focus .it

newsletter del Registro del ccTLD .it

anno 0 n.1 - Nov. 2004

sotto controllo

Registro del ccTLD.it

sommario / summary

3 **il punto / *the point***
di Anna Vaccarelli

4 **il fatto / *the fact***

".eu" aspettando l'alba

".eu" waiting for the sunrise

8 **diritto in rete / *law online***

la parrocchiana,
internet e la privacy

the parishioner,
the internet and privacy

14 **primo piano / *feature***

whois,
navigare a vista

whois,
contact surfing

22 **tecnica / *tech corner***

spam, l'importante è prevenire

spam, prevention is the key

27 **eventi / *events***

il gotha di internet alla settima assemblea del registro

the internet elites for the seventh assembly of the registrar

focus .it
newsletter del Registro del ccTLD .it

Anno 0, numero 1
Novembre/November 2004

Direttore responsabile
Director in charge
Prof. Franco Denoth

Responsabile di redazione
Editing
Luca Trombella

Progetto grafico, impaginazione e elaborazione immagini
Graphics , paging and image processing
Patrizia Andronico

Fotografie
Photos
Maurizio Papucci

Hanno collaborato a questo numero
This number publications board
Ana Corujo, Stefania Fabbri, Daniela Medda, Francesca Nicolini

Si ringrazia per la preziosa collaborazione
Special thanks
"Quark"; Michael Mann, Ingeborg Gaspard, Anna Parmegiani (Commissione Europea)

Stampa
Printed by
Tipografia Digiprint Srl
Piazza Dossetti 7
56012 Calcinaia (PISA, IT)

Redazione
Publication office
Registro del ccTLD .it
Relazioni Esterne

Via G. Moruzzi, 1
I-56124 Pisa
tel. +39 050 313 98 11
fax +39 050 315 27 13
e-mail: newsletter@nic.it
website: http://www.nic.it/

Iscrizione al Tribunale di Pisa n. 2141 del 17 settembre 2004 (richiesta di variazione depositata il 18 ottobre 2004)

Stampato su carta ecologica
Printed on ecologic paper

Chiuso in redazione
Closed for printing
17 november 2004

la memoria della rete e il diritto all'oblio

di **Anna Vaccarelli**
Responsabile della Unità Relazioni Esterne del Registro del ccTLD ".it" / *Head of ccTLD ".it" Registry External Relations*

La prima novità l'avete tra le mani: questo numero di "Focus .it". Una newsletter nuova nel titolo come nei contenuti, nella veste grafica come nel taglio redazionale. Per il Registro essa è il simbolo di un impegno che si rinnova, focalizzandosi sulle esigenze, sulle richieste, sulle proposte, sugli argomenti "caldi" dei suoi registrar. Un impegno che ha assunto e assumerà diverse forme, dalla costituzione della Commissione Regole alla liberalizzazione dei nomi a dominio per i privati cittadini. E che ha come fine ultimo favorire e migliorare la comunicazione tra noi e voi.

"Focus .it", così come la newsletter che l'ha preceduta, ha un indirizzo e-mail dedicato: **newsletter@nic.it**. A oggi, invero, vi ho trovato solo spam e qualche sporadica richiesta di aiuto che reindirizzo alla struttura tecnica. L'auspicio è che torni a essere un canale di comunicazione con i registrar per dare contenuti utili e interessanti alla newsletter. Noi abbiamo delle idee: vorremmo conoscere le vostre.

Per il momento siamo certi di aver letto nei vostri pensieri scegliendo di trattare, tra i tanti, l'argomento della privacy: focalizzando l'attenzione (è il nostro motto oltre che... il nostro titolo) sulla tutela dei dati personali nell'era di Internet. La Rete può rappresentare, nelle sue espressioni deteriori, una costante minaccia alla nostra privacy: essa è memoria, oltre che fonte di fatti, di dati e di notizie. La diffusione di un singolo brandello di informazione non violerà i nostri diritti. Ma l'aggregazione dei dati può diventare critica, rubandoci una parte della nostra identità e negando persino il diritto all'oblio.

Abbiamo raccolto il parere del Garante della privacy, di esperti legali, di tecnici del settore e di informatici del Registro. E abbiamo dato spazio anche ad argomenti più tecnici, benché legati alla tutela dei dati sensibili, come i suggerimenti per la configurazione di un server di posta elettronica blindato contro lo spam.

Il primo numero di "Focus .it" è anche l'ultimo del 2004. Per me e per tutto lo staff del Registro è un'occasione preziosa per augurarvi una buona fine d'anno e un 2005 all'insegna dei migliori auspici.

the memory of the web and the right to oblivion

The first piece of news is in your hands now: this issue of "Focus .it". A newsletter with a new title, new contents, a new graphic design and a new approach. For the Registry, it is the symbol of the new efforts focussed on the requirements, the demands, the proposals, the "hot" issues of its registrars. Efforts that have taken and will take different forms, from the establishment of the Rules Committee to the liberalisation of domain names for private people. Whose ultimate purpose is to promote and improve communication between you and us.

"Focus .it", just like the old newsletter, has a dedicated email address: ***newsletter@nic.it*** *. So far indeed I have only found spams and a few occasional calls for help that I send on to our technical unit. Our hope is that it will be again a communication channel for registrars, giving useful and interesting contents to the newsletter. We have ideas: we would like to know about yours.*

For the time being, we are sure we have read your minds when we decided to speak of privacy: we preferred to focus our attention (it is our motto as well as...our name) on the protection of personal details in the Internet age. The web at its worst can be a relentless threat to our privacy. It is the memory, as well as the source, of facts, data and news. The spread of a single scrap of information will not breach our rights. But putting information together can become critical, stealing part of our identities and denying even the right to oblivion.

We have asked the opinions of the privacy watchdog, legal experts, industry professionals and Registry's computer scientists. And we have given space to more technical issues as well, although they relate to the protection of sensitive information, such as suggestions for configuring a spam-proof email server.

The first issue of "Focus .it" is also the last one of 2004. For me and all the staff at the Registry, it is an invaluable opportunity to wish you a great winter 2004 and a most successful 2005.

La lunga corsa al dominio europeo

Tappa su tappa le date (stimate e non ancora ufficiali) del cammino verso la registrazione dei nuovi domini europei.

Dicembre 2004 - Conclusione delle trattative con ICANN per inserire il nuovo dominio ".eu" nel root nameserver e garantirne così la piena raggiungibilità.

Febbraio / Marzo 2005 - Varo delle norme per la risoluzione alternativa delle dispute (Adr). Traduzione del contratto con i registrar e delle procedure di registrazione in tutte le lingue ufficiali dell'Unione. Accreditamento dei primi operatori i cui nomi saranno pubblicati sul sito di Eurid.

Aprile 2005 - Sviluppo del sito Internet di Eurid (www.eurid.org) che conterrà tutte le informazioni chiave per la registrazione dei domini a targa ".eu".

Firmato a Bruxelles il contratto che rende operativo il nuovo dominio Internet comunitario. Colasanti (Ue): "Entro il prossimo anno via alle registrazioni per imprese, organizzazione e privati"

".eu", aspettando l'alba

di Daniela Medda

Entro il 2005 l'Europa avrà la sua targa Internet. La firma del contratto di servizio tra EURid e l'Unione Europea, siglato il 12 ottobre scorso a Bruxelles dal direttore generale della Società dell'Informazione dell'Ue, Fabio Colasanti, e dai rappresentanti delle tre *anime* del consorzio (Franco Denoth per l'Istituto di Informatica e Telematica del Cnr di Pisa, Pierre Verbaeten per il registro belga Dns.be e Ander Janson per il registro svedese Nic.se) – chiude la lunga parentesi d'attesa e regala all'associazione la sospirata, piena operatività. Colasanti non ha mancato di sottolineare l'importanza dell'evento, uno degli ultimi passaggi critici verso l'attuazione del sospirato *top level domain* comunitario. "Questo accordo – ha evidenziato – rappresenta un passo importante verso la disponibilità del ".eu". Con il Registro pienamente operativo le imprese, le organizzazioni e i privati cittadini dell'Unione Europea saranno finalmente in grado di registrare i propri nomi a dominio sotto il TLD comunitario entro l'anno prossimo".

EURid (acronimo di European Registry of Internet Domain Names), organizzazione no-profit scelta dall'Ue il 21 maggio 2003 per la gestione dei domini *made in europe*, è ora in grado di intraprendere tutte le azioni necessarie per predisporre un servizio di registrazione rapido, puntuale ed efficiente. Nel fitto calendario di iniziative che precederanno la nascita del dominio europeo c'è innanzitutto la stipula dell'accordo con Icann, il gestore della rete a livello mondiale che dovrà garantire la piena raggiungibilità dei futuri siti ".eu": un passo fondamentale che potrebbe concretizzarsi già in occasione del prossimo meeting Icann in programma il primo dicembre a Cape Town, in Sudafrica.

Altro impegno del consorzio sarà quello di accreditare i provider tramite i quali imprese e cittadini potranno registrare

Eurid è un'associazione *no-profit* costituita nell'aprile del 2003. Ne sono soci fondatori l'**Istituto di Informatica e Telematica** del Cnr di Pisa, gli svedesi di **Nic.se** (Network Information Centre) e i belgi di **Dns.be** (Domain Name Registration Services Belgium). Nel maggio del 2003 l'Unione Europea ha affidato al consorzio la gestione del dominio continentale a targa ".eu": si è trattato in assoluto della prima concessone di pubblico servizio nella storia dell'Ue.

Eurid opererà esclusivamente attraverso una rete di "registrar", al fine di incentivare la concorrenza. Le prospettive del dominio ".eu" sono enormi: l'associazione stima un potenziale di un milione di registrazioni nel solo primo anno di attività.

Maggio 2005 - Annuncio ufficiale della data d'inizio del Sunrise period e delle relative regole di registrazione.

Luglio / Agosto 2005 - Inizio della "fase uno" del Sunrise period (durerà due mesi): priorità di registrazione per gli organismi pubblici e i titolari di marchi registrati.

Ottobre / Novembre 2005 - A due mesi dal varo del Sunrise period, via alla "Fase due": potranno registrarsi sotto il ".eu", oltre ai titolari di marchi registrati e gli enti pubblici, anche i titolari di altri diritti tutelati dalle leggi nazionali degli stati membri.

Fine 2005 - Chiusura del Sunrise period (durata prevista: quattro mesi). Apertura delle registrazioni a tutti coloro che ne faranno richiesta secondo il meccanismo del "first-come, first-served".

i propri domini a targa ".eu": non appena disponibile, il contratto verrà pubblicato sul sito . Non secondarie le questioni tecniche, tra cui la traduzione delle informazioni chiave sul nuovo dominio in tutte le lingue ufficiali dell'Ue (che, come noto, con l'allargamento sono passate da 9 a 20).

Poi, finalmente, l'alba: e l'inizio del sospirato *Sunrise period*. Il periodo delle pre-registrazioni sarà articolato in due fasi, di due mesi ciascuna, aperte a chi detiene diritti di prelazione: prima sarà il turno dei nomi per esteso e degli acronimi relativi a pubbliche amministrazioni, marchi registrati a livello nazionale o comunitario e delle indicazioni geografiche; poi, a seguire, toccherà ad aziende, opere letterarie e artistiche, marchi non registrati. Terminato il *Sunrise*, il dominio europeo spalancherà le porte a organizzazioni e privati cittadini appartenenti ai 25 paesi membri dell'Ue. Il criterio con cui verranno effettuate le registrazioni sarà il noto "first come, first served": con il rispetto rigoroso dell'ordine cronologico di arrivo delle richieste.

Due lettere, un simbolo

di **Franco Denoth**
direttore dell'Istituto di informatica e telematica del Cnr di Pisa

Una targa Internet per l'Europa: capace di unire sotto la stessa bandiera la tecnologia, il know-how, il valore aggiunto che da sempre contraddistingue la produzione intellettuale e materiale del Vecchio Continente.

Oggi che il dominio ".eu" vive la sua alba, l'associazione Eurid si appresta finalmente a raccogliere i risultati di due lunghi anni di lavoro. Un'operazione complessa ma che ha solide radici: quelle esperienze specifiche in materia di registrazione dei nomi a dominio che le tre anime di Eurid - l'Istituto di informatica e telematica del Cnr di Pisa (gestore tra l'altro del Registro italiano dei nomi a dominio sotto il ccTLD ".it"), i belgi di Dns.be e i colleghi svedesi di Nic.se - hanno saputo fondere ed esaltare, proponendo alla Commissione europea una soluzione a tutto campo e di ampie prospettive.

La strada, da quel lontano 25 ottobre 2002 quando Eurid depositò ufficialmente la propria candidatura, non è stata sempre in discesa. Tra la concessione del servizio (il primo del settore pubblico nella storia dell'Ue) del maggio 2003 alla firma del contratto operativo (ottobre 2004) sono passati lunghi mesi: necessari, però, per armonizzare le differenti vedute sulla gestione del suffisso ".eu" che hanno contraddistinto i paesi membri dell'Europa allargata.

Eurid, da parte sua, non ha sprecato tempo, presentandosi all'appuntamento con la firma con già in tasca un pacchetto di regole di politica pubblica (le cosiddette public policy rules) concordate con l'Ue. Su di esso si fonderanno la stabilità e l'efficienza del sistema Internet made in Europe.

L'Istituto di informatica e telematica, realtà dinamica nel settore delle tecnologie dell'informazione, è pronto a raccogliere la nuova sfida, forte dell'entusiasmo con il quale la comunità, italiana ed europea, ha accolto la nascita del suo nuovo segno distintivo: due lettere, una targa che la accompagnerà per sempre nel lungo viaggio nella rete delle reti.

".eu", waiting for the sunrise

Signed in Brussels the agreement to operate the new EU Internet domain: "Registrations for businesses, organisations and citizens open by next year"

by Daniela Medda

"Pierre Verbaeten (left) shaking hands with Fabio Colasanti: Eurid finally becomes operational." (Photo: courtesy of European Commission Press and Communication Unit)

"Pierre Verbaeten (a sinistra) e Fabio Colasanti si stringono la mano: Eurid entra finalmente nella fase operativa." (Foto: Uff. stampa e comunicazione della Commission Europea)

By 2005, Europe will have its own EU number-plate. The signing of the service agreement between EURid and the European Union which took place in Brussels on October 12th between the general manager of the EU Information Society, Fabio Colasanti, and delegates from the three *souls* of the association (Franco Denoth for the Informatics and Telematics Institute at the National Research Council in Pisa, Italy, Pierre Verbaeten for the Belgian Registry, Dns.be, and Ander Janson for the Swedish registry, Nic.se) – closes this long wait and gives the association its long-awaited full operation.

Colasanti did not fail to recall the importance of the event, one of the last critical steps towards the implementation of the much yearned-for EC *top-level domain*. "This

Eurid is a *non-profit* association established in April 2003. Its founding partners are the **Informatics and Telematics Institute** at CNR (National Research Council) in Pisa, the Swedish **Nic.se (**Network Information Centre) and the Belgian **Dns.be (**Domain Name Registration Services Belgium).
In May 2003, the European Union appointed the association to manage the ".eu" continental domain: it was the very first time a public service was granted in the history of the EU.
Eurid will only work through a network of "registrars", in order to boost competition. The prospects of the ".eu" domain are huge: the association expects a number of one million registration in the first year alone.

The long race to the European domination

Step after step, the (estimated, not official yet) dates along the path to the registration of the new European domains.

December 2004 - Closing of negotiations with Icann to include the new ".eu" domain in the root nameserver to ensure it will be fully accessible.

February / March 2005 - Launch of regulations on alternative dispute resolution (Adr). Translation of the agreement with registrars and registration procedures into all official EU languages. Accreditation of first operators whose names will be published in the web site of Eurid.

contracts – he added – is an important step towards the availability of .eu. This will permit the Registry to become fully operational so as to ensure that businesses, organisations and citizens in the European Union are able to register their domain names within the .eu TLD by next year".

EURid (which stands for European Registry of Internet Domain Names), a non-profit organisation appointed by the EU on May 21st 2003 as manager of the European domains, can now do all it takes to develop a quick, efficient and accurate registration service. In the tight schedule of initiatives in the run-up to the establishment of the European domain, one of the most important is the signing of the agreement with Icann, the world's web manger that will have to ensure that the future ".eu" web sites will be perfectly accessible: a key step that could become a reality even during the next Icann meeting due in Cape Town, South-Africa, on December 1st.

The association also undertook to accredit the providers through which the businesses and citizens will be able to register their ".eu" domains: as soon as it is available, the agreement will be published on . And technical matters are not to be underestimated, first and foremost the translation of key information on the new domain into all the official EU languages (which, as everybody knows, after the accession have risen from 9 to 20).

Two letters, one symbol

by **Franco Denoth**
Director of the Informatics and Telematics Institute at CNR (National Research Council) in Pisa

An Internet numberplate for Europe: successfully bringing together, under one flag, the technology, the know-how, the added value that has always been the trademark of the intellectual and material production of the Old Continent. Now that the ".eu" domain is at its dawn, at last Eurid is getting ready to reap the fruits of two long years of work. A complex operation that has deep roots: those specific experiences in domain name registration that the three souls of Eurid – the Informatics and Telematics Institute at CNR (National research Council) in Pisa (which also manages the Italian Registry of ccTLD ".it" domain names), the Belgians with Dns.be and the Swedish with Nic.se – have successfully combined and enhanced by submitting to the European Commission a far-ranging, bright solution.
Since the distant 25th October 2002, when Eurid officially sent in its nomination, the road has not always been downhill. Long months have passed from the granting of the service (the first public one in the history of the EU) in May 2003 to the signature of the executive agreement (October 2004), which were necessary, however, to reconcile the different views of the management of the ".eu" suffix of each member country of the broader Europe.
Eurid on its part has wasted no time and has showed up on the set date, ready with a signed package of public policy rules agreed with the EU. The stability and the efficiency of the made in Europe *Internet system will be based on them. The Informatics and Telematics Institute, a dynamic actor of the information technology market, is ready to rise to the new challenge, relying on the enthusiasm with which the Italian and the European Community have welcomed the birth of its new trademark: two letters, a numberplate that will travel with it forever through the network of networks.*

Then, the sunrise, at last: and the beginning of the longed-for *Sunrise period*. The pre-registration period will consist of two phases, lasting two months each, open to those who have pre-emptive rights: the first registrations will be open to full names and acronyms of public administrations, nation-wide or EC-wide registered trademarks and geographical names, followed by companies, literary and artistic works, unregistered marks.

After the *Sunrise* period, the European domain will open its doors wide to organisations and citizens from the 25 EU member countries. Registrations will be on a "first come, first served" basis, strictly following the chronological order in which applications are received.

April 2005 - Development of the web site of Eurid (*www.eurid.org*) containing all key information for ".eu" domain registration.

May 2005 - Official announcement of the starting date of the *Sunrise period* and attendant registration rules.

July / August 2005 - Start of "phase one" of the *Sunrise period* (due to last two months): registration priority to public organisations and trademark holders.

October / November 2005 - Two months after the launch of the *Sunrise period*, start of "Phase two": as well as public organisations and trademark holders, also holders of other rights protected by the national regulations of the member states can register under ".eu",

La Rete come il far west? L'avvocato specialista nella tutela dei dati personali smentisce il luogo comune. E, citando un caso emblematico, rilancia: "La visibilità globale del web aumenta il rischio di incappare nei rigori della legge".

la parrocchiana, internet e la privacy

di Patrizio Menchetti

Secondo una delle leggende metropolitane correnti Internet é una specie di far west telematico, un cyber-spazio dove le norme del mondo off-line, comprese quelle sulla privacy, non troverebbero applicazione. Da un punto di vista giuridico questa è sicuramente una affermazione impropria; tutto ciò che è illecito off-line lo è anche on-line, e il cyberspazio esiste solo nei libri di fantascienza di William Gibson.

In realtà le attività su Internet, proprio grazie alla loro visibilità globale, sono più soggette ad incappare nei rigori della legge. E il caso di una signora svedese preso in esame dalla Corte di Lussemburgo lo dimostra ampiamente.

La signora in questione, il cui nome non può essere fatto in questa sede (c'é la legge sulla privacy), lavorava come volontaria in una parrocchia svedese come formatrice di comunicandi. La signora aveva seguito un corso di informatica e aveva creato, a casa sua e con un personal computer, un sito Web composto di alcune pagine allo scopo di consentire ai parrocchiani che si preparavano alla cresima di ottenere facilmente le informazioni di cui avevano bisogno. Le pagine contenevano informazioni sulla signora in questione e su 18 suoi colleghi della parrocchia, con il loro nome e cognome oppure soltanto il nome.

La signora aveva anche riportato sul sito, in termini scherzosi, le mansioni dei colleghi e le loro abitudini nel tempo libero. In molti casi era inoltre descritta la loro situazione familiare, erano indicati i loro recapiti telefonici ed erano presenti altre informazioni su di loro. In particolare veniva riferito il fatto che una collega, essendosi ferita ad un piede, era in congedo parziale per malattia. La signora non

Patrizio Menchetti, 48 anni, è avvocato del foro di Milano e membro del *Legal advisory board* della direzione generale "Società dell'Informazione" della Commissione Europea. Laureato in legge "magna cum laude" all'Università di Siena, egli è professore a contratto di diritto commerciale e membro del comitato ordinatore nel master in diritto della Rete istituito dall'Università di Padova. Menchetti opera prevalentemente nei settori delle tecnologie dell'informazione, telecomunicazioni, protezione dei dati personali, antitrust, proprietà industriale e nell'ambito più generale delle questioni legate all'alta tecnologia.

Nel corso della sua attività professionale egli ha assistito operatori di telecomunicazioni italiani ed esteri e alcuni Internet provider per le problematiche relative a regolamentazione, proprietà industriale ed intellettuale e privacy, e operatori nel settore dei media per questioni relative a protezione dei dati personali e proprietà industriale ed intellettuale. È stato inoltre incaricato dalla Commissione Europea della verifica della liberalizzazione delle telecomunicazioni in Lussemburgo.

aveva informato i suoi colleghi, né aveva chiesto il loro consenso. Inoltre, non aveva notificato il trattamento alla Data-Inspektion, l'equivalente svedese del nostro Garante, come richiesto dalla legge svedese.

Alcuni colleghi non gradirono, e la signora prontamente cancellò le pagine. Questo non la mise però al riparo da un procedimento penale, per non avere notificato il trattamento, per aver pubblicato dati sensibili sulla ferita al piede senza il consenso e per aver trasferito all'estero dati personali sottoposti a trattamento non autorizzato (il caricamento delle pagine web sul server).

Il quadro di base della normativa sulla privacy è dettato dalla Comunità Europea, e l'autorità ultima in questa materia è la Corte di Giustizia delle Comunità Europee. Il tribunale svedese ha pensato bene di richiedere una interpretazione alla Corte, che nella sua sentenza ha confermato l'applicabilità della normativa sulla privacy alle attività della signora. Anzi, la Corte ha sostenuto che effettivamente il semplice fatto di porre sul sito la notizia della ferita al piede comportava una diffusione di dati sensibili.

"PUBBLICARE IN RETE DATI PERSONALI NON ESENTA MAI DAGLI OBBLIGHI DELLA LEGGE SULLA PRIVACY"

Non solo, secondo la Corte nel caso di pubblicazione su Internet di dati personali, dato che tali dati sono resi accessibili ad un numero indefinito di persone non si applica mai l'esenzione dagli obblighi della normativa sulla privacy per attività esclusivamente personali, prevista anche dalla nostra legislazione.

La Corte ha invece escluso che il mero accesso ad una pagina web costituisca esportazione di dati, mentre lo è il caricamento delle pagine su un server localizzato fuori UE. Come si vede, la Corte non ha esattamente sposato la tesi che Internet sarebbe una "zona franca", ma anzi ha stabilito per Internet criteri più rigorosi.

paese che vai, normativa che trovi

Cosa possiamo imparare dall'episodio della signora svedese? Innanzitutto va detto che le sanzioni sono decise dalla normativa nazionale, e quindi il fatto che una attività sia sanzionata penalmente in Svezia non implica necessariamente che lo sia anche in Italia.

I principi generali dettati dalla Corte nel caso svedese rimangono invece applicabili anche da noi. Difatti le sentenze della Corte di Giustizia vincolano nell'interpretazione sia le autorità amministrative sia i giudici di tutti gli Stati Membri. Quindi, sulla base di ciò che ha statuito la Corte, è abbastanza chiaro che le attività su siti web, quando comportino gestione di dati personali, sono sempre soggette alla normativa sulla privacy, sia da parte di privati che da parte di aziende ed enti pubblici.

Il secondo argomento che ha trattato la Corte risolve un problema di interpretazione sulla questione dei cosiddetti dati sensibili. La normativa (anche quella italiana) pone delle protezioni particolari alla diffusione di specifici dati, come quelli afferenti lo stato di salute, convinzioni politiche o religiose, e altro. A questo punto è ben chiaro che perché scatti la protezione per i dati relativi allo stato di salute non è necessaria la pubblicazione su di un sito web dell'estratto di una cartella clinica o di analisi, ma bastano anche indicazioni molto generiche, come il dire che una persona si é ferita ad un piede.

L'impostazione che ha seguito la Corte per l'esportazione di dati al di fuori dell'Unione Europea (UE) e dello Spazio Economico Europeo (SEE) è di ragionevolezza, ma lascia dei punti interrogativi. Difatti, se la Corte ha ribadito che il solo porre dei dati personali su un sito web non costituisce una esportazione (sostanzialmente perché sono gli altri che se li vengono a prendere), questa ha anche confermato che l'attività di caricamento sul server costituisce trasferimento dei dati. E pertanto, se il caricamento delle pagine web contenenti dati personali é effettuato su di un server localizzato al di fuori del territorio della UE o del SEE sarà necessario il consenso espresso del soggetto cui si riferiscono i dati, a meno che non si tratti di una persona giuridica.

Ma sicuramente la Corte avrà occasione di ritornare sull'argomento, anche in relazione alle specifiche norme sulle comunicazioni elettroniche.

Rbot, il worm spione che s'impadronisce della webcam

C'è un nuovo nato nella famiglia dei worm informatici: è *W32/Rbot*, codice malizioso che si propaga con facilità attraverso i sistemi non aggiornati o protetti da password di facile individuazione. Tra le tante, *Rbot* vanta una caratteristica particolarmente insidiosa: il worm può infatti catturare e registrare immagini su pc che montano una webcam e, attraverso micidiali backdoor, trasmetterle all'esterno. L'idea, invero, non è nuovissima: già in passato worm e trojan avevano preso di mira le webcam degli utenti. La diffusione di massa delle telecamere ha però impresso un'accelerazione anche su questo versante, aumentando esponenzialmente il rischio di violazioni della privacy e di spionaggio industriale.

e il gigante AOL mette all'asta la Porsche dello spammer

Una Porsche all'asta. Nulla di strano, se non fosse che il banditore dell'incanto è America on Line, Internet company del colosso Time Warner, e la sportiva di lusso il provento (più o meno diretto) di una proficua attività di spam. L'untore, che secondo l'azienda avrebbe guadagnato migliaia di dollari intasando con un miliardo di mail spazzatura le caselle postali degli utenti Aol, si è infatti visto sequestrare il gioiello a quattro ruote al termine di una lunga battaglia legale. La Porsche, una "Boxter S" del valore di circa 47mila dollari, è stata messa all'asta tra tutti gli abbonati maggiorenni di America on line: un gesto simbolico che ha inteso dimostrare la fermezza con la quale il colosso americano intende perseguire la piaga dello spam. Per Aol è la quinta causa giudiziaria intentata ai danni dei nuovi untori del web.

Servizi a cura di Stefania Fabbri

The web like the Far West? A lawyer expert in the protection of personal details disclaims the cliché. And, mentioning a case in point, he retorts: "The global visibility of the web increases the risk of being prosecuted".

the parishioner, the internet and privacy

by **Patrizio Menchetti**

According to a current urban legend, the Internet is a sort of virtual Far West, a cyberspace where the rules of the offline world, including privacy laws, are not enforced. Legally, this is an incorrect statement; all that is unlawful in the offline world is unlawful in the online world as well, and cyberspace exists only in William Gibson's science fiction books.

In fact, the activities that take place in the web, just because of their global visibility, are more prone to being prosecuted. As it has been aptly proven by the case of a Swedish lady, which was referred to the Court of Luxembourg.

This lady, whose name cannot be mentioned here (there's Privacy Act!!), was doing volunteer work in a Swedish parish church as a catechist to communicants. The lady had attended a computer course and had set up at home, with a personal computer, a web site consisting of a few pages in order to give the parishioners who were getting ready for confirmation easy access to the information they needed. The pages contained information on the lady and 18 of her parish mates, with their names and surnames or just their first names.

The lady had also included in the web site, in a light-hearted tone, her mates' tasks and hobbies. In addition, she had also given a description of the family life of many of them, their telephone numbers and other details. In particular, she had reported the fact that a colleague who had hurt her foot was on sick leave. The lady had not informed her mates nor had she asked for their consent. In addition, she had not informed Data-Inspektion, the Swedish counterpart of our Watchdog, as established by the laws of Sweden.

Some of her mates did not like it, so the lady quickly deleted the pages. But this did not spare her a lawsuit for not having served notice of the use of personal details, for publishing sensitive data on the wounded foot without

Patrizio Menchetti is qualified in Italy and member of the Milan Bar. He focuses his practice on information technology, data protection, intellectual property, antitrust, telecommunications and generally high technology matters. He has assisted several telecom and Internet operators as well as registries for top-level domain names in regulatory, data protection and IP matters; media companies in privacy and IP-related issues; and the European Commission with the assessment of telecom liberalization in Luxembourg. He has also been retained by the European Commission as an expert to evaluate projects in the area of new technologies.

Patrizio Menchetti is a visiting professor to Padua University, where he currently holds the chair of commercial law in the LLM course in Internet law, and a member of the Legal Advisory Board of the European Commission's "Information Society" Directorate-General. He is the author of several publications and articles, in Italian and in English, including the section on Italy in International Privacy, Personality and Publicity Laws and Legal Aspects of Standardisation in Italy in Legal Aspects of Standardisation in the EC and EFTA.

He earned a magna cum laude law degree from the University of Siena. A former trainee with the European Commission's "Competition" Directorate-General, before entering private practice he served as an in-house lawyer with ENI and Alcatel Italia.

consent and for transferring abroad personal details submitted to unauthorised processing (the loading of the web pages onto the server).

The basic framework of the privacy act is set forth by the European Community, and the supreme authority for this subject is the Court of Justice of the European Communities. The Swedish Court justly decided to ask the court for its judgement, and the Court confirmed that the privacy act was applicable to the lady's activity. Actually, the Court ruled that the simple fact of publishing the news of the wounded foot on the web site involved the disclosure of sensitive data.

Not only that: according to the Court, when personal details are published on the Internet, as such details are made accessible to an indefinite number of people, the exemption from the obligations of the privacy act never applies to purely personal activities, just like in Italy.

The Court ruled out, instead, that the mere access to a web page constitutes a case of data export, while the loading of pages on a server located outside the EU would constitute a case of data export. As you can see, the Court did not exactly embrace the assumption that the Internet is a "free area", but actually set forth stricter criteria for the Internet.

and the AOL giant puts the spammers' Porsche up for auction

A Porsche up for auction. It wouldn't sound so strange, but for the fact the auctioneer is *America on Line*, the Internet company of Time Warner, the industrial giant, and the luxury sports car is the fruit (more or less direct) of a fruitful spamming business. The plague-spreader who, according to the company, earned thousands of dollars by jamming the Aol users' mailboxes with a billion junk mails has actually seen his four-wheel gem be taken away at the end of a time-consuming legal battle. The Porsche, a "Boxter S" model, worth approximately 47 thousand dollars, has been put up for auction among all America on line subscribers: a symbolic gesture meant to prove the determination with which the US giant intends to pursue the spamming plague. For Aol, this is the fifth lawsuit lodged against the new plague-spreaders of the web.

when in Rome, do as the Roman do

What can we learn from the lesson of the Swedish lady? First and foremost, we should say that sanctions are established by the national legislations, and therefore the fact an activity is subject to sanctions in Sweden does not mean it will be in Italy as well. The general criteria set forth by the Court in the Swedish case, instead, remain applicable in our country as well. The judgements of the Court of Justice are binding in interpretation on the administrative authorities and the judges of all member states. So, based on the decision of the Court, it is fairly clear that activities carried out on web sites, when they involve the handling of personal details, are always subject to the privacy act, no matter if there involve private people or corporations or public bodies.

The second subject that the Court addressed solved a problem of construction of the so-called sensitive data issue. The regulations (including the Italian ones) provide special protection against the disclosure of some specific details, such as the state of health, political or religious beliefs, and more. At this point, it is clear that, for enforcing protection of someone's health details, one does not have to publish on a web site an abstract of a medical record or a test, but general information, for instance saying that someone has hurt one's foot, is enough.

The approach of the Court on the export of details outside the European union (EU) and the European economic Space (EES) is based on sensibleness, but it leaves some questions open. If the Court insisted that just placing personal details on a web site does not constitute a case of export (basically, because it is other people who come and take the details), it also confirmed that the loading of details onto a server constitutes a case of data transfer. And, therefore, if web pages containing personal details are loaded onto a server located outside the EU or EES, the person whom such personal details refer to must give its authorisation, unless it is a legal person. But certainly the Court will have other opportunities to get back to this, also in connection with the specific regulations on electronic communication.What can we learn from the lesson of the Swedish lady? First and foremost, we should say that sanctions are established by the national legislations, and therefore the fact an activity is subject to sanctions in Sweden does not mean it will be in Italy as well.

"PUBLISHING PERSONAL DETAILS ON THE INTERNET DOES NOT EXEMPT ANYONE FROM THE OBLIGATIONS OF THE PRIVACY ACT"

Rbot, the spy worm that steals the web cam

There is a newborn in the computer worm family: it is the *W32/Rbot*, a mischievous code that easily propagates through those systems that have not been updated or that are protected by easily-identifiable passwords. One of the many features that the *Rbot* can boast, one is particularly treacherous: the worm can capture and record images from Pc fitted with web cams and, through deadly backdoors, send them outside. The idea is not so new, to be honest: in the past, worms and Trojans had already picked on the users' web cams. The mass spreading of video cameras, however, has tremendously sped up this phenomenon, with a huge increase in the risk of breaching privacy laws and industrial espionage.

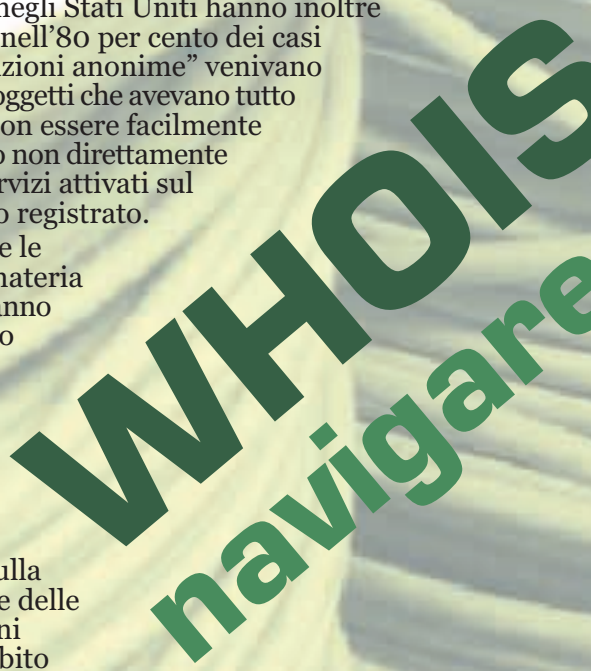
Article arrangements by Stefania Fabbri

Il Whois e' uno dei più antichi protocolli di Internet: implementato nel 1982 come indispensabile strumento di lavoro per i gestori tecnici delle reti, è sopravvissuto praticamente senza modifiche fino ai giorni nostri (l'unica "rettifica" è del settembre scorso) seguendo di pari passo il boom della diffusione dei nomi a dominio nel mondo. Oggi, anche attraverso un sistema di consultazione via web rapido ed efficiente, chiunque può infatti accedere ai database pubblici e verificare i dati relativi all'esistenza di un dominio nonché i riferimenti, tecnici e amministrativi ad esso associati. Nel Whois, inevitabilmente, confluiscono anche i principali dati personali di chi registra un nome a dominio. Non solo: la persona fisica o giuridica che richiede un qualunque nome a dominio sotto il ccTLD ".it" autorizza il gestore del registro a renderne libera la consultazione attraverso l'interfaccia pubblica del Whois. Nome e cognome, indirizzo, numero di telefono, così come gli indispensabili dettagli tecnici e amministrativi di coloro che hanno scelto di garantirsi una

"mostrare solo l'essenziale"

di **Gianluca Pellegrini**

Il servizio Whois standard (o *Whois port 43*), conoscendo un nome a dominio registrato, consente di reperire dati e contatti referenziati al dominio stesso, tramite una query (interrogazione) al database del registry competente.
Per i servizi Whois implementati in questi termini, il livello di "pubblicità" dei dati (in particolare per quanto concerne la posizione registrante), dovrebbe di per sè costituire una garanzia o quantomeno contribuire fortemente a disincentivare registrazioni di nomi a dominio da parte di soggetti intenzionati ad attivare sugli stessi servizi illegali.
Attualmente la tendenza sempre più diffusa a livello internazionale è certamente quella di mostrare, tramite il Whois ad accesso pubblico, soltanto i dati ritenuti essenziali, omettendo quelli (di fatto i contatti "fax" e "e-mail") definiti "appetibili" da chi fa azioni di "data-mining" per svolgere successivamente campagne marketing proprie o per conto terzi. Al contempo però gli stessi registries che hanno introdotto "policy restrittive", limitandosi appunto a mostrare solo alcune tipologie di dati, hanno sentito l'esigenza di implementare servizi Whois ad accesso riservato (con vari meccanismi di autenticazione). In tal modo solo i soggetti autorizzati hanno accesso ai dati in forma espansa, ad esempio per garantire ai propri registrars la possibilità di svolgere compiutamente le operazioni necessarie al mantenimento delle registrazioni attive.
Credosia importante ricordare le raccomandazioni di Icann nei confronti dei registries e dei registrars, con le quali l'organismo chiede agli stessi di fornire servizi Whois pubblici basati esclusivamente sul principio "Domain such Domain": eliminando quindi qualsiasi altro tipo di query ad eccezione di quella basata sul "nome a dominio", che rimane consentita al fine di verificare i soggetti referenziati a quello specifico dominio nella registrazione depositata presso il registry competente. Recentemente alcuni registries più "commerciali", così come alcuni registrars operanti essenzialmente nell'ambito dei *generic Top Level Domain* ".com" e ".net", hanno provato a introdurre concetti di "anonimato" o registrazioni "by proxy", mascherandosi dietro lo slogan del "garantire la privacy del registrante". Ma questi tentativi si sono ben presto rivelati meri escamotage di marketing per chiedere degli "extra" ai registranti. Alcune ricerche svolte negli Stati Uniti hanno inoltre dimostrato che nell'80 per cento dei casi queste "registrazioni anonime" venivano sottoscritte da soggetti che avevano tutto l'interesse nel non essere facilmente rintracciabili e/o non direttamente associabili ai servizi attivati sul nome a dominio registrato.
Molte sono state le discussioni in materia di privacy che hanno in qualche modo fatto riferimento al "servizio Whois". Onestamente credo che per i Whois implementati sulla base dei criteri e delle raccomandazioni maturate in ambito internazionale sopra menzionate, la tutela ed il trattamento dei "dati personali" siano certamente garantiti, in conformità alla legge e anche al buon senso.
In estrema sintesi: è certamente auspicabile e forse anche necessario far evolvere i servizi Wois dei vari registries per adeguarli al contesto dell'Internet attuale, rendendoli idonei a contrastare efficacemente azioni di "data-mining". Ma è altresì indispensabile che questi servizi continuino ad esistere per le esigenze e gli scopi per i quali sono stati concepiti.



visibilità in rete, divengono pertanto di pubblico dominio: una prassi che, se da una parte facilita lo sviluppo della rete (e consente alle autorità di reprimerne gli abusi), dall'altra rischia di esporre gli assegnatari a ingerenze non sempre apprezzate.
Sulla necessità o meno di pubblicizzare i dati è da tempo in atto un braccio di ferro che coinvolge, a vario titolo, tutti gli organismi e le associazioni che gravitano attorno al mondo Internet: ciascuna con argomentazioni concrete e condivisibili. Ne abbiamo scelte due: dando voce a Gianluca Pellegrini (Tuonome.it) e Giorgio Giunchi (figura tra le più rappresentative tra le centinaia di migliaia di assegnatari di nomi a dominio .it). Ad arricchire il dibattito abbiamo chiamato anche l'Autorità garante sulla Privacy e lo stesso Registro del ccTLD ":it": che in queste pagine propone in anteprima la propria soluzione al dilemma del Whois in linea con le scelte operate dalla maggior parte dei ccTLD mondiali. (f.n.)

"l'identità civile: un bene da tutelare"

di **Giorgio Giunchi**

In Internet nessuno e' proprietario di niente – siamo tutti *assegnatari* di *oggetti* – e sarebbe bene che il database della rete identificasse e distinguesse limpidamente gli uni e gli altri. L'oggetto *domain* ha le sue proprietà formali:
- di identità (nome a dominio) con i riferimenti di costituzione e scadenza/rinnovo
- di "residenza e domicilio" (fondamentalmente la zona, gli indirizzi IP nameserver, il mnt)
- di referenza e responsabilità funzionale (postmaster, technet)
- di assegnazione in uso (admin-c)

Qui mi interessa approfondire alcuni temi di *id/entità* e distinzione, proprie e reciproche, di mnt e assegnatari di nome a dominio – in un database di pubblico dominio. I due, tremila oggetti mnt con contratto @Registro richiamano, direi statutariamente, l'opportunità di pubbliche "pagine gialle". Con utile connotazione della *identità_imprenditoriale_in_rete*: registrar, hoster, pagemaker, fornitore di accesso, banda, lan, van, wan, produttore di tecnologia et cetera. Non è essenzialmente un problema di marketing, che a me tra l'altro come assegnatario proprio non interessa. E' questione di pubblico servizio di informazioni che serve a tutti: alla comunità mnt stessa, agli assegnatari del nome, e a chi per la prima volta si avvicina alla rete.

In logica di trasparenza sono a favore di chiavi di ricerca multiple che pure permettano di restituire i dati di penetrazione dei singolari business nel mercato, e nei suoi segmenti. Tutti i canali di contatto con le *identità_imprenditoriale_in_rete* (telefoni, fax, address, mail, icq e chi più ne ha ne metta) sono senz'altro da pubblicizzare senza problema.

Per il milione di assegnatari di nome a dominio serve probabilmente un diverso approccio, impostato alla rigorosa esposizione non di quella civica e privata, ma della formale *identità_in_rete*.

Laddove l'assegnatario è imprenditore e il nome a dominio rinvia ad un servizio propriamente business, senz' altro vale la pubblica esposizione che sopra cercavo di delineare per i mnt. Ma, oltre che probabilmente già attuale, è senz'altro e sempre più pronosticabile lo scenario di web personali e di collettivi for-no-profit. A questo livello a mio avviso il Whois, e il registro della sua manutenzione, rischiano obiettivamente di essere intercettati per ridondante e pure impertinente divulgazione di dati sensibili, con argomentata violazione della privacy.

Ogni riferimento alla *identità civile* di admin-c (anagrafe estesa, recapiti domiciliari e telefonici..) a mio avviso crea più problemi di quanti ne risolve.

Alla ragionata confutazione che il titolare di nome a dominio deve pur scontare un proporzionale grado di pubblicità, obietto che questa viene positivamente risolta dai canonici identificativi di rete, qui in veste di proprii ed efficaci canali pseudonimi: codice admin-c, nic handle, chiave pubblica, indirizzo@PE. Riguardo alla *manutenzione* sono per principio a favore del più alto grado di autocertificazione in prospettiva di compilazione - aggiornamento del record proprio in modalità protetta. Sarebbe ben utile uno strato di Whois riservato, sociologicamente dettagliato, basato su questionari, a cura e riserbo del Registro, con servizio di elaborazione dei dati macro, ovviamente anonimi, all'attenzione di operatori e studiosi.

Rubo due righe, in fine, per una sollecitazione: positive indicazioni possono venire da un più generale dibattito sulla formalizzazione trilaterale "dei diritti e dei doveri", rispettivi e reciproci, di Registro, mnt, assegnatari.

Servizi a cura di Francesca Nicolini

whois e protezione dei dati personali: dal caso italiano le linee guida per un progetto pilota europeo

di **Cosimo Comella**
Dirigente informatico – Ufficio del Garante per la protezione dei dati personali

Una premessa d'obbligo: i dati contenuti nei Whois database, oggi, non riguardano più solo una minoranza di persone con competenze tecniche specifiche e pertinenti, ma si riferiscono in gran parte a semplici utilizzatori che, in virtù del sempre maggiore coinvolgimento e interesse del pubblico nei confronti della rete, hanno visto i loro dati personali confluire in quei database, il più delle volte all'atto della registrazione di un nome a dominio.
Ciò detto, dal punto di vista della privacy occorre comunque far riferimento ai principi di liceità dei trattamenti, di necessità, di proporzionalità e di finalità, che rappresentano in generale le condizioni di liceità per il trattamento dei dati personali, e che derivano non solo dalla normativa italiana (articoli 3, 11 e 18 del decreto legislativo n. 196/2003, il cosiddetto "Codice della privacy") ma dall'uniforme orientamento internazionale.

La situazione europea, con l'insieme di tutele introdotte a livello comunitario con la direttiva 95/46/CE e ribadite dalla direttiva 2002/58/CE sulla privacy nelle comunicazioni elettroniche, è quella che desta maggiormente l'attenzione anche in rapporto all'interazione tra il mondo Internet europeo e quello nordamericano.

L'applicazione di tali principi prevede che i dati personali richiesti per l'attivazione di determinati servizi e destinati a diffusione sulla rete siano soltanto quelli effettivamente necessari, che non siano eccedenti e che siano utilizzati per fini specifici e dichiarati sulla base di un consenso libero e informato da parte dell'interessato, ovvero della persona alla quale si riferiscono i dati. Presupposto di una corretta applicazione dei principi di liceità è quindi un'attenta riflessione sulle finalità del sistema e sulla congruità a queste dell'attuale configurazione dei servizi. Mentre infatti tali finalità erano ben definite negli anni precedenti l'esplosione di Internet come fenomeno di massa (quando il Whois era davvero uno strumento efficace per la risoluzione di problemi della rete: chi aveva i propri dati registrati nel database era con elevata probabilità un tecnico competente in grado di intervenire), oggi l'utilità del Whois come strumento di gestione tecnica è quantomeno limitata, proprio per la diversa natura della popolazione censita.

Né ha più alcun senso difendere le prassi non in linea con leggi poste a tutela di valori fondamentali della persona per costringere gli odierni utenti, visti come neofiti, a esaudire una sorta di debito morale nei confronti delle antiche tradizioni. Per quanto riguarda gli aspetti tecnici del servizio, anche a livello di protocolli, questi sono rilevanti anche in rapporto a specifici diritti garantiti dalla disciplina del trattamento dei dati personali: basti pensare alla necessità di realizzare idonee ed efficienti procedure per l'accesso, la verifica, la cancellazione o la correzione dei dati personali da parte degli interessati, ovvero per consentire l'esercizio dei diritti sanciti, nel nostro ordinamento nazionale, dal Codice della privacy all'articolo 7, oppure per rendere un'adeguata informativa secondo le previsioni dell'articolo 13 dello stesso testo normativo.
In questa materia è quindi importante la collaborazione costruttiva tra tecnici informatici e giuristi al fine di individuare le migliori forme di bilanciamento di interessi che tengano conto del contesto internazionale, delle esigenze della rete e delle esigenze dettate dalle leggi: collaborazione già avviata in diverse aree e che vede giuristi e tecnici impegnati insieme anche in diversi consessi di studio e istituzionali.

Il caso italiano, che vede la gestione del dominio nazionale affidata a un ente pubblico di ricerca, potrebbe poi rappresentare un prototipo a livello europeo per una corretta implementazione dei principi della protezione dei dati personali.

775 i ricorsi decisi dal Garante per la protezione dei dati personali dal primo gennaio 2003 al marzo di quest'anno. Il tasso di crescita (enorme: nel 2001 le decisioni sui ricorsi erano state 169; 390 nel 2002; per arrivare alle 608 dell'anno solare 2003) conferma come nel sentire comune si preferisca affidare la risoluzione delle controversie al Garante piuttosto che all'autorità giudiziaria.

il database di domani: pochi rischi, massima efficienza

di **Maurizio Martinelli**
Responsabile tecnico del Registro del ccTLD ".it"

Scoraggiare le operazioni di *data mining* e, al contempo, permettere ai registrar di usufruire di strumenti di interrogazione sempre più efficaci per la loro attività. Su questi obiettivi si fonda la "riforma" del Whois messa in cantiere dal Registro del ccTLD ".it". Una soluzione in linea con quanto già messo in atto da altri registri TLD e ufficialmente presentata anche alla Commissione regole al fine di garantire il più ampio consenso.

Il rischio principale cui è esposto il servizio Whois è quello delle interrogazioni continue e ripetute al server. Soluzioni tampone quali l'introduzione di una soglia massima al numero di richieste provenienti dallo stesso Ip o in un arco di tempo prestabilito sono state considerate insoddisfacenti in quanto potenzialmente discriminanti nei confronti di coloro che utilizzano ad esempio server proxy o reti Nat. Al di là dei limiti insiti nello sbarramento per Ip (si pensi, ad esempio, alla difficoltà di limitare le richieste attivate con connessioni dialup e quindi con indirizzo dinamico), resterebbe comunque il dilemma di definire una soglia equa e un arco di tempo ragionevole per le richieste multiple. La soluzione individuata dal Registro prevede una ristrutturazione del servizio Whois secondo cinque linee guida fondamentali.

La prima contempla l'accesso "pubblico" tramite connessione diretta sulla porta Tcp 43 del server ma con limitazioni precise nella visualizzazione dei campi "a rischio" (e-mail, telefono, fax e via dicendo); ugualmente "pubblica" la seconda possibilità di accesso via Web, vincolata però all'inserimento di un codice alfanumerico generato di volta in volta e proposto dall'interfaccia sotto forma di immagine: l'utente potrà sì visualizzare tutti i dati contenuti negli oggetti cercati; ma non sarà in grado di automatizzare il processo (e quindi attivare procedure di *data mining*) perché l'operazione richiederà l'intervento manuale dell'operatore a ogni singola richiesta. Un terzo livello di accesso "pubblico" sarà riservato a connessioni dirette su una porta Tcp prestabilita del server: ma esso concederà solamente di verificare l'esistenza o meno di un nome a dominio (il cosiddetto *check domain*) per verificarne la disponibilità. Due, invece, i livelli di accesso "riservato" le cui chiavi saranno concesse solo ai registrar. Nel primo caso l'operatore potrà visualizzare, attraverso un portale Web e previa autenticazione, tutti i dati di propria pertinenza (ma non, indiscriminatamente, quelli altrui) ed esportare i dati in formato Csv o Xml; nel secondo, la medesima opportunità sarà offerta con accesso al server via protocolli tipo Soap, Xml-Rpc o altri.

Il servizio del ccTLD ".it"

Il ccTLD ".it" offre un servizio Whois "privato" e uno "pubblico". Quello privato è strettamente riservato agli addetti ai lavori del Registro e contiene informazioni che vanno oltre i dati forniti dal registrar nel modulo tecnico di registrazione.
Il servizio pubblico è invece accessibile attraverso un'interfaccia Web, una connessione diretta al server e un motore di ricerca "user-friendly", denominato Wise e sviluppato dall'Unità Sistemi del Registro. Quest'ultimo permette all'utente di effettuare, via Web, ricerche complesse e ottenere, tra l'altro, anche la lista dei registrar operativi nel ccTLD ".it".
Nel Whois sono presenti quattro tipologie distinte di oggetti:
- l'oggetto *domain*, che identifica un nome a dominio registrato e le informazioni salienti ad esso associate (assegnatario, contatto amministrativo, tecnico, ecc.);
- l'oggetto *mntner*, che identifica un registrar e le modalità di autenticazione da esso utilizzate per proteggere gli oggetti da lui registrati;
- l'oggetto *person*, che contiene le informazioni riguardante i contatti amministrativi e tecnici referenziati in un oggetto *domain* e *mntner*;
- l'oggetto *role*, che contiene, analogamente all'oggetto *person*, informazioni riguardanti i contatti tecnici e amministrativi ma, a differenza di quest'ultimo, descrive un ruolo che può essere ricoperto da più persone.

I dati restituiti all'utente in seguito a un'interrogazione sono, a parte piccole eccezioni, i dati forniti dal registrar al Registro con il modulo tecnico. Non sono visualizzate informazioni quali il codice fiscale dell'utente e le modalità di autenticazione del registrar. Non vi sono limiti al numero di richieste, anche se esistono strumenti di monitoraggio delle stesse per evitare abusi. Nel caso di interrogazioni tramite il motore di ricerca Wise è però restituito all'utente, in maniera casuale, solamente un massimo di 1.500 risultati. (m.m.)

WHOIS
contac

Whois is one of the oldest Internet protocols: implemented in 1982 as an essential working tool for technical network administrators, it has basically survived unchanged up to these days (the only "amendment" was made last September), keeping pace with the boom of domain names across the globe. Today, through a quick and efficient online consultation system, anyone can have access to public databases and check the existence of domains and the technical and administrative details associated with them. Inevitably, Whois also stores the main personal details of those who register a domain name. Not only that: the legal or natural persons that apply for any domain name under the ccTLD ".it" authorise the Registry's administrator to allow free consultation of such details through the public interface of Whois. Full name, address, telephone number as well as the essential technical and administrative details of those who have decided to gain more visibility online thus become public domain: a practice tha exposing the assignees to unwelcome i There have been fierce confrontations move within the orbit of the Internet Gianluca Pellegrini (Tuonome.it) and Watchdog and the ccTLD ".it" Registry made by most of the world's ccTLDs. (

"let's show the essential info only"

by **Gianluca Pellegrini**

The standard Whois service (*or Whois port 43*) can be used to find data and contacts referred to that domain from a registered domain name through a query sent to the database of the relevant registry.
For Whois services implemented like that, the level of data "publicity" (in particular, about the registrant's position) should in itself guarantee or at least substantially contribute to discourage domain name registrations made by persons who intend to open illegal services on such domain names.

At present, the increasingly widespread tendency across the world is certainly to show, through the public Whois, only assumedly essential data and to omit those (basically, fax and email contacts) that are considered "desirable" by those who engage in "data-mining" in order to conduct marketing campaigns on their own or on behalf of third parties. At the same time, though, the registries who have introduced "restrictive policies" to show only some types of data felt the need to implement restricted-access Whois services (with different authentication mechanisms). In this way, only authorised persons can access expanded data, for instance to let their registrars carry out the operations needed to maintain the registration.

I think we should not forget the recommendations given by Icann to the registries and registrars, in which they asked them to supply public Whois services based only on the "Domain such Domain" principle: that is, by removing any other type of query, except those based on "domain names" which are still accepted in order to check any subject referred to that specific domain in the registration lodged with the relevant registry.

Recently, some of the most "commercial" registries, as well as some registries that essentially work in the *generic Top Level Domains* ".com" and ".net", have tried to introduce "anonymity" concepts or registrations "by proxy", hiding themselves behind the slogan: "guaranteeing the registrant's privacy". But these attempts soon turned out to be simple marketing tricks to ask the registrants for "extras". In addition, some surveys conducted in the United States have proven that 80 percent of these "anonymous registrations" were signed by subjects that were most interested in not being easily tracked down and/or not directly associable with the services opened on the registered domain name.

Many have been the discussions on privacy that have somehow made reference to the "Whois service". I honestly believe that, for any Whois based on the aforesaid new criteria and recommendations, the protection and processing of "personal details" are certainly guaranteed by the law and also by commonsense.

To sum up: a development of the Whois services of the different registries is certainly desirable and perhaps even necessary in order to adapt them to the current Internet scenario, so that they will be fit for effectively fighting any "data-mining" action. But it is also absolutely necessary that these services continue to exist for the needs and purposes for which they have been designed.

Article arrangements by Francesca Nicolini

S

ct surfing ?

at, while making it easier for the web to develop (and for authorities to prevent any misuse), risks intrusions.
on about the need to publicise details, involving all the bodies and associations that one way or other world: each one with matter-of-fact and reasonable arguments. We chose two, through the voice of Giorgio Giunchi (on behalf of users). To make the discussion more gripping, we also called the Privacy y, which in these pages offers a preview of its solution for the Whois dilemma in line with the choices f.n.)

"civil identity should be protected"

by **Giorgio Giunchi**

In the Internet, nobody owns anything – we are all *assignees* of *objects* – and the web database should clearly identify and distinguish the two things.
The *domain* object has its own formal properties:
- id/entity (domain name), with establishment and expiry/renewal references;
- "residence and domicile" (essentially, the area, the nameserver IP addresses, the mnt)
- reference and functional responsibility (postmaster, tech-c)
- assignment (admin-c)

Here, I would like to go into the details of some issues regarding own and mutual *id/entity* and distinction of mnt and domain name assignees – in a public database.
The two, three thousand mnt objects under a @Registrar agreement recall, I'd say statutorily, the opportunities of a sort of public "Yellow Pages".
With a useful connotation of the *business_identity_in_the_web*: registrar, hoster, pagemaker, access provider, band, lan, van, wan, technology manufacturer, etc.
It is not essentially a marketing problem, which I am not even interested in as an assignee: it is a matter of a public informational service, which is useful to everyone: to the mnt community, to the name assignees and to those who are approaching the web for the very first time.
In a transparent approach, I like multiple search keys that can also feedback the market penetration figures of unique businesses and their segments.All the contact channels for the *business_identities_in_the_web* (telephones, faxes, addresses, mails, icq and so on and so forth) are certainly to be publicised, without any problem.
The one million domain name assignees probably need a different approach, based on a clear expression, not of the civil and private identity, but of the formal_*identity_in_the_web*.
Whenever the assignee is a businessman and the domain name refers to a strictly business-like service, the public expression I was trying to define before for mnt certainly applies.
But a scenario of non-profit personal and collective webs is not only probably topical, but also increasingly to be expected.
At this level, I think the Whois and its maintenance registrar objectively risk being tapped for their superfluous and even cheeky dissemination of sensitive data, on the grounds of breaching the privacy act.
In my opinion, any reference to the *civil identity* of admin-c (full details, house addresses and telephone numbers) causes more problems that it solves.
To the reasoned argument that a domain name holder must somehow suffer some publicity, I object that this is successfully solved by regular web usernames, which act here as veritable fictitious channels: admin-c code, nic handle, public key, address@PE.
As far as *maintenance* is concerned, in principle I support the highest degree of self-certification with a view to having records filled in – updated in a protected mode.
It would be extremely useful to have a sociologically-detailed, confidential Whois layer, based on questionnaires to be held and protected by the Registrar, with a service for processing anonymous macro data offered to operators and researchers.I'll grab a couple of lines to remind you of this: positive suggestions can came from a broader debate on the trilateral finalisation of the respective and mutual "rights and duties" of the Registrar, the mnt, the assignees.

the whois and the protection of personal details: from the italian scenario, the guidelines for an european pilot project

by **Cosimo Comella**
Computer Manager -Watchdog Department for Protection of Personal Details

An introduction is in order: today, the details contained in the Whois databases do not longer concern just a minority of people with specific and relevant technical skills, but largely concern simple users, who, because of the increasing involvement and interest of the public in the web, have seen their personal details flow into those databases, most of the times when they registered a domain name. Saying that, in terms of privacy, we have to refer to the principle of lawfulness for data processing, need, proportion and aim, which are the general principles of lawfulness for the processing of personal details and which are laid down not only by the Italian legislation (articles 3, 11 and 18 of Act 196/2003, the co-called "Privacy Act"), but by the international standard regulations.

The European scenario, with the sets of protective measures introduced in the EU member states by Directive 96/46/EC and substantiated by Directive 2002/58/EC about privacy in electronic communication, is the one that attracts most attention, also in view of the interaction between the European and the North American Internet worlds.

In order to enforce these principles, the personal details required for using specific services to be disclosed via the web must be only those that are actually needed, they must not be in excess, they must be used for specific purposes and they must be provided with the free and informed consent of the person concerned, that is, the person to whom such details refer. The prerequisite for the proper enforcement of the lawfulness principles is therefore a careful consideration of the purposes of the system and the consistency between these principles and the current configuration of the service. While such purposes had been clearly defined in the past, the Internet boom as a mass phenomenon (when the Whois was really an effective means to solve any problem of the web: those who had their details recorded in the database were most probably skilled technicians who knew how to work), today the usefulness of the Whois as a technical management system is, to say the least, limited, just because of the different nature of the registered population.

Neither does it make any sense to defend practices that do not comply with the laws that have been issued to protect essential personal values to force today's users, viewed as novices, to fulfil a sort of moral debt towards the old traditions. As to the technical aspects of the service, also in terms of protocols, these are also relevant for some specific rights guaranteed by the laws on the processing of personal details: just think of the need to implement suitable and effective procedures for the access,

775 are the appeals decided by the Watchdog for protection of personal details between January 1st 2003 and March 2004. The growth rate (a huge one: in 2001 decisions on appeals had been 169; 390 in 2002, then 608 in 2003) proves that people prefer to have disputes settled by the Watchdog than by the judiciary.

check, deletion or correction of personal details by the people concerned, i.e. to let them assert the rights that are sanctioned by the Privacy Code article 7 of our national legislation or else to give adequate information pursuant to the provisions of article 13 of the same Act.

In this regard, therefore, factual cooperation between computer engineers and jurists is essential to find the best ways to balance interests, in the attempt to comply with the international scenario, the needs of the web and the requirements set forth by the laws: cooperation that has already been put in place in several areas and which sees jurists and engineers working together also at several research

9 is the average number of daily enquiries about spamming and more generally unwanted commercial messages that are received by the Watchdog's call centre. Protection from "junk" mail is more and more of a deeply-felt problem: in 2003, the Watchdog's inspections also produced a report to the judiciary against a businessman who was charged for sending commercial emails without the addressees' prior informed consent.

and political meetings. After this consideration, though, it is all the more urgent to see to providing effective and more suitable regulations for the Whois services. The Italian scenario, which sees the management of the Italian domain being entrusted to a public research institute, then could be a prototype for all of Europe, for the proper implementation of the principles of protection of personal details, which would be even more appreciable in the light of the role of such institute: recognised all over Europe for its involvement in the management of the European domain ".eu".

the database of tomorrow: few risks, freat efficiency

by **Maurizio Martinelli**
Technical Manager at the ccTLD ".it" Registry

Discouraging *data mining* while letting the registrars use increasingly effective search engines for their jobs. These are the goals on which the "reform" of the Whois that has been started by the ccTLD ".it". registry is based.

the ccTLD ".it" service

The ccTLD ".it" offers a "private" and a "public" Whois service. The private one is restricted to the Registrar's operators only and contains information that goes beyond the information supplied by the registrar by means of the technical registration form.
The public service, instead, is accessible through a web interface, a direct connection to the server and a "user-friendly" search engine, called Wise and developed by the System Unit of the Registrar. The latter allows the user to make advanced searches via the web and to obtain, among other things, a list of the registrars who work within the ccTLD ".it".
The Whois contains four different types of objects:
- the *domain* object, which identifies a registered domain name and the key information associated with it (assignee, administrative contact, technical contact, etc.);
- the *mntner* object, which identifies a registrar and the authentication methods used by the registrar to protect the registered objects;
- the *person* object, which contains information on the administrative and technical contacts referred to by the *domain* and *mntner* objects;
- the *role* object, which contains, like the *person* object, information on the technical and administrative contacts, but, unlike that, it describes a role that can be played by more than one person.
The information sent back to the user following a query is, apart from some minor exceptions, the information supplied by the registrar to the Registry through the technical form. Such information as the user's taxpayer's code and the registrar's authentication methods are not displayed. There are no limits to the number of queries, even if there are systems to monitor them in order to prevent abuse. If Wise is used as a search engine, only up to 1,500 results are sent back to the user, on a random basis. (m.m.)

A solution that is consistent with what has already been implemented by other TLD registries and officially submitted to the Rules Commission in order to build the widest consensus.The main risk for the Whois service consists in continued and repeated queries to the server. Stop-gap solutions, such us the introduction of a maximum limit for the number of queries coming from the same Ip or in a fixed time period, have been considered unsatisfactory, as they can potentially discriminate against those who use, for instance, proxy servers or Nat networks. Apart from the limits inherent in the Ip blockage (think, for instance, how difficult it would be to limit queries made through dialup connections, which have dynamic addresses), the dilemma of defining a fair limit and a reasonable time period for multiple queries would not be solved. The solution proposed by the Registry involves a reorganisation of the Whois service according to five basic guidelines.

The first one involves "public" access through a direct connection to the port Tcp 43 of the server, but with very specific limits in the view of "risky" fields (email, telephone, fax and so on); equally "public" is the second access via the web, subject however to entering an alphanumerical code generated from time to time and proposed by the interface in the form of a picture: the user can of course view all the information contained in the searched objects; but the user will not be able to automate the process (and therefore to open any *data mining* procedures), because the operation would need a manual operation at every query. A third level of "public" access will be restricted to direct connections to a Tcp port as decided by the server: but it will only be used to check whether a domain name exists or not (the so-called *check domain*) and see if it is available.

Two are instead the levels of "restricted" access whose keys will only be granted to the registrars. In the first case, the operator can view, through a web portal and subject to authentication, all the information relevant to the user (but not indiscriminately those of any third party) and export the information in Csv or Xml format: in the second case, the same opportunity will be offered by direct access to the server through such protocols as Soap, Xml-Rpc or others. A double guarantee for quick and effective searches.

The web portal, as well as the aforesaid "advanced" functions of the Whois, will allow registrars to monitor in real time other essential services, such as the billing or registration status.

spam l'importante è prevenire

di **Stefano Ruberti**
Responsabile del laboratorio di posta elettronica dello IIT-CNR

La posta elettronica è oggi uno dei più popolari mezzi di comunicazione. E negli ambiti più disparati: da mero strumento accademico, infatti, esso si è tramutato negli anni nel più diffuso mezzo di comunicazione anche nelle realtà aziendali. Il processo di informatizzazione nelle comunicazioni, se da un lato ha favorito lo scambio di informazioni in maniera efficace ed efficiente, dall'altro mostra inesorabilmente il fianco a tutta una serie di "usi impropri": diffusione su vasta scala di messaggi pubblicitari non richiesti, distribuzione di virus, sovraccarico dei sistemi per far fronte ad un traffico spesso inutile se non dannoso. E' opinione diffusa che tali limiti siano dovuti alla natura del protocollo di comunicazione (*Smtp*) utilizzato per il servizio di posta, ormai datato e dunque incapace di sostenere le moderne esigenze di privacy e riservatezza delle comunicazioni digitali. A chi non è capitato, a seguito dell'attivazione di una semplice casella postale, di ricevere offerte più o meno "esplicite" di materiale e servizi di dubbio gusto?

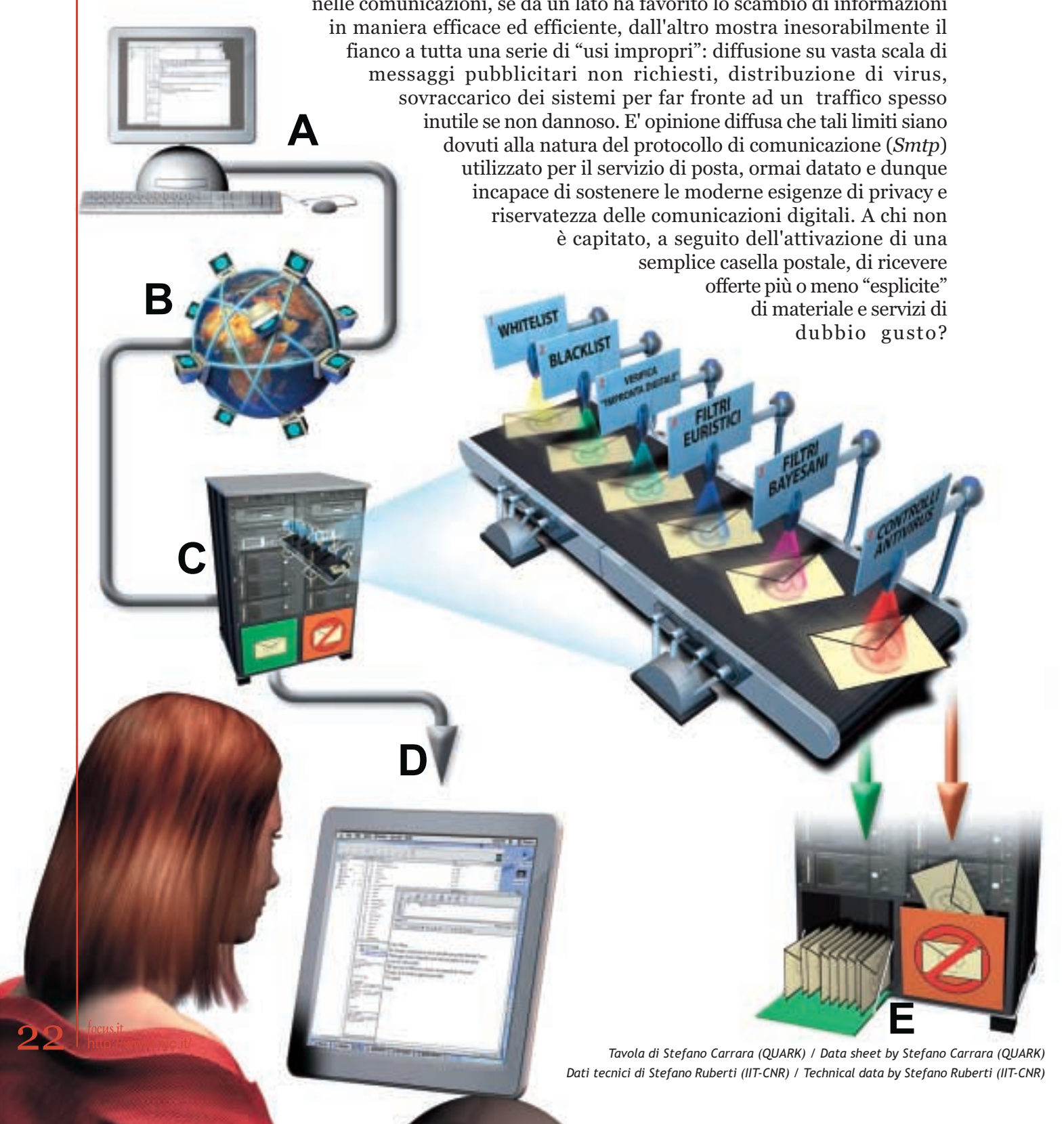


Tavola di Stefano Carrara (QUARK) / Data sheet by Stefano Carrara (QUARK)
Dati tecnici di Stefano Ruberti (IIT-CNR) / Technical data by Stefano Ruberti (IIT-CNR)

Pianificazione e dimensionamento del sistema

Nella struttura operativa del Registro del ccTLD ".it", ad esempio, vengono ricevuti in media 22 mila messaggi al giorno pari a circa 120 MByte di traffico: più del 50 per cento di essi sono classificati come "indesiderati". Un fenomeno diffuso ormai ovunque: il servizio di posta elettronica dello Iit-Cnr, l'Istituto che ospita il Registro, si allinea infatti sugli stessi risultati. L'attivazione di sistemi per il controllo anti-spam e anti-virus dei messaggi scambiati dal Registro, operativa da circa due anni, ha sicuramente migliorato la qualità del servizio: tuttavia ci ha impegnati in una complessa messa a punto di un sistema integrato per la gestione del server di posta elettronica che rispettasse vicoli di robustezza e integrità e facesse riferimento a strumenti Open-source.

"OCCORRE AVER CHIARO IL VOLUME DI MESSAGGI DA TRATTARE"

Per dimensionare correttamente un server di posta in grado di effettuare controlli efficaci deve essere innanzitutto chiaro il volume di messaggi che devono essere trattati, attivando in maniera proporzionale un congruo numero di processi concorrenti per il sistema di analisi dei contenuti. Nel caso del Registro abbiamo impostato un numero massimo di 10 processi per Cpu: un valore comunque dipendente dalla quantità massima di memoria Ram attiva sul sistema, dal momento che ciascuna istanza impegna dai 25 ai 30 MByte di memoria.

Per quanto riguarda gli anti-virus da impiegare, invece, è necessario prediligere gli strumenti meno esosi di risorse. Le stime si ottengono analizzando a posteriori il comportamento dei singoli prodotti dopo una robusta fase di test del sistema. Per citare un caso concreto, il medesimo prodotto anti-virus utilizzato come client su piattaforme Linux impiega mediamente 80 ms, ma se trasferito su piattaforma Solaris vede scendere il valore di un ordine di grandezza. Le operazioni di verifica sui messaggi effettuate dai più comuni strumenti di analisi dei contenuti (*content-checking*) vengono generalmente applicate sia ai messaggi in ingresso che in uscita e possono essere riassunte in 6 passi principali: verifica della presenza del mittente nella whitelist e/o blacklist generale e individuale del destinatario, verifica della "impronta digitale" del messaggio, filtri euristici, filtri bayesiani, controlli anti-virus (vedi schema a lato).

Soluzioni tecniche: il caso concreto

Risulta arduo elencare la rosa delle soluzioni tecniche possibili per allestire un sistema di posta elettronica di questo tipo, in quanto per i controlli sono disponibili prodotti sia commerciali che gratuiti. Il Registro, ad esempio, offre il servizio di posta su server SUNFire 280R con due processori Ultra Sparc, 4GByte di Ram e Raid 5. Utilizziamo Sendmail in congiunzione con MailScanner che a sua volta fa uso di SpamAssassin per i controlli anti-spam e due antivirus in cascata (Sophos e ClamAV). In questo contesto non abbiamo necessità di fornire particolari servizi, in quanto non sono attivi utenti reali. La soluzione tecnica utilizzata dallo Iit-Cnr, invece, fa uso di un server HP ProLiant DL380, equipaggiato con 2 processori, 2GB Ram, 6x36Gbyte hard disk in Raid 5 Hot

A: Pc mittente: da qui parte l'e-mail / *Sender's PC: the email is sent from here*;
B: Viaggia attraverso internet / *It travels through the Internet*;
C: Il sistema di posta di destinazione (Mailserver) inizia i controlli. / *The recipient's mail system (Mailserver) starts checking*;
D: Passati i filtri arriva a destinazione / *After passing through the filters, it reaches the recipient.*
E: I messaggi ritenuti fidati dai filtri sono recapitati al destinatario / *Messages considered "trustworthy" by the filters are sent to the recipient.*

Le e-mail sospette vengono eliminate dal server di posta. / *Suspect emails are removed from the mailserver.*

Swap e sistema operativo Linux. La configurazione software risulta più complessa, in quanto il sistema fa uso anche di un database Sql per memorizzare i profili utente e la gestione capillare della quarantena dei messaggi di spam. In particolare utilizziamo Postfix come Smtp server. Il sistema per l'analisi dei contenuti è l'Amavisd che a sua volta utilizza SpamAssassin per le verifiche anti-spam e due antivirus in mutua esclusione (F-prot e ClamAV). E' attivo anche un servizio di webmail offerto tramite l'impiego di Squirrelmail, client di posta Imap scritto in Php. Esso include un ottimo supporto per i messaggi in formato Mime, è molto semplice da configurare ed è espandibile tramite l'impiego di plugin specifici. La gestione della quarantena dei messaggi di tipo spam può così essere affidata direttamente agli utenti.

Problematiche ricorrenti

A seguito di un intenso quanto inevitabile traffico di messaggi indesiderati, siano essi spam o virus, è buona norma verificare il numero di email in attesa di essere controllate. Analoga attenzione si dovrà porre nella personalizzazione della configurazione dell'eventuale database server che, anche in questo caso, dovrà essere in grado di gestire correttamente la quantità di connessioni contemporanee da parte sia del sistema di controllo dei contenuti sia del sistema di posta per la verifica dell'esistenza dei destinatari e la loro relativa autenticazione.

spam
prevention is the key

di **Stefano Ruberti**
Manager of the IIT-CNR email Unit

Today, email is one of the most popular communication media. And in the most diverse settings: from a merely academic instrument, over the years it has turned into the most widespread communication systems, even in professional settings. The communication-computerisation process, while promoting effective and efficient exchanges of information, could not help laying itself open to a whole range of "misuses": widespread proliferation of unwanted advertising messages, virus attacks, system overloads to tackle useless or even harmful traffic. It is a widespread opinion that such limits are associated with the nature of the communication protocol (Smtp) used for the email service, which is obsolete and therefore unable to fulfil the modern needs for privacy and confidentiality in digital communication. Who has ever escaped, after opening a simple mailbox, being bombarded with more or less "explicit" offers of unsavoury goods and services?

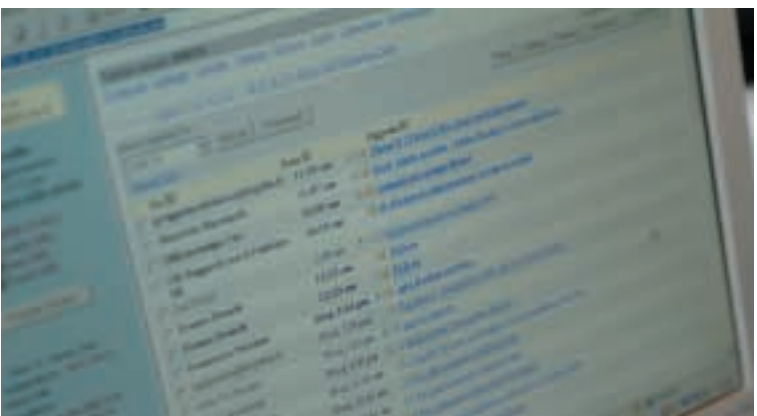
System planning and scaling

The operating unit of the ccTLD ".it" registry, for instance, receives on average 22 thousand messages a day, equal to approximately 120 MByte of traffic. Over 50 percent of them are classed as "unwanted". A phenomenon that has caught on everywhere by now: the email service of Iit-Cnr, the institute that hosts the Registry, reports the same results. The anti-spam and anti-virus systems that check the messages exchanged through the Registry and that have been implemented for approximately two years have certainly improved the quality of the service: however, this required developing a complex integrated system for the management of the email server based on robustness and integrity constraints and referred to Open-source tools.

To give the email service the right size to perform effective checks, the volume of messages to be handled must be clear beforehand, so that an adequate number of concurring content-checking systems may be implemented. With the registry, we have set a maximum of 10 processes per CPU: a value that still depends on the max amount of active Ram in the system since each case takes 25 to 30 Mbytes.

As to the anti-virus systems to be used, the tools to be chosen are those that need fewer resources. This is estimated by analysing in retrospect the behaviour of each product after a robust system-testing phase. To make a real example, the same anti-virus product used as a client on a Linux platform uses up, on average, 80ms, but, if it is moved to a Solaris platform, such figure drops by one size.

The message checks carried out by ordinary content-checking tools generally apply to both ingoing and outgoing messages and can be summed up in 6 main steps: checking whether the sender is included in the addressee's general and special white list and/or black list, checking the message "fingerprint", heuristic filters, Bayesian filters, anti-virus checks (see diagram across).



Technical solutions: a real case

It is difficult to list a selection of possible technical solutions to set up such an email service, since both commercial and free products are available for such checks. The Registry, for instance, offers an email service on a SUNFire 280R server with two Ultra Sparc processors, 4GByte Ram, and Raid 5. We use Sendmail, in conjunction with MailScanner, which in turn uses SpamAssassin for the anti-spam checks and two cascade-like anti-virus systems (Sophos and ClamAV). In this scenario, we do not need to supply any special service, since no real users are involved. The technical solution used by Iit-Cnr is based, instead, on a HP ProLiant DL380 server, equipped with 2 processors, 2GB Ram, 6x36Gbyte hard-disk in Raid 5 Hot Swap and a Linux operating system. The software configuration is more complex, since the system also uses an Sql database to store the users' profiles and for the intensive management of quarantined spam messages. In particular, we use Postfix as an Smtp server. The content-checkingsystem is Amavisd, which in turn uses SpamAssassin for the anti-spam checks and two mutually-exclusive anti-virus systems (F-prot and ClamAV). A web mail service is also offered by Squirrelmail, an Imap mail client written in Php. It includes an excellent support for Mime format messages, it is very simple to configure and can be expanded by means of specific plug-ins. So, the management of quarantined spam messages can be left to the users themselves.

Frequent problems

After intensive but unavoidable flows of unwanted messages, no matter if they are spam messages or viruses, it is a good rule to check the number of emails that are waiting to be checked.

The same attention must be paid to customising the configuration of any database server, which once again must be able to correctly manage the quantity of connections taking place at the same time, in terms of content-checking and in terms of email service, in order to check the addressees' existence and the authentications.

tutti gli appuntamenti
all events

nov 23

Assemblea del Registro
Pisa, Italy

Incontro annuale degli Internet Service Provider che hanno sottoscritto un contratto con il Registro del ccTLD.it./ *Annual meeting of the Internet Service Provider that have entered into contract with the ccTLD ".it" Registry*
http://www.nic.it/

nov 30 - dic 1-2

Corso Linux
Verona, Italy

Corso rivolto principalmente ai provider/maintainer che desiderano approfondire il sistema operativo Linux e apprenderne le principali funzionalità e caratteristiche. / *The Linux course is mainly targeted to those providers/maintainers wishing to approach the Linux operating system and become familiar with its main features and functions.*
http://www.nic.it

dic 3

Corso Legale
Verona, Italy

Lezioni finalizzate a dotare i partecipanti degli strumenti più idonei per operare correttamente nel settore delle registrazioni dei nomi a dominio sotto il ccTLD "it", fornendo elementi per conoscere nello specifico le procedure di risoluzione delle dispute sia giudiziali che stragiudiziali nonché quelle derivanti dal Regolamento di assegnazione e gestione dei nomi a dominio sotto il ccTLD.it. / *Course aiming to provide the participants with the most suitable means to work properly in the registration of domain names under the ccTLD "it", by providing specific information on the procedure for the settlement of at-court and out-of-court disputes as well as disputes arising from the ccTLD "it" domain names assignment and maintenance Rules.*
http://www.nic.it

dic 1-5

ICANN 2004
Cape Town, South Africa

Tra i meeting che ICANN organizza annualmente, l'evento di dicembre è senza dubbio quello più importante della stagione. / *Among all meetings organised by ICANN every year, this is with no doubt the most important of 2004.*
http://www.icanncapetown.co.za/

feb 22-23

CENTR general Assembly 25
Bruxelles, Belgium

CENTR è un'associazione che raggruppa molti dei registri del ccTLD, come ad esempio il .it in Italia e il .fr in Francia. / *CENTR is an association of Internet Country Code Top Level Domain Registries, such as .it in Italy and .fr in France.*
http://www.centr.org/

dic 1

W3C 10th Anniversary
Boston, MA

Creato nell'ottobre 1994, il World Wide Web Consortium (W3C) si occupa dello sviluppo di tecnologie interoperabili e protocolli comuni (specifiche, linee guida, programmi e tool) al fine di garantire la piena potenzialità della Rete. Il W3C è un gruppo di discussione per l'informazione, il commercio e la comunicazione. / *The World Wide Web Consortium (W3C), which was created in October 1994, develops interoperable technologies and common protocols (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, and communication.*
http://www.w3c.org/2004/09/W3C10.html

dic 6-8

OSDI '04
San Francisco, CA

Sesto simposio sulla creazione e l'implementazione dei sistemi operativi. OSDI è un appuntamento rivolto a professionisti provenienti sia dal mondo accademico che industriale e rappresenta un importante gruppo di discussione per tutti gli aspetti inerenti alla creazione e l'attivazione dei sistemi operativi. / *6th Symposium on Operating Systems Design and Implementation. OSDI brings together professionals from academic and industrial backgrounds in what has become a premier forum for discussing the design, implementation, and implications of systems software.*
http://www.usenix.org/events/osdi04/

dic 9-10

Chinese-European Network Symposium
Shanghai, Cina

Symposium con una base molto importante per i ricercatori nella comunicazione e cooperazione fra L'Europa e la Cina, nell'area di network avanzata e soluzioni broadband / *Symposium with an important platform for researchers to communicate and cooperate between Europe and China in the field of advanced network and broadband solutions*
http://www.ec-bridge.org/shanghai.shtml

gen 24-28

IT-Defense 2005
Cologne, Germany

Il tema della sicurezza informatica sarà trattato in occasione della terza edizione della conferenza IT-defense, che si terrà a Colonia dal 24 al 28 gennaio 2005. / *IT security will be discussed on the occasion of the third edition of the IT-Defense Conference, taking place in Cologne from 24th to 28th January 2005.*
http://www.it-defense.de/intro.html

feb 3-4

NDSS'05
San Diego, California

Simposio annuale sulla sicurezza delle reti e dei sistemi distribuiti / *Annual Symposium on Network and Distributed System Security*
http://www.isoc.org/isoc/conferences/ndss/05/index.shtml

Servizi a cura di Ana Corujo

il gotha di internet a convegno per la settima assemblea del registro

the internet elite meets for the seventh assembly of the registrar

Nuovi strumenti di lavoro per i registrar, statistiche aggiornate sulla diffusione di Internet in Italia, tempi e prospettive del nuovo TLD ".eu". Sono gli argomenti caldi all'ordine del giorno della settima assemblea del Registro del ccTLD ".it". L'evento, che annualmente richiama sotto la torre i massimi esponenti della comunità Internet italiana e l'esercito di registrar che quotidianamente interagisce con il Registro, si svolgerà il 23 novembre nella sala convegni dell'Area di ricerca del Cnr di Pisa. Introdurrà i lavori il professor Franco Denoth, direttore dello IIT e responsabile del Registro. A seguire le relazioni di tutti i responsabili delle unità e dei progetti connessi all'attività di registrazione dei nomi a dominio. Come consuetudine, il Registro presenterà anche i risultati dello studio della diffusione di Internet in Italia, quest'anno focalizzato sulle persone fisiche e sulle associazioni *no-profit*.
A chiudere i lavori dell'assemblea l'intervento di Joy Marino, presidente della Commissione regole, che illustrerà il bilancio del primo anno di attività dell'organismo tecnico-consultivo del Registro incaricato di formulare le regole e procedure tecniche per l'assegnazione e gestione dei nomi a dominio ".it".

New work tools for the registrars, updated statistics on the use of the Internet in Italy, timelines and prospects of the new TLD ".eu". These are the hot issues on the agenda of the seventh assembly of the ccTLD ".it" Registrar. The event, which every year brings under the tower the leading figures of the Italian Internet community and the army of registrarsthat interact every day with the Registrar, will be held on November 23rd in the meeting hall of the Research Area of CNR (National Research Council) in Pisa. The agenda will be introduced by professor Franco Denoth, director of ITT and manager of the Registrar. This will be followed by presentations of managers from all units and projects connected with the domain name registration activity. As usual, the Registrar will also announce the results of the survey of the use of the Internet in Italy, which this year focussed on natural persons and non-profit organisations.
The assembly will be closed by a speech by Joy Marino, president of the Rules Committee, who will illustrate the balance sheet for the first business year of the technical-advisory body of the Registrar in charge of developing the technical rules and procedures for the assignment and management of ".it" domain names.

una risposta per tutto
we answer your questions

Telefono / *Phone number*:
+39-050-3139811

Gli operatori rispondono nei giorni feriali con il seguente orario: 9:30-12:30 e 14:30/18:00.

The Registry help-desk operators answer your calls on working days, 9:30 - 12:30 a.m. and 2:30 - 6:00 p.m.

FAX

Per comunicazioni con l'Unità Relazioni Esterne / *External Relations Unit fax:*
+39-050-3152713

Lettere di assunzione di responsabilità / *Letter of assumption of responsibility:*
+39-050-542420

Solo cambi provider/maintainer, trasferimenti, cancellazioni ed altre operazioni sui nomi a dominio / *Only for provider/maintainer changes, transfers of domain names and other operations on domain names:*
+39-050-570230

E-MAIL

hostmaster@nic.it:
per informazioni sulle procedure e regole di registrazione di nomi a dominio / *information requests on the procedures and rules to register domain names under ccTLD "it"*

fatture@nic.it:
per informazioni sulle fatture verso provider/maintainer / information requests on invoices sent by Registry to the providers/maintainers that have a contract to register under ccTLD ".it"

webmaster@nic.it:
per suggerimenti e commenti sul sito web del Registro / *comments and tips regarding the Registry website*

corsi@nic.it:
per i corsi organizzati dal Registro / *information requests on Registry courses*

corso-linux@nic.it:
per i corsi Linux organizzati dal Registro / *information requests on Registry Linux courses*

corsi-pki@iit.cnr.it:
per i corsi PKI organizzati dal Registro / *information requests on Registry PKI-courses*

newsletter@nic.it:
per contattare la redazione della newsletter del Registro / *to contact the Registry newsletter offices*