

Diritto ed economia delle nuove tecnologie
Collana a cura di Daniele Minotti

2

Sicurezza e anonimato in rete

Profili giuridici e tecnologici della navigazione anonima

A cura di
ANDREA MAGGIPINTO
e
MICHELE IASELLI

Prefazione di
DANIELE MINOTTI

CON I CONTRIBUTI DI
Stefano Aterno
Michele Iaselli
Andrea Maggipinto
Giovanni Nacci
Massimiliano Redolfi

NYBERG EDIZIONI - MILANO

ISBN 88-901299-7-2

TUTTE LE COPIE DEVONO RECARE IL CONTRASSEGNO DELLA
SIAE

© Copyright 2005 Nyberg S.r.l. - Milano - Tutti i diritti riservati. È consentita la riproduzione o fotocopia solo nei limiti stabiliti dalla legislazione vigente. La traduzione, l'adattamento totale o parziale, nonché la memorizzazione elettronica, sono riservati per tutti i Paesi.

Tipografia Copy & Photo S.r.l., via Caruso 2, 20133 Milano

INDICE SOMMARIO

Prefazione di Daniele Minotti	<i>pag.</i> 5
--	------------------

Capitolo I
NAVIGAZIONE ANONIMA IN RETE
di Michele Iaselli

1. Cos'è la navigazione anonima e perché si ricorre ad essa	9
2. Legittimità o illegittimità della navigazione anonima	12
3. Privacy e tecnologia: l'eterna contrapposizione.....	15
4. Privacy ed Internet: le principali problematiche.....	18

Capitolo II
ANONIMATO IN RETE: NOTE TECNICHE
di Massimiliano Redolfi

1. Reti digitali	25
1.1. Architetture e standard di telecomunicazione	26
1.2. Internet.....	27
1.3. Internet: il protocollo IP.....	29
1.4. Internet: il protocollo TCP ed i servizi applicativi.....	30
1.4.1. La posta elettronica	31
1.4.2. Il World Wide Web.....	32
1.4.3. Il peer-to-peer	32
2. Anonimato e offuscamento dell'informazione.....	32
2.1. Principi base per l'anonimizzazione.....	34
2.2. Navigazione anonima. I server proxy	34
2.3. Posta anonima.....	39
2.4. File Sharing.....	40
2.5. Considerazioni generali sulla navigazione anonima	42
2.6. Contromisure per l'identificazione	42
2.6.1. Log dei flussi dati	43
2.6.2. Analisi statistica del traffico.....	43
3. Il futuro	44

Capitolo III
ANONIMATO IN RETE: PROFILI GIURIDICI E DI SICUREZZA
di Andrea Maggipinto

1. Circolazione delle informazioni e <i>disgregazione informativa</i>	47
1.1. Privacy e sicurezza nella Società dell'Informazione.....	48
1.2. Libertà e standardizzazione dei comportamenti	50
2. In Rete: e-privacy e network security	52
2.1. Internet e i soggetti interessati dalla disciplina sulla privacy.....	52
2.2. Le caratteristiche della Rete.....	53
2.3. Perché porsi il problema della privacy in Internet?.....	54
2.4. Il quadro normativo	56
2.5. Profili di sicurezza	58
2.6. Sicurezza in rete	59
2.6.1. Quali disposizioni a tutela della sicurezza dei dati su Internet	60
2.6.2. Gli standard di sicurezza informatica (rinvio)	63
3. Identità e anonimato in rete	63
3.1. I dati anonimi nel Codice privacy	65
3.2. L'anonimato protetto	66

Capitolo IV
SICUREZZA INFORMATICA E GESTIONE DEL RISCHIO
di Giovanni Nacci

1. Anonimato: definizione e origine dell'esigenza	69
2. Sicurezza, privacy e anonimato nella Società dell'Informazione.....	72
3. Sicurezza informatica: definizioni.....	76
3.1. Definizione <i>aziendalistica</i>	77
3.2. Definizione <i>proattiva</i>	77
3.3. Definizione <i>qualitativa</i>	77
3.4. La definizione <i>funzionale</i>	78
4. Valutazione e gestione del rischio.....	79
4.1. Identificazione del profilo di utenza.....	80
4.2. Identificazione delle risorse <i>appetibili</i>	81
4.3. Identificazione dei rischi reali.....	83
4.4. Identificazione delle minacce.....	84
4.5. Valutazione dell'impatto e reazione al rischio	85

4.6. Conclusioni.....	86
5. Internet: sicurezza, anonimato e misure antiterrorismo	87

Capitolo V
PROFILI PENALI DELL'ANONIMATO IN RETE
di Stefano Aterno

1. Il desiderio di anonimato e il rapporto con il diritto penale	93
2. Le condotte criminose penalmente rilevanti	100
2.1. I compartecipi anonimi nella commissione di reati in rete: il problema della configurabilità del reato di associazione a delinquere.....	110
2.2. Cyber-terrorismo e reati connessi al terrorismo.....	114
3. La recente legislazione antiterrorismo. La conservazione ed il monitoraggio dei dati di traffico	117
3.1. L'affievolimento del diritto all'anonimato.....	124
3.2. L'affievolimento del diritto alla privacy	127
4. Privacy: trattamento dei dati anonimi e irrilevanza penale	128
5. Un anonimato ed una sicurezza sostenibili. La "Securacy"	129

BIBLIOGRAFIA

<i>Studi e Volumi</i>	131
<i>Articoli e Saggi</i>	135

PREFAZIONE

di Daniele Minotti

daniele@minotti.net

“Without anonymity there can never be true freedom of speech”.

Questo brano è tratto dal sito di Freenet, progetto voluto dallo scozzese Ian Clarke per la realizzazione di un sistema atto a garantire la libertà di espressione su Internet mediante una comunicazione anonima.

Il progetto, già operativo anche se in continuo affinamento, si dichiara, dunque, veicolo ideale di libertà e democrazia proprio per l'opportunità di comunicare senza il timore di essere identificati ed eventualmente perseguiti.

Ma è vera libertà? È vera democrazia? Non è questa la sede per scomodare troppo le categorie della filosofia; ma, di certo, il tema dell'anonimato, inteso come strumento per la realizzazione del massimo grado di libertà di espressione senza vincoli e censure, è sempre stato nodale. E, oggi, lo è ancor di più con l'avvento delle nuove tecnologie, specie quella telematica.

Se, infatti, Internet garantisce un flusso di comunicazioni inimmaginabile sino a poco tempo fa (divenendo, così, moltiplicatore proprio di libertà e di democrazia), se la stessa tecnologia ha portato con sé nuovi strumenti per il singolo (ad esempio i server anonimi) è pur vero che la Rete, anche a causa della sua diffusione, si pone come uno dei mezzi più attaccabili, specie se gestita e utilizzata senza una sufficiente consapevolezza.

È fin troppo facile ricordare 1984; soprattutto, sarebbe riduttivo. Nell'era di Internet la partita si gioca su altri livelli, contro mezzi assai più subdoli, meno palesi, semplicemente diversi: in una parola, tecnologici.

Il controllo muta fisionomia e si ha l'impressione che non serva più soltanto ad inibire comportamenti, ma anche a colpirli a posteriori dimenticando la natura di *extrema ratio* di qualsiasi punizione. Basta ricordare il saggio di Foucault dal titolo emblematico: Sorvegliare e punire.

Proprio in tale cornice, nella sensazione di trovarsi in un Panopticon tecnologico, l'anonimato è divenuto l'ultima frontiera dei diritti civili al di là del non più sufficiente diritto all'oblio. Necessità percepita anche dal nostro legislatore con la recente disciplina sui dati personali.

Anonimato, dunque, non come annullamento dell'"individuo", ridotto al nulla, ma sua massima esaltazione. Mera utopia? No, non è questo il punto. Piuttosto, il lato debole della teoria che in Freenet trova la sua espressione più estrema è lo smaccato individualismo.

Se esistono i diritti dei singoli, ancorché fondamentali, gli stessi singoli sono comunque elementi vitali della società che si identifica nello Stato nella sua espressione democratica.

Il singolo gode di diritti anche come associato, non soltanto in quanto "Unico" come nell'idea anarchica - e pur suggestiva - di Stirner. La società ha il diritto di difendersi pure dagli attacchi dei singoli secondo una scala di valori che, inevitabilmente, patisce l'influenza delle contingenze, non potendo cristallizzarsi indipendentemente dai fattori spazio-temporali. E, d'altro canto, la società non può prevaricare il singolo in nome (o con la scusa) della sicurezza comune.

La storia, in concreto, ci narra di continui ribaltamenti di fronte: sicurezza vs. anonimato e anonimato vs. sicurezza. Viviamo, specie dopo il drammatico "9/11", in un periodo di emergenza. Tutti lo conosciamo e sarebbe irresponsabile sminuire lo stato dei fatti o, peggio, ignorarlo.

La legislazione dell'indomani è indubbiamente una reazione che cavalca il destriero più veloce del palio, ma anche il più indomabile: il terrore. E se da un lato la scelta di un campione così apparentemente performante può dimostrarsi fallimentare, dall'altro, per ciò che riguarda più da vicino la produzione legislativa dell'emergenza, non si può negare che, in questo clima, è facile dare una parvenza di legalità e desiderabilità a strumenti che, talvolta, appaiono voluti soltanto per facilitare l'operato dei controllori in assenza di una vera strategia della prevenzione e con qualche imbarazzante abbattimento di limiti comunemente riconosciuti.

Intercettazioni preventive (introdotte non a caso con il d.l. 18 ottobre 2001, n. 374 subito dopo gli attentati di New York), obblighi di conservazione di dati telefonici e telematici per un periodo di tempo non irrilevante e scollamenti dal rito accusatorio (imposti dopo gli attacchi a Londra) sono soltanto alcuni esempi di legislazione emergenziale.

Misure inevitabili, dovute, giuste? Non è facile dare una risposta. Sicuramente certe regole possono dirsi accettabili soltanto se vigenti a

tempo determinato, come dichiarato proprio dal legislatore nel d.l. 27 luglio 2005, n. 144. Ci auguriamo senza proroghe pretestuose nella fase della cessata (o ridotta) emergenza.

Mai dimenticare, però, che l'anonimato è una condizione "normale" che non può essere criminalizzata a meno che non si voglia cadere in un'imbarazzante contraddizione proprio con il "Codice in materia di protezione dei dati personali".

L'argomento, come spero di aver reso chiaro in queste mie brevi considerazioni, non riguarda soltanto i giuristi impegnati sul fronte del diritto di Internet. Sia che si parteggi per una tutela assoluta dell'anonimato del singolo, sia che si ritenga dovuta una qualche forma di controllo, il tema non può essere ignorato da chi ha compreso l'importanza della Rete: come singolo e come consociato, qualità che riguardano ogni creatura sociale.

Capitolo I

NAVIGAZIONE ANONIMA IN RETE di Michele Iaselli¹

SOMMARIO: 1. Cos'è la navigazione anonima e perché si ricorre ad essa 2. Legittimità o illegittimità della navigazione anonima 3. Privacy e tecnologia: l'eterna contrapposizione 4. Privacy ed Internet: le principali problematiche.

1. Cos'è la navigazione anonima e perché si ricorre ad essa

La diffusione di Internet e principalmente l'evoluzione delle linee digitali (xDSL) che sta avvenendo in Europa e che è avvenuta negli Stati Uniti già da tempo, ha praticamente portato Internet "24 ore su 24", in modo continuativo e fisso nelle case di molti uffici e famiglie; ma se da un lato migliorano con passi da gigante la velocità di connessione e la potenza dei PC, dall'altro non si assiste ad un perfezionamento dei parametri di sicurezza degli utenti, che sono sempre più spiati, mettono a repentaglio la loro privacy e sono sempre più vittime di hacker, virus e pirati informatici. Ormai tutti sappiamo che quando ci si connette alla rete, il nostro provider ci assegna un indirizzo univoco (IP address) che identifica da quel momento in poi tutto ciò che avviene durante la nostra connessione. Tramite questo indirizzo, che rimane registrato per molto tempo nei log del provider, chiunque può risalire in qualsiasi momento e in poco tempo all'username dell'utente collegato in quel momento ed eventualmente, qualora lo richieda un'indagine, anche al numero di telefono del chiamante.

Molti hanno l'impressione che la navigazione in Internet sia anonima, che si possa andare da un sito all'altro senza lasciare traccia,

¹ Avvocato, Funzionario del Ministero della Difesa, è Docente in materia di Legislazione New Economy (CARID - Università di Ferrara) e in materia di informatica giuridica presso la scuola forense di Capitanata. Ha pubblicato diverse monografie in materia di diritto delle nuove tecnologie nonché articoli e saggi su riviste in formato elettronico e cartaceo.

che si possa leggere questa o quella pagina, entrare in questo o quel sito senza il pericolo di essere identificati.

E che dire della posta? Sembra che basti aprire un account con un nome fittizio per poter spedire messaggi nella totale anonimità. Naturalmente tutto ciò non è vero. In realtà, nel momento in cui si entra in un sito, si compila una form, si spedisce una lettera, siamo immediatamente identificati. Il server del sito, e quindi il gestore del sito ma anche qualsiasi autorità interessata, riceve e conserva dati quali il tipo di browser, la risoluzione video, il sistema operativo, quale sito abbiamo visitato in precedenza, ma soprattutto il nostro indirizzo IP.

L'indirizzo IP, una serie di numeri tipo "194.25.65.221", identifica con precisione il nostro computer, meglio ancora di un'indirizzo stradale, perché arriva fino alla nostra scrivania, alla nostra tastiera, come se fosse un'impronta digitale.

Dall'indirizzo IP è possibile sapere non solo da quale rete chiamiamo (una Lan aziendale, un Isp, un Adsl...) ma il più delle volte esattamente il computer che stiamo usando per navigare. E quindi la persona che è entrata nel sito, ha letto quella pagina, ha compilato quel modulo, ha spedito quella mail.

Ma al di là di questa prima considerazione, la cosa forse più grave è che molti dei programmi installati sul nostro computer oggi sono capaci di trasmettere e rivelare molte informazioni personali sui siti dove navighiamo e tutto ciò non viene mai detto o accennato dai produttori di software, avviene in modo invisibile, all'insaputa degli utenti ignari, che in questo modo diventano vittime inconsapevoli di spammers (coloro che inviano montagne di e-mail pubblicitarie sulle caselle di posta) e degli hackers. Penso che nessuno di noi avrebbe installato Internet Explorer 5 se avesse saputo fin dal principio che questo browser mette a rischio la privacy e che rende il computer vulnerabile ai virus provenienti via e-mail, eppure queste cose non sono state mai dette e vengono fuori soltanto adesso dopo che la maggior parte degli utenti ha installato e usa Explorer 5.

A questo punto per evitare di essere identificati facilmente in rete con tutti i rischi conseguenti esiste la possibilità di navigare in modo anonimo e cioè mascherare l'IP. Questo è possibile, innanzitutto, tramite alcuni specifici software, si pensi ad esempio a *Multiproxy* nato per Windows 95 e 98 che nasconde l'indirizzo IP dell'utente utilizzando una lista di server proxy pubblici; oppure *Jap* programma free che nasconde l'indirizzo IP dell'utente durante la navigazione, basandosi su una serie di Mix in cascata che codificano le informazioni nel passaggio tra un Mix e l'altro; o ancora *Primedius Web Tunnel* programma dall'uso

semplicissimo, la cui configurazione è operata in modo automatico senza obbligare l'utente a modifiche nella configurazione di Internet Explorer. La versione Freeware permette di navigare in modo anonimo per un traffico limitato a 4Mbyte al giorno, utile per controllare un nuovo account di posta sul web o per postare in newsgroup o forum di discussione in cui il traffico è molto basso.

In realtà, al di là di questi programmi per navigare anonimamente è senz'altro più comodo utilizzare alcuni siti i quali offrono il servizio di navigazione anonima, cioè mascherata, in maniera gratuita o a pagamento. Quello che succede, a livello tecnico, è che le nostre richieste di pagine Web vengono inviate al centro servizi, il quale effettua la richiesta al sito che vogliamo chiamare e ci inoltra le risposte. Il sito più famoso che offre un servizio di questo tipo è *Anonymizer*² un servizio gratuito che ci “presta” un suo IP casuale, senza registrarne i dati, attraverso il quale possiamo navigare in qualsiasi sito lasciando un IP anonimo. Per usare il servizio non serve alcuna registrazione, basta andare alla url www.anonymizer.com/index.shtml e digitare la url del sito che vogliamo visitare in modo anonimo. Da quel momento navigheremo senza che nessuno possa risalire alla nostra identità.

In effetti il server di Anonymizer si frappone fra noi ed i siti che visitiamo. Ogni volta che clicchiamo su un link, la richiesta arriva ad Anonymizer, che provvede a caricare la pagina ed a rispedircela. Il server del sito richiesto vede solamente l'IP di Anonymizer, e non può sapere che fine faccia, che strada prenda la pagina richiesta.

Ma ciò comporta anche degli inconvenienti e cioè innanzitutto un'effettiva lentezza nel download delle pagine e poi nel puro stile di Internet la possibilità di scegliere tra due opzioni: una navigazione gratuita con il vincolo, piuttosto fastidioso, della visualizzazione di banner (sponsorizzazione e pubblicità varie) nelle pagine che visualizziamo in maniera anonima oppure una navigazione a pagamento previa sottoscrizione di un abbonamento, diviso in tre tipologie, ma possiamo dire che per l'utenza standard il primo è quello più indicato: per la modica cifra di 50 dollari all'anno ci viene offerto Anonymous Web Browsing con “protezione sicura”.

Possiamo quindi navigare in maniera “invisibile” per i siti che visitiamo, per indagini di marketing o nei siti dei concorrenti, per “spiarli” senza far loro sapere che li abbiamo chiamati.

² www.anonymizer.com/.