fasulla. Alcuni accennano ad aggiornamenti per cui si rende necessario l'aiuto urgente del cliente della banca in questione, come se le banche non eseguissero *backup*! Altri parlano di danni accidentali al database della società. Seppure un tale evento dovesse malauguratamente verificarsi, un recupero dei dati di accesso fatto *ad personam* richiederebbe una tempistica inaccettabile, procurando all'istituto un danno di immagine di non poco conto. E le Poste Italiane che si trasformano in lotterie a premi?

5. Conclusioni

Noi oggi letteralmente "affoghiamo" nel mare di campagne di informazioni sul *phishing*, ma vedere e sentire non significano affatto riflettere, capire ed astrarre.

C'è bisogno di interpretare quello che riceviamo ma, ragionare su un messaggio può richiedere troppo tempo

quando si è abituati a vivere in una società ad alta velocità come la nostra.

Dai risultati della ricerca è emerso come, seppur non manchi, tale consapevolezza dei pericoli della rete sembrerebbe diventare sempre meno riflessiva. Per modificare la nostra "stamperia di idee" può bastare anche solo una semplice immagine di un logo o un *design* particolarmente professionale.

Si tende cioè sempre più spesso a passare da *homo sapiens*, fatto di astrazione, simbolo e ragione, a *homo videns*, più "animale" e sprovvisto di "anticorpi critici".

Che sia migliore o peggiore non lo si può dire a priori in quanto dipende ovviamente dal contesto. Certamente però è un uomo diverso che almeno apparentemente sembra andare indietro nel processo evolutivo.

La tecnologia invade oggi infatti tutta la nostra vita. Si tende spesso a giudicarla in maniera negativa, può scoraggiare, può essere ritenuta non sicura, ma di fronte alla possibilità di essere truffati, scegliere la strada dell'eremitaggio elettronico non rappresenta certo la soluzione ottimale, ma la fine privata della propria individualità.

Cosa fare allora? Sicuramente contro il *phishing* non esiste nessuna filosofia delle "soluzioni semplici", ma cosa certa è che bisognerebbe tornare un po' più *sapiens*, tornare cioè ad esercitare il nostro spirito critico fermandoci ad elaborare in maniera meno superficiale ciò che ci viene richiesto.

RIVISTE

Il Corriere giuridico

Mensile di giurisprudenza, legislazione e opinione

Direttore scientifico: Piero Schlesinger

Comitato scientifico: Vincenzo Carbone, Mario Cicala, Claudio Consolo, Adolfo Di Majo, Giuseppe Lombardi, Vincenzo Mariconda

Periodicità: mensile

Corriere Giuridico è il mensile di diritto e procedura civile che non trascura gli spunti innovativi offerti dal diritto penale e amministrativo e affronta con tempestività e autorevolezza tutte le problematichette con le quali si misurano gli operatori del diritto. Offre un duplice aggiornamento: segnala in forma sintetica le pronunce della Corte costituzionale, della Corte di giustizia CE, della Corte di cassazione, del Consiglio di Stato e della Corte europea dei diritti dell'uomo con note di richiamo ai precedenti e agli orientamenti della dottrina; pubblica per esteso, con approfonditi commenti, le novità legislative e giurisprudenziali di maggior interesse. Trimestralmente Corriere Giuridico viene affiancato da INT'L LIS, il prestigio-

so supplemento dedicato al diritto processuale internazionale e all'arbitrato internazionale.

Il **servizio online**, riservato esclusivamente agli abbonati e consultabile all'indirizzo www.ipsoa.it/ilcorrieregiuridico, permette all'utente di accedere con tempestività a tutte le novità d'interesse.

Abbonamento annuale € 190,00

Per informazioni

• Servizio Informazioni Commerciali

(tel. 02.82476794 – fax 02.82476403)

• Agente Ipsoa di zona (www.ipsoa.it/agenzie)

• www.ipsoa.it



Il Quotidiano Giuridico



LO STRUMENTO INDISPENSABILE PER ESSERE SEMPRE AGGIORNATI!

Il Quotidiano che garantisce ogni giorno l'informazione sulle più importanti **novità normative e giurisprudenziali** in materia **civile, penale e amministrativo** con **commenti a firma di autorevoli esperti e Approfondimenti** sui temi di maggiore attualità e interesse per i professionisti. I contributi di Quotidiano Giuridico si caratterizzano per la **tempestività** dell'informazione, **l'autorevolezza** dei contenuti e la **facile ricercabilità**.

E in più un omaggio

Abbonandosi a **Il Quotidiano Giuridico** potrà **GRATUITAMENTE** effettuare ricerche nell'archivio di **www.dottrinaediritto.it**: il più completo sistema di ricerca per navigare con facilità nell'immenso patrimonio dottrinale delle riviste giuridiche Ipsoa, **oltre 30.000 articoli** pubblicati dal 1985 ad oggi, di cui potrà consultare una sintesi.



**Provi subito
il servizio
per 2 mesi
a € 30,00**

www.quotidianogiuridico.it

Compila e invia il coupon **via fax allo 0282476799** oppure in busta chiusa a **Wolters Kluwer Italia s.r.l. Gestione abbonamenti Ipsoa**, Strada 1 Palazzo F6, 20090 Milanofiori/Assago (MI) o rivolgiti **all'agenzia Ipsoa della tua zona**. Servizio Informazioni Commerciali Ipsoa tel. 0282476794.

- (709920300) Sì, desidero abbonarmi per **2 mesi** a partire da oggi a **Il Quotidiano Giuridico**, a € 30,00 + IVA (Offerta riservata agli abbonati alle riviste giuridiche Ipsoa)
 (00015049) Sì, desidero abbonarmi a **Il Quotidiano Giuridico**, per un anno a partire da oggi a € 178,00 + IVA

Cognome e Nome	Azienda/Studio
Via	CAP
Città	
Tel.	Fax
E-mail	Cod. cliente
Partita IVA	Codice Fiscale

Addebitare l'importo di € _____ sulla mia carta di credito: Mastercard (16 cifre) American Express (15 cifre) VISA (16 cifre) Diner's (14 cifre)

n° _____ Data di scadenza _____

Nome e indirizzo titolare carta di credito _____

Timbro e firma _____

• Diritto di recesso. Clausola di ripensamento ai sensi dell'art. 5 D.Lgs. n. 185/1999. Decorsi 10 giorni lavorativi dalla data di ricevimento del bene da parte del cliente senza che questi abbia comunicato con raccomandata A.R. inviata a Wolters Kluwer Italia S.r.l. Milanofiori - Assago (o mediante e-mail, telegramma, telex o facsimile confermati con raccomandata A.R. nelle 48 ore successive), la propria volontà di recesso, la proposta si intenderà impegnativa e vincolante per il cliente medesimo. In caso di recesso da parte del cliente, entro lo stesso termine (10 giorni lavorativi dal ricevimento) il bene dovrà essere restituito per posta a Wolters Kluwer Italia S.r.l., Milanofiori, Strada 1 - Pal. F6, 20090 Assago (MI). Le spese di spedizione saranno a carico di Wolters Kluwer Italia S.r.l.
• Ai sensi dell'art. 13 n. 196 del D.Lgs. n. 30.6.2003. La informiamo che i Suoi dati sono conservati nel data base informatico del titolare del trattamento, Wolters Kluwer Italia S.r.l. Responsabile del trattamento: Ufficio MID. L'elenco aggiornato di tutti i responsabili del trattamento potrà essere richiesto per scritto all'Ufficio MID presso la sede della società. I Suoi dati saranno utilizzati dalla nostra società, da enti e società esterne ad essa collegati, nonché da soggetti terzi, titolari autonomi del trattamento, solo per l'invio di materiale amministrativo-contabile, commerciale e promozionale. Ai sensi dell'art. 7 del citato D.Lgs., Lei ha diritto di conoscere, aggiornare, rettificare, cancellare i Suoi dati, nonché di esercitare tutti i restanti diritti ivi previsti, mediante comunicazione scritta a Wolters Kluwer Italia S.r.l., Ufficio MID, Milanofiori, Strada 1 - Palazzo F6, 20090 Assago (MI).



IPSOA
Gruppo Wolters Kluwer

Y10BT LE

Rassegna bibliografica

a cura di **Francesco Brugaletta, Carmelo Giurdanella, Andrea Lisi, Giuseppe Vaciago**

Parte dei testi selezionati sono recensiti nella sezione *on line* della Rivista www.ipsoa.it/diritto dellinternet

■ Diritto amministrativo

Mariangela Benedetti

Innovazione digitale, in *Giornale di diritto amministrativo*, 2008, fasc. 2, 137

Alessandro Natalini

La semplificazione e l'amministrazione digitale, in *Giornale di diritto amministrativo*, 2008, fasc., 1, 105

■ Diritto della proprietà intellettuale e diritto della concorrenza

David D'Agostini, Giuseppe Bellazzi, Massimo Farina

I contratti dell'informatica. Aspetti civilistici e fiscali
Forlì, Experta, 2008, 292

Stefania Ercolani

Una sommissa riflessione sul diritto d'autore all'epoca della convergenza, in *Diritto d'autore (II)*, 2008, fasc. 1, 1

Mario Fabiani

Nuove prospettive dell'accesso ai contenuti-interoperabilità e diritto di autore, in *Diritto d'autore (II)*, 2008, fasc. 1, 63

Nicola Lucchi

Sistemi di digital rights management per i contenuti digitali: il prodotto può causare effetti collaterali, in *Studium Iuris*, 2008, fasc. 3, 358

Massimiliano Molinari

La fruizione delle opere dell'ingegno in ambiente digitale - Brevi riflessioni in tema di «Podcasting», in *Diritto d'autore (II)*, 2008, fasc. 2, 218

Andrea Zincone, Marcello Santopadre

La nozione di originalità del software alla luce delle ultime pronunce della cassazione: come salvare la creatività?, in *Diritto d'autore (II)*, 2008, fasc. 1, 69

■ Diritto penale

Paolo Carretta, Tecla Succi, Venanzio Di Cicco, Antonio Cilli, Lucio D'Andrea, Salvatore Tramis, Antonio Montemurro

Crimine economico e computer forenser
Forlì, Experta, 2008, 738

Cesare Maioli e Roberto Cugnasco

Profili normativi e tecnici delle intercettazioni. Dai sistemi analogici al voice over IP
Gedit, Bologna, 2008, 224

Mario Morra

I reati in materia di diritto d'autore. Le fattispecie incriminatrici e le altre disposizioni penali
Milano, Giuffrè, 2008, 308

Andrea Monti

Tutela del minore, community on-line responsabilità penale del fornitore di servizi internet, in *Cassazione penale*, 2008, fasc. 2, 748

Paolo Scognamiglio

Criminalità informatica. Commento organico alla Legge 18 marzo 2008, n. 48
Napoli, Edizioni Simone, 2008, 110

Luigi Viola

Non si può creare un account di posta elettronica con un nome di altri, in *Studium Iuris*, 2008, fasc. 3, 365

■ Diritto tributario

Valerio Artina, Mascia Dalmaggioni

Modello informatico unificato, in *Pratica Fiscale e professionale*, 2008, fasc. 12, 13

Daniela Pizzi e Giulia Ballardini

La denuncia telematica Emens
Trento, Seac Editrice, 180, 2008

■ E-Commerce, contratti on-line e contratti informatici

Pietro Gobio Casali

La fornitura di software tra contrattualistica e diritto d'autore, in *Giurisprudenza italiana*, 2008, fasc. 3, 791

Alessandro Scarso

Ancora sulla nozione (generale) di consumatore, in *Obbligazioni e contratti*, 2008, fasc. 1, 27

■ Firma digitale e documento informatico

Cristiana Napoleone

Validità della comunicazione telematica all'indirizzo elettronico del difensore, in *Diritto e pratica delle società*, 2008, fasc. 7, 90

Claudia Sandei

Valore formale e probatorio del documento informatico alla luce del d.lgs. 4 aprile 2006, n. 159, in *Nuove leggi civili commentate (Le)*, 2008, fasc. 1, 3

Mariagiovanna Scarpa

Le nuove frontiere dell'efficacia probatoria dei documento informatico, in *Rivista trimestrale di diritto e procedura civile*, 2008, fasc. 1, 251

■ Informatica giuridica e diritto dell'informatica

Manuel Castells

La nascita della società in rete
Milano, Edizioni EGEA, 2008, 602

■ Privacy e Sicurezza

Enrico Barraco, Andrea Sitzia

La tutela della privacy nei rapporti di lavoro
Milano, Ipsosa, 2008, 271

Matteo Bascelli

Possibile ruolo dei whistleblowing schemes nel contesto della corporate e della control governance. Profili di compatibilità con l'ordinamento italiano e, in particolare, con la disciplina in materia di protezione dei dati personali, in *Responsabilità amministrativa delle società e degli enti (La)*, 2008, fasc. 1, 125

Giuseppe Busia

Niente nomi dei debitori negli atti di vendite giudiziarie e aste online - con lo stop alle informazioni «eccedenti» ripristinato il principio di proporzionalità, in *Guida al diritto*, 2008, fasc. 11, 106

Leonardo Filippi

La sentenza Dupis c. Francia: la stampa "Watchdog" della democrazia tra esigenze di giustizia, presunzione d'innocenza e privacy, in *Cassazione penale*, 2008, fasc. 2, 813

Cristina Petrucci, Stefano Taddei

Solo un'adeguata "policy" aziendale può tutelare imprenditore e lavoratori, in *Guida al Diritto*, 2008, fasc. 3, 77

■ Profili costituzionali e comparatistici

Laura Corazza

Internet e democrazia. La globalizzazione e l'interculturalità in rete
Bologna, Clueb, 2008, 120

Erik Trijo Gunnar

GoogleCrazia
Roma, Leconte, 2008, 180

■ Tecnologie per l'attività giudiziaria

Marcello Clarich

Per una giustizia amministrativa moderna servono informatica e un codice di rito, in *Guida al diritto*, 2008, fasc. 10, 11

■ INDICE AUTORI

Bufa Francesco	
La comunicazione di cancelleria a mezzo <i>e-mail</i>	359
Cassano Giuseppe	
Redditi <i>on-line</i>	329
Cisterna Alberto	
Il sistema unico nazionale d'intercettazione tra contenimento della spesa e regole processuali.....	394
Clarizia Renato	
La pubblicazione <i>on-line</i> delle dichiarazioni dei redditi.....	333
Contaldo Alfonso	
Le regole tecniche del nuovo casellario giudiziario telematico.....	411
Garbagnati Giovanni	
Per la configurabilità del reato di abusivo mantenimento nel sistema informatico è necessario che l'agente sia consapevole di agire <i>invito domino</i>	366
Fantini Monia	
<i>Phishing</i> : strategie operative dell'inganno	421
Gorga Michele	
Le regole tecniche del nuovo casellario giudiziario telematico.....	411
Marongiu Daniele	
La posta elettronica: una complessa qualificazione tra prassi, giurisprudenza e legge.....	386
Pani Mattia	
Procedura di gara e annotazione nel casellario informatico per la mancata dimostrazione del possesso dei requisiti dichiarati	376
Sangiovanni Valerio	
L'informazione del consumatore nella commercializzazione a distanza di servizi finanziari.....	399
Trucco Lara	
Il nome (di dominio) di associazioni (politiche) tra profili ideologici e interessi mediatici	340
Villecco Alessandra	
L'atto digitale e la procura: una ragionevole soluzione sul rilascio della procura speciale	349

■ INDICE CRONOLOGICO DEI PROVVEDIMENTI

Giurisprudenza civile	
<i>Corte di cassazione</i>	
19 febbraio 2008, n. 4061, sez. Lavoro.....	356
<i>Tribunale</i>	
1 febbraio 2008, Milano, ord.	347
12 marzo 2008, Roma	339
17 marzo 2008 Roma, Sez. IX, ord.	389

Giurisprudenza penale

<i>Tribunale</i>	
11 dicembre 2007, n. 488, Nola.....	365
11 marzo 2008, n. 348, Brescia.....	390

Giurisprudenza amministrativa

<i>Consiglio di Stato</i>	
18 marzo 2008, n. 1127.....	390
<i>TAR</i>	
21 febbraio 2008, n. 562, sez. I, Puglia, Lecce.....	383
8 febbraio 2008, n. 664, Napoli, sez. I.....	390
1 aprile 2008, n. 2773, Sez. III, Lazio, Roma.....	375

Giurisprudenza internazionale

Tribunal de Grande Instance de Lyon, 13 marzo 2008.....	392
Tribunal de Grande instance de Paris, 18 marzo 2008	392
Michele Mazur v. eBay Inc., Hot Jewelry Auctions.com d/b/a Jewelry Overstock Auctions and Paramount Auctions, et al., No. C 07-03967 MHP (N.D. Ca., March 4, 2008).....	392
A.V., et al. v. iParadigms, Limited Liability Company Civ. Act. No. 07-0293 (E.D. Va., March 11, 2008)...	393

Normativa

Ministero dell'Interno, decreto 9 gennaio 2008 «Individuazione delle infrastrutture critiche informatiche di interesse nazionale» (G.U. 30 aprile 2008, n. 101)	335
Autorità per le garanzie nelle comunicazioni «Procedura selettiva per la cessione del quaranta per cento della capacità trasmissiva delle reti digitali terrestri - termine per la presentazione delle domande» (G.U. 2 maggio 2008, n. 102)	335
Autorità per le garanzie nelle comunicazioni, deliberazione 12 marzo 2008, n. 130/08/CONS «Modificazione della delibera n. 54/08/CONS, recante "Modifiche ed integrazioni al regolamento in materia di procedure sanzionatorie in attuazione dell'articolo 14 bis del decreto-legge 4 luglio 2006, n. 223, convertito dalla legge 4 agosto 2006, n. 248, e del regolamento in materia di impegni di cui alla delibera n. 645/06/CONS"» (G.U. 23 aprile 2008, n. 96)	335
Autorità per le garanzie nelle comunicazioni, deliberazione 12 marzo 2008, n. 131/08/CONS «Modifiche al regolamento in materia di impegni di cui alla delibera n. 645/06/CONS» (G.U. 3 maggio 2008, n. 103 - <i>Suppl. ord. n. 112</i>).....	336
Ministero dell'Economia e delle Finanze, decreto 7 marzo 2008 «Individuazione del gestore del sistema di interscambio della fatturazione elettronica nonché delle relative attribuzioni e competenze» (G.U. 3 maggio 2008, n. 103)	336
Ministero dell'economia e delle finanze, decreto 29 aprile 2008 «Modifica del decreto 18 marzo 2008, concernente i parametri tecnici per la trasmissione telematica delle ricette» (G.U. 10 maggio 2008, n. 109).....	337
Garante per la protezione dei dati personali, provvedimento 6 maggio 2008 «Misure in ordine alla pub-	

blicazione in Internet di dati relativi alle dichiarazioni dei redditi» (G.U. 8 maggio 2008, n. 107) 337

INDICE ANALITICO

Appalto

Procedura di gara e annotazione nel casellario informatico per la mancata dimostrazione del possesso dei requisiti dichiarati (T.A.R. Lazio, Roma, sez. III, 1 aprile 2008, n. 2773) di *Mattia Pani* 375

La posta elettronica: una complessa qualificazione tra prassi, giurisprudenza e legge (T.A.R. Puglia, Lecce, sez. I, 21 febbraio 2008, n. 562) di *Daniele Marongiu*... 383

E-commerce

L'informazione del consumatore nella commercializzazione a distanza di servizi finanziari di *Valerio Sangiovanni* 399

Giustizia penale

Le regole tecniche del nuovo casellario giudiziario telematico di *Alfonso Contaldo* e *Michele Gorga* 411

Intercettazioni

Il sistema unico nazionale d'intercettazione tra contenimento della spesa e regole processuali di *Alberto Cisterna*..... 394

Nome e domain name

Il nome (di dominio) di associazioni (politiche) tra profili ideologici e interessi mediatici (*Tribunale di roma*, 12 marzo 2008) di *Lara Trucco* 339

Privacy

Redditi on-line di *Giuseppe Cassano* 329

La pubblicazione on-line delle dichiarazioni dei redditi di *Renato Clarizia*..... 333

Procedimento civile

La comunicazione di cancelleria a mezzo e-mail (*Cassazione civile, sez. Lavoro*, 19 febbraio 2008, n. 4061) di *Francesco Buffa*..... 356

Processo civile telematico

L'atto digitale e la procura: una ragionevole soluzione sul rilascio della procura speciale (*Tribunale di Milano* 1 febbraio 2008, ord.) di *Alessandra Villecco*..... 347

Phishing: strategie operative dell'inganno di *Monia Fantini*..... 421

Reati informatici

Per la configurabilità del reato di abusivo mantenimento nel sistema informatico è necessario che l'agente sia consapevole di agire *invito domino* (*Tribunale di Nola* 11 dicembre 2007, n. 488) di *Giovanni Garbagnati* 365

RIVISTE

Il Corriere del Merito

Mensile di giurisprudenza civile, penale e amministrativa commentata

Direzione scientifica Civile: Guido Alpa, Vincenzo Carbone, Claudio Consolo, Vincenzo Cuffaro, Vincenzo Mariconda, Pietro Rescigno

Direzione scientifica Penale: Stefano Corbetta, Emilio Dolcini, Angelo Giarda, Giorgio Marinucci

Direzione scientifica Amministrativa: Francesco Caringella, Giuseppe Chiné, Rosanna De Nictolis, Fabio Francario, Marco Lipari

Periodicità: mensile

Dal n. 1/2008 la **Rivista** si è rinnovata! L'obiettivo è quello di offrire un **panorama giurisprudenziale sempre più ricco ed aggiornato** e un'attenzione particolare alla **fruibilità dei contenuti**.

Tra le **novità**:

- gli "**Osservatori**", **organizzati per Regione** ed arricchiti dall'esposizione del **caso concreto** ("in fatto") ricavato dal testo ufficiale dei provvedimenti massimati;
- l'introduzione delle **parole chiave in neretto** e l'**evidenziazione dei passaggi più importanti** all'interno del commento;
- inserimento di una **tabella di sintesi** nella rubrica "**I Contrasti**" che segnerà i **principali orientamenti giurisprudenziali** inerenti all'argomento trattato.

In più, **ogni anno** riceverà **tre fascicoli** che tratteranno, di volta in volta, **Rassegne di giurisprudenza e dottrina ragionata** in ambito di diritto **civile, penale e amministrativo**.

Il servizio on-line, riservato agli abbonati e consultabile all'indirizzo **www.ipsoa.it/ilcorriedelmerito**, permette all'utente di accedere a tutte le novità d'interesse e all'anteprima della Rivista cartacea.

Abbonamento annuale Euro 180,00

Per informazioni e acquisti

- **Servizio Informazioni Commerciali** (tel. 02.82476794 - fax 02.82476403)
- **Agente Ipsoa di zona** (www.ipsoa.it/agenzie)
- **http://ipsoshop.ipsoa.it**

