ASSOCIAZIONE CULTURALE
PER LO STUDIO DEL DIRITTO

techne

Direttore responsabile
Glauco Riem

Redazione
Stefano Corsini
Francesco Mirabelli
Luca Zenarolla
Paolo Vicenzotto

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

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

Stampa
Lithostampa, Pasian di Prato (UD)

Reg. Trib. di Pordenone n. 514 del 27.07.2004

SOMMARIO

EDITORIALE

Glauco Riem

In questo numero «Techne» ospita diversi illustri contributi alla conoscenza operativa del fenomeno dell'*e-government*.
Dušan Kričej, vicedirettore generale dell'Ufficio ministeriale per le procedure amministrative a distanza della Repubblica di Slovenia, ci parla dell'operatività della *e-uprava*, termine che indica tutto ciò che riguarda l'amministrazione digitale in Slovenia: molti i progetti già operativi e molta la sperimentazione d'avanguardia.

Dino Cozzi, presidente dell'Insiel, delinea in breve i profondi rinnovamenti, anche sul piano culturale, del nuovo corso della società ove si intende declinare investimenti per il rinnovo dei prodotti ed alleanze nell'ITC a tutto campo.

Pier Luca Montessoro, ordinario di Sistemi di Elaborazione presso l'Università di Udine, affronta il magmatico tema della sicurezza delle reti nella Pubblica Amministrazione e nell'impresa: qualche breve cenno storico sul vertiginoso sviluppo delle tecnologie informatiche e poi una doviziosa serie di indicazioni di sicuro interesse per affrontare una problematica in perenne mutazione.

Marco Vianello, avvocato e membro della Commissione di *Information Technology Law* della CCBE, dice – in un prezioso studio che pubblichiamo per intero – dei problemi legati alla giustizia telematica e alla gestione del processo civile, amministrativo e contabile così come delineato dal Dpr 123/01 e successive regole tecniche. «Il processo telematico – afferma – è

sopratutto un problema di mentalità» e si interroga: «Siamo davvero pronti a lasciare a terra la carta e sollevarci verso l'extraterritorialità della rete?».

Andrea Sirotti Gaudenzi, docente al Master della Rete presso l'Università di Padova, delinea gli aspetti problematici e le novità del Codice dell'amministrazione digitale, con il quale tutti i cittadini, le pubbliche amministrazioni e le imprese dovranno, nel breve, confrontarsi. Un'analisi di sicuro fascino che pur tuttavia apre prospettive e scenari di 'inquietudine' gestionale e di alfabetizzazione informatica.

Infine la vignetta di Federico Cecchin.

UVODNIK
Glauco Riem

V tej številki revija «Techne» predstavlja mnenja uglednih ljudi, ki so prispevali k praktičnemu znanju na področju e-uprave.
Dušan Kričej, namestnik generalnega direktorja pri uradu Ministrstva za javno upravo Republike Slovenije govori o učinkovitosti e-uprave, izrazu, ki označuje vse, kar je povezano z digitalno administracijo v Sloveniji, ter o številnih projektih, ki že potekajo in naprednih raziskovanjih.

Dino Cozzi, predsednik družbe Insiel SpA, je z nekaj besedami opisal korenite spremembe v kulturi in nove usmeritve družbe, v povezavi z vlaganji v prenovo proizvodov ter združevanja na vseh področjih komunikacijskih tehnologij.

Pier Luca Montessoro, redni profesor za Sisteme za obdelavo na Univerzi v Vidmu govori o vroči temi, in sicer zaščiti omrežij v javni upravi in podjetništvu ter na kratko opisuje vrtoglavi razvoj informacijske tehnologije. Navaja tudi obsežen niz splošno uporabnih navodil za obvladovanje vprašanja v stalnenm spreminjanju.

Marco Vianello, pravnik in član 'Komisije za informacijsko tehnologijo Law, CCBE-ja' piše o dragoceni študiji, ki jo objavljamo v celoti, o problemih v zvezi s pravnimi zadevami prek interneta in upravljanjem v civilnih, upravnih in računovodskih sporih, navedenih v Odloku Predsednika Republike št. 123/01 ter v naknadnih izvedbenih aktih. Avtor meni, da je elektronska obravnava predvsem problem miselnosti in se sprašuje: «Ali smo se res pripravljeni posloviti od papirja in preiti na zunajozemeljsko omrežje?».

Andrea Sirotti Gaudenzi, docentka na podiplomskem študiju Master omrežja na Univerzi v Padovi opisuje problematične vidike in novosti v Kodeksu digitalne uprave, s katerim se bodo kmalu morali soočiti državljani, podjetja in upravni organi. Gre za resnično zanimivo analizo, ki se ukvarja z vprašanji negotovosti v upravi in računalniškega opismenjevanja.

Za zaključek pa še ilustracija Federico Cecchin.

EDITORIAL

Glauco Riem

This issue of «Techne» contains several distinguished contributions about the operative knowledge of the e-government phenomenon.
Dušan Kričej, vice-director general of the ministerial Office for remote administrative procedures of the Slovenian republic talks about the operativity of e-uprava. The term stands for everything relative to digital administration in Slovenia: several already operational projects and a lot of innovative experimentation.

Dino Cozzi, Chairman of Insiel, gives us a short outline of the important updates, of a cultural nature as well, that are part of the new course of the company involving new investments for the updating of products and the forging of new wide spectrum strategic alliances in the ITC.

Pier Luca Montessoro, regular of Processing Systems at the University of Udine, analyzes the magmatic subject of safety in public administration networks and business: a few brief historical notes on the amazing development of computer technologies and an exhaustive series of useful suggestion to deal with this constantly mutating issue.

Marco Vianello, lawyer and member of the 'Information Technology Law Commission of the CCBE', talks about the problems connected to computerized justice and the management of civil, administrative and accounting proceedings, as it is outlined by the Dpr 123/01 and the subsequent technical regulations. «The computerized trial is most of all – he says – a question of approach» and asks a poignant question: «Are we really ready to drop paper and move to the extraterritoriality of the network?».

Andrea Sirotti Gaudenzi, teacher at the Network Master at the University of Padova, describes the new and potentially problematic elements of the Digital Administration Code, a new entity that citizens, public administrations and businesses will have to confront. A fascinating analysis that opens up new and sometimes worrying scenarios of management and computer alphabetization.

A final light note with the cartoon by Federico Cecchin.

LEITARTIKEL
Glauco Riem

In dieser Ausgabe hat «Techne» einige prominente Experten zu Gast, die ihre Beiträge zum Thema der Operativität des e-government vortragen. Dušan Kričej, Hauptvizepräsident des Ministerialbüros für die Fern-Verwaltungsprozeduren des Republik Slowenien schildert uns das Betriebssystem der E-Uprava – ein Sammelbegriff für alle Aspekte des digitalen Verwaltungssystems in Slowenien: zahlreiche Projekte sind bereits

operativ und der aktuelle Stand der Testversuche ist in vielen Bereichen sehr fortschrittlich.

Dino Cozzi, Präsident der Insiel SpA erläutert uns kurz die grundlegenden auch im kulturellen Bereich in Aussicht gestellten Innovationen für das neue Gesellschaftsjahr, wobei es Hauptziel der Gesellschaft ist Investitionen für die Produktentwicklung und globale ITC- Bündnisse einzubringen.

Pier Luca Montessoro, Ordinarius für Verarbeitungssysteme an der Universität Udine beschäftigt sich mit dem magmatischen Thema der Sicherheit der Datennetze öffentlicher und betriebsinterner Verwaltungssysteme: kurze geschichtliche Einleitung über den rasanten Fortschritt im Bereich der Informatiktechnologie und dann eine Reihe von sicherlich sehr interessanten Ratschlägen, wie man diese ständig in Wandlung stehende Problematik am besten angeht.

Marco Vianello, Rechtsanwalt und Mitglied der 'Kommission Information Technology Law der CCBE' erläutert – in seiner sehr aufschlußreichen Studie, die wir komplett veröffentlichen – alle mit der telematischen Prozeßführung von Zivil-, Verwaltungs- und Buchhaltungsrechtsstreiten verbundenen Probleme, wie sie sich mit dem Gesetzbeschluß Dpr 123/01 und folgende technische Richtlinien abzeichnen. «Der telematische Prozeß – sagt er – ist vor allem ein Auffassungsproblem» und fragt sich desweiteren: «Sind wir tatsächlich bereits so weit den Papierprozeß seinem Niedergang zu weihen und uns auf die Exterritorialität des Datennetzes zu verlassen?».

Andrea Sirotti Gaudenzi, Dozent für Datennetz - Master an der Universität Padua erörtert die problematischen Aspekte und die Neuheiten des digitalen Verwaltungsgesetzbuches mit dem sich in Kürze alle Bürger, die öffentlichen Verwaltungen und die Privatbetriebe auseinandersetzen müssen. Eine zweifellos faszinierende Analyse, die jedoch 'besorgniserregende'

Perspektiven und Szenarios bezüglich der informatischen Verwaltung und Alphabetisierung aufzeigt.

Abschließend die Witzzeichnung von Federico Cecchin.

VEZÉRCIKK

Glauco Riem

«Techne» ezen számában vendégül lát számos olyan neves személyt, akik az e-government jelenséget operatív szempontból is rendkívül jól ismerik. Dušan Kričej, a Szlovén Köztársaság távadminisztrációval foglalkozó miniszteri hivatalának vezérigazgató-helyettese, az e-uprava működéséről beszél nekünk, mely terminus magában foglalja mindazt, ami a Szlovéniában létező digitális adminisztrációval kapcsolatos: számos a már működő projekt és legalább ennyi az újító terv is.

Dino Cozzi, az olasz Insel elnöke röviden felvázolja azokat a jelentős kulturális és az új társadalmi kihívásokat érintő innovációkat, melyeknek célja, hogy csökkentsék az Információ Technológia és Távközlés területéhez tartozó új termékek és társulások költségeit.

Pier Luca Montessoro, az udinei egyetem adatfeldolgozó rendszerekkel foglalkozó tanszékének professzora a közigazgatási és céges számítógépes hálózatok biztonságának szövevényes témáját tárgyalja: az ugrásszerűen fejlődő informatikai technológiák rövid történelmi áttekintése után részletes felsorolást ad azokról a megoldásokról, melyek segíthetnek szembenézni ezzel a örökösen visszatérő és megújuló problematikával.

Marco Vianello, az 'Európai Uniós Ügyvédi Kamarák Tanácsa (CCBE)' Elektronikus Távközlésjogi Bizottságának tagja, egészében leközölt, hasznos tanulmányában beszél folyóiratunknak azokról a problémákról, melyek

szorosan kapcsolódnak a telematikus igazságszolgáltatáshoz, a különböző perek (polgári illetve közigazgatási és pénzügyi) lebonyolításához, amint azt a 123/01-es olasz miniszteri rendelet és a későbbi technikai szabályok felvázolják. Vianello azt állítja, hogy a telematikus per kapcsán leginkább mentalitásbeli problémák vannak, és felteszi a kérdést: «Valóban készek vagyunk arra, hogy a földön hagyjuk a papírt és felemelkedjünk a hálózat földön kívüli területeire?».
Andrea Sirotti Gaudenzi a padovai egyetem a Master in rete *számítógépes hálózatokkal foglalkozó posztgraduális képzésének docense, felvázolja azt, hogy milyen kérdések és újdonságok merülnek fel a digitális adminisztráció törvényeivel kapcsolatban, amelyekkel hamarosan minden polgárnak és közigazgatási dolgozónak is szembesülnie kell majd. Mindazonáltal ebben a lenyűgöző cikkben betekinthetünk azokba a 'nyugtalanító' részletekbe is, amelyek a szervezést illetve az 'informatikai írás-olvasás' széleskörű oktatásának problémáját érintik.*

Végezetül megtaláljuk Federico Cecchin elmaradhatatlan karikatúráját.

E-GOVERNMENT NELLA SLOVENIA: TRA PROGETTI ED OPERATIVITÀ

Dušan Kričej
Vicedirettore generale dell'Ufficio ministeriale per le procedure amministrative a distanza della Repubblica di Slovenia

E-uprava è una abbreviazione con la quale si intende l'amministrazione elettronica *on-line* e gli altri numerosi servizi a distanza, che la parola sottintende. Nell'ultimo anno i cittadini hanno apprezzato i grandi vantaggi ed i benefici della 'amministrazione *on-line*'. Molti sono infatti i progetti indirizzati a singole categorie di cittadini impiegati nell'amministrazione, ma anche ad imprese ed enti anche privati.
Il sito denominato *Portal* è il principale punto di accesso ai diversi contenuti proposti ai cittadini. Si tratta di un portale statale dell''amministrazione *on-line*' e vi si può accedere digitando: http://e-uprava.gov.si.
Il *Portal* rappresenta un semplice ed efficiente sistema per reperire informazioni ed il sistema di consultazione permette una navigazione chiara e collegamenti a documenti ed informazioni precise.
Portal è dotato di un sistema digitale che permette all'utente che sia fornito di *password* e di *User ID* di accedere ad ulteriori informazioni maggiormente personalizzate. Il sito disponibile anche in lingua inglese, è stato realizzato per soddisfare le esigenze di eventuali portatori di handicap e risulta di semplice usabilità.
Il portale è stato reso accessibile con terminali e 'chioschi telematici' posti anche in luoghi pubblici come quelli denominati 'infomat', 'webomat' o 'tele punti'.
Con l'applicazione di 'E-impiego', dedicato all'occupazione, il portale permette ad ogni cittadino di conoscere tutte le offerte di lavoro e le opportunità di un determinato settore di attività: si stabilisce così un immediato ed impor-

tante collegamento fra la domanda e l'offerta di lavoro e ciò in modo semplice e diretto. Il cittadino, con questo servizio, riceve immediatamente importanti informazioni sul mondo del lavoro e dell'economia.
Chi si collega al sistema 'E-democrazia', ottiene un servizio utile a conoscere le procedure burocratiche nei diversi settori dell'amministrazione e conosce direttamente quale sia il corretto approccio per istruire una pratica evitando così eventuali *impasse* procedurali. La modulistica viene così spedita via posta elettronica dall'indirizzo predisposto: oao.predlogi@gav.si.
Il servizio permette poi ai cittadini di esprimere le proprie opinioni e i suggerimenti resi al fine di un migliore funzionamento del sistema.
Il portale permette inoltre di far conoscere ai cittadini il testo dei regolamenti e delle leggi e ciò anche nella fase di formazione ed emendamento prima che essi siano approvati.
Ulteriori servizi sono resi in formato elettronico: si possono ottenere a distanza certificati di ogni genere ed anche attestati di buona condotta. Per la corrispondenza elettronica si adoperano tutti gli attestati digitali, certificati e riconosciuti dalla Repubblica di Slovenia, attraverso i diversi dispositivi digitali denominati 'SIGEN-CA', 'SIGOV-CA', 'AC.NL', 'POSTAR-CA', 'HALCOM'.
Attualmente si può accedere a circa quaranta tipi di servizi elettronici statali e ad undici relativi all'amministrazione locale che si ottengono proprio attraverso il *Portal* statale dell''amministrazione *on-line*' e, sempre con lo stesso portale, i cittadini possono consultare ed estrarre i documenti contenuti nei Registri catastali e nei Registri dell'amministrazione giudiziaria e naturalmente inviare la propria dichiarazione dei redditi *on-line*, servizio quest'ultimo già attivo da tre anni.
Con il sistema denominato 'E-VEM' (tutto in un posto) il cittadino può iscriversi elettronicamente al Registro delle imprese della Repubblica di Slovenia che è gestito direttamente dall'Agenzia per le pratiche pubbliche giuridiche slovena. Con la stessa modalità il cittadino in breve tempo può anche registrarsi presso l'assicurazione sanitaria obbligatoria di Slovenia.
Il sistema naturalmente permette al cittadino, ove necessario, di modificare anche i dati presenti nel Registro d'affari della Repubblica di Slovenia, di cancellarsi *on-line* dal Registro delle imprese oppure di reperire informazioni

che gli siano utili al fine della gestione dell'impresa. Ciò è possibile semplicemente visitando uno dei duecento punti d'accesso oppure collegandosi ad Internet. A questo progetto hanno collaborato quattordici enti. Il sistema permette di consultare quattro registri pubblici e di ottenere circa venti tipi di servizi diversi.
Questo breve *excursus* è naturalmente solo un accenno del più complesso ed articolato sistema che permette l'interoperabilità dei dati e delle informazioni fra tutti gli enti sopra detti.
In ogni buon conto anche se esso è in funzione da meno di sei mesi, i risultati sono molto positivi, e l'incremento delle nuove iscrizioni al Registro delle imprese con il metodo *on-line* ha subito un aumento di oltre il 20%.
Tutte le suddette modalità di svolgimento a distanza del governare hanno portato l'amministrazione ad un risparmio di centottanta milioni di Sit (talleri sloveni).
È stato sviluppato poi il progetto – ideato e realizzato dal Ministero delle Finanze sloveno – relativo al pagamento delle tasse via posta elettronica 'E-EDP', che include anche quello denominato 'E-DDV' che è relativo al pagamento della tassa sul valore aggiunto per persone giuridiche.
Si sta lavorando poi ai progetti 'E-dogana' ed 'E-rapporto' che raccolgono informazioni e dati statistici per conto delle Agenzie governative.
Quando poi sarà in funzione il nuovo registro elettronico dei veicoli, i cittadini potranno rinnovare la patente di guida anche via Internet.
Crediamo, quindi, che la Slovenia abbia creato un''amministrazione *on-line*' concorrenziale perfino a quella della Comunità Europea.

ELEKTRONSKA UPRAVA IN ELEKTRONSKE STORITVE ZA DRŽAVLJANE IN PRAVNE OSEBE

Dušan Kričej

E-uprava je kratica za elektronsko upravo in številne elektronske storitve, ki se izvajajo v okviru le-te. V zadnjem letu so državljani lahko občutili že veliko prednosti in pozitivne učinke e-uprave. Izvajajo se številni projekti, namenjeni posameznim zakl-

jučenim skupinam, kot so državljani, zaposleni v upravi in gospodarski subjekti ter druge organizacije.
Kot enotna vstopna točka do različnih spletnih vsebin za državljane je aktualen Državni portal e-uprava (http://e-uprava.gov.si). Portal predstavlja učinkovito kombinacijo informacij in elektronskih storitev s pregledno navigacijo in povezavami na ciljne vsebine. Omogoča osebne prilagoditve, ki se izvajajo s pomočjo digitalnega spletnega potrdila ali na podlagi uporabniškega imena in gesla. Portal je pripravljen tudi v angleškem jeziku in kar je se posebej vredno, priiagojen je ljudem s posebnimi potrebami. Na voijo je tudi verzija, ki podpira javno dostopne točke (infomati, webomati, teletočke). V okviru portala deluje tudi aplikacija e-zaposlitve, ki omogoča celovito ponudbo zaposlitev na enem mestu. Omogoča tudi ustrezno povezavo in kontakte med ponudniki in iskalci zaposlitev. V zadnjem času lahko drlžavijani dobijo pomembne informacije tudi v zvezi z e-demokracijo in odpravo administrativnih ovir. Svoje predloge lahko pošljejo na poseben predal oao.predlogi@gov.si in podajo svoje mnenje, predloge. Pravilniki in zakoni so na voljo drlžavljanom že v svoji zgodnji fazi nastajanja (torej še pred sprejemom).
Od eiektronskih storitev lahko naštejemo elektronske vloge za pridobivanje različnih izpiskov iz uradnih evidenc, pridobivanje potrdila o nekaznovanju, naznanilo kaznivega dejanja. Za potrebe elektronskega podpisovanja se uporabljajo vsa kvalificirana digitalna potrdila priznana v RS (SiGEN-CA, SIGOV-CA, AC-NL, POŠTAR-CA, HALCOM. Danes je na voljo blizu 40 elektronskih storitev na nivoju države in 11 eiektronskih storitev za lokalno samoupravo, ki se prav tako izvajajo preko državnega portala e-uprava. Za drlžavljane so podprti elektronski vpogledi v zemlijiško knjigo, zemljiški kataster, sodni register. Dohodnino (e-dohodnina) bodo drlžavljani lahko oddali po elektronski poti že tretjič.
Sistem VEM (Vse na Enem Mestu) in elektronska podpora e-VEM, omogoča bodočemu samostojnemu podjetniku, da na enem mestu (tudi preko interneta) opravi vpis podjetnika v Poslovni register Slovenije, ki ga vodi Agencija Republike Slovenije za javnopravne evidence in storitve, posreduje davčne podatke, ki jih je podjetnik dolžan posredovati ob ustanovitvi s.p., na Davčno upravo Repubiike Slovenije. Hkrati se lahko prijavi v obvezno zdravstveno zavarovanje na Zavod za zdravstveno zavarovanje Siovenije ter prijavi otroke do 18. leta starosti v obvezno zdravstveno zavarovanje na Zavod za zdravstveno zavarovanje Slovenije. Če želi, lahko vpi spremembe podatkov v Poslovni register Slovenije, izbriše svojo dejavnost samostojnega podjetnika iz Poslovnega registra Slovenije ter naroči izpisek podatkov iz Poslovnega registra Slovenije za poljubnega samostojnega podjetnika.

Registracijo lahko opravimo z obiskom ene od 200 fizičnih vstopnih točk ali direktno na internetu. V projektu je sodelovalo 14 ustanov, povezali smo 4 registre ter 20 strežnikov. Opisane funkcionalnosti nakazujejo na kompleksnost sistema, saj se podatki izmenjujejo med vsemi zgoraj naštetimi institucijami. Sistem je v produkciji manj kot pol leta, rezultati so zelo pozitivni, saj beležimo rast novoustanovljenih s.p.-jev za več kot 20%. Ocenjeni prihranki: 180 mio sit/ietno. Velik napredek v smeri razvoja e-uprave je Slovenija naredila z izpeljavo projekta Eiektronsko Davčno Plačevanje (EDP), ki obsega tudi sistem e-DDV (Davek na Dodano Vrednost) za pravne osebe. Nosilec tega projekta je Ministrstvo za finance RS. Velik napredek je tudi na področju e-Carine in e-letna poročila ki se oddajo na Agencijo za javnopravne evidence in storitve.

Projekti, ki omogočajo povezave med evidencami javne uprave so še posebej koristni, saj prinašajo tudi največje prihranke. Enostavno državljanom ni potrebno več prinašati raziičnih potrdil, sai vse opravijo uradniki sami. Pri tem jim znatno pomaga informacijska tehnologija.

Tik pred produkcijo je tudi razširjeni portal e-uprava z novimi življenjskimi dogodki in generičnimi aplikacijami za pripravo elektronskih obrazcev, elektronskimi plačili in elektronskim vročanjem. Takoj, ko bo v produkciji novi register vozil, bomo predali v uporabo tudi aplikacijo za spletno podaljšanje registracije motornih vozil. Državljani bodo lahko prometno dovoljenje podaljšali kar preko interneta.

Z izvajanjem projektov za državljane, gospodarske subjekte in druge organizacije pa Slovenija vzpostavlja e-upravo, ki je tudi konkurenčna Evropski uniji.

INSIEL: PROFONDI RINNOVAMENTI CULTURALI E ALLEANZE NELL'ITC A TUTTO CAMPO

Dino Cozzi
Presidente di Insiel SpA

In Friuli Venezia Giulia la domanda pubblica di servizi informativi è da lungo tempo una domanda uniforme, diversamente da quanto si registra in ambito nazionale in cui essa è particolarmente frammentata e dove ogni Pubblica Amministrazione ha ricercato autonomamente il proprio fornitore dando vita ad un'offerta altrettanto frammentata fra fornitori privati e pubblici e, in questo modo, non si sono realizzate sufficienti economie di scala che, invece, sarebbero attuabili se la domanda fosse unica. Il panorama nazionale, sul fronte della domanda e dell'offerta, non è esaltante e presenta un livello di informatizzazione della Pubblica Amministrazione complessivamente disomogeneo che, accanto a punte di eccellenza, trova larghe sacche di ritardi e inefficienze. Sul fronte dell'offerta ci sono tante aziende, fondamentalmente piccole, non in grado di sviluppare completamente ricerca e innovazione, e tutte concentrate sul mercato nazionale. Insiel SpA, azienda di proprietà della Regione FVG – leader nello studio, progettazione e realizzazione di soluzioni informatiche per le pubbliche amministrazioni locali e la Sanità – è l'unico fornitore per il FVG e questo ha portato benefici all'intero sistema; forte della sua trentennale esperienza, intende, quindi, portare i suoi servizi e prodotti, ampiamente testati in FVG, anche al resto del territorio nazionale. Punta altresì a partecipare alla creazione di società regionali di informatica in quelle regioni dove sono allo studio soluzioni analoghe. Per questo, Insiel si propone come *partner* e come apportatore di *know-how*. Nello stesso tempo la sua esperienza può essere di estremo interesse in alcuni mercati esteri, in particolare quelli dell'Est europeo. L'esperienza di Insiel si caratterizzerà non solo come fornitore di soluzioni informatiche, ma come sog-

getto in grado di trasferire il *know-how* organizzativo e gestionale nel settore della Sanità e della Pubblica Amministrazione, proponendosi come soggetto capace di ridisegnare i sistemi di governo amministrativo di questi Paesi. Questo ruolo impegna Insiel ad un profondo cambiamento e adeguamento organizzativo e culturale, già iniziato con l'insediamento del nuovo *management*, che prevede un cambio di cultura e di organizzazione per rendere la società maggiormente competitiva sul mercato. Un cambiamento che si declina in investimenti per rinnovare i prodotti, in una politica di alleanze a livello nazionale e internazionale, nel coinvolgimento delle aziende ICT della Regione, in un nuovo modello organizzativo in grado di essere più vicino al mercato sia culturalmente sia geograficamente, in un approccio a nuovi mercati – pubbliche amministrazioni centrali, *utilities*, logistica – nazionali e internazionali con particolare riguardo all'Est europeo.

INSIEL: GRUNDLEGENDE KULTURELLE INNOVATIONEN UND GLOBALE ITC- BÜNDNISSE

Dino Cozzi

Die öffentliche Nachfrage in Friaul- Julisch- Venetien an informatischen Dienstleistungen ist seit langem sehr uniform; anders auf nationaler Ebene, wo eine extrem fragmentarische Nachfrage zu verzeichnen ist und wo sich jedes öffentliche Verwaltungsamt eigenständig einen Dienstleistungsanbieter ausgewählt hat. Dies hat zu einem ebenso fragmentarischen Angebot an privaten und öffentlichen Dienstleistungsanbietern geführt und auf diese Weise wurden nicht genügend Einsparungen realisiert, die im Falle einer uniform ausgebildeten Nachfrage möglich wären. Das Nationalpanorama der Nachfrage und des Angebots an Dienstleistungen im Bereich der Informatiktechnologie ist nicht gerade rosig, da sich der Computerisierungsstand der öffentlichen Verwaltungsämter im allgemeinen sehr inhomogen zeigt und neben den zu nennenden exzellenten Beispielen leider weitreichend sehr lückenhaft ist und viele Verspätungen und Unzulänglichkeiten aufweist. Im Bereich des Angebots gibt es zahlreiche, insbesondere kleine Betriebe, die nicht in der Lage sind Forschung und Innovation komplett in ihr Betriebssystem einzubringen und die sich zu sehr auf den Nationalmarkt konzentrieren. Die Insiel SpA, ein

Gesellschaftsbetrieb der Region Friaul- Julisch- Venetien, und Leader im Bereich der Planung und Realisierung von informatischen Systemen für die lokale Öffentliche Verwaltung und das Gesundheitswesen, ist der einzige Dienstleistungsanbieter in diesem Marktbereich für die Region Friaul- Julisch- Venetien, was für das gesamte System von Nutzen gewesen ist. Gestärkt durch ihre dreißigjährige Erfahrung beabsichtigt die Insiel SpA ihre ausgiebig in Friaul- Julisch- Venetien getesteten Dienstleistungen und Produkte auch in den restlichen Regionen Italiens und auf internationaler Ebene einzuführen. Desweiteren strebt sie danach aktiv an der Kreation von regionalen Gesellschaften im Bereich der Computertechnologie teilzunehmen in Regionen, wo bereits ähnliche Projekte erarbeitet werden. Aus diesem Grund bietet sich die Insiel SpA als Partner und Know-how- Experte an. Gleichermaßen kann ihre Erfahrung in einigen Auslandsmärkten, insbesondere auf dem Osteuropäischen Markt von großem Interesse sein. Die Betriebserfahrung der Insiel SpA charakterisiert sich nicht nur als Anbieter von informatischen Dienstleistungen, sondern auch als Anbieter von organisatorischem und betriebswissenschaftlichem Know-how im Bereich der Öffentlichen Verwaltung und dem Gesundheitswesen. Sie präsentiert sich daher als Gesellschaftsbetrieb, der in der Lage ist in diesen Ländern die staatlichen Verwaltungsstrategien zu überarbeiten. Diese Rolle verpflichtet die Insiel SpA zu grundlegenden Veränderungen und Innovationen im organisatorischen und kulturellen Bereich, die bereits mit dem Amtsantritt des neuen Managements, das eine neue Gesellschaftskultur und Betriebsorganisation zu Gunsten der Konkurrenzfähigkeit plant begonnen haben. Veränderungen, die sich in Investitionen für die Produktforschung und – innovation, in einer Bündnispolitik auf nationaler und internationaler Ebene, in der Einbeziehung der ICT- Betriebe der Region, in einem neuem Organisationsmodell, das den nationalen und internationalen insbesondere den osteuropäischen neuen Märkten – wie öffentliche Zentralverwaltungen, Utilities, Logistik- sowohl kulturell als auch geographisch näher ist, artikulieren.

INSIEL: WIDE SPECTRUM PROFOUND INNOVATIONS AND ALLIANCES IN THE ITC

Dino Cozzi

Public demand for information services in FVG has been for a long time uniform, as opposed to what happens in a national context in which demand is generally more

fragmented and every public administration has been seeking its supplier individually. This approach produced an equally fragmented offer among public and private suppliers, and this in turn prevented the development of enough scale economies which would be possible if the demand was uniform. The national field, as far as demand and offer are concerned, is not encouraging and presents a level of computerization of public administrations generally heterogeneous, punctuated by areas of excellence but in the whole marked by delays and inefficiences. On the offer front, there are many firms, substantially small, unable to properly develop research and innovation, and all concentrated on the national market. Insiel SpA, property of the Friuli Venezia Giulia Region, is a leader in the study, design and realization of computerized solutions for Public Administrations and Public Health – it is the only supplier for FVG and this brought many benefits to the whole system. On the strength of thirty years of experience, Insiel is ready to offer its products and services, widely tested in FVG, to the rest of the national territory. It aims as well to participate in the creation of regional computer technology firms in those regions were similar solutions are going to be adopted. To this end Insiel is offering its partnership and know how. At the same time its experience can be extremely interesting in some international markets, particularly Eastern Europe. Insiel will not only bring computerized solutions to the table, but will also become a subject capable to transfer organizational and managerial know how in the public health sector and PA, offering the knowledge to redesign administration systems in those countries. For this reason Insiel is engaged in a profound organizational and cultural transformation, already underway under the new management, that will render the company more competitive. A transformation brought about through investment and updating of product, in a series of alliances on a national and international level, with the involvement of the ITC companies in the region, in a new organizational model capable to be culturally and geographically closer to the market, and an approach to new national and international markets – central public administrations, utilities, logistics – with particular attention to Eastern Europe.

Corso on-line certificato per dipendenti di aziende

PRIVACY E CORRETTO TRATTAMENTO DEI DATI IN AZIENDA

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

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

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

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

SCIOGLI OGNI NODO SULLA PRIVACY

→ D.lgs 196/03

IALweb.it

IAL agenzia formativa Friuli Venezia Giulia

in collaborazione con STUDIO LEGALE RIEM

LA SICUREZZA DELLE RETI NELLA PUBBLICA AMMINISTRAZIONE E NELL'IMPRESA

Pier Luca Montessoro

Scusandomi fin da subito con il lettore per l'approccio poco convenzionale che seguirò in questo scritto, desidero prima di tutto richiamare solo brevemente alcuni concetti che ritengo ormai noti a tutti, in quanto scritti e ripetuti pressoché in ogni articolo sulla sicurezza informatica: le reti di calcolatori sono uno strumento fondamentale di piccole e grandi organizzazioni, dalla piccola impresa alla Pubblica Amministrazione nazionale al sistema planetario di gestione delle prenotazioni dei voli; le attività svolte sulle reti di calcolatori e in particolare sulla rete Internet, sono sempre più critiche in termini di tipologia e finalità dei dati trasferiti (si pensi ai bonifici bancari mediante i servizi di *home banking* o al trasferimento di informazioni riservate e tutelate dalla legge sulla *privacy*); la sicurezza è ormai un requisito irrinunciabile dei sistemi informatici pubblici e privati, in molti contesti obbligatorio per legge, e richiede risorse e sforzi organizzativi; considerando i costi globali ed i rischi a cui ci si espone in assenza di una politica di sicurezza informatica si osserva che l'attuazione della sicurezza è una scelta, anche dove non obbligatoria, del tutto conveniente.
Detto questo, vorrei affrontare alcune domande che ritengo fondamentali per la comprensione dell'argomento 'sicurezza informatica' e per la nascita di un atteggiamento corretto e consapevole nei confronti dei problemi che vi sono annessi. Atteggiamento che deve maturare ancor prima degli aspetti operativi di definizione delle strategie di difesa e delle politiche di gestione dei propri sistemi e dei propri dati.

Perché i nostri sistemi sono (sempre più) vulnerabili?

La storia delle reti di calcolatori vede concentrata in meno di quattro decen-

ni una vertiginosa quantità di sviluppi tecnologici e di conseguenze sociali come forse non era mai accaduto nella storia dell'uomo. Visti dalla prospettiva attuale, possiamo dire che i paradigmi fondamentali su cui sono state sviluppate le architetture di rete erano del tutto inadeguati ad un impiego così diffuso e complesso come quello moderno. La sicurezza è in realtà soltanto uno dei molti punti deboli delle nostre reti; per esempio l'assenza di tecniche per garantire la cosiddetta 'qualità del servizio' in modo nativo (senza cioè richiedere appositi apparati e programmi) rende ancora difficile o impossibile un utilizzo generalizzato della rete Internet per applicazioni di telefonia o di videocomunicazione. Ritornando alla sicurezza, va innanzi tutto ricordato che le prime tecnologie di rete nascono per essere impiegate in ambienti dove tutti si adoperano per il miglior funzionamento possibile della rete stessa e dei servizi che essa veicola. In tali condizioni, la preoccupazione per la sicurezza è naturalmente minima. Inoltre, per loro natura le reti mirano a connettere più sistemi possibili, e quindi ad ogni espansione della rete Internet, a partire dalla prima rete del Dipartimento della Difesa Americano alla fine degli anni '60, si è sempre mantenuta il più possibile la compatibilità dei meccanismi di comunicazione con le reti esistenti. Per questo ancora oggi utilizziamo sistemi che sono intrinsecamente vulnerabili.
Non è difficile progettare sistemi più sicuri, il problema è convincere tutto il resto del mondo ad adottarli, altrimenti si rimane isolati: serve a poco un ottimo sistema di posta elettronica se poi i nostri corrispondenti non sono in grado di ricevere o leggere i messaggi. Il processo di migrazione verso sistemi più sicuri è quindi inevitabilmente lento ed estremamente difficile.
Le debolezze intrinseche nei nostri sistemi di rete sono numerose. Per semplificare la trattazione mi limiterò a citare il fatto che tutta la rete Internet si basa sullo scambio di messaggi digitali secondo un meccanismo di comunicazione ('protocollo', in gergo) detto IP (*Internet Protocol*, appunto). In base a questo protocollo i messaggi viaggiano 'in chiaro', cioè sono chiaramente leggibili da chiunque possa veder transitare il messaggio stesso lungo il suo cammino nella rete. È come se il sistema postale prevedesse esclusivamente l'utilizzo di buste completamente trasparenti. Come nel sistema postale, non è facilissimo accedere al messaggio in transito, ma la vulnerabilità intrinseca

del sistema lo rende inadatto, così com'è, per molti servizi (quanti verserebbero un assegno sul proprio conto corrente inviandolo alla banca per posta?). Addentrandoci più nel dettaglio in questo parallelismo, va detto che le buste non si chiudono neanche troppo bene, rendendo possibile alterarne il contenuto. Come nel sistema postale, poi, l'indirizzo del mittente può non essere autentico e questo apre il problema della gestione dell'identità in rete di cui parlerò più avanti.
In questi anni stiamo assistendo ad un mastodontico sforzo per migliorare i protocolli di rete e adeguare di conseguenza apparecchiature, computer e programmi. I risultati sono tangibili ed evidenti (molti servizi oggi esistono solo grazie ad essi), ma ancora molta strada resta da percorrere.
Altra fonte di vulnerabilità dei nostri sistemi risiede nella qualità del software che utilizziamo. Applicazioni sempre più potenti, versatili e facili da usare comportano programmi sempre più complessi, e quindi più soggetti agli inevitabili errori di programmazione. Tali errori sono sistematicamente utilizzati dagli *hacker* per violare la sicurezza dei sistemi. Per questa ragione la Microsoft ha predisposto un sistema di aggiornamento automatico via rete dei propri sistemi operativi, essendo impossibile provvedervi manualmente, visto che la frequenza con cui vengono individuati errori e vulnerabilità è ormai quasi quotidiana.
Ed è proprio nei programmi del nostro computer che oggi possono annidarsi le più pericolose insidie. Da quando, alla fine degli anni '80, comparvero i primi virus informatici, è chiaro che i nostri personal computer sono soggetti a 'infiltrazioni' di programmi non voluti che possono svolgere attività più o meno dannose. I virus che si limitavano a far comparire una pallina che rimbalzava sui contorni dello schermo sono soltanto più un ricordo. I virus (e derivati) attuali tendono sempre più a non rivelarsi, carpendo a nostra insaputa (i cosiddetti *spyware*) informazioni riservate quali codici, *password* e indirizzari *e-mail*, i primi per l'ovvio fine di compiere attività illecite assumendo la nostra identità, gli indirizzi di *e-mail* per andare ad arricchire gli elenchi dei futuri obiettivi di *spam*, i messaggi di posta non desiderati che veicolano pubblicità di dubbio gusto e nulla utilità, truffe e ancora virus.
Sempre più spesso un computer attaccato con successo non mostra all'u-

tente comune alcuna anomalia nel funzionamento. Questo consente ai virus di operare per tempi lunghi, carpire più informazioni o addirittura utilizzare a nostra insaputa il computer come base di partenza per ulteriori attacchi ad altri computer nella rete oppure come deposito di *file* (tipicamente illeciti). In quest'ultimo caso il nostro sistema informatico viene utilizzato come nodo di una delle reti illegali di condivisione di *file* e subiamo l'ulteriore danno di un utilizzo non autorizzato del nostro collegamento di rete, talvolta con dirette conseguenze economiche.
La lista delle tipologie di attacco sarebbe troppo lunga per cercare in questa sede di affrontarla sistematicamente. Ai fini della trattazione è sufficiente la comprensione del fatto che i problemi di sicurezza sono numerosi e diffusi a più livelli. Non ci si può illudere che possano essere risolti soltanto con interventi tecnologici: è necessaria la prevenzione anche in termini organizzativi e comportamentali, una vera e propria cultura della sicurezza informatica.

Di chi posso fidarmi?
In numerose attività quotidiane affidiamo i nostri beni o la nostra stessa vita a chi ha progettato o costruito gli oggetti che noi utilizziamo. Basti pensare alla fiducia che implicitamente riponiamo nell'impianto frenante della nostra automobile. Con i sistemi informatici la cosa non è molto differente: quando utilizziamo un computer, il suo sistema operativo e i programmi applicativi, diamo fiducia a chi li ha progettati e realizzati. Ogni nostra azione potrebbe essere spiata o manipolata ad arte per scopi illeciti e fraudolenti. Tuttavia, produttori di computer, sistemi operativi e programmi applicativi non hanno certo interesse a rovinarsi con tali azioni illegali (tra l'altro, vista l'enorme diffusione dei loro sistemi, non passerebbe molto tempo prima di essere scoperti), quindi il problema della fiducia non si pone, come avviene per l'automobile, l'aereo, la cucina a gas, ecc. Discorso ben diverso è quello del software scaricabile gratuitamente dalla rete Internet, specialmente da siti poco sconosciuti e non appartenenti a organizzazioni o produttori ufficiali, soprattutto se non di tipo *open source* (i programmi *open source* sono disponibili anche in forma sorgente, il che permette ai programmatori di tutto il mondo di controllarne l'affidabilità prima di utilizzarli e di segnalare even-

tuali pericoli), soprattutto se copie illegali di programmi commerciali o programmi dedicati ad eseguire attività illegali. Scaricare e utilizzare programmi di questo tipo significa rischiare di consegnare le 'chiavi di casa' (il nostro computer) a sconosciuti. Neanche le più evolute tecnologie sono attualmente in grado di tutelarci da questo tipo di vulnerabilità. È indispensabile unire alla tecnologia una metodologia organizzativa e gestionale della rete e degli utenti. Le soluzioni sono necessariamente di compromesso, in quanto implicano una limitazione alla libertà dell'utente di utilizzare il proprio computer (per esempio imponendo che soltanto i tecnici sistemisti possano installare nuovi programmi, previa verifica di assenza di vulnerabilità). Nelle pubbliche amministrazioni e nelle imprese questo approccio è sicuramente attuabile in quanto in generale la gestione dei sistemi informativi è delegata a tecnici specializzati. Tuttavia richiede uno sforzo non trascurabile di organizzazione del lavoro e di configurazione degli elaboratori e della rete. Un aiuto può venire dall'adozione – ora indispensabile per legge – di sistemi antivirus e, possibilmente, *anti-spyware*. Questi sistemi possono essere adottati per l'intero ente o azienda, e possono e devono essere configurati in modo da distribuire automaticamente gli aggiornamenti a tutti i computer. Va però ricordato che tali sistemi sono di tipo reattivo: sono in grado di proteggerci dal software malevolo 'dopo' che questo è stato identificato dal produttore del software antivirus o *anti-spyware*, quindi un uso prudente e consapevole della rete è comunque indispensabile.

Sicuramente degna di poca fiducia è la posta elettronica, salvo la cosiddetta 'posta elettronica certificata' di recente introduzione. La posta elettronica comune, infatti, si presta facilmente alla falsificazione dell'identità del mittente e all'invio di messaggi protetti dall'anonimato. Questo la rende un veicolo ideale per invio di virus e *spyware*, di inviti a visitare siti web contenenti software pericolosi (ebbene sì, anche la semplice navigazione in Internet può 'infettare' il nostro computer, a causa di sempre più numerosi automatismi di *browser* quali Internet Explorer), oppure di vere e proprie truffe, per esempio richieste di fornire dati relativi al proprio conto corrente bancario

per improbabili esigenze tecniche o per ancor più improbabili promesse di facili guadagni. Per quanto i sistemi di posta possano filtrare la maggior parte dei messaggi pericolosi, a condizione che questo rientri nelle politiche dell'ente o dell'azienda, un numero non trascurabile di questi messaggi raggiunge comunque l'utente, e così ancora una volta il suo comportamento diventa determinante ai fini della sicurezza complessiva del sistema.
Il comportamento dell'utente è però fonte di preoccupazione da parte dei responsabili di organizzazioni complesse (pubbliche amministrazioni e imprese medio-grandi in primo luogo) perché esiste anche un altro problema: il danno informatico per dolo. Con numeri elevati di dipendenti non si può escludere il rischio che qualcuno per ragioni diverse attenti deliberatamente dall'interno alla sicurezza informatica. Addirittura, si inizia ad assistere allo sviluppo di politiche di gestione atte a controllare l'attività degli stessi tecnici sistemisti in quanto in realtà particolarmente complesse non è possibile o sufficiente fidarsi ciecamente della loro lealtà.
Infine, parlando di fiducia, è necessario soffermarsi sul problema dell'identità in rete, che è forse il più infido dei problemi legati alla fiducia. Se siamo utenti scrupolosi, subordiniamo praticamente tutte le attività che svolgiamo sul nostro computer e sulla rete Internet al riconoscimento di un interlocutore (persona, servizio o sito web) fidato. Ne parlavamo poco fa a proposito dei programmi scaricati da Internet e dei mittenti dei messaggi di posta elettronica. Per chi gestisce un servizio di rete è oggi possibile accertarsi dell'identità di un utente all'atto del collegamento con livelli di sicurezza adeguati (tecnicamente si potrebbe arrivare ad un'identificazione quasi perfetta, ma i costi sono tali da imporre soluzioni di compromesso), mentre per l'utente è molto più difficile essere sicuro dell'identità del *server* a cui si collega. Per esempio, tutte le truffe informatiche ai danni di utenti di banche *on-line* fanno uso di siti web clonati dai siti ufficiali, cosicché l'utente crede di lavorare effettivamente con la propria banca. Anche a questo problema c'è una soluzione, ma è necessario che l'erogatore del servizio faccia uso di un certificato digitale: il nostro *browser* potrà così verificare che il sito a cui ci colleghiamo sia autentico interrogando una *certification authority*, ente fidato riconosciuto a livello internazionale. Inoltre, l'utente deve controllare

le indicazioni che il suo *browser* gli fornisce riguardo all'effettivo utilizzo dei certificati e della crittografia per proteggere il contenuto della comunicazione. Analogamente, per quanto riguarda la posta elettronica, esiste il servizio di posta elettronica certificata, ma attualmente è ancora poco diffuso e comunque costoso, quindi non adatto ad un utilizzo diffuso per messaggi comuni. La soluzione, in questo caso, è usare prudenza, evitando di utilizzare tale strumento per informazioni riservate o per lo scambio di *file* che potrebbero essere o diventare portatori di virus. (È poco noto il fatto che esistono strumenti per lo scambio di *file* molto più efficienti e sicuri dell'utilizzo degli allegati alla posta elettronica. Per esempio siti web personali, protetti da *username* e *password*, che possono essere attivati anche sul proprio personal computer, oppure servizi FTP – *File Transfer Protocol* – insieme alle diverse moderne varianti orientate alla sicurezza).
Affrontando in termini più generali il tema della fiducia, ci si imbatte in importanti aspetti che non sono più di pertinenza esclusiva della sicurezza informatica. In particolare, esiste il problema sociale della scorretta percezione dell'affidabilità delle informazioni che riceviamo dalla rete Internet. Data l'importanza e la diffusione del web come fonte di dati e notizie, esiste una diffusa tendenza a paragonare tale strumento a mezzi di comunicazione di massa tradizionali, quali televisione o giornali, trascurando però il fatto che nella maggior parte dei siti web la pubblicazione non è soggetta ad alcun controllo né verifica. È quindi possibile pubblicare e diffondere informazioni distorte o false, magari con scopi fraudolenti, e sta quindi all'utente valutare quanto un sito sia degno di fiducia ed eventualmente verificare l'informazione prima di utilizzarla.

Per completare questo scenario piuttosto sconfortante bisogna anche affrontare la tipica domanda: 'Sulla mia rete viaggiano dati che non possono interessare a nessuno al di fuori della mia azienda; perché qualcuno dovrebbe attaccarmi?'. Purtroppo il fatto stesso di essere sistemi informatici rende quelli delle imprese, degli enti pubblici e privati e anche i semplici personal computer dei privati cittadini potenziali obiettivi, una volta che siano collegati alla rete Internet. In primo luogo, come già detto, possono essere utilizzati come punti di partenza per ulteriori attacchi, magari più mirati, proteggendo

l'autore nell'anonimato (gli attacchi risultano provenire da un computer senza alcuna relazione con lui/lei), ma va anche considerata la dilagante presenza di sistemi automatici di violazione della sicurezza che, una volta attivati dall'*hacker* di turno, operano in rete in totale autonomia e colpiscono sistematicamente qualunque sistema trovino collegato. Per questo è necessario che la sensibilità a questi problemi si diffonda ad ogni livello e maturi una cultura della sicurezza informatica in tutti gli utenti della rete Internet.

Che linee guida è bene adottare?

Nell'attesa che vengano sviluppati nuovi sistemi informatici che possano prevenire i problemi di sicurezza in modo sempre più trasparente ed affidabile, è possibile adottare politiche di gestione dei sistemi (da parte di tecnici e progettisti) e di utilizzo di servizi (da parte degli utenti) che consentono di conseguire un elevato grado di sicurezza permettendoci di sfruttare in tranquillità tutti i benefici della rete.

Entrare nei dettagli tecnici richiederebbe una trattazione troppo lunga e tecnica, che esula dallo scopo di questo articolo. Mi limiterò a tracciare delle linee guida generali che potranno essere applicate, di volta in volta, ai vari contesti.

Limitare il rischio che utenti non autorizzati accedano ai sistemi e alla rete richiede un'accurata gestione degli *account* (i dati e le autorizzazioni associate agli utenti):

- imporre che a ciascun *account* sia associata una persona fisica, evitando *account* condivisi da più utenti o, peggio ancora, anonimi;
- controllare periodicamente che gli *account* attivi siano tutti e solo quelli necessari alle normali attività;
- mantenere una lista degli utenti cancellati (talvolta proprio gli ex-utenti, magari ex-dipendenti, sono veicoli se non sorgenti di attacco);
- imporre l'uso di *password* non banali, possibilmente con scadenza periodica (attenzione all'equilibrio tra difficoltà di indovinare la *password* e difficoltà di ricordarla: essa serve a poco se poi viene scritta su un *post-it* attaccato al monitor del computer!).

Sempre con l'obiettivo di prevenire gli accessi illegali, alcuni semplici accorgimenti possono dare grandi risultati, soprattutto in organizzazioni complesse:

- limitare il numero di connessioni simultanee per ciascun utente: quando un utente è collegato, un ulteriore collegamento a suo nome da un altro computer è sintomo di un probabile collegamento illegale;
- rilevare i *login* falliti e prevedere meccanismi automatici di blocco degli *account*, prevenendo il rischio che le *password* vengano scoperte per tentativi da programmi che provano in sequenza un gran numero di parole e nomi;
- limitare gli orari in cui è accessibile la rete: molti attacchi avvengono di notte o nei week-end;
- limitare gli indirizzi MAC (identificativi delle schede di rete dei computer) da cui un utente può accedere alla rete, permettendogli così l'accesso esclusivamente dal computer aziendale del suo ufficio;
- limitare l'accesso fisico alle postazioni di lavoro: gli attacchi avvengono anche dall'interno degli edifici dove circolano persone non autorizzate all'uso della rete e poco controllate (si pensi agli edifici aperti al pubblico o all'accesso notturno ai locali da parte delle imprese di pulizie).

Per attuare una efficace politica di protezione e prevenzione i responsabili informatici dovrebbero adottare strategie di sicurezza fin dalla fase di progettazione della propria rete e dei propri servizi. Per esempio:

- prevedere strategie di autenticazione dei *server* e dei servizi, con l'utilizzo di certificati digitali;
- proteggere fisicamente l'accesso a cavi, apparati di rete e computer;
- scegliere protocolli sicuri, che includano tecniche di crittografia per proteggere le informazioni trasmesse;
- proteggere la rete interna mediante apparecchiature di controllo del traffico (*firewall*);
- controllare rigidamente gli *account* privilegiati (che consentono di agire sulla configurazione della rete e dei sistemi), con particolare attenzione a quelli dedicati all'amministrazione remota;
- effettuare periodicamente un *audit* dei propri sistemi, cioè un'analisi della vulnerabilità mediante la simulazione di attacchi secondo tutte le tecniche conosciute (esistono aziende specializzate in questo tipo di servizi).

La protezione del computer dell'utente è un argomento delicato, in quanto va spesso in conflitto con l'esigenza o il desiderio dell'utente stesso di poter

utilizzare nella massima libertà la propria stazione di lavoro. Alcune scelte utili sono:

- imporre l'installazione esclusivamente di software originale prelevato da confezioni sigillate;
- educare gli utenti alla chiusura della sessione di lavoro quando abbandonano la stazione e ad utilizzare correttamente i sistemi di autenticazione (per esempio mantenere riservata la propria *password*);
- impedire l'utilizzo di lettori di CD-ROM, DVD, floppy disk e penne di memoria USB, possibili veicoli di software non autorizzato e di furto di dati riservati (è chiaro che questa non è una scelta indolore, tipicamente viene adottata in ambienti molto critici, quali quelli militari);
- utilizzare e mantenere aggiornato un sistema anti-virus commerciale, per la protezione automatica di tutti i computer della propria rete.

Infine, non va trascurato il problema della prevenzione dalla perdita dei dati. Le conseguenze di attacchi alla sicurezza (ma anche di semplici malfunzionamenti) possono essere drammatiche se comportano la perdita delle informazioni memorizzate nei sistemi. Purtroppo, ci si accorge dell'importanza di un dato soltanto quando esso non è più disponibile. È quindi necessario studiare e attivare una politica di *backup* periodico e automatico, possibilmente non soltanto dei *server* centrali ma anche dei computer degli utenti, controllare periodicamente, a campione, la leggibilità dei dati nei *backup* e conservare i *backup* stessi in luogo sicuro, separato da quello che ospita i computer. A seconda della criticità del contesto, è anche opportuno prevedere piani di intervento per il *disaster recovery*, in quanto può non essere sufficiente avere copia dei dati: è anche necessario poterli rendere nuovamente disponibili e riattivare i servizi in tempi accettabili.

SAFETY IN THE PA AND BUSINESS NETWORK

Pier Luca Montessoro

I will give here a few general guidelines that could be applied to the various contexts. To reduce the risk that unauthorized users gain access to systems and networks an

accurate management of accounts becomes necessary (data and authorizations related to users):

- *any account must be associated to a physical person, avoiding the sharing by many users or, worse even, anonymous users;*
- *check periodically that active accounts are those and only those necessary to normal activity;*
- *keep a list of cancelled users (sometimes ex-users, or ex-employees, are vehicles if not originators of attacks);*
- *make it obligatory to use passwords that are not trivial, possibly with an expiry date (watch for the delicate balance between guessing a password and the difficulty to remember it: it becomes useless if it's written on a post-it attached to the computer monitor!).*

To prevent illegal access a few simple precautions can produce excellent results, especially in complex organizations:

- *restrict the number of simultaneous connections by each user: when a user is connected, another connection with his name from another computer is a clue of a probable illegal connection;*
- *detect failed logins and activate automatic system to block the accounts, preventing the risk that password are discovered by programs that try a number of words and names in sequence;*
- *restrict the time of access to the network: many attacks happen by night or during week-ends;*
- *restrict the number of MAC addresses (identification of computer network cards) that a user can utilize to access the network, allowing him access exclusively from his office or workplace computer;*
- *restrict physical access to workstations: attacks often come from inside buildings, where unauthorized persons can move freely (think of buildings open to the public or nighttime access to buildings by cleaners).*

To implement an efficient protection and prevention policy, safety strategies must be adopted in the designing phase of the network or services. For instance:

- *devise authentication strategies for servers and services, for instance utilizing digital certification;*
- *physically shield access to wiring, network apparatus and computers;*
- *always choose safe protocols, including for instance cryptography techniques to protect data transfers;*
- *protect the internal network through traffic control systems ('firewall');*
- *strictly control preferential accounts (that allow to operate on network and*

systems configuration), with particular care to those relative to remote administration;
- *periodically execute an 'audit' of the system, that is an analysis of vulnerability through the simulation of attacks with all known techniques (specialized companies can provide this kind of service).*

The protection of the user computer is a delicate matter, often in conflict with the need or desire of the user himself to freely utilize his/her workstation. These are some useful suggestions:
- *install original software coming from sealed packages only;*
- *instruct users to close the working session when they leave the workstation and to correctly utilize authentication systems (for example keeping a confidential password);*
- *forbid use of CD-ROM, DVD readers, floppy discs and USB memory pen, all possible vehicles of non-authorized software and theft of confidential data (obviously a painful choice, usually adopted in critically important environments, such as military installations);*
- *utilize and keep updated a commercial anti-virus system for the automatic protection of all computers in a given network.*

Finally, do not forget the problem of prevention of data loss. The consequences of attacks to security (or even simple malfunctions) can be dramatic if they involve the loss of stored data. Unfortunately we often realize the importance of certain information only when it's not available anymore. Therefore it becomes imperative to devise and activate a periodical and automatic backup protocol, not only, if possible, in central servers but in users computers also; a periodic sample check of data availability and the preservation of the backup themselves in a safe place, separate from the computers stations. According to the criticality of the context it is good policy to contemplate an action plan of 'disaster recovery'; a simple copy of the aforementioned data could not be sufficient: it is also necessary to make the data promptly available again and restore service efficiency in an acceptable time.

GIUSTIZIA TELEMATICA: UNA SFIDA CULTURALE

Marco Vianello
Componente della Commissione di *Information Technology Law* del CCBE (www.ticosoci.it)

Qualche tempo fa mi ha colpito una notizia apparsa sulla stampa secondo la quale il 1º luglio 2003 in Danimarca si è celebrato l'*E-Day*, ossia si è schiusa l'era della comunicazione digitale: dal luglio 2003, infatti, tutta la Pubblica Amministrazione danese comunica esclusivamente per via digitale, senza l'utilizzo di carta.
Ma l'utilizzo dell'informatica nel sistema giustizia? L'idea ha radici relativamente remote.
Secondo un articolo di Marco Boretti apparso su «Dirittosuweb»[1], già nel XVI secolo un giudice francese propose un sistema chiamato 'Algoritmo di Bridoie' il quale, sempre secondo l'autore, mediante un calcolo matematico, tenendo conto caso per caso di una serie di variabili, sceglieva tra due soluzioni: colpevole o innocente.
In realtà quel sistema, di stampo medioevale, era basato più sul fato che sul calcolo: da fonti diverse[2] si evince, infatti, che «il giudice Bridoie di Rabelais emetteva sentenze secondo il fato, essendo esso molto in voga presso i Greci. Metteva in un'urna un'infinità di lettere dell'alfabeto o di parole composte, le maneggiava e le versava e ciò che compariva nell'insieme delle lettere formava la risposta di questa specie di Oracolo di Stregoneria».
È notizia di stampa, sempre per quanto riguarda l'applicazione alla giustizia penale, che in Brasile è entrata in vigore una sorta di 'giudice elettronico'. Pedro Valls Feu Rosa, magistrato della Suprema Corte Federale, ha introdotto un programma che permette, sin dall'intervento degli agenti delle forze dell'ordine in casi di circolazione stradale (tant'è che il sistema è denomina-

to anche *Justice-on-Wheels*), di accedere alle banche dati, inserire le variabili e le circostanze del caso e ottenere la decisione seduta stante[3].
Tra il 1999 ed il 2000 si è assistito all'avvento dell'ADR (*Alternative Dispute Resolution*), ma presto l'acronimo si è tramutato in ODR (*On-line Dispute Resolution*), essendo ormai opinione diffusa che un metodo moderno non avrebbe potuto essere avulso dall'utilizzo dell'informatica.
E così si è fatto strada il metodo cosiddetto *blind offer* (cieco o automatico), con il semplice utilizzo di una macchina che scambia 'al buio' tra le parti offerte in un periodo di tempo variabile, ma predefinito e con incrementi o decrementi minimi (a seconda delle parti: attore o convenuto) pure concordati preventivamente (normalmente il 5%).
Naturalmente la disputa tratta solo quel che riguarda il *quantum debeatur*; viene raggiunta la soluzione quando la differenza tra le offerte è inferiore a una certa percentuale predefinita e accettata dalle parti (solitamente attorno al 30%): in questo caso il valore medio di tali ultime offerte corrisponde all'importo che il debitore dovrà pagare al creditore.
S'interrompe la trattativa, invece, quando decorso un termine pattuito, la differenza rimane superiore a un determinato margine.

Il 'mondo giustizia' istituzionale oggi è tutto proteso verso il processo telematico civile che, com'è noto, in Italia deve ancora decollare e sta sperimentandosi solo nelle menti di chi se ne sta occupando per professione.
È utile qui, tuttavia, solo notare che il progetto è ancora carente di mezzi e, soprattutto, mentalità. La sfida non si potrà affrontare fintantoché non sarà diffusa la cosiddetta 'cultura informatica'.
Un recente sondaggio in tema di informatizzazione promosso dalla Commissione di *Information Technology Law* del CCBE (*Council of the Bars and Law Societies of the European Union*)[4] ha dimostrato che:

- solo in pochi Paesi (e in molti casi solo in teoria) è possibile la comunicazione digitale con gli uffici giudiziari;
- salvo qualche raro esempio di evoluzione, non è prevista la comunicazione elettronica tra parti del processo;
- vi sono previsioni, perlopiù solo normative e non applicative, sull'utilizzo

della firma elettronica nelle comunicazioni ufficiali;
- per lo più non vi sono o sono scarsi i servizi legali offerti *on-line*, ma dove sono previsti vengono resi disponibili anche nei siti istituzionali forensi;
- i codici deontologici non contemplano i servizi *on-line* o le comunicazioni elettroniche in generale, a eccezione di quelli di Francia, Italia, Polonia, Repubblica Slovacca, Slovenia, Ungheria;
- solo in alcuni Paesi le istituzioni forensi hanno sviluppato delle Intranet o dei sistemi di comunicazione interni per incentivare l'utilizzo dei sistemi elettronici di comunicazione.

Merita intanto, quindi, sperimentare i metodi alternativi o, comunque, conciliativi delle controversie.
Noto da sempre agli psicologi come il 'metodo dell'arancia', ma meno agli avvocati, un buon esempio di negoziazione aiuta a comprendere come si può 'allargare la mente' e scoprire come rivolgere in positivo ciò che siamo soliti professionalmente stimolare come una soluzione conciliativa che consente risultati certi in tempi rapidi privando ciascuna delle parti di una quota della propria pretesa, ma prevenendo o definendo una lite. Ciò naturalmente ai giuristi deriva spontaneo dalla definizione fornita più tradizionalmente dai nostri codici (art. 1965 cod. civ.).
Riporto il racconto testualmente:

> Due sorelle litigavano per un'arancia. Una di loro riteneva di averne più diritto in quanto l'aveva presa per prima, invece l'altra argomentava che il diritto corrispondeva a lei essendo la primogenita. La loro madre, nel tentare una soluzione imparziale, offrì di tagliare il frutto a metà: le bambine rifiutarono fermamente la soluzione proposta e continuarono a litigare. La nonna, che osservava attenta la scena, decise di chiedere ad ognuna delle bambine perché volevano l'arancia. La più piccola rispose che aveva sete, l'altra che voleva la buccia per preparare una torta perché aveva fame. Così la nonna grattugiò la buccia dell'intera arancia e la offrì alla nipote per la sua torta, e spremette la polpa dell'intera arancia e la offrì all'altra[5].

Ma veniamo all'ODR, termine inteso nell'accezione di cosiddetto 'modello aperto', opposto a quello cieco di cui si è detto, ove l'intervento del terzo

super partes è elemento indispensabile per dirimere la controversia.
Un primo dato normativo applicativo lo troviamo nell'art. 19 del D.Lgs. 9 aprile 2003, n. 70, che ha recepito la direttiva 2000/31/CE sul commercio elettronico: in tema di composizione delle controversie la norma, infatti, attribuisce alle parti la facoltà di adire «anche organi di composizione extragiudiziale che operano anche per via telematica».
Certamente in materia di commercio elettronico, come anche in ambito di domìni Internet (*domain name*) si constata una esperienza apprezzabile di utilizzo dell'ODR, dovuta anzitutto a una *forma mentis* degli operatori sicuramente più predisposta.
In tale ambito, infatti, si annotano molte esperienze, dal VMAG (*the Virtual Magistrate*) nato nel 1996 negli Stati Uniti, all'attuale progetto della Camera Arbitrale della Camera di Commercio di Milano (a cui collaborano CNR, Ministero della Giustizia, Associazione Italiana Internet Providers, Fondazione Calamandrei), che è un vero e proprio arbitrato irrituale, con proprie procedure e caratterizzato da costi particolarmente contenuti.
Per arrivare alle esperienze nel Nord-Est si ricordano almeno due punti di riferimento: l'Associazione culturale per lo studio del Diritto in Friuli Venezia Giulia[6] e WebCuria, un servizio del Centro di mediazione e arbitrato di Curia Mercatorum in Veneto[7].
Vediamo ora dappresso quali istituti, in mancanza di un vero e proprio rito regolato in Italia da leggi specifiche, ci possano guidare tra i sentieri che conducono verso una procedura adattabile alla giustizia telematica.
Anzitutto la legge 5 gennaio 1994 n. 25, che – com'è noto – ha riformato il giudizio arbitrale, ha innovato l'art. 807 c.p.c. La norma ora riconosce come rispettata la forma scritta (come sappiamo, prevista a pena di nullità per compromesso, clausola compromissoria e deliberazione e redazione del lodo) anche quando la volontà delle parti è espressa per telegrafo o telescrivente.
La Suprema Corte nel 2000[8] ha più volte affermato che la clausola arbitrale può essere perfezionata in documenti separati, a distanza e in momenti diversi.
In verità già la Convenzione di New York del 10 giugno 1958[9], che ha regolato il riconoscimento e l'esecuzione delle sentenze arbitrali straniere, ammetteva – pur con il rispetto della forma scritta – la non necessità

della contestuale presenza delle parti.
La Convenzione di Ginevra del 1961[10], intitolata 'Convenzione Europea sull'arbitrato commerciale internazionale' non solo ha previsto la clausola compromissoria conclusa tramite scambi di comunicazioni a mezzo telescrivente, ma ha innovato introducendo l'ammissibilità delle convenzioni concluse con altri mezzi nei rapporti tra paesi le cui leggi non prevedono obbligatoriamente la forma scritta.
Il nostro Codice di procedura civile, a seguito delle modifiche introdotte dalla legge 25/94, ha aggiunto un capo (capo VI: art. 832 e seguenti)[11] che regola l'arbitrato tra parti di cui almeno una è residente all'estero; oppure prestazioni che devono essere eseguite in prevalenza all'estero.
In tali casi l'art. 832 c.p.c. prevede che si applichi la disciplina dell'arbitrato nazionale, ma con salvezza in ogni caso delle norme stabilite in convenzioni internazionali. Così facendo è introdotta nel nostro ordinamento dal 1994 un'apertura di fatto a una parziale deroga alla forma scritta *ad substantiam*.
Quanto alla forma delle deliberazioni, l'art. 823 c.p.c., che regola l'arbitrato nazionale, prevede espressamente che le decisioni debbano esser prese a maggioranza in conferenza personale.
L'art. 837 c.p.c., invece, in ambito di arbitrato internazionale, ammette che la conferenza personale possa essere anche videotelefonica.
Daniele Ricciardi in uno scritto pubblicato su «Diritto & Diritti»[12], esaminando le questioni inerenti la sede dell'arbitrato telematico, ha fornito un'interpretazione estensiva dell'art. 816 c.p.c., che attribuisce alle parti o, in subordine agli arbitri, il potere di stabilirne la sede. E ciò, secondo l'autore, in modo assolutamente autonomo rispetto ai luoghi dove effettivamente si trovano di volta in volta le parti o gli arbitri coinvolti. Si pensi, infatti, alla possibilità d'interloquire per via telematica a mezzo di strumenti portatili da luoghi diversi per ogni sessione dello stesso procedimento, addirittura fuori sede o in viaggio.
Ma nella realtà più recente sono state introdotte alcune norme – certamente di più ampio respiro – che da un lato agevolano l'arbitrato telematico, addirittura con il rispetto in qualche misura delle forme tradizionali; dall'altro impongono nuove regole e adempimenti di non poco momento.

- Il Testo Unico in materia di documentazione amministrativa è stato intro-

dotto con il Dpr 28 dicembre 2000, n. 445, ma i principi in esso contenuti in realtà erano applicabili fin dal 1997, e anche ai rapporti tra privati. La legge Bassanini[13], infatti, già nel 1997 affermava che «Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge».

- La direttiva 1999/93/CE, recepita solo con il D.Lgs. 23 gennaio 2002, n. 10[14], ha tracciato all'epoca un primo 'quadro comunitario per le firme elettroniche' e, per quanto qui c'interessa, all'art. 5 ha stabilito che le firme elettroniche 'certificate':
  - posseggono i requisiti legali di una firma in relazione ai dati in forma elettronica così come la firma autografa li possiede per i dati cartacei;
  - sono ammesse come prove in giudizio.

Sappiamo, infatti, che la firma cosiddetta 'pesante', cioè quella definitiva dall'art. 2, n. 2, della direttiva come 'firma elettronica avanzata', è identificata per soddisfazione dei requisiti di:
- essere connessa in maniera unica al firmatario;
- essere idonea ad identificare il firmatario;
- essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
- essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Anche per effetto dei software cui si abbina per il suo utilizzo la 'firma pesante', cioè certificata, nel senso appena espresso, possiede delle caratteristiche insostituibili, soprattutto nei casi di sottoscrizione a distanza o non contestuale. Infatti essa:
- garantisce l'identificazione di chi firma e, quindi, la provenienza del documento;
- garantisce l'immodificabilità del documento e, quindi, la sua integrità;
- consente di crittografare messaggi di posta elettronica, anche se contenenti allegati e, quindi, la riservatezza.

Sia il Dpr 445/2000 sia il D.Lgs. 10/2002, tuttavia, nel nome dell'apprezzabi-

lissimo scopo, sempre auspicato dai giuristi, di coordinare le norme in corpi legislativi omogenei, sono stati di recente abrogati (rispettivamente parzialmente e totalmente) con l'avvento del Codice dell'amministrazione digitale[15], di cui si parlerà a breve.

- Il Dpr 13 febbraio 2001, n. 123, ha introdotto il cosiddetto processo civile telematico, che in realtà coinvolgerà non solo il processo civile vero e proprio, ma anche il processo amministrativo ed il processo innanzi le sezioni giurisdizionali della Corte dei Conti. Il regolamento attuativo, previsto dall'art. 3, comma 3 del Dpr 123/01, come si diceva poc'anzi, è ancora una bozza non licenziata dal Ministro.
Ma quel che è certo è che le sette sedi designate dal governo per la sperimentazione (Bari, Bergamo, Bologna, Catania, Genova, Lamezia Terme e Padova) all'avvio giocheranno sul campo – o forse sarebbe più consono dire nella rete – le partite processuali vere e proprie.

- Il già richiamato D.Lgs. 9 aprile 2003, n. 70, attuativo della Direttiva 2000/31/CE sul commercio elettronico.

- Il Testo Unico in materia di protezione dei dati personali con il D.Lgs. 30 giugno 2003, n. 196[16], entrato in vigore nel suo corpo principale dal 1º gennaio 2004 ma, stante la 'lentezza' del nostro Paese ad assorbire la cultura della riservatezza, alcuni adempimenti sono slittati fino al marzo 2006.
Il Codice della privacy all'art. 31 e seguenti individua gli obblighi da osservare e le misure da adottare in tema di sicurezza dei dati e dei sistemi.

- Il D.Lgs. 17 gennaio 2003, n. 6, ha riformato la disciplina delle società di capitali e cooperative, introducendo principi innovativi quali quelli portati dall'ultimo periodo aggiunto del primo comma dell'art. 2388 del codice civile che indica che «lo statuto può prevedere che la presenza alle riunioni del consiglio avvenga anche mediante mezzi di telecomunicazione». In realtà la giurisprudenza aveva già in parte anticipato i tempi: troviamo, infatti, una decisione del Tribunale di Roma del 1997[17], la cui massima recita: «è legitti-

ma la clausola dello statuto di società a responsabilità limitata che prevede la possibilità che le riunioni del consiglio di amministrazione si svolgano per tele/videoconferenza, a condizione che tutti i partecipanti siano identificabili e possano intervenire in tempo reale nella discussione». La condizione posta dal Tribunale di Roma («che tutti i partecipanti siano identificabili e possano intervenire in tempo reale nella discussione») è fondamentale per comprendere quali devono essere i requisiti minimi per operare a distanza per formare sistemi giuridicamente validi.
Di recente, come si preannunciava, vi sono stati altri due importanti interventi:

- il Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3, introdotto con Dpr 11 febbraio 2005, n. 68 (in GU 28 aprile 2005 n. 97, s.o.), ha stabilito «le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata»;
- il Codice dell'amministrazione digitale, introdotto con D.Lgs. 7 marzo 2005, n. 82 (in GU 16 maggio 2005 n. 112, s.o.), è entrato in vigore il 1º gennaio 2006, ha confermato e rafforzato la dignità giuridica del documento elettronico.

Si pensi, infatti, alla portata dell'art. 6 del Codice (istituzionalizzazione dell'utilizzo della posta elettronica certificata nelle comunicazioni tra pubbliche amministrazioni e tutti i soggetti interessati che ne hanno fatto richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata) in uno con le norme che equiparano documento cartaceo e documento informatico (art. 20), che forniscono di valore probatorio il documento informatico (art. 21) e ancor più a tutte le disposizioni che tendono a sviluppare la 'cultura informatica' con iniziative per favorire la cosiddetta 'alfabetizzazione informatica dei cittadini' (art. 8), nonché la istituzionalizzazione della fornitura di una costante consulenza in materia ai ministeri competenti (art. 18).

A questo punto tutte le regole sembrano illuminare intermittenti la pista di decollo della giustizia (privata e pubblica) con mezzi telematici.

Proposte: naturalmente oggi dobbiamo immaginare una procedura elaborata con gli strumenti giuridici a nostra disposizione, ma è naturale immaginare che un Codice di procedura civile moderno[18], che recepisca al suo interno – anziché in un testo di legge diverso – il processo civile telematico, potrebbe anche regolare i metodi alternativi di risoluzione delle controversie a distanza, introducendo, oltre ai principi sopra richiamati, un foro competente (ad esempio quello del convenuto), un sistema di utilizzo di prove testimoniali (ad esempio quale quello utilizzato dal rito penale italiano in tema di investigazioni difensive: art. 391 bis e seguenti c.p.p. con audizione delle persone in videoconferenza – con le cautele sopra indicate della compresenza e possibilità di comunicare contemporaneamente – solo eventuale, a richiesta di almeno una delle parti e con provvedimento formale degli arbitri di ammissione, ove ritenuto assolutamente indispensabile) o di indagini tecniche.
Nel frattempo, tuttavia, è possibile contrattare elettronicamente a mezzo della firma digitale, inserendo una clausola arbitrale o conciliativa, attivare la procedura prevista e instaurare l'arbitrato *on-line*, stabilire la sede, scambiare memorie e documenti nel rispetto della riservatezza dei dati tramite posta certificata, raggiungere un'intesa o una decisione in forma digitale sottoscritta elettronicamente dagli arbitri a distanza. Eseguirla presso il Tribunale del luogo sede dell'arbitrato.
Naturalmente i procedimenti su base documentale non presenteranno particolari difficoltà.
Di diversa e maggiore difficoltà sarà per il momento l'utilizzo di prove orali, con introduzione di persone informate sui fatti o perizie. Questi soggetti in sede arbitrale tradizionale non prestano giuramento: pur con le difficoltà che non si possono sottovalutare, avendo a che fare con soggetti endoprocessuali (ma non parti processuali in senso stretto), spesso privi di firma digitale o di propensione agli strumenti informatici, la raccolta delle dichiarazioni potrà certamente avvenire a distanza, se del caso in videoconferenza, previa identificazione del dichiarante. Ad avviso del sottoscritto, salvo diverso accordo delle parti (esempio per l'utilizzo di dichiarazioni scritte e sottoscritte, purché identificato il dichiarante), certamente si dovrà assolve-

re alla condizioni di contemporaneità delle presenze dei partecipanti, di identificazione, di possibilità per ciascuno di intervento in tempo reale nella discussione.
Siamo a questo punto davvero pronti a lasciare a terra la carta e sollevarci verso l'extraterritorialità della rete?
Io penso che non ci resti che provare.

NOTE
[1] *Il Giudice Robot*, avv. Marco Boretti:
http://www.dirittosuweb.com/aree/rubriche/record.asp?idrecord=13&cat=11
[2] http://assoc.wanadoo.fr/astrid01/dictionnaire%20sorciere.htm#debut
La prima versione in ipertesto di *The Dictionary of Phrase and Fable* di E. Cobham Brewer tratta dall'edizione nuova e ampliata del 1894:
http://www.bootlegbooks.com/Reference/PhraseAndFable/data/175.html
[3] http://news.bbc.co.uk/1/hi/sci/tech/726837.stm
[4] http://www.ccbe.org/en/comites/it_law_en.htm
[5] Il testo è tratto da un'interessante tesi della scuola di specializzazione delle professioni legali presso la Facoltà di Giurisprudenza dell'Università di Firenze dal titolo *La Conciliazione Stragiudiziale tra Teoria e Prassi*, disponibile in Internet (http://www.fi.camcom.it/informazioni/Files/2052/Tesi%20per%20SITO%20CCIAA.doc); la tesi citata tratta ampiamente la materia e offre interessanti spunti e fonti.
[6] http://www.e-curia.it/tribunale/z.htm
[7] http://www.webcuria.com/
[8] Per tutte Cassaz., sez. I, 22/2/2000, n. 1989; Cassaz., sez. III, 19/12/2000, n. 15941.
[9] La cui adesione è intervenuta con la legge 19 gennaio 1968 n. 62 (pubblicata in GU 21/2/1968 n. 46).
[10] Ratificata ed eseguita con la legge 10 maggio 1970 n. 418 (pubblicata in GU 6/7/1070 n. 167).
[11] Art. 832 c.p.c: «qualora alla data della sottoscrizione della clausola compromissoria o del compromesso almeno una delle parti risieda o abbia la sede effettiva all'estero oppure qualora debba essere eseguita all'estero una parte rilevante delle prestazioni nascenti dal rapporto al quale la controversia si riferisce, le disposizioni dei capi da I a V del presente titolo si applicano all'arbitrato in quanto non derogate dal presente capo. Sono in ogni caso salve le norme stabilite in convenzioni internazionali».
[12] http://www.diritto.it/articoli/dir_tecnologie/ricciardi.html
[13] L'art. 15, comma 2, della legge 15 marzo 1997 n. 59 (cosiddetta 'Bassanini 1').
[14] E oggi abrogata per mano del Codice dell'amministrazione digitale, come si dirà *infra*.

[15] D.Lgs. 7 marzo 2005 n. 82 (in GU 16 maggio 2005 n. 112, s.o.).
[16] Pubblicato in GU, serie generale, n. 174 del 29 luglio 2003.
[17] T. Roma, 24/2/1997, Soc. Srd Internet Provider, in Società, 1997, 695, n. Colavolpe.
[18] E non la 'legislazione alluvionale', come è stata definita di recente sulla stampa, in occasione dell'avvento del D.Lgs. 80/2005, modificativo di alcune frammentarie quanto rilevanti regole procedurali.

TELEMATISCHE JUSTIZ- EINE KULTURELLE HERAUSFORDERUNG
Marco Vianello

Vorschläge: selbstverständlich müssen wir uns mit den zur Verfügung stehenden Rechtsmitteln heute eine komplizierte telematische Prozeßführung vorstellen, wobei es korrekt ist eine moderne Zivilprozeßordnung in Aussicht zu stellen, die imstande ist den telematischen Zivilprozeß in ihren eigenen- und nicht in einem getrennten-Gesetzestext einzugliedern. Der telematische Zivilprozeß könnte auch alternative Methoden für die Prozeßführung von Fernrechtsstreiten bieten und neben den oben aufgeführten Prinzipen auch folgende Leitaspekte einführen: ein zuständiger Gerichtshof (zum Beispiel der des Beklagten), ein System für die Aufnahme von Zeugenaussagen (wie es beispielsweise im italienischen Strafprozeß im Bereich der Verteidigungsbeweisführung eingesetzt wird: Artikel 391 bis und folgende der italienischen Strafprozeßordnung mit Zeugenverhör in Videokonferenz – mit den oben aufgezeigten Vorsichtsmaßnahmen wegen der gleichzeitigen Anwesenheit der zu verhörenden Personen und dem damit verbundenen Kommunikationsrisiko – und zwar nur in Ausnahmefällen, auf Anfrage mindestens einer Partei und mit einer formellen gerichtlichen Verfügung für die Zulassung der Schiedsrichter, soweit es als unerläßlich erachtet wird) oder technische Ermittlungsverfahren.
In der Zwischenzeit ist es möglich mit Hilfe der Digitalunterschrift auf elektronischem Wege zu verhandeln, wobei eine Schieds- oder Vergleichsklausel einzugeben ist, die vorgesehene Prozeßführung zu aktivieren und ein Online- Schiedsgericht einzurichten, den Gerichtshof festzulegen, Schriftsätze und Prozeßunterlagen zu versenden, wobei die versendeten Daten als bescheinigte Post geschützt sind, einen Vergleich zu schließen oder einen elektronisch von den Fernschiedsrichtern unterzeichneten Beschluß in Digitalform zu treffen. Und nicht zuletzt den so gefaßten Beschluß beim örtlichen Gerichtshof des Schiedsgerichts vollstrecken zu lassen.

Natürlich können Dokumentarprozesse auf diese Weise mehr oder weniger problemlos abgewickelt werden.
Kritischer ist derzeit der Einsatz der mündlichen Beweisführung mit Zeugen bzw. technischen Gutachtern. Diese Personen werden bei einem traditionellen Schiedsprozeß nicht vereidigt: trotz den hierbei auftretenden und nicht zu unterschätzenden Problematiken bei der Teilnahme von endoprozessuellen Individuen (nicht Klageparteien im engen Sinne), die oft über keine Digitalunterschrift verfügen bzw. mit dem Gebrauch von Datenverarbeitungssystemen nicht vertraut sind, kann die Einholung der Aussagen bzw. Stellungnahmen sicher auch im Fernverfahren erfolgen, zum Beispiel mit Hilfe von Videokonferenzen, wobei sich die jeweiligen Zeugen vorher ausweisen müssen. Ich bin in diesem Sinne der Meinung, dass mit Ausnahme einer anders lautenden Vereinbarung zwischen den Parteien (beispielsweise für den Einsatz von schriftlichen und unterschriebenen Erklärungen mit geeigneter Identifizierung des Unterzeichners) sicherlich alle Bedingungen für die gleichzeitige Anwesenheit der Teilnehmer, deren Identifizierung und der Möglichkeit für jeden einzelnen seine Beiträge an der Diskussion in Realzeit vortragen zu können geschaffen werden müssen.
Sind wir also tatsächlich bereits so weit den Papierprozeß seinem Untergang zu weihen und uns auf die Exterritorialität des Datennetzes zu verlassen?
Ich bin der Ansicht, dass es in jedem Fall einen Versuch wert ist.

TELEMATIKUS IGAZSÁGSZOLGÁLTATÁS: EGY KULTURÁLIS KIHÍVÁS
Marco Vianello

Az intézményes igazságszolgáltatás világa ma még óvatosan kezeli a telematikus polgári perek kérdését, és mint köztudott Olaszországban ez praktika még elindításra vár; csak azoknak az embereknek az agyában formálódik még éppen, akik ezzel hivatásszerűen foglalkoznak.
Érdemes itt megjegyezni, hogy a projekt még eszközhiányban szenved, és a mentalitás is változtatásra vár. Ezzel a kihívással nem tudunk szembenézni mindaddig, amíg az informatika kultúrája nem lesz elterjedt országunkban.
Az Európai Uniós Ügyvédi Kamarák Tanácsának (CCBE) Elektronikus Távközlésjogi Bizottsága által készített friss felmérés eredményei alapján az informatikai ismeretek és alkalmazások elterjedtsége a következő képet mutatja:

- *csak kevés országban (és sokszor ezekben is csak elméletben) van lehetőség a bírósági hivatalokkal történő digitális kommunikációra;*
- *kivéve néhány ritka esetet, az elektronikus kommunikáció a perben lévő felek között nem kivitelezhető;*
- *vannak viszont kezdeményezések, leginkább normatívak, mint gyakorlatiak, az elektronikus aláírás alkalmazására a hivatalos közleményekben;*
- *továbbá többnyire nincsenek, vagy hiányosak a on-line jogi szolgáltatások, viszont ahol megtalálhatók, ott a bírósági intézményes weboldalakon is elérhetők;*
- *az etikai kódex nem terjed ki az ilyen irányú on-line szolgáltatások kérdésére ill. az elektronikus kommunikációra általánosságban, kivéve Franciaországot; Olaszországot, Lengyelországot, Szlovákiát, Szlovéniát és Magyarországot;*
- *csak néhány ország intézményes bírósági szervezetében fejlesztettek ki Intranetet illetve belső kommunikációs rendszert, hogy ösztönözzék az elektronikus rendszerrel történő kommunikálást.*

Tehát időközben megérné kikísérletezni azokat az alternatív lehetőségeket, melyek a vitákra és nézeteltérésekre békítően hathatnának.

IL CODICE DELL'AMMINISTRAZIONE DIGITALE: NUOVI DIRITTI PER I CITTADINI E LE IMPRESE

Andrea Sirotti Gaudenzi

Sulla base della spinta data dal legislatore negli ultimi anni, si può affermare che l'informatizzazione del diritto amministrativo è in larga parte compiuto 'almeno sulla carta'. Prima ancora dell'emanazione del nuovo Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82), gli interpreti riconoscevano come l'utilizzo (diffuso) degli strumenti informatici e telematici potesse ben sostituire quelli 'tradizionali'. Solo per citare un esempio (assai significativo e in larga parte precursore di norme dettate dal nuovo Codice), è accaduto di recente che la giustizia amministrativa abbia dichiarato come l'onere di pubblicità di un procedimento fosse legittimamente assolto con la pubblicazione sulla Gazzetta Ufficiale di un avviso volto a rendere nota l'esistenza del procedimento, contenente un rinvio ad un sito Internet per la consultazione del bando integrale, delle istruzioni applicative e dei modelli da compilare (in tal senso si è pronunciato il TAR Lazio, sez. III, 8 marzo 2004, n. 2159, in «Giornale di diritto amministrativo», 2005).
Si avvertiva la necessità, tuttavia, di un *corpus* organico di norme che potesse sistematicamente indicare determinati obblighi di standardizzazione delle autorità amministrative e, al contempo, introducesse *expressis verbis* una serie di diritti soggettivi in capo ai cittadini.
Tale intento fortemente programmatico è espresso dall'art. 3 del Codice, che riconosce a cittadini ed imprese il diritto di 'richiedere' ed 'ottenere' «l'uso delle tecnologie dell'informazione e della comunicazione nei rapporti con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali».
Il primo concreto passo verso l'informatizzazione della Pubblica

Amministrazione e verso il riconoscimento di 'nuovi diritti' legati al cosiddetto *e-government* è rappresentato dalla legge 241/90. La legge 7 agosto 1990, n. 241 («Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi»), ha avuto il fondamentale ruolo di 'innovare radicalmente i rapporti tra Pubblica Amministrazione e cittadini', sviluppando appieno i supremi principi dettati dall'art. 97 della Carta costituzionale. La normativa nazionale si basava sulla raccomandazione n. 81/89 del 25 novembre 1981 del Comitato dei Ministri del Consiglio d'Europa che affermava il diritto di ogni persona ad ottenere, su sua richiesta, informazioni in possesso delle autorità pubbliche. L'originaria formulazione dell'art. 22 della legge 241/90, infatti, sanciva il riconoscimento del diritto di accesso ai documenti amministrativi a chiunque vi avesse interesse «per la tutela di situazioni giuridicamente rilevanti», con possibilità di esaminarli ed estrarne copia.
Nonostante talune interpretazioni puntassero ad affermare come il riconoscimento del diritto d'accesso fosse imprescindibilmente legato all'esistenza di una posizione qualificata nell'ambito del procedimento amministrativo, sembrò consolidarsi l'orientamento secondo cui il diritto di accesso doveva essere riconosciuto non solo a chi risultasse essere titolare di un diritto o interesse legittimo, ma anche nel caso in cui vi fosse una circostanza capace di incidere comunque sulla sfera giuridica dell'istante (TAR Lazio, 15 settembre 1993, n. 1534 in «Riv. Giur. Scuola», 1994).
Peraltro, si affermò l'opinione in virtù della quale il combinato disposto degli artt. 22 e 25 della legge 241/90 – prevedendo espressamente il diritto dell'interessato ad ottenere dalla Pubblica Amministrazione copia anche degli «atti interni o comunque utilizzati ai fini dell'attività amministrativa» – consentisse di estendere tale diritto anche agli atti dei procedimenti non ancora conclusi (TAR Calabria, Reggio Calabria, 9 ottobre 1993, n. 871 in «Foro Amm.», 1994), comprendendo anche gli atti interni e qualsiasi atto che, seppur non realizzato dalla Pubblica Amministrazione, venga usato per finalità inerenti all'attività amministrativa (TAR Lazio, Latina, 8 luglio 1994, n. 742 in «Foro Amm.», 1995).
Nel corso degli anni, quindi, «la giurisprudenza ha esteso il più possibile i

confini del diritto d'accesso», ogni qual volta l'istante fosse in grado di fornire un'adeguata evidenza alla natura dell'interesse che fosse in grado di radicare tale diritto (Cons. Stato, sez. IV, 20 maggio 2003, n. 2721), pur senza trasformare l'istituto in una sorta di azione popolare diretta a consentire una forma di controllo generalizzato sull'amministrazione (Cons. Stato, sez. VI, 30 maggio 2003, n. 3000).
Recentemente, la legge 11 febbraio 2005, n. 15 («Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa», pubblicata nella GU n. 42 del 21 febbraio 2005), nel riscrivere alcuni (importanti) passi della legge 241/90, ha tentato di ridefinire la categoria di soggetti cui riconoscere il diritto di prendere visione e di estrarre copia di documenti amministrativi, identificando gli interessati in «tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso». Come rilevato dalla miglior dottrina (Cammarata), la nuova formulazione della norma renderà sicuramente più complicato il riconoscimento e l'esercizio del diritto (l'«interesse» in grado di far sorgere il diritto dev'essere, infatti, «diretto, concreto e attuale»). Inoltre, non deve dimenticarsi che la novella sottrae all'accesso una serie di documenti amministrativi particolarmente corposa (si veda la nuova formulazione dell'art. 24 della legge 241/90).
Nonostante le recenti modifiche, il diritto d'accesso è pur sempre un diritto di fondamentale importanza nel nostro ordinamento, il cui pieno riconoscimento è possibile solo laddove la Pubblica Amministrazione sia concretamente in grado di far fronte alle richieste che pervengono da chi sia titolare del diritto, gettando le basi per una semplificazione dell'azione amministrativa e una maggiore efficienza nei rapporti tra Pubblica Amministrazione e cittadino.
Come chiarito da Taddei Elmi, «la nuova regolamentazione del diritto di accesso agli atti amministrativi trovi un fortissimo alleato nella informatizzazione totale della Pubblica Amministrazione», tant'è che non è oggi immaginabile una effettiva messa in pratica di quanto disposto dalla legge 241/90 in assenza del contributo degli strumenti informatici. E proprio gra-

zie agli apporti offerti dalla *new technology*, può affermarsi il concetto di 'amministrazione amica ed efficiente', forte di un impianto sistematico ed organico, che obbligherà – almeno nelle intenzioni degli autori del Codice – l'intera organizzazione ed i dipendenti pubblici non solo a fare ricorso all'informatica, ma ad accettarla quale principale strumento operativo.
Nel proprio parere del 7 febbraio 2005, il Consiglio di Stato ha rilevato come la bozza del Codice costituisse di un'opera di indubbio rilievo sistematico, «che può fornire ai cittadini, alle imprese e alle stesse pubbliche amministrazioni». In particolare, si è ritenuto che il Codice rappresentasse uno strumento fondamentale non soltanto per ottenere l'erogazione di servizi più efficienti e veloci, ma anche per «consentire forme innovative di partecipazione alla vita amministrativa e politica», con la conseguenza di mettere i destinatari dell'innovazione (i cittadini, le imprese, la società civile) nelle condizioni di avvicinarsi ai suoi protagonisti (gli amministratori, i funzionari e gli impiegati pubblici) «nella nuova 'amministrazione digitale', attraverso un intervento più tradizionale e di chiara leggibilità come è un codice, ossia una raccolta organica di disposizioni legislative».
Colpisce, in questo senso, la previsione di nuovi obblighi per le pubbliche amministrazioni, quale quello di scambiare *on-line* i dati relativi alle pratiche di cittadini ed imprese, evitando inutili percorsi tra i diversi uffici per ottenere documenti e certificati, o di l'attesa di mesi – come avviene oggi – prima che avvenga il trasferimento cartaceo delle pratiche tra le varie amministrazioni pubbliche. Conseguenza di ciò è la previsione per le pubbliche amministrazioni di riorganizzare i propri siti web in modo da individuare una serie di contenuti minimi e necessari, compresa la disponibilità di moduli e formulari per via telematica (in questo senso, rappresenta un notevole incoraggiamento la cosiddetta 'Legge Stanca').

I nuovi diritti
Nel solco di quanto introdotto dalla legge 241, la sezione II del Codice contiene un elenco di diritti soggettivi riconosciuti ai 'cittadini' ed alle 'imprese'. Colpisce la dizione utilizzata dal legislatore, il quale ha inteso menzionare sia i 'cittadini', che le 'imprese'.

I diritti enunciati dal Codice sono i seguenti:
- diritto all'uso delle tecnologie (art. 3);
- diritto a partecipare al procedimento amministrativo e diritto di accesso ai documenti amministrativi esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione (art. 4);
- diritto ad effettuare i pagamenti alle pubbliche amministrazioni centrali in forma digitale (art. 5);
- diritto ad ottenere l'utilizzo da parte delle pubbliche amministrazioni centrali delle comunicazioni tramite posta elettronica certificata (art. 6);
- diritto alla qualità del servizio e alla misura della soddisfazione (art. 7);
- diritto alla alfabetizzazione e diritto alla partecipazione (artt. 8 e 9).

Inoltre, non debbono tralasciarsi gli artt. 10 e 11 del Codice, che disciplinano – rispettivamente – gli Sportelli per le attività produttive e il Registro informatico degli adempimenti amministrativi per le imprese.
Come anticipato, l'art. 3 del Codice, con una norma dal contenuto decisamente dirompente, definisce i contenuti del diritto all'uso delle tecnologie, disponendo che sia i cittadini sia le imprese hanno «diritto a richiedere ed ottenere l'uso delle tecnologie telematiche» nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali. Il tutto può avvenire nei limiti di quanto previsto dal Codice.
Il contenuto dell'art. 3 si sposa agli *imput* comunitari in tema di *e-government*, ovvero l'uso di Tecnologie dell'Informazione e della Comunicazione (TIC) nelle amministrazioni pubbliche associato a cambiamenti a livello organizzativo e all'acquisizione di nuove competenze da parte del personale, con l'obiettivo di migliorare i servizi al pubblico, rafforzare il processo democratico e sostenere le politiche pubbliche (si veda, in tal senso: Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale e al Comitato delle Regioni del 26 settembre 2003. *Il ruolo dell'*e-government *per il futuro dell'Europa*). Il passaggio necessario per rendere praticabile il diritto all'uso delle tecnologie è rappresentato dalla possibilità che tutti i cittadini abbiano accesso ai servizi pubblici. Forse è proprio questo l'obiettivo più ambizioso (e più complicato da realizzare) della Pubblica Amministrazione (si veda l'art. 8 del Codice). Solo un

accesso effettivo a tutti i cittadini e a tutte le imprese consente di evitare la formazione di una nuova frattura sociale (temuta nel piano d'azione 'e-Europe 2005').
L'art. 4 offre agli utenti la possibilità di «partecipare al procedimento amministrativo e il diritto di accesso ai documenti amministrativi» tramite l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli artt. 59 e 60 del Dpr 28 dicembre 2000, n. 445.
La conseguenza di tale possibilità è che ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione, se formato ed inviato nel rispetto della vigente normativa (art. 4, comma secondo).
Alla luce di quanto anticipato, è importante rilevare come l'art. 41 del D.Lgs. 5 marzo 2005, n. 82, imponga alle pubbliche amministrazioni di gestire i procedimenti amministrativi «utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente», prevedendo peraltro come all'atto della comunicazione dell'avvio del procedimento ai sensi dell'art. 8 della legge 241/90, vengano comunicate agli interessati le modalità per esercitare in via telematica i diritti previsti dall'art. 10 della stessa legge in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
L'art. 5 prevede che, con decorrenza 30 giugno 2007, «le pubbliche amministrazioni centrali con sede nel territorio italiano consentono l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione». L'art. 38 del Codice, nel disciplinare la materia dei pagamenti informatici, dispone che il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati verrà effettuato secondo le regole tecniche stabilite ai sensi dell'art. 71.
Il Codice si occupa anche dell'utilizzo della posta elettronica certificata (a tal proposito, si vedano le note di Vicenzotto pubblicate nel numero 1/2005 di questa rivista). Come noto, l'*e-mail* (acronimo di *Electronic Mail*) è oggi la forma di comunicazione più frequentemente utilizzata nell'intero globo. Grazie ad Internet, questo strumento consente di trasmettere informazioni,

documenti, immagini con una velocità sorprendente. Grazie al Dpr 11 febbraio 2005, n. 68, il legislatore ha disciplinato la Posta Elettronica Certificata (PEC), vale a dire un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.
Vengono così 'certificati' i due momenti fondamentali nella trasmissione dei documenti informatici, ovvero: a) l'invio e b) la ricezione.
L'art. 6 del nuovo Codice consente ai soggetti interessati che ne fanno richiesta di usufruire dello strumento offerto dalla posta elettronica certificata «per ogni scambio di documenti e informazioni» con le pubbliche amministrazioni centrali. Condizione imprescindibile è che tali soggetti abbiano preventivamente 'dichiarato' il proprio indirizzo di posta elettronica certificata. Tali disposizioni si applicheranno anche alle pubbliche amministrazioni regionali e locali, sempre che non sia diversamente stabilito.
L'art. 7 del Codice rafforza il diritto sancito dall'art. 3, mettendo le pubbliche amministrazioni centrali nelle condizioni di dover provvedere alla «riorganizzazione ed all'aggiornamento» dei servizi resi, nell'ottica dello sviluppo dell'utilizzo delle «tecnologie dell'informazione e della comunicazione». Per far questo, il Codice indica la strada della «preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti». Si delinea quindi, l'affermazione di un modello che segue il «sistema di qualità», già indicato dal legislatore nazionale in altre fonti (per tutte, si veda il DPCM del 16 gennaio 2002 sulle procedure di sicurezza nella gestione del patrimonio informativo delle pubbliche amministrazioni).
L''obbligo positivo' imposto alle pubbliche amministrazioni centrali viene ancor più rafforzato dalla previsione in ordine alla trasmissione – entro il 31 maggio di ciascun anno – di una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie.
Come indicato nel 2003 dalla Commissione Europea, l'istruzione e la formazione sono elementi indispensabili per garantire che i cittadini dispongano delle necessarie conoscenze in informatica per poter trarre beneficio dai

servizi offerti dalla rivoluzione digitale (Comunicazione del 26 settembre 2003). Tuttavia, colpisce la formulazione dell'art. 8 del Codice dell'amministrazione digitale, che sembra disporre come lo Stato promuova le iniziative volte a favorire l'alfabetizzazione informatica dei cittadini, non solo per favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni, ma per renderli realmente partecipi dei cambiamenti portati dall'*information technology.*
Il Codice prevede anche un diritto alla partecipazione democratica elettronica (art. 9), imponendo allo Stato di favorire l'uso delle nuove tecnologie «per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi».

KODEKS DIGITALNE UPRAVE: NOVE PRAVIC FIZIČNIH IN PRAVNIH OSEB

Andrea Sirotti Gaudenzi

Po močni spodbudi zakonodajalca v preteklih letih, lahko zaključimo, da je informatizacija upravnega prava, vsaj na papirju, v večji meri že zaključena. Še pred objavo novega «Kodeksa digitalne uprave» (Zakonodajni odlok št. 82 z dne 7. marca 2005), so tolmači zakona zaključili, da bi (razširjena) uporaba informacijskih in telekomunikacijskih sredstev lahko kvalitetno zamenjala 'tradicionalna' sredstva. Navedimo le en dokaj pomemben primer, ki je v večji meri tudi botroval novim določbam, ki jih predpisuje novi Kodkes: Nedavno je upravno sodišče izjavilo, da je obveznost oglaševanje postopka izpolnjena z objavo oglasa o potekanju postopka v Uradnem listu ter povezavo na spletno stran, na kateri je objavljeno celotno besedilo razpisa, navodila za prijavo ter obrazci za izpolnjevanje. To je potrdilo tudi Tretji odsek Deželnega upravnega sodišča v Laziu, s sodbo št. 2159, z dne 8. marca 2004, v «Giornale di diritto amministrativo», 2005).
Vendarle je bilo čutiti potrebo po poenotenem korpusu določil, s katerimi bi se sistematično določile obveznosti upravnih organov glede standardizacije ter bi se izrecno določile pravice državljanov.

ASSOCIAZIONE CULTURALE PER LO STUDIO DEL DIRITTO

da tre lustri la cultura del diritto nell'innovazione tecnologica

Per informazioni: Vicolo Chiuso 5, Pordenone
tel. 0434 522866 - fax 0434 246429 - associazione@e-curia.it - www.e-curia.it

CORSI	DESTINATARI
Il trattamento *ex lege* dei dati personali nelle Pubbliche Amministrazioni e nelle imprese: privacy, misure minime di sicurezza e formazione obbligatoria ai sensi dell'Allegato B al D.lgs 196/03 (art. 19.6) Tecniche di redazione di Documento Programmatico sulla Sicurezza nel trattamento dei dati personali	- Enti Pubblici Territoriali e Istituzionali - Aziende Sanitarie e Ospedaliere - Strutture sanitarie private - Imprese - Associazioni di categoria - Professionisti
Il nuovo *"Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti"* pubblicato nella G.U. n. 300 del 23 dicembre 2004. I problemi e le tutele accordate agli utenti inseriti nelle banche dati del rischio creditizio. Gli obblighi del gestore della banca dati	- Istituti di credito - Gestori di banche dati sul rischio creditizio
Il nuovo *"Codice delle Amministrazioni Digitali"*. Aspetti giuridici e pratici del documento elettronico, della firma digitale e posta elettronica certificata	- Enti Pubblici Territoriali e Istituzionali - Aziende Sanitarie e Ospedaliere
Il futuro degli acquisti nelle Pubbliche Amministrazioni. Sistemi di e-procurement (D.P.R. 101/2002) e acquisti sottosoglia	- Enti Pubblici Territoriali e Istituzionali - Aziende Sanitarie e Ospedaliere

Condizioni di abbonamento

Abbonamento annuale (3 numeri): € 20,00 IVA inclusa.
L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri relativi all'annata. Il pagamento può avvenire con versamento sul conto corrente n. 62833595 - Banco Posta, Via S. Caterina, 8/10 - 33170 Pordenone - ABI 07601, CAB 12500, intestato a: Associazione Culturale per lo Studio del Diritto. Causale: *Abbonamento rivista Techne 2005*.
L'abbonamento si intende rinnovato per l'anno successivo se non disdetto entro 1 mese dalla scadenza. I fascicoli non pervenuti devono essere reclamati al ricevimento del fascicolo successivo. Le variazioni di indirizzo vanno comunicate all'editore.

Pubblicità

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

La vignetta di Federico Cecchin

COPIA OMAGGIO

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

PROMOZIONE
ABBONAMENTI 2006

Condizioni di abbonamento
Abbonamento annuale (3 numeri): e 20,00 IVA inclusa.
L'abbonamento decorre dal 1 gennaio di ogni anno e dà diritto a tutti i numeri relativi all'annata. Il pagamento può avvenire con versamento sul conto corrente n. 62833595 - Banco Posta, Via S. Caterina, 8/10 - 33170 Pordenone
ABI 07601, CAB 12500, intestato a: Associazione Culturale per lo Studio del Diritto.
Causale: Abbonamento rivista Techne 2006.