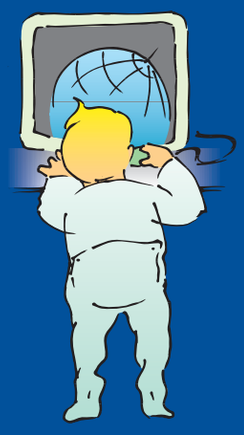


www.socialnews.it

Anno 8 - Numero 2
Febbraio 2011

realizzazione e distribuzione gratuita

SOCIAL NEWS

Rai Con il patrocinio Segretariato Sociale
www.segretariatosociale.rai.it

CULTURE A CONFRONTO - MENSILE DI PROMOZIONE SOCIALE

PREMIATO EUROMEDITERRANEO 2008

WIKI
LEAKS... PEDIA...

I WEB SEGRETI OPEN SOURCE.
SOCIAL NETWORK, PRIVACY, HACKERS,
CYBERCRIMINE, WEBSECURITY

ha collaborato HACKER REPUBLIC

Poste Italiane s.p.a. Spedizione in A.P. - D.L. 353/2003 (Conv. in L. 27/02/2004 n. 46) art. 1. comma 2, DBC TS

INDICE

Per contattarci:
redazione@socialnews.it, info@auxilia.fvg.it

I SocialNews precedenti. **Anno 2005**: Tsunami, Darfur, I genitori, Fecondazione artificiale, Pedopornografia, Bambini abbandonati, Devianza minorile, Sviluppo psicologico, Aborto. **Anno 2006**: Mediazione, Malattie croniche, Infanzia femminile, La famiglia, Lavoro minorile, Droga, Immigrazione, Adozioni internazionali, Giustizia minorile, Tratta e schiavitù. **Anno 2007**: Bullismo, Disturbi alimentari, Videogiochi, Farmaci e infanzia, Acqua, Bambini scomparsi, Doping, Disagio scolastico, Sicurezza stradale, Affidi. **Anno 2008**: Sicurezza e criminalità, Sicurezza sul lavoro, Rifiuti, I nuovi media, Sport e disabili, Energia, Salute mentale, Meritocrazia, Riforma Scolastica, Crisi finanziaria. **Anno 2009**: Eutanasia, Bambini in guerra, Violenza sulle donne, Terremoti, Malattie rare, Omosessualità, Internet, Cellule staminali, Carcere. **Anno 2010:** L'ambiente, Arte e Cultura, Povertà, Il Terzo Settore, Terapia Genica, La Lettura, Il degrado della politica, Aids e infanzia, Disabilità a scuola, Pena di morte. **Anno 2011:** Cristianesimo e altre Religioni.

Direttore responsabile:
Massimiliano Fanni Canelles

Redazione:
Capo redattore
Claudio Cettolo
Redattore
Ilaria Pulzato
Valutazione editoriale, analisi e correzione testi
Tullio Ciancarella
Grafica
Paolo Buonsante
Ufficio stampa
Elena Volponi, Luca Casadei, Alessia Petrilli
Ufficio legale
Silvio Albanese, Roberto Casella, Carmine Pullano
Segreteria di redazione
Paola Pauletig
Edizione on-line
Gian Maria Valente
Relazioni esterne
Alessia Petrilli
Newsletter
David Roici
Spedizioni
Alessandra Skerk
Responsabili Ministeriali
Serenella Pesarin (Direttrice Generale Ministero Giustizia), Paola Viero (UTC Ministero Affari Esteri)
Responsabili Universitari
Cristina Castelli (Professore ordinario Psicologia dello Sviluppo Università Cattolica), Pina Lalli (Professore ordinario Scienze della Comunicazione Università Bologna), Maurizio Fanni (Professore ordinario di Finanza Aziendale all'Università di Trieste), Tiziano Agostini (Professore ordinario di Psicologia all'Università di Trieste)

Responsabili e redazioni regionali:
Grazia Russo (Regione Campania), Luca Casadei (Regione Emilia Romagna), Tullio Ciancarella (Regione Friuli Venezia Giulia), Angela Deni (Regione Lazio), Roberto Bonin (Regione Lombardia), Elena Volponi (Regione Piemonte), Rossana Carta (Regione Sardegna)

Collaboratori di Redazione:
Federica Albini
Alessandro Bonfanti
Davide Bordon
Roberto Casella
Giulia Cella
Eva Donelli
Marta Ghelli
Alma Grandin
Elisa Mattaloni
Cristian Mattaloni
Anna Mauri
Cinzia Migani
Maria Rita Ostuni
Francesca Predan
Enrico Sbriglia
Cristina Sirch
Claudio Tommasini

Vignette a cura di:
Paolo Buonsante
Vauro Senesi

Periodico Associato

Grafici:
ISTAT. Istituto nazionale di statistica è un ente di ricerca pubblico

Con il contributo di:
Yvette Agostini
Nanni Bassetti
Alessandro Bogliolo
Luca Bovino
Renato Brunetta
Roberta Bruzzone
Massimo Condemi
Sara Crisnaro
Antonio Di Pietro
Rita Forsi
Paolo Gentiloni
Davide Giacalone
Fabio Ghioni
Nicola Grauso
Antonio Irlando
Andrea Zapparolo Manzoni
Gabriele Marra
Walter Paolicelli
Massimo F. Penco
Fabio Pietrosanti
Marco Pingitore
Francesco Pizzetti
David Roici
Sofia Scozzari
Roberto Setola
Luca Sileni
Luca Sofri
Francesco Soro
Mauro Volpatti

QR CODE

Questo periodico è aperto a quanti desiderino collaborarvi ai sensi dell'art. 21 della Costituzione della Repubblica Italiana che cosi dispone: "Tutti hanno diritto di manifestare il proprio pensiero con la parola, lo scritto e ogni mezzo di diffusione". Tutti i testi, se non diversamente specificato, sono stati scritti per la presente testata. La pubblicazione degli scritti è subordinata all'insindacabile giudizio della Redazione: in ogni caso, non costituisce alcun rapporto di collaborazione con la testata e, quindi, deve intendersi prestata a titolo gratuito.

Tutte le informazioni, gli articoli, i numeri arretrati in formato PDF li trovate sul nostro sito:
www.socialnews.it Per qualsiasi suggerimento, informazioni, richiesta di copie cartacee o abbonamenti, potete contattarci a: **redazione@socialnews.it**

Ufficio stampa: **ufficio.stampa@socialnews.it**

Registr. presso il Trib. di Trieste n. 1089 del 27 luglio 2004 - ROC Aut. Ministero Garanzie Comunicazioni n° 13449. Proprietario della testata: Associazione di volontariato @uxilia onlus www.auxilia.fvg.it - e-mail: info@auxilia.fvg.it

Stampa: **AREAGRAFICA - Meduno PN - www.areagrafica.eu**

Cosa è WIKI

Un wiki è un sito web (o comunque una collezione di documenti ipertestuali) che viene aggiornato dai suoi utilizzatori e i cui contenuti sono sviluppati in collaborazione da tutti coloro che vi hanno accesso. La modifica dei contenuti è aperta, nel senso che il testo può essere modificato da tutti gli utenti (a volte soltanto se registrati, altre volte anche anonimi) procedendo non solo per aggiunte, come accade solitamente nei forum, ma anche cambiando e cancellando ciò che hanno scritto gli autori precedenti. Ogni modifica è registrata in una cronologia che permette, in caso di necessità, di riportare il testo alla versione precedente; lo scopo è quello di condividere, scambiare, immagazzinare e ottimizzare la conoscenza in modo collaborativo. Il termine wiki indica anche il software collaborativo utilizzato per creare il sito web e il server. Wiki, in base alla etimologia, è anche un modo di essere.

Da Wikipedia, l'enciclopedia libera.

Vorrei che Hacker Republic diventasse una community di persone sveglie che mantengono un livello di attenzione alto e contribuiscono a generare informazione utile a tutta la comunità e, magari, anche a un movimento di opinione. Fabio Ghioni (pag. 35)

Ci ha lasciato Luciano Viaro, pilota di automobilismo storico e collaboratore di SocialNews. La redazione è vicino ai familiari in questo difficile momento e condivide l'immenso dolore. Uomo di talento e sensibilità, Luciano ha portato l'Alfa Romeo alla vittoria nella corsa piu' spettacolare del mondo,la Mille Miglia oltre altre sue numerosissime vittorie,prima tra le quali quelle di guidare le auto piu' spettacolari al mondo e farle ammirare a piccoli e grandi.Tra le varie iniziative promosse da Luciano volevamo ricordare il Progetto Mite che ha portato le persone non vedenti a far da navigatore a Luciano vincendo prima di tutto una sfida personale.

SocialNews Religioni errata corrige:

Nel numero di gennaio 2011 'Cristianesimo e altre religioni', nell'articolo del Prof. Giangiorgio Pasqualotto dal titolo 'Buddhismo e Cristianesimo', pag. 22, segnaliamo che i due termini karun e anatt mancavano di accento lungo sulle a finali. Inoltre, si precisa che il Prof. Pasqualotto insegna 'Estetica' e 'Storia della Filosofia Buddhista'.

Aspettando il 2012

di Massimiliano Fanni Canelles

Il 3 luglio 1969, il professor Leonard Kleinrock trasmise parte di una parola da un computer ad un altro, distante fisicamente oltre 500 km. Considerato un visionario, profetizzava un futuro caratterizzato dalla presenza di una rete "sempre funzionante, sempre disponibile, presente in tutti i luoghi e liberamente accessibile a tutti". Quel futuro e quella rete sono oggi realtà. Ogni giorno, milioni di persone navigano e lavorano su internet. Il Web 2.0 ha modificato profondamente il nostro modo di vivere e lavorare. Non solo. È diventato il terreno su cui hanno luogo relazioni, informazione, rivoluzioni, guerre. Alcuni Governi tentano di controllarlo, ma senza riuscirvi. "La rete è inarrestabile perché è globale e globalmente neutrale" (A. Bogliolo). Permette a chiunque di esprimersi e dare spazio alla propria creatività. Consente una collaborazione libera fra milioni di utenti, i quali, come in un enorme puzzle, possono divenire parte di un progetto, di un ideale, di un obiettivo, di un prodotto finale che spesso ha complessità e raffinatezza maggiore di quanto potrebbe ottenere un singolo gruppo di lavoro. La parola chiave di questo fenomeno è WIKI, un sistema aperto che permette a ciascuno di aggiungere il proprio tassello: un servizio, un'esperienza, un cliente. WIKI è software, giornalismo, informazione, conoscenza. È un sistema di collaborazione spontanea, che travolge tutto. Persino la comunità scientifica ha dapprima accettato, non senza difficoltà, la libera enciclopedia Wikipedia e si è poi convertita al sistema con Wikigenes, un motore di ricerca supportato dal Memorial SloanKettering Cancer Center, sede del primo esperimento per il trasferimento delle informazioni contenute nei geni umani. WikiLeaks si inserisce in questo scenario. Si impone all'attenzione internazionale divulgando informazioni riservate riguardanti il mondo politico e finanziario e scatenando le reazioni più disparate fra chi promuove la libertà di espressione e chi invoca il pericolo di destabilizzazione del potere costituito. Indipendentemente dalla posizione assunta al riguardo, il tema della sicurezza in rete costituisce comunque un problema reale. È necessario proteggere i dati, tutelare la privacy e prevenire la divulgazione e l'utilizzo delle informazioni per finalità non legittime. La libertà di circolazione delle idee è un veicolo fondamentale per lo sviluppo sociale ed economico dei Paesi moderni, ma, così come accade nel mondo reale, anche nella rete possono verificarsi fenomeni criminali assolutamente inaccettabili. Cybercrimini da contrastare con decisione, ma che non devono costituire la scusa per opporsi al nuovo movimento culturale, collaborativo ed "open source", che pone in discussione il concetto stesso di proprietà intellettuale finalizzata al profitto. I Creative Commons, le nuove licenze alternative al copyright, stanno invadendo la rete ed indeboliscono l'idea di proprietà ed i diritti commerciali su cui le multinazionali traggono i loro utili. Una rivoluzione nella rivoluzione, un nuovo modo di vivere contrapposto agli attuali valori costituiti da competizione, contrapposizione, ricerca del potere e della ricchezza ad ogni costo. 10 anni fa, Amazon era solo un fiume del Sud America, Yahoo! una parola coniata da Jonathan Swift per I Viaggi di Gulliver, Google un numero infinito formato dalla cifra uno e un centinaio di zeri. Grazie alla rete, ed alla sua caratteristica di mettere in relazione milioni di utenti, il mondo come lo conosciamo oggi non sarà più lo stesso. La rete come un'unica intelligenza planetaria e l'uomo come sua cellula portante stanno forse realizzando la profezia Maya che prevede, nel 2012, la fine del mondo come noi lo conosciamo.

"No, no, per carità, Galileo fermati! Il libero pensiero è attaccaticcio come un'epidemia. Ognuno ha da serbare il proprio rango, chi in vetta e chi nel fango". B.Brecht, Vita di Galileo.

Alessandro Bogliolo
Professore associato di Sistemi di Elaborazione dell'Informazione presso l'Università degli Studi di Urbino

La forza della rete

Il caso WikiLeaks mette in luce aspetti della rete e della comunicazione digitale che non avevano mai assunto una tale evidenza e una tale rilevanza, pur essendo riconducibili ai principi stessi sui quali si basa il funzionamento di Internet.

Riservatezza dei documenti digitali
Un documento digitale può essere cifrato utilizzando algoritmi talmente sofisticati e chiavi crittografiche talmente complesse da raggiungere livelli di sicurezza che hanno indotto diversi governi a vietarne l'uso per timore di perdere la capacità di controllo e compromettere l'efficacia delle azioni di intelligence. Ma per quanto inviolabile sia la cifratura di un documento, il suo utilizzo comporta la decifrazione su un sistema informatico e l'esposizione all'utente. Diversamente da ciò che accade nel mondo fisico, in cui circolano documenti cartacei, è impossibile mostrare a qualcuno un documento digitale senza rilasciarglie-ne una copia in chiaro, a meno di non avere pieno controllo del computer su cui il documento viene aperto. Peggio, nulla impedisce all'utente di produrre copie in chiaro del documento che ha letto e nulla rende le copie diverse dall'originale. La riservatezza dei documenti digitali è quindi affidata al contegno delle persone autorizzate ad accedervi, che possono rendersi direttamente o indirettamente responsabili dei leak (fughe di notizie).

Fornitori di anonimato
Un leaker (informatore), come ogni individuo, è responsabile delle proprie azioni. Ma, perché gli vengano attribuite, deve poter essere identificato. Chi naviga in Internet è identificato da un indirizzo numerico (l'indirizzo IP) assegnatogli (il più delle volte in modo temporaneo) dal provider che gli fornisce connettività. Quando l'utente utilizza un'applicazione in rete messa a disposizione da un server (come la posta elettronica, la chat, un servizio di trasferimento file, un blog o un wiki), l'unico dato certo (oltre a quelli che l'utente spontaneamente fornisce al gestore del servizio), è il suo indirizzo IP di provenienza. Finché il gestore del servizio traccia la corrispondenza tra azioni compiute e IP di provenienza, ed il provider traccia la corrispondenza tra indirizzo IP e identità personale, l'autorità giudiziaria può chiedere ad entrambi di accedere a tale documentazione ed associarla per ricondurre l'azione a chi l'ha compiuta. In molti casi, la catena di responsabilità è più lunga, ma il principio non cambia: ad ogni passo vengono tenute tracce (log) percorribili a ritroso per risalire all'utente. Poiché, per rispetto della privacy, solo l'autorità giudiziaria può accedere a tutte le tracce, l'utente può nascondere la propria identità agli altri utenti, ma non alla legge. Il meccanismo è semplice, sembra ineludibile. In realtà, è molto più vulnerabile di quanto sembri. Innanzitutto, la catena può essere lunghissima: un utente può rimbalzare attraverso decine di server assumendo indirizzi sempre diversi prima di presentarsi all'applicazione nei confronti della quale vuole mantenere l'anonimato. Ripercorrere a ritroso la catena di responsabilità può richiedere tempi e sforzi incompatibili con qualsiasi inchiesta. Se i server sono distribuiti su diversi Paesi, ai problemi tecnici si aggiungono quelli legali di competenza territoriale. Se poi anche uno solo dei server è installato in un Paese che non pretende la tracciatura, l'intera catena si spezza, rendendo l'utente definitivamente anonimo anche agli occhi della legge e del diritto internazionale. Esistono veri e propri fornitori di anonimato in rete che sfruttano questo meccanismo. TOR è uno di questi e WikiLeaks ne consiglia l'uso a tutela delle proprie fonti.

Diffusione
Quando il documento arriva nelle mani di WikiLeaks, occorre verificarne l'autenticità, esaminarne il contenuto, valutare l'opportunità di pubblicarlo e conservare ciò che si è deciso di non pubblicare. Tutte le verifiche e le valutazioni pongono problemi di tipo deontologico, prima ancora che tecnologico. Se la pubblicazione avviene direttamente su WikiLeaks, l'unico filtro deontologico applicato è quello a cui WikiLeaks stessa decide di attenersi in base alla propria mission. Se la pubblicazione avviene tramite organi di stampa, come nel caso delle ultime rivelazioni, a questo si aggiunge l'ulteriore filtro della deontologia giornalistica. I documenti che superano questi filtri diventano pubblici e nulla può più arrestarne la diffusione attraverso i media on-line, i social networks ed i media tradizionali.

Conservazione
La conservazione di ciò che non è (ancora) stato pubblicato rimette in gioco la crittografia. La persona a cui i documenti sono stati affidati (per intenderci, Assange) cifra i documenti con chiavi segrete che solo lui conosce e li affida ad un numero elevato di persone di sua fiducia che non conoscono la chiave. Ad altre persone di fiducia può affidare copie della chiave per tutelare la propria incolumità personale.

Invulnerabilità
È possibile opporsi a questo fenomeno? No. Si può solo complicare la vita a WikiLeaks attraverso forme di embargo che gli rendano difficile approvvigionarsi di ciò di cui ha bisogno per operare: server su cui pubblicare le proprie pagine, connessione Internet, nomi di dominio, donazioni... Ognuno di questi servizi è offerto da una o più società che operano in Internet e sulle quali i governi possono esercitare pressioni affinché interrompano i servizi erogati. Se ciò non basta, ogni servizio può divenire oggetto di attacchi informatici volti ad impedirne il funzionamento. Ma nei confronti di entrambe le forme di boicottaggio, la rete oppone difese immunitarie tanto più efficaci quanto più popolari sono i servizi da tutelare. La prima forma di difesa è la ridondanza: esistono migliaia di siti mirror che rilanciano i contenuti di WikiLeaks e molti nomi di dominio che li rendono raggiungibili (basta cercare "WikiLeaks" su Google per rendersene conto). La seconda forma di difesa è l'attacco: i sostenitori più scaltri di WikiLeaks possono portare attacchi informatici contro chiunque boicotti il servizio, esercitando pressioni opposte a quelle dei governi e non meno efficaci.

In 50 anni, la rete sembra diventata ben più potente del Dipartimento della Difesa degli Stati Uniti da cui ebbe origine. Ma la potenza della rete va anche oltre WikiLeaks: non solo saprebbe trovare alternative al suo smantellamento, ma, soprattutto, agisce con straordinaria efficacia a monte di ogni segreto con il cosiddetto "giornalismo dal basso" e con le testimonianze dirette diffuse sui social networks e sui media partecipativi che impediscono a molte informazioni di diventare segrete. La rete è inarrestabile perché è globale e globalmente neutrale.

Renato Brunetta
Ministro per la Pubblica Amministrazione e l'Innovazione

Innovazione e semplificazione

Semplificare è un lavoro faticoso, che richiede determinazione e tenacia. Le norme e l'adozione di misure organizzative e tecnologiche sono indispensabili, ma non bastano.

Le analisi condotte dalle principali organizzazioni internazionali individuano nella complicazione burocratica una delle prime cause dello svantaggio competitivo dell'Italia nel contesto europeo e nell'intera area Ocse. Com'è noto, la Commissione europea ha stimato per l'Italia un'incidenza dei costi amministrativi derivanti dai diversi livelli di governo pari al 4,6% del PIL, il che equivale ad un costo complessivo di circa 70 miliardi l'anno. È indubbio che, di fronte alla crisi, il peso degli oneri amministrativi sia ancor più intollerabile per le imprese e per l'intero sistema Paese. Per questa ragione, tagliare i costi della burocrazia per le imprese e disboscare la giungla delle procedure è divenuto un impegno prioritario. Di fronte alla crisi, il Governo Berlusconi ha così impresso una forte accelerazione agli interventi di semplificazione amministrativa. Il "Piano per la semplificazione amministrativa per le imprese e le famiglie 2010-2012", che ho presentato nel Consiglio dei Ministri del 7 ottobre 2010 e condiviso con le associazioni imprenditoriali, fornisce il quadro dei risultati raggiunti dal "taglia-oneri" (ne parlo più avanti) e definisce obiettivi, strumenti e piani operativi volti ad intensificare e completare le attività in corso e conseguire, entro il 2012, il traguardo di un taglio di oltre il 25% dei costi della burocrazia. Una delle più importanti novità del Piano è rappresentata dalla logica di risultato: il successo si misura sull'effettiva riduzione degli oneri e dei tempi burocratici per le imprese. Per ciascun intervento vengono stimati i risparmi attesi e definiti i tempi e le responsabilità. I risultati raggiunti vengono verificati con il coinvolgimento delle associazioni imprenditoriali. Non vanno sottovalutate le difficoltà e le forti resistenze radicate nei comportamenti consolidati delle amministrazioni. Semplificare è un lavoro faticoso, che richiede determinazione e tenacia. Le norme e l'adozione di misure organizzative e tecnologiche sono indispensabili, ma non bastano: è essenziale un'attenzione nuova all'implementazione e alla comunicazione. Il risultato, infatti, non è pienamente raggiunto se non è effettivamente percepito dalle imprese. In coerenza con gli impegni assunti in sede comunitaria, è quindi ormai a regime il cosiddetto "taglia-oneri": un'attività di misurazione e riduzione degli oneri amministrativi sulle PMI essenziale per tagliare in modo sistematico i costi della burocrazia. La misurazione è realizzata dall'apposita task-force coordinata dall'Ufficio per la semplificazione del Dipartimento della funzione pubblica, con la partecipazione delle associazioni imprenditoriali e l'assistenza tecnica dell'ISTAT. Essa consente di individuare le procedure e gli adempimenti più costosi da semplificare e di valutare l'efficacia di ogni intervento sulla base della stima dei risparmi. Con il "taglia-oneri", sono già state sottoposte a misurazione 71 procedure ad alto impatto sulle imprese, selezionate con le associazioni imprenditoriali: sono stati stimati costi burocratici per 21,5 miliardi di euro all'anno e adottati interventi di semplificazione in materia di lavoro, previdenza, prevenzione incendi e beni culturali che comportano un 'taglio' stimato di 5,5 miliardi di euro all'anno. Il risparmio atteso a regime dalle attività previste dal Piano per il completamento della misurazione e riduzione dei costi burocratici è pari a circa 12 miliardi di euro annui. Ad arricchire il quadro dei numerosi interventi di semplificazione operativi o in itinere vi sono anche le misure adottate in materia di edilizia libera, SCIA e Conferenza dei servizi, da tempo attese dal mondo imprenditoriale. Con la manovra finanziaria è stata inoltre introdotta un'innovazione senza precedenti per l'Italia: il principio di proporzionalità per gli adempimenti amministrativi, che verranno differenziati in relazione alla dimensione, al settore in cui l'impresa opera e all'effettiva esigenza di tutela degli interessi pubblici, in linea con le previsioni dello Small Business Act adottato a livello comunitario. Si tratta di un'operazione di semplificazione nuova per le oltre 4.500.000 PMI (il 95% delle quali ha meno di 10 addetti) che consentirà, tenendo conto anche dei risultati della misurazione, di eliminare o semplificare adempimenti inutili o eccessivi per le PMI sulla base del criterio di proporzionalità, e di estendere l'autocertificazione e l'uso delle tecnologie. Il Ministero per la Pubblica Amministrazione e l'Innovazione è già al lavoro per la predisposizione degli appositi regolamenti, con il coinvolgimento delle amministrazioni interessate e delle associazioni imprenditoriali, le quali hanno indicato le prime aree sulle quali intervenire: ambiente, prevenzione incendi e sicurezza sul lavoro. Non è tutto. Il disegno di legge collegato alla finanziaria 2010 contiene numerose e importanti misure di semplificazione, tra le quali si ricordano la previsione della "Carta dei doveri delle amministrazioni pubbliche" per contrastare le molestie amministrative ed assicurare l'effettività ai diritti delle imprese e dei cittadini, le misure in materia di privacy, il permesso di costruire on-line e l'estensione della riduzione degli oneri alle Regioni, agli Enti Locali e alle Autorità indipendenti. Sono stati inoltre definitivamente approvati e pubblicati i regolamenti sullo Sportello unico e sull'agenzia delle imprese. Accanto all'impegno del Governo e ad una nuova cooperazione tra Stato, Regioni ed Enti Locali, il fattore vincente di una politica di semplificazione è però rappresentato dall'ascolto e dal coinvolgimento delle imprese e delle loro associazioni, che partecipano con grande impegno alle attività di misurazione e riduzione degli oneri ed alla semplificazione per le PMI. Per questo ho deciso di promuovere sul web questa iniziativa. È in linea con le migliori esperienze di partecipazione europee (la consultazione francese Ensemble simplifions, il Kafka point belga, l'olandese Last van de overheid) e in un anno ha raccolto 370 segnalazioni concrete, puntuali e di qualità (il 24% delle quali proveniente da imprese e liberi professionisti) che hanno tracciato un quadro ampio e articolato della domanda di semplificazione in Italia.

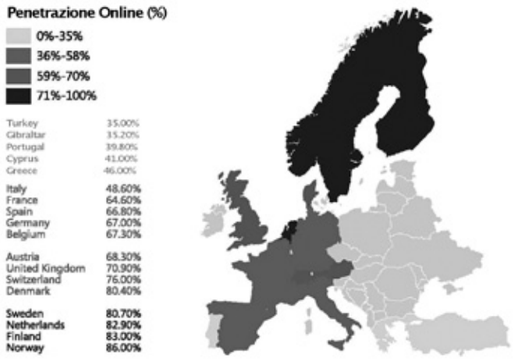
Paolo Gentiloni
Deputato, già Ministro delle Telecomunicazioni, Responsabile FORUM ICT PD

La fine della censura

Il direttore del New York Times, Bill Keller, ha riconosciuto, sia pur con qualche ritrosia, che l'attività di WikiLeaks può sostanzialmente definirsi "giornalismo" ed ha affermato che "i giornalisti dovrebbero provare un senso di forte allarme di fronte a qualsiasi azione che punti a perseguire Assange per un'attività che è propria di ogni giornalista".

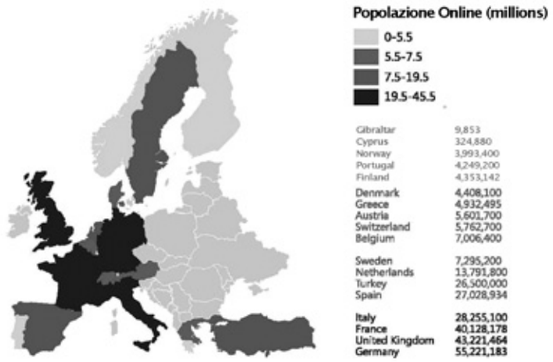
Solo tre mesi fa, il nome di Julian Assange non era certo noto a tutti. Il personaggio, tuttora misterioso e controverso, ha spesso polarizzato il dibattito in modo estremo: con Assange o contro? Trovo però più utile riflettere sulla portata complessiva del fenomeno WikiLeaks, il quale ha modificato gli equilibri delle diplomazie ed il ruolo della rete. Le riflessioni non riguardano un solo campo. Prima di tutto, dobbiamo interrogarci sul nuovo rapporto fra internet e trasparenza. Il web 2.0, con particolare riferimento all'affermazione dei social network, ha evidenziato come il concetto di privacy sia stato completamente scardinato e posto in discussione. Eppure, fino alla pubblicazione dei cablo, sembrava che il problema riguardasse solo i privati cittadini. WikiLeaks ha invece rivoluzionato anche la riservatezza dei governi e del potere. Il confine tra trasparenza e segreto di Stato non potrà più essere quello di una volta. L'amministrazione Obama ha investito, più di qualunque altra nella storia americana, sulla trasparenza e sulla condivisione delle informazioni attraverso il web ed i social media. Eppure, la reazione alla pubblicazione dei documenti ha dimostrato il suo timore nei confronti della libertà della rete, in precedenza tanto celebrata. L'approccio liberale proposto nel bellissimo discorso su Internet tenuto da Hillary Clinton al Newseum di Washington è stato ridimensionato. Al di fuori dell'aspetto politico, l'azione di WikiLeaks risulterà ancora più rilevante se riuscirà ad accendere i riflettori sul mondo finanziario, evidenziando i meccanismi economici che hanno scatenato la crisi mondiale. Un riferimento può essere considerato Rospil, un sito russo strutturato sul modello WikiLeaks: è guidato da Alexei Navalny, un avvocato che si è posto l'obiettivo di smascherare la rete di corruzione finanziaria attiva nei settori pubblico e privato in Russia. Un'altra riflessione riguarda il rapporto di WikiLeaks col giornalismo tradizionale e l'impatto provocato su di esso. I cabli sono stati pubblicati soprattutto da cinque grandi testate internazionali, The New York Times, Le Monde, El Pais, The Guardian e Der Spiegel. È grazie ad essi se WikiLeaks è riuscita anche a superare il blocco censorio esistente nella rete. Inoltre, i social media, la rete, quindi, hanno permesso una divulgazione immediata e simultanea. Ma il fenomeno ha sicuramente messo in crisi il sistema editoriale tradizionale. Alcuni giorni fa, il direttore del New York Times, Bill Keller, ha riconosciuto, sia pure con qualche ritrosia, che l'attività di WikiLeaks può sostanzialmente definirsi "giornalismo" ed ha affermato che "I giornalisti dovrebbero provare un senso di forte allarme di fronte a qualsiasi azione che punti a perseguire Assange per un'attività che è propria di ogni giornalista". Una dichiarazione del genere identifica WikiLeaks non solo quale fonte, ma addirittura come entità giornalistica e stimolo per il giornalismo d'inchiesta. L'impatto di WikiLeaks si riscontra anche nella nascita di siti cloni (Openleaks, Localeaks, ecc.), i quali, a differenza dell'originale, non controllano e centralizzano le informazioni ricevute. L'impatto è evidente anche nei nuovi progetti nati all'interno delle redazioni di alcuni grandi giornali ed alcune televisioni: al New York Times e ad Al Jazeera, per esempio, stanno nascendo uffici e servizi che consentono anche ad informatori anonimi l'invio di documenti. Da una parte, dunque, assistiamo ad un ridimensionamento della sfera della riservatezza, dall'altra, osserviamo un flusso di informazioni sempre meno filtrate. Una risposta censoria al fenomeno sarebbe inutile: Iran, Tunisia ed Egitto ci hanno mostrato come, nei Paesi privi di libertà e Democrazia, Internet rappresenti un'eccezionale spinta al cambiamento. Ma anche in Nazioni come l'Italia, dopo WikiLeaks, sarà molto difficile tollerare nelle istituzioni la mancanza di trasparenza e la carenza di risposte verso le esigenze di informazione dei cittadini. Nuovi equilibri nelle diplomazie, dunque, regole del giornalismo che cambiano, interrogativi sul rapporto fra riservatezza e rete. Al di là di ogni giudizio su Julian Assange e sui suoi metodi, è indubbio che WikiLeaks rappresenti un punto di non ritorno.

UTILIZZO DI INTERNET E DEI LIVELLI DI PENETRAZIONE DI TUTTA L'AREA EMEA



Datasource: Internet World stats, internet usage in Europe, December 2008

"Paesi Nordici che hanno un tasso di penetrazione di internet del 76% in media rispetto al 45% nel Sud Europa..."



Antonio Di Pietro
Deputato, già Ministro dei Lavori Pubblici e delle Infrastrutture, Presidente IDV

Una nuova censura

Con la scusa di tutelare la privacy e garantire la sicurezza sul web, il Governo e Agcom limitano la libertà d'espressione, opinione e condivisione della conoscenza. L'approccio più valido è quello che considera la libertà di circolazione delle idee un veicolo fondamentale per lo sviluppo sociale ed economico dei Paesi moderni.

In una società di diritto, le libertà individuali e collettive dovrebbero procedere di pari passo e in modo armonioso, senza mai autoescludersi. Quando si parla di rete, però, il tentativo di Governo e Agcom di limitare la libertà d'espressione, opinione e condivisione della conoscenza è palese, e viene mascherato con la finalità di tutelare la privacy e garantire la sicurezza sul web. L'Italia dei Valori è da sempre impegnata a difendere la diffusione delle informazioni su internet, contro ogni forma di censura. L'approccio che riteniamo più valido è infatti quello che considera la libertà di circolazione delle idee un veicolo fondamentale per lo sviluppo sociale ed economico dei Paesi moderni. Ma questa posizione, che non dovrebbe mai essere messa in discussione, pone la questione cruciale di come far convivere questo obiettivo con gli interessi di sicurezza della rete e con la tutela della privacy. In questo contesto, il Governo, in nome di obiettivi di facciata, ha investito l'Agcom del potere di chiudere siti e pagine web invocando la necessità di tutelare i cittadini, applicando il famoso bavaglio alla rete. In realtà, la privacy non viene intaccata quando informazioni già pubbliche trovano diffusione sulla rete. E non si viola il diritto d'autore, concetto attualmente in fase di evoluzione storica, nella condivisione tra cittadini. Al pari di una biblioteca dalla quale vengono presi in prestito dei libri, internet è diventato il non-luogo in cui i contenuti digitali possono muoversi a beneficio della comunità. I valori e le necessità collettive, nella società che immaginiamo, devono prevalere sugli interessi privati, così come afferma anche l'Onu in materia di sviluppi futuri della proprietà intellettuale. Il metodo applicato dal Governo in questa vicenda è, invece, conforme al modo di fare politica di questa classe dirigente: vengono scavalcate le altre istituzioni per accentrare potere e controllo, in quella che nel resto del mondo viene considerata censura. La delega all'Agcom scavalca in un colpo solo magistratura e Parlamento: la prima viene privata del compito di controllo e sanzione, tanto che non saranno i magistrati a definire la chiusura delle pagine web eventualmente accusate di violazione delle regole, ma direttamente l'autorità garante. Il Parlamento, invece, sede istituzionale nella quale dovrebbe essere discussa questa materia fondamentale, non viene nemmeno preso in considerazione. Allo stesso tempo, il vero approccio del Governo al tema appare evidente analizzando la vicenda del decreto Pisanu. Dopo aver rallentato per anni lo sviluppo di una rete wi-fi libera ed accessibile sul territorio italiano, il famigerato decreto era stato abrogato lo scorso dicembre. Ma, alle aperture ed alle speranze delle scorse settimane, ha fatto seguito una brusca frenata: un'ondata di burocrazia che ha fermato ancora una volta la crescita del numero degli access point liberi nel nostro Paese. La più recente uscita dell'Agcom, poi, contiene in sé tutte le note dell'anticostituzionalità e dell'oscurantismo: la possibilità di bloccare siti web stranieri dai contenuti "scomodi". E, ovviamente, sarebbe sempre l'Agcom a definire il concetto di "scomodo". Serve una moratoria sulle nuove regole della rete, che non possono essere calate dall'alto, ma devono essere condivise, sia tra i gruppi politici in Parlamento, sia in un tavolo il più ampio possibile, alla presenza anche delle associazioni che si occupano di rete e libertà digitali. Uno dei principi da preservare è l'equilibrio tra la difesa del diritto d'autore e la tutela dell'accesso alla conoscenza. Sarà importante anche definire una strategia condivisa, un'agenda digitale che fissi i passi da compiere per recuperare la distanza dal resto d'Europa, dove la diffusione e l'uso della rete, oltre che il rispetto nella quale è tenuta, sono avanti anni luce rispetto al dibattito nostrano. La libertà di informazione va tutelata da ogni censura preventiva. E in quest'ottica, il web deve restare uno strumento di partecipazione democratica a disposizione della società.

* *Autorità per le Garanzie nelle Comunicazioni*

Rita Forsi
Direttore dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)
Ministero dello Sviluppo Economico – Dipartimento per le Comunicazioni

Webinsicurity

Il fenomeno della diffusione delle informazioni condizionerà sempre più le sorti dei popoli. Nei prossimi anni, tali dinamiche tenderanno ad accentuarsi sempre più in concomitanza con la diffusione dell'alfabetizzazione informatica. La formazione di idee e movimenti può favorire il progresso sociale, ma risulta anche suscettibile di possibili strumentalizzazioni.

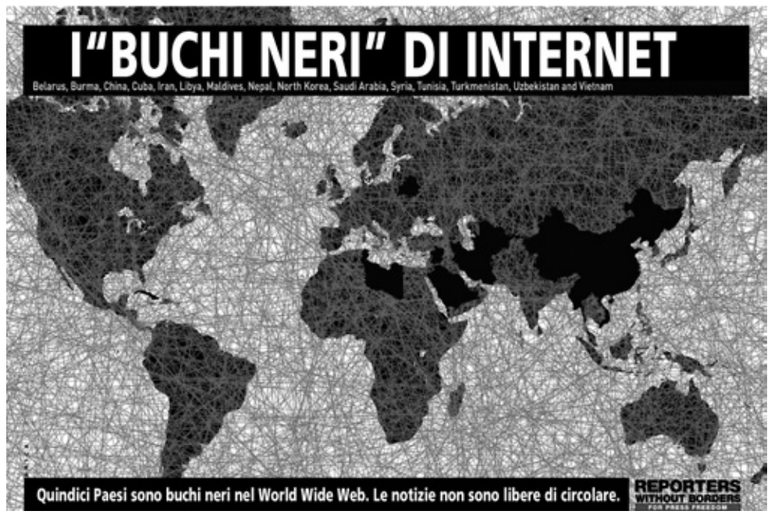
La diffusione inarrestabile di Internet degli ultimi decenni porta con sé importanti potenzialità di sviluppo economico, opportunità di incontro tra culture anche molto distanti e grande facilità nella diffusione delle informazioni. Tuttavia, alle opportunità derivanti dallo sviluppo della rete si accompagnano anche dinamiche complesse e rischi potenziali che vanno tenuti presenti. Il fenomeno della diffusione delle informazioni condizionerà sempre più le sorti dei popoli, in quanto capace di incidere profondamente nelle coscienze, nella formazione delle opinioni e del consenso politico. È sotto gli occhi di tutti come in Paesi quali Iran, Albania ed Egitto, i mezzi offerti da Internet, difficilmente controllabili dai governi nazionali, diversamente dalla televisione, abbiano modificato gli equilibri politici. Facile prevedere che, nei prossimi anni, tali dinamiche tenderanno ad accentuarsi sempre più, in concomitanza con la diffusione dell'alfabetizzazione informatica nelle popolazioni, riservata, al momento, solo alle nuove generazioni. La formazione di idee e movimenti attraverso una partecipazione diretta delle persone può favorire il progresso sociale, ma risulta anche suscettibile di possibili strumentalizzazioni. Il web, in quanto distribuito in varie Nazioni ed alimentato da tutti i potenziali fruitori della rete, è lo strumento caratterizzante questo processo. Il fenomeno WikiLeaks si inserisce in questo contesto, attraverso la divulgazione di informazioni riservate riguardanti il mondo politico e finanziario, originata da una fuga di notizie dall'interno. La vastità e l'estensione del bacino di utenti di Internet rende vano qualsiasi tentativo di controllo di tale fuga di notizie e di un rimedio a posteriori. A rendere il quadro WikiLeaks ancora più complesso, sono state le posizioni assunte e gli interventi effettuati dagli attori principali di Internet per contenere, da una parte, e mantenere in vita, dall'altra, il fenomeno. Si può intravedere uno scenario di vera e propria "guerra informatica". Amazon, che ospitava il sito di WikiLeaks sui suoi server, dopo lo scoppio dello scandalo ha sospeso il servizio di hosting. Paypal e mastercard, dal canto loro, hanno bloccato il flusso finanziario dei sostenitori di WikiLeaks. Un hacker di nome Jester è stato protagonista di un attacco volto ad oscurare i siti web di WikiLeaks. Al contrario, il gruppo di hacker "Anonymous", con l'operazione Payback, ha modificato il virus LOIC ("Low Orbit Ion Cannon") in maniera tale che i sostenitori della causa WikiLeaks, anche privi di qualunque conoscenza informatica, potessero diventare "pericolosi soldati nel loro esercito informatico". Si delinea in questo scenario la figura di un nuovo tipo di hacker, l'"hacker etico", un esperto di informatica che compie atti di pirateria non a fini di lucro, ma, tuttavia, non privi di implicazioni legali. Probabilmente, pochi, tra questi, conoscevano i risvolti legali di ciò che stavano facendo. È notizia di pochi giorni fa che una quarantina di questi attivisti sono stati arrestati in Francia e Gran Bretagna. La questione della sicurezza in rete è in realtà un problema sentito ben prima della nascita di WikiLeaks. In particolare, la tutela della privacy dei cittadini è una questione impostasi negli ultimi tempi in molti Paesi. Si è avvertito universalmente, nello sviluppo delle tecnologie informatiche, il rischio concreto di divulgazione ed utilizzo delle informazioni dei privati cittadini per finalità non legittime. Per questo motivo, molti Paesi si sono dotati di legislazioni sulla privacy assieme ad un quadro di misure tecnologiche volte ad impedire la rivelazione, la manipolazione e la distruzione dei dati personali immagazzinati e trasferiti sulla rete. La vulnerabilità della rete rispetto a potenziali attacchi informatici è oggetto di discussione nei governi nazionali e nei consessi internazionali. In particolare, l'Unione Europea, attraverso l'Agenda Europea del Digitale ed ENISA (l'Agenzia Europea per la Sicurezza delle Reti), ha posto la questione della sicurezza informatica tra i primi punti da affrontare per fare in modo che lo sviluppo delle tecnologie dell'informazione e della comunicazione favoriscano una crescita economica rapida e sostenibile dei Paesi europei che si concili con le esigenze di sicurezza e privacy dei cittadini. ENISA ha recentemente avviato delle esercitazioni europee contro gli attacchi cibernetici che hanno visto la partecipazione congiunta dei governi finalizzata a rafforzare la cooperazione degli Stati Membri. Il Ministero dello Sviluppo Economico, per il tramite dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, del Dipartimento Comunicazioni, ha partecipato attivamente all'iniziativa Cyber Europe 2010, coordinando un tavolo tecnico al quale hanno aderito i principali attori italiani operanti nel campo della sicurezza informatica. Il Direttore dell'Istituto Superiore CTI siede nel Management Board di Enisa. L'impegno è quello di recepire da tale consesso le esperienze più avanzate attualmente realizzate in Europa, ma anche di sollecitare, in ambito italiano, il massimo sforzo per catalizzare ogni singola iniziativa, magari già in essere ed anche di eccellenza, verso un percorso comune per aumentare il grado della sicurezza informatica in Italia. La fiducia dei cittadini in Internet, obiettivo prioritario dell'Agenda Europea del Digitale, è la condizione propedeutica per un effettivo utilizzo delle tecnologie informatiche come volano economico, in Europa e nel mondo. La condizione di buon utilizzo, invece, dipende dalla consapevolezza delle potenzialità dello strumento, dalla crescita della formazione in materia di sicurezza informatica e dalla necessaria adozione di opportune misure di protezione a sostegno di tutte le infrastrutture, con particolare attenzione a quelle critiche.

Nicola Grauso
Fondatore Video On Line, primo Internet provider italiano

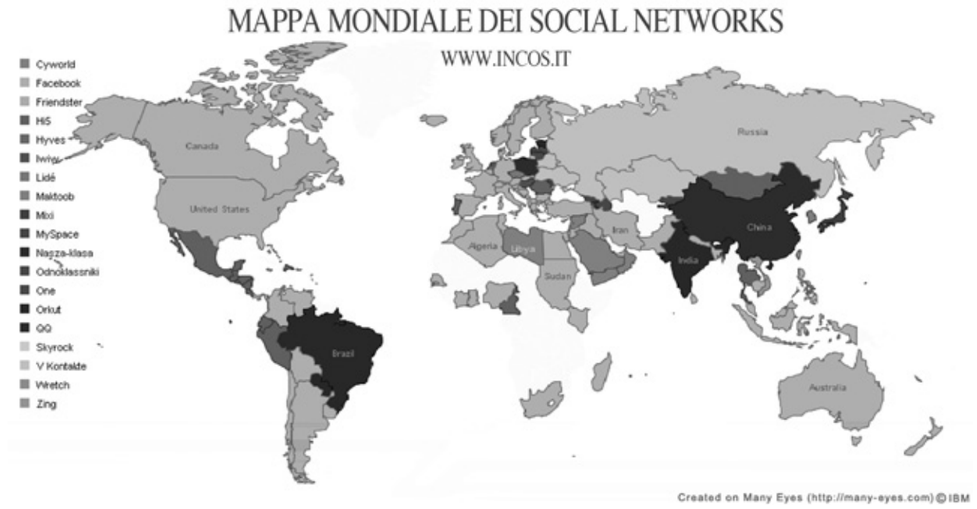
Voglia di privacy

Il tema della privacy, un tempo relativa soprattutto ai diritti di protezione, accesso e trasparenza dei cittadini rispetto all'invasività dello Stato, deve oggi essere affrontato dal legislatore con inevitabile ed indispensabile riguardo al fatto che la raccolta ed il trattamento di un numero sempre crescente di dati personali siano divenuti uno strumento essenziale e vitale per lo stesso funzionamento delle imprese commerciali.

Mettendo a nudo la fragilità delle misure di sicurezza con cui la diplomazia statunitense custodiva i propri "segreti", l'eco mediatica del caso WikiLeaks riporta all'attenzione degli operatori, giuridici, economici ed informatici, un problema che, pur diverso da quello strettamente connesso alle "imprese" di Julian Assange, ne è comunque prepotentemente evocato: la sicurezza nel trattamento dei dati personali, in un'epoca in cui questo avviene con l'uso normale della rete internet e di strumenti elettronici e, data la consolidata globalizzazione economica, assume una rilevanza pienamente transnazionale. Il tema della privacy nel trattamento dei dati personali, un tempo relativa soprattutto ai diritti di protezione, accesso e trasparenza dei cittadini rispetto all'invasività dello Stato (all'insegna dell'habeas corpus), deve oggi essere affrontato dal legislatore, dagli operatori economici e da quelli del settore informatico con inevitabile ed indispensabile riguardo al fatto che la raccolta ed il trattamento di un numero sempre crescente di dati personali siano divenuti uno strumento essenziale e vitale per lo stesso funzionamento delle imprese commerciali. Al di là di attività oggettivamente invasive e fastidiose (come quelle di numerosi call center), la rete internet assume un ruolo ormai normale, e tendente alla preponderanza, negli usi commerciali. Essi spaziano dalla fornitura alla clientela di informazioni essenziali alla stessa esecuzione di prestazioni di vendita e fornitura di beni e servizi, attività che tocca ormai tutti i settori, dal semplice scaricamento di musica alla vendita di beni ad elevato valore tecnologico e venale. In questo contesto, gli interessi delle imprese e quelli dei cittadini al mantenimento del pieno controllo sui propri dati personali devono essere contemperati. Diventa quindi importantissimo, e sovente trascurato, il tema delle misure di sicurezza volte a garantire l'effettività di un trattamento sicuro dei dati personali. Questi vanno posti al riparo da accessi abusivi, sottrazioni indebite e cancellazioni le quali, oltre ad un danno per le stesse imprese, si traducono in una menomazione di fatto del diritto/potere di controllo dei titolari dei dati. Quanto a sensibilità a questa problematica, l'Italia si è dimostrata all'avanguardia rispetto agli standard della legislazione europea (in special modo quella dei Paesi dell'Unione Europea, largamente ispirata a principi uniformi) e mondiale, dettando il Codice della Privacy. Sono state varate disposizioni meticolose, le quali, molto al di là degli standard europei, tendono a "coprire" ogni possibile punto critico sull'effettiva conservazione e l'effettivo trattamento dei dati in condizioni di sicurezza. Ad esempio, viene prescritto l'uso della crittografia per i dati sensibili e giudiziari trattati da soggetti pubblici o la cui azione abbia rilevanza pubblica, come quella di medici ed avvocati. Ma vi è una domanda a cui è necessario fornire una risposta, in considerazione del carattere spiccatamente transnazionale delle transazioni commerciali che avvengono attraverso internet (si pensi solo alla diffusione di servizi di pagamento come PayPal): qual è, nelle misure di sicurezza prescritte o adottate negli altri Paesi, la situazione in tema di effettiva protezione dei dati personali trattati dai soggetti diversi dallo Stato? A tale riguardo, e questo è un dato di fatto a cui si deve prestare suprema attenzione, specie in un'epoca come questa in cui nuovi attori si affacciano sulla scena del commercio internazionale fino ad avviarsi a divenire protagonisti, va detto che prevale una certa coincidenza tra il carattere più o meno "democratico" di uno Stato e la sua sensibilità a tale problematica. Se l'approccio statunitense, sul quale ci soffermeremo infra, è profondamente diverso dal nostro, si può dire che i Paesi dell'Europa (ivi compresi anche quelli extracomunitari come Svizzera, Norvegia e, forse insospettabilmente, Federazione Russa) e i Paesi più avanzati dell'America Latina (Argentina, Messico, Cile, Colombia) e dell'Africa settentrionale (Marocco, Tunisia), prevedono disposizioni puntuali che si basano principalmente sul dovere per gli operatori di adottare le soluzioni tecnologicamente



più avanzate (promossa, quindi, la crittografia, laddove essa possa essere assicurata a condizioni economiche vantaggiose). Altri Paesi, con sensibilità decisamente inferiore rispetto ai diritti ed agli interessi dei cittadini, e talora, delle stesse imprese, trascurano il problema, se non sono addirittura privi di una legge organica sulla protezione dei dati personali o non proibiscono od ostacolano la stessa raccolta dei dati. Un riscontro quasi matematico al riguardo, a parte casi scontati come la Cina, ci deriva dalla situazione dell'Egitto, Paese al centro di recenti e drammatici fatti: l'uso della crittografia cadeva di fatto sotto il totale potere del Governo, il quale poteva quindi ordinare l'indiscriminato deposito delle chiavi di cifratura, attribuendosi così il diritto di penetrare in modo generalizzato nella "vita" di ciascuno, in quanto "leggibile" attraverso i dati personali. Si può quindi affermare che la sensibilità al tema della sicurezza si muove di pari passo col progresso democratico, ma, per altro verso, anche con l'incrementarsi o il consolidarsi dei rapporti commerciali con i Paesi europei. Il fenomeno impone l'adozione di regole uniformi anche riguardo al trattamento dei dati personali, soggetti, attraverso lo scambio transfrontaliero, a "viaggiare" da un Paese all'altro: è il caso di Marocco e Tunisia, che hanno adottato legislazioni moderatamente avanzate, in forza, soprattutto, della spiccata influenza francese. L'esperienza statunitense è notevolmente diversa, anche se ultimamente soggetta ad una rapida evoluzione verso il modello "europeo". Negli Stati Uniti, il problema maggiormente sentito è storicamente quello della salvaguardia dei cittadini nel mantenimento del controllo dei propri dati personali di fronte allo Stato ed al potere pubblico in generale, ivi compresi persino i servizi segreti. Espressione di questo atteggiamento è l'atto legislativo denominato Freedom of Information Act (FOIA), il quale, costituendo un leading case per altri Paesi di tradizione giuridica anglosassone, soprattutto africani, a determinate condizioni, accorda a chiunque, non solo ai cittadini statunitensi, il diritto di ottenere informazioni circa il contenuto di atti custoditi dal Central Intelligence Service (CIA). Viceversa, il rapporto tra cittadini ed operatori economici, laddove comporti il trattamento e la conservazione di dati personali da parte di questi ultimi, è stato storicamente letto e regolato in un'ottica più strettamente contrattualistica: a prescindere dall'emanazione, a livello di singoli Stati, di leggi particolarmente severe rispetto all'invio di informazioni commerciali indesiderate attraverso internet (cosiddetto Spam, più tecnicamente definito Unsolicited Commercial Email), i rapporti tra consumatori ed imprese tendono ad essere regolati con la semplice sottoposizione, a carico di queste, di una Privacy Policy avente impostazione e natura molto più stringata ed essenziale rispetto all'informativa sulla privacy prevista negli ordinamenti europei. Non sono previste particolari garanzie sulla protezione dei dati, se non l'obbligo, da tempo generalizzato a livello di legislazioni statali uniformi, di informare tempestivamente i consumatori delle eventuali anomalie o "rotture" di sicurezza (Security Breeches) che si siano verificate, onde consentire ai consumatori stessi di adottare le opportune contromisure. Tuttavia, anche negli Stati Uniti, se per un verso si fa più stringente che in passato la pressione delle associazioni e dei movimenti di tutela dei diritti civili e dei consumatori sulla protezione dei dati personali, dall'altro, la necessità di adeguamento alle condizioni praticate in quello che per gli USA rappresenta ancora un "mercato" fondamentale, quale quello europeo, spinge anche il pragmatico sistema americano verso le logiche "europee". Ciò è già realtà sul terreno fiscale, con l'obbligo per le imprese americane di far pagare la Value Added Tax – la nostra IVA ed analoghe imposte vigenti in tutta l'Unione Europea – ai clienti europei. Così, alcuni Stati, in particolare l'importante Massachusetts, hanno ora adottato disposizioni addirittura più severe di quelle italiane ed europee, in ordine alla necessità di proteggere i dati personali da accessi abusivi, intrusioni ed alterazioni, con la più adeguata delle misure: la crittografia. Gli osservatori esperti nel campo giuridico e delle tecnologie IT ritengono che tale ottica si estenderà gradualmente all'intero Paese. La "resa" degli stessi Americani evidenzia come il futuro della protezione dei dati personali, a livello mondiale, sarà sempre più "crittografico": la tendenza alla riduzione dei costi determinata dal perfezionarsi delle tecnologie e dalla loro diffusione porterà non solo le grandi imprese e quelle con particolari esigenze di sicurezza (come gli istituti bancari), ma anche i piccoli e medi operatori economici a dotarsi di strumenti di cifratura dei dati personali raccolti. I quali, se via via comporteranno costi effettivi sempre minori per le imprese, per altro verso assicureranno, a livello globale, il controllo davvero effettivo dei cittadini sul destino e sulla protezione dei propri dati.



Francesco Pizzetti
Presidente dell'Autorità garante per la protezione dei dati personali

Nuove sfide di protezione

I social networks costituiscono un'applicazione web di recente sviluppo che ha ormai rivoluzionato il modo di comunicare e muoversi nel mondo digitale. Indubbiamente di grande utilità, ma progettata valorizzando un unico aspetto, la facilità di immissione e condivisione delle informazioni sulla rete, comprimendo al massimo quel diritto fondamentale che è il controllo dei propri dati.

Quando si parla di protezione dei dati personali nell'era digitale, si fa riferimento ad un concetto ben più esteso ed articolato della semplice tutela della privacy. Proteggere i dati personali, in un mondo caratterizzato da un'impensabile capacità di raccolta, elaborazione e conservazione di informazioni di qualunque genere, è un compito delicato che ha assunto un'importanza strategica in tutti i Paesi. Tale compito, pur basandosi sulla tutela di un bene intangibile ed immateriale quale l'informazione, ha assunto ormai un ruolo di tutela dell'individuo in quanto "essere": sempre più spesso, le informazioni del mondo digitale rivelano implicazioni nel mondo reale, con ripercussioni sulla vita delle persone e sui comportamenti della società. L'evoluzione delle tecnologie informatiche e le innovazioni nel settore delle telecomunicazioni hanno sicuramente apportato grandi benefici al genere umano. Nello stesso tempo, hanno però ampliato in modo vertiginoso la quantità di informazioni amministrate dai calcolatori e trasmesse sulle reti, senza che mai fosse affiancata a questo processo un'adeguata cultura della protezione e della sicurezza e senza che venissero poste quelle domande e quei dubbi sollevati oggi dalle Autorità di protezione dei dati di molti Paesi. Efficace è il paragone del moderno settore delle telecomunicazioni con gli albori dell'industria automobilistica. Le prime auto messe in circolazione erano state infatti progettate senza riflettere su aspetti importanti, non ritenuti fondamentali in principio, come la sicurezza ed il consumo. Oggi sarebbe impensabile circolare su un'auto sprovvista di airbag o senza meccanismi di frenata sicura. Allo stesso modo, si può notare come molte delle più famose applicazioni web progettate finora abbiano largamente (o, in alcuni casi, volutamente) ignorato molti aspetti importanti legati alla protezione dei dati personali. La tutela dei dati sulla rete Internet dipende oggi da due fattori cruciali: controllo e sicurezza. Il controllo è legato alla possibilità di immettere informazioni in rete (attraverso un canale qualsiasi, come siti web, blog, social networks) mantenendo la capacità di gestire le informazioni e la facoltà di modificarle, cancellarle, diffonderle o, al contrario, limitarne la diffusione secondo regole certe e stabilite a priori. La sicurezza è invece legata a tutte le misure e le cautele previste per scongiurare eventi avversi che possano mettere a rischio i dati personali. Purtroppo, molti servizi ed applicazioni della rete Internet non hanno pienamente valutato l'importanza di questi due elementi. Le garanzie di controllo e sicurezza dei dati personali in rete non sono quindi sempre certe ed omogenee. Il futuro della protezione dei dati dovrà quindi svilupparsi su due aspetti fondamentali: la sicurezza delle infrastrutture della rete, che devono essere protette e poste al riparo dagli attacchi e, parallelamente, la necessità di regolare l'uso dei vari applicativi supportati dalla connettività. Prendiamo ad esempio i servizi di on-line banking, nati per consentire la fruizione agevolata dei servizi bancari da remoto, abbattendo così i costi di gestione di filiali e sportelli. Nella sua concezione originaria, il servizio ha largamente sottovalutato il fattore sicurezza. L'errore ha condotto all'esplosione di fenomeni quali il phishing, la crescita dei furti d'identità e le frodi telematiche legate al trasferimento illecito di fondi. In questo caso, l'errore iniziale è stato quello di concepire un'applicazione attraverso la rete Internet priva di adeguate misure di sicurezza, decidendo di equiparare e porre sullo stesso piano il personal computer domestico degli utenti con il terminale della filiale di una banca. Il terminale di una filiale è da sempre tutelato da elevate misure di sicurezza, logica e fisica (che vanno dalla guardia all'ingresso a reti informatiche blindate e segregate). Al contrario, un personal computer domestico non offre la stessa affidabilità e le stesse protezioni, essendo esposto ai rischi di una rete aperta come Internet. La mancata riflessione iniziale sull'importanza di allestire connessioni sicure e computer protetti nello sviluppo dell'on-line banking ha causato i problemi menzionati, che potevano essere evitati attribuendo il giusto peso al fattore sicurezza ab origine. Solo in tempi recenti l'importanza delle misure di sicurezza nell'on-line banking è stata rivalutata col giusto peso, spingendo le banche ad investire sull'uso di tecnologie più sicure (come l'autenticazione "two-factor", mediante cellulare o token)

e sull'educazione degli utenti per un uso prudente dei servizi (cambio forzato delle password, uso di software antivirus, protezione del personal computer, ecc.). In modo simile, si potrebbe affiancare a questo esempio il caso dei social networks rispetto alla facoltà di controllo sui dati personali. I social networks costituiscono un'applicazione web di recente sviluppo che ha ormai rivoluzionato il modo di comunicare e muoversi nel mondo digitale. Ma è ancora troppo presto per valutarne a fondo effetti e conseguenze. Si tratta di un servizio di connettività sociale tra persone. Indubbiamente di grande utilità, ma progettato valorizzando un unico aspetto, la facilità di immissione e condivisione delle informazioni sulla rete, comprimendo al massimo quel diritto fondamentale che è il controllo dei propri dati. La cancellazione dei dati immessi su un social network, la limitazione della diffusione, la possibilità di decidere da chi e come debbano essere trattate le informazioni inserite sono facoltà inconsapevolmente (o volutamente) limitate dai gestori delle piattaforme dei social networks nella fase di lancio dei loro servizi. Ancora una volta, e solo recentemente, si corre ai ripari con l'aggiunta continua, all'interno delle piattaforme di social networks, di quelle opzioni di controllo sui dati e di tutela della privacy che nella fase iniziale erano sembrate superflue Si può quindi affermare che lo scenario di riferimento in cui si muove la protezione dei dati sia un terreno insidioso ed in continuo movimento. Vi è un'incessante evoluzione delle tecnologie, le quali hanno in breve tempo messo in crisi l'impianto della direttiva europea, spingendo il legislatore a creare una normativa maggiormente dettagliata, com'è avvenuto, ad esempio, per disciplinare la conservazione delle comunicazioni elettroniche. Come si fa a parlare di "consenso informato" rispetto a fenomeni complessi ed in divenire come Facebook? Fornire un'informazione adeguata su Facebook richiede modalità più complesse rispetto a quanto poteva immaginare chi ha scritto la direttiva senza pensare ai social networks. Allo stesso modo, non si può pensare di fronteggiare i problemi di cyber-security senza la creazione di meccanismi automatici e mutuamente riconosciuti tra i diversi Paesi, i quali consentano di reagire in modo celere ed efficace ad eventuali attacchi informatici di vasta portata. Serve quindi una regolamentazione internazionale, un Wto della protezione dei dati. Un organismo sovranazionale che vigili sulla rete, altrimenti in futuro non saremo in grado di garantire la protezione dei dati. È infine opportuno proporre una considerazione sul recente fenomeno di "WikiLeaks" e sul proliferare di siti web dedicati alla pubblicazione di materiale riservato appartenente a governi ed aziende (il cosiddetto fenomeno del "whistlebowling"). In questo caso, il problema non ha nulla a che vedere con la sicurezza della rete. Evidenzia, semmai, una carenza di misure di sicurezza alla fonte, nei luoghi in cui le informazioni ritenute segrete vengono prodotte, memorizzate e poi trafugate. Uno dei massimi esperti di cyber-security americano ha recentemente fatto notare che i governi stanno imparando ciò che l'industria musicale e quella del cinema hanno già sperimentato da molto tempo: copiare e distribuire documenti digitali in rete è terribilmente facile perché richiede poco tempo e pochissime risorse. I governi si trovano ad affrontare ora il problema WikiLeaks e la pubblicazione di file riservati proprio come l'industria musicale, molti anni fa, si è trovata a fronteggiare il problema del peer-to-peer e della condivisione dei brani musicali in rete. L'industria musicale e quella del cinema hanno già compreso che per sopravvivere sarà necessario modificare il proprio modello di business. Allo stesso modo, i governi dovranno persuadersi che il cuore del problema non è WikiLeaks, ma il modello di protezione dei dati da adottare per le informazioni segrete: questo dovrà evolvere per cercare di essere efficace anche nella nuova era digitale.

L'open source

Un po' di storia

La nascita del software open source risale agli albori dell'informatica, essendone il modello "primogenito". Con l'avvento dei sistemi operativi, divenne possibile utilizzare lo stesso programma anche su hardware diversi. Ovviamente, si trattava di un codice chiuso, non visibile per gli utenti. I malfunzionamenti costituivano un investimento a lungo termine: veniva appositamente rilasciato software con bug e, poco tempo dopo, questo veniva debellato, lasciando spazio ad un altro. Gli utilizzatori erano così costretti a comperare gli aggiornamenti di volta in volta. Vi erano anche dei casi limite: qualche software house inseriva volutamente istruzioni di ritardo nei loro programmi per poi toglierle, o ridurne l'efficacia, nelle versioni successive. Potevano così vantare l'aumentata velocità della nuova versione.

Alcuni idealisti, guidati da Richard Stallman, non lo trovarono corretto. Per questo motivo, nel 1985, fondarono la Free Software Foundation (FSF), che intendeva promuovere la filosofia del software libero. Esso doveva soddisfare le seguenti 4 caratteristiche:

1. libertà di lanciare il programma per qualunque scopo;
2. libertà di studiare il codice di partenza e modificarlo secondo le proprie esigenze;
3. possibilità di riprodurre copie del programma a favore di altri;
4. libertà di distribuire pubblicamente copie implementate del programma, in modo tale che tutta la comunità potesse trarne beneficio.

Concetto principale: "libertà" di usare il codice come meglio si ritenesse opportuno. Ma, nella lingua inglese, la parola "free" contenuta in "free software", oltre che "libero", significa anche "gratis": molti lo associavano erroneamente a "freeware", il software effettivamente gratuito. Udendo il termine "gratis", le aziende si irrigidirono. Bisognava trovare un altro nome, ma tutti i possibili sostituti sembravano ancora peggiori. Fu allora proposta la parola "open source": nonostante non rendesse bene l'idea come "free", molti accettarono la definizione, mentre gli idealisti, tra cui Stallman, la rifiutarono. Ritenevano che, con il nuovo nome, si sarebbe perso lo spirito di libertà originario. Nacque così un gruppo distinto, che assunse il nome di OSI ("Open Source Institution"), con il compito di diffondere il modello Open Source. I due gruppi esistono ancora e, di fatto, la filosofia e le applicazioni pratiche differiscono solo per qualche sfumatura. Le due diverse strutture collaborano sugli stessi software e per le medesime finalità. Si può concludere che i sostenitori del "free software" sono più idealisti (il codice deve essere aperto per rispettare la libertà degli utenti e degli autori), quelli dell'"open source" sono più pratici e guardano ai risultati concreti (il codice deve essere aperto perché si tratta di una scelta commerciale valida per le aziende).

I vantaggi derivanti dall'uso del software open source sono molti:

1. possibilità per chiunque di modificare e personalizzare liberamente il software;
2. il codice di partenza è sottoposto ad una revisione da parte di diverse persone, sotto il controllo di uno o più maintainer. Il feedback da parti degli utenti è continuo;
3. le nuove release si susseguono velocemente;
4. la scoperta di bug e malfunzionamenti è più rapida e semplice; più persone testano il software in scenari d'uso diversi;
5. i bug scoperti vengono spesso evidenziati in appositi indici accessibili a chiunque;
6. a differenza del software proprietario, l'open source supporta meglio l'hardware datato;
7. non esistono specifiche di proprietà e informazioni non pubblicate di alcun tipo;
8. il codice di partenza è trasparente; la possibilità di inserire malware o spyware è pressoché nulla. Chiunque può essere d'aiuto; si presta a programmazione, beta testing, traduzione, libere offerte.

David Roici

Francesco Soro
Presidente Corecom - Comitati Regionali per le Comunicazioni

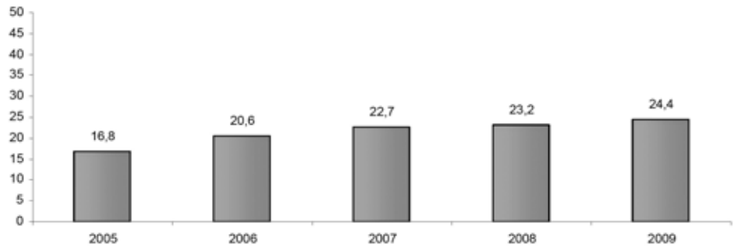
L'era di Twitter

La e-security e le misure necessarie a garantire la sicurezza della navigazione on-line, diventano, con la diffusione dell'uso di internet, sempre più grandi temi sui quali è necessario concentrarsi. Non va poi dimenticato che il vasto pubblico di internet è composto, per la maggioranza, da minori e giovanissimi, cresciuti nell'era della tecnologia e maggiormente esposti ai rischi della navigazione in rete. Ed è proprio ai minori che va rivolta la maggiore attenzione.

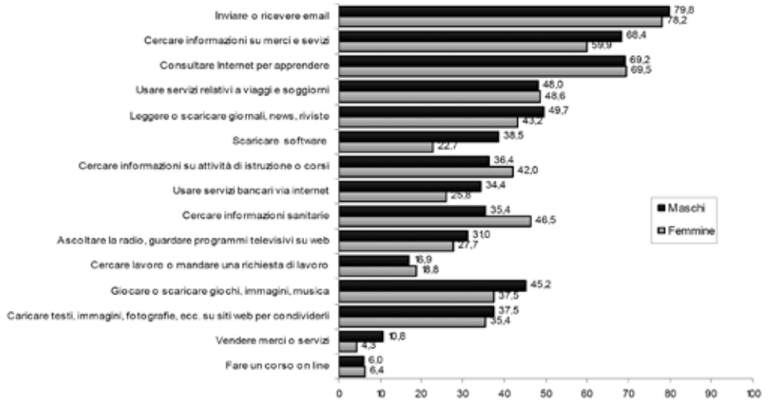
Un mondo globale che si muove sulla rete, un flusso ininterrotto di informazioni che in tempo reale raggiungono milioni di utenti di ogni età, ovunque. È l'era di internet, quel mondo virtuale e parallelo in grado di annullare le distanze e rendere accessibili al grande pubblico notizie che resterebbero invece patrimonio di pochi. Un mondo nel quale si scardina la piramide tra produttori e consumatori di notizie: non più pochi (produttori) per molti (consumatori), ma molti per molti. Anzi, per moltissimi. Le fonti si moltiplicano, e con loro si moltiplicano, in modo esponenziale, gli utenti. Tutto ciò stravolge le coordinate classiche del dominio delle informazioni, vero cardine del potere contemporaneo. Le conseguenze sono imprevedibili e potenzialmente dirompenti. Basti pensare a quel che sta accadendo ai nostri dirimpettai dell'Africa mediterranea: una dura crisi economica (frutto, peraltro, paradossale dello sviluppo di quei Paesi, nei quali il costo dei beni primari è cresciuto più della capacità di spesa dei cittadini) per la prima volta è diventata rivolta sociale, capace di destabilizzare un'intera regione grazie anche al ruolo dei social network. Twitter e Facebook hanno contribuito alla diffusione della protesta con un passaparola tra giovani utenti difficile da interrompere, se non con l'oscuramento della rete. E non è un caso se tutti i regimi non democratici tendono a censurare in modo più o meno massiccio l'uso della Rete. Assistiamo anche a profonde trasformazioni nelle relazioni interpersonali e nella comunicazione, specialmente tra i più giovani: chi controlla l'autenticità delle notizie diffuse e, soprattutto, come è possibile evitare che "informazioni sensibili" finiscano con un click alla mercé di chiunque? La e-security e le misure per garantire la sicurezza della navigazione on-line diventano, con la diffusione di internet, sempre più grandi temi sui quali è necessario concentrarsi. Non va poi dimenticato che il vasto pubblico di internet è composto, per la maggioranza, da minori e giovanissimi, cresciuti nell'era della tecnologia e maggiormente esposti ai rischi della navigazione in rete. Ed è proprio ai minori che va rivolta la maggiore attenzione. Se si considerano i dati diffusi dall'Unione Europea sull'uso di internet, i quali indicano in 8 milioni i giocatori abituali on-line, in 18 milioni gli utenti iscritti a "Second life", e in 500 milioni i registrati a Facebook, e l'incremento esponenziale delle vendite di beni e prodotti on-line, con un ricavato che raggiunge il miliardo di dollari, appare evidente che i rischi maggiori sussistono soprattutto per le giovani generazioni, peraltro in possesso di minori strumenti per valutare criticamente i rischi derivanti da un uso eccessivo di internet. I dati pubblicati nel 10° Rapporto Nazionale dell'Infanzia e dell'Adolescenza di Eurispes e Telefono Azzurro ci confermano l'aumento dell'utilizzo delle nuove tecnologie tra i giovani. Secondo quanto rilevato, il 71,1% degli adolescenti possiede un profilo su Facebook, il 17,1% su MySpace e una percentuale minore (10,4%) utilizza Habbo. Dati Istat raccolti in occasione dell'indagine "Cittadini e nuove tecnologie" informano che, dal 2005 al 2008, l'utilizzo del pc e di internet è cresciuto soprattutto per la fascia di età compresa tra gli 11 e i 19 anni. I maggiori incrementi nell'uso di internet si rilevano, invece, nella fascia di età 11-14 anni (15,1%) e in quella 15-17 (13,2%), con un aumento meno consistente (4,8%) per la fascia di età 18-19 anni. Secondo gli ultimi dati Comscore, rilevati a dicembre 2008, su 282,7 milioni di utenti internet in Europa al di sopra dei 15 anni di età, circa 211 milioni (il 74,6% del totale) hanno visitato un social network: il primato va alla Gran Bretagna con il 79,8%, seguita da Spagna, Portogallo e Danimarca. L'Italia si colloca al quinto posto, con un 69,3% di visite. Le ultime indagini condotte e pubblicate nel 10° Rapporto Nazionale rivelano, poi, come quasi la metà degli adolescenti (47%) abbia maturato esperienza di contatti in rete allo scopo di fornire dati personali, il 41,4% è entrato in siti che indicavano il divieto di accesso ai minori e il 39,8% ha ricevuto almeno una volta richieste di incontro dal vivo da uno sconosciuto sul web. Non mancano poi contatti con persone che hanno rivelato di aver falsato la propria identità e percentuali allarmanti su visioni di immagini inadatte (24,9%) o ricezione di messaggi volgari e offensivi (20,7% degli utenti intervistati). Per accedere ad un social network, o semplicemente acquistare qualcosa sui siti specializzati, è sufficiente creare un proprio "profilo", ossia condividere informazioni personali. In poche parole, "raccontarsi", o mettere a disposizione di estranei i cosiddetti "dati sensibili". Ed un minore incontra maggiori difficoltà a comprendere quanto questo possa risultare rischioso in termini di sicurezza personale. È per questo che la web security, specialmente sul tema della tutela dei minori, rappresenta oggi una delle nuove frontiere del diritto. D'altra parte, pur consapevoli delle difficoltà che comporta l'esaurire in modo esaustivo la normativa sul rapporto tra internet e minori, si tratta di un aspetto al quale chi, come me, è alla guida di un Ente già impegnato a vigilare sulla tutela dei minori in rapporto al mondo te-

levisivo e ai media tradizionali, non può che essere particolarmente sensibile. Mentre, infatti, ai sensi dell'ampia giurisprudenza esistente in materia di minori e televisione, l'Autorità per le Garanzie nelle Comunicazioni (AgCom) ha delegato alle sue articolazioni territoriali – i Comitati Regionali per le Comunicazioni (Corecom) -, l'attività di vigilanza e monitoraggio sulla programmazione televisiva locale, comprese le eventuali violazioni in materia di tutela dei minori, la complessità del mondo internet e la continua evoluzione delle fonti giurisprudenziali impediscono di essere altrettanto efficaci nel raggiungimento dell'obiettivo. Ma proprio per questo, per l'esperienza derivante dall'essere un po' il "front office" nel rapporto tra utenti ed operatori di settore, oltre che istituzioni, ritengo che l'AgCom, e le sue articolazioni rappresentate dai Corecom, possano e debbano intervenire soprattutto nella definizione delle strategie e delle modalità di intervento in ambito di new media. Intendiamoci: so bene che il cammino è lungo, ma la continua evoluzione delle nuove tecnologie non può che spingerci oltre, specie a garanzia di quelle nuove generazioni, nate nell'era internet, che debbono necessariamente vederci impegnati al fine di tutelarne la crescita e garantirne un corretto sviluppo. D'altra parte, il progresso fa sì che la nostra sia una società in perenne cambiamento. È quindi compito delle autorità quello di garantire la regolamentazione dei fenomeni e fornire la certezza del diritto. Guardo con interesse all'esperienza maturata in altri Paesi e a tutte le azioni che, a livello europeo ed internazionale, apportano al fenomeno quella necessaria visione globale che comporta il parlare di "rete". A tal proposito, desidero ricordare che il nostro Paese, assieme agli altri Stati membri dell'Unione Europea, sarà tra gli "animatori" dell'ottava edizione del "Safer Internet Day", che si svolge, come ogni anno, nella seconda settimana di febbraio. Rivolta principalmente ai giovani, l'iniziativa cerca di promuovere le migliori prassi e di informare gli utenti più giovani sulle "accortezze" da porre in essere per tutelarsi nella navigazione on-line. Lo slogan di quest'anno "Non è un gioco, è la tua vita" è volto a sensibilizzare specialmente gli utenti che utilizzano la rete per accedere ai social network ed ai giochi di ruolo. L'obiettivo è quello di ricordare che tutte le informazioni fornite nelle registrazioni necessarie all'utilizzo di tali piattaforme sono indelebilmente raccolte e riutilizzabili, per altri fini, anche da estranei. Non sempre i giovani sono consapevoli dei rischi ai quali vanno incontro nelle loro navigazioni. Forse non lo sono nemmeno i genitori. Tuttavia, non ci si può esimere dall'agire nell'interesse dei minori e degli adolescenti. Non si può non rilevare l'aumento dei furti di identità e l'hackeraggio ad opera di pirati informatici che vedono accrescere il proprio campo d'azione con il diffondersi dell'uso dei social network, tanto che persino il creatore di Facebook, o il Presidente francese Sarkozy, sono rimasti vittime di cyber incursioni, dimostrando quanto sia difficile il controllo sistematico della Rete. Come pure sono in aumento gli episodi di cyber bullismo, una nuova frontiera nel rapporto tra adolescenti alla quale si deve prestare la massima attenzione. Per il raggiungimento di una regolamentazione complessiva della materia, risulta quindi necessario coinvolgere non solo gli attori istituzionali, ma anche quanti operano nell'ambito della rete. Penso agli internet providers, costituiti in associazione già dal giugno 1995, e che contano oggi 44 associati, con l'obiettivo di definire standard qualitativi e regole di comportamento nell'ambito dell'offerta internet a favore dei minori. La globalizzazione della rete impone un intervento coordinato che obblighi ad una "navigazione responsabile" non solo i responsabili dei siti e gli operatori del settore, ma anche gli utenti. E, soprattutto, il codice di autoregolamentazione deve essere condiviso. Non può essere calato dall'alto e deve rispondere alle "sensibilità", ma direi soprattutto alle capacità di intervento di ogni singolo attore, in modo tale da essere realmente efficace ed il più possibile completo. Ecco perché continuo a ritenere che i Corecom debbano giocare un ruolo di primo piano. Ecco perché ho ragione di ritenere che possa partire proprio dall'autorità più prossima alla vigilanza e alla difesa dei minori quell'azione in grado di tutelare gli internauti più piccoli dai pericoli della rete. Ma ciò non potrà mai sostituirsi all'attenzione che ciascun genitore deve porre nel cercare di proteggere i propri figli nella navigazione in rete. Solo agendo tutti insieme riusciremo, forse, a far sì che la tutela sia davvero complessiva e rispondente ai bisogni anche del piccolo pubblico.

Persone di 14 anni e più che hanno usato Internet negli ultimi 12 mesi e hanno ordinato o comprato merci e/o servizi per uso privato su Internet negli ultimi 12 mesi - Anni 2005-2009 *(per 100 persone di 14 anni e più che hanno usato Internet negli ultimi 12 mesi)*



Persone di 6 anni e più che hanno utilizzato Internet negli ultimi 3 mesi per attività svolta e sesso. Anno 2009 *(per 100 persone di 6 anni e più dello stesso sesso che hanno utilizzato Internet negli ultimi 3 mesi)*



Massimo F. Penco
Consulente dell'FBI, membro dell'Institute of Electronic Engineers USA.
Ricercatore di computer crime, sicurezza dei sistemi di comunicazione e reti informatiche

La sicurezza nei social networks

Nell'era di WikiLeaks, abbiamo scoperto quanto siano vulnerabili le informazioni e la corrispondenza, segreta o meno, di intere Nazioni. A maggior ragione, i nostri dati personali che pubblichiamo on-line sui social network o sono contenuti in banche dati non adeguatamente protette.

Più sicurezza, meno privacy, dicono i fautori del ricorso massiccio alla tecnologia per i controlli personali. Anche Internet ed i social network divengono fonti di informazione e profiling dell'identità digitale di una persona. L'attività su FB viene sempre più spesso esaminata da società di ricerca personale. Si desidera comprendere le caratteristiche di un individuo, il suo orientamento politico, le amicizie e tutto ciò che scrive nel suo profilo, incrociandolo con quello degli amici, dei gruppi che frequenta ed altro ancora, come la correlazione fra quanto inviato nel curriculum e quanto pubblicato on-line: è la propria identità digitale. Cito Facebook perché in Italia siamo i più "grandi consumatori" di questo social network. Ovviamente, neanche a farlo apposta, è di questi giorni una particolare attenzione di FB sulla privacy. Qui di seguito il nuovo link che appare a tutti gli iscritti quando inseriscono un post on-line. Ottima cosa, senz'altro, anche se assomiglia molto al famoso adagio "si chiude la stalla quando i buoi sono scappati": http://www.facebook.com/privacy/explanation.php.

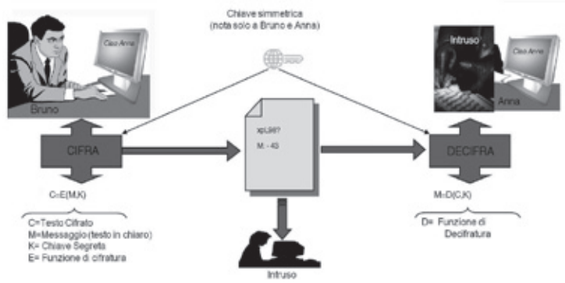
Nell'era di WikiLeaks, abbiamo scoperto quanto siano vulnerabili le informazioni e la corrispondenza, segreta o meno, di intere Nazioni. A maggior ragione, i nostri dati personali che pubblichiamo on-line sui social network o sono contenuti in banche dati non adeguatamente protette. Nel link http://www.youtube.com/watch?v=KpLNlSKugHw&feature=related, si mostra come la CIA usi FB per raccogliere informazioni, pescando nel grande "serbatoio" dello stesso. Che sia vero o meno, è qualcosa su cui riflettere. Se si leggono le condizioni di FB, accettate da ognuno di noi nel momento in cui cediamo le nostre informazioni alla rete, c'è da rimanere attoniti: "*Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (eg. photo tags) in order to provide you with more useful information and a more personalized experience. By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.*" Praticamente, FB può fare quello che vuole del nostro profilo. In merito alle condizioni con cui accediamo a FB e ad altri social network, ecco la lista parziale delle informazioni messe a disposizione di chiunque: nome, dati anagrafici, indirizzo, telefono, e-mail, sesso, abitudini, preferenze, credo politico e religioso, corso di studi, ed un'infinità di altre informazioni facilmente ricavabili dai post inseriti. Potenti software sono stati predisposti per incrociare le informazioni e profilarle, fino ad arrivare ad esprimere una valutazione di ciascuno di noi in base a quanto ricercato o richiesto. Curioso è il termine forgiato per indicare il fenomeno: "data mining"[1] . Un dato significativo da tenere a mente è che FB, come youtube ed ogni altro social network, dispone di centinaia di milioni di foto e consente un'attività definita "sosia network": è facile trovare un nostro sosia utilizzando un apposito software, creato inizialmente per gioco, vedi quello della Coca Cola, e poi usato anche per indagini di polizia, il cosiddetto "forensic". Questa attività illegale è divenuta una vera e propria fabbrica di identità rubate. Risulta infatti semplice clonare una persona rubandogli quanto di più personale possiede: il proprio volto. La stessa FB ha indirettamente ammesso questa pratica creando una propria area denominata Reporting Fake/Fraudulent Profile, http://www.facebook.com/topic.php?uid=69178204322&topic=16194. Ovviamente, anche qui la parola Mafia esce fuori. Osservate questo link: User ID's from Mafia Wars profile page? http://www.facebook.com/topic.php?uid=71775107787&topic=198262. L'uso di queste tecnologie per scopi delinquenziali è ancora tutto da scoprire. Ad esempio, è possibile creare un profilo identico ad un'altra persona basandosi sulle informazioni di un terzo. Al contrario, si può partire da una foto e creare intorno ad essa un altro profilo, dando vita ad una persona completamente identica nelle fattezze, ma con diverse informazioni e dati personali. Sarà un gioco da ragazzi realizzare un documento di identità falso o un'"identità digitale" interamente nuova. Questo è uno dei tanti avvisi di una scuola americana "*Facebook, a social network service, is increasingly being used by school administrations and law enforcement agencies as a source of evidence against student users. The site, a popular online destination for college students, allows users to create profile pages with personal details. In the early years of the site, these pages could be viewed by other registered users from the same school, including resident assistants, campus police, or others who signed up for the service. The user privileges and terms of service of the site have since been changed to allow users to control who has the ability to view their content. Recent disciplinary actions against students based on information made available on Facebook has spurred debate over the legality and ethics of school administrators' harvesting such information. Facebook's Terms of Use specify that "the website is available for your personal, noncommercial use only", misleading some to believe that college administrators and police may not use the site for conducting investigations. However, Facebook spokespeople have made clear that Facebook is a public forum and all information published on the site should be presumed available to the general public, school administrators included. Legal experts agree that public information sources such as Facebook can be legally used in criminal or other investigations*". In Italia ci si sta avviando verso un uso esteso della rete e verso la raccolta di dati che interessano l'intera popolazione. Alcuni dei progetti riguardano il fascicolo personale elettronico, sostenuto dall'adozione della CEC PAC, contenente le comunicazioni tra Cittadino e Pubblica amministrazione ed il fascicolo sanitario elettronico, contenente i dati sanitari di tutti i cittadini. Questi si aggiungono ad un numero indefinito di banche dati tenute da vari enti, in via di completa digitalizzazione ed ancora non interoperabili tra loro. Alcune sono però già fruibili on-line. Le più comuni sono l'anagrafe dei comuni, l'Agenzia delle Entrate, il Pubblico Registro Automobilistico, oltre a tutte le strutture che raccolgono informazioni on-line tramite moduli di iscrizione più o meno protetti e più o meno plausibili. I segreti dei polverosi archivi cartacei stanno per essere violati e trasformati in bit. Il passaggio dalla carta al virtuale è epocale e quanto mai necessario. Siamo preparati? Direi di no. Non lo siamo mentalmente e non lo siamo neanche tecnicamente. Non mi risulta sia stato eseguito uno studio su cosa ciò significhi. Nulla si è fatto per garantire la sicurezza degli archivi che contengono i dati di tutti gli Italiani. È un po' come andare alla cieca: poi qualcosa si farà o avverrà! Sono solo alcuni esempi, ma ci sarebbe da scrivere libri in materia. Per questo sono arrivato alla convinzione che: OGNI BASE DATI È A RISCHIO INTERCETTAZIONE NEL WEB. NON ESISTE

L'ASSOLUTA SICUREZZA DEI DATI. È una sorta di sport mondiale tra gli hackers, quello di violare i dati altrui. Uno sport che richiede impegno, forza ed è assolutamente rischioso. Ma, alla fine, è un piacere immenso mettere le informazioni violate a disposizione di tutti! WikiLeaks insegna! In Italia, il tema dell'identità digitale è quanto mai attuale, alla luce di clamorosi e recenti episodi di cronaca nera e di processi giudiziari che hanno coinvolto emotivamente l'opinione pubblica. Diventa sempre più spesso determinante la "prova digitale": si può essere assolti o condannati in base alle "tracce d'uso" di computer e telefoni cellulari ed alle frequentazioni dei social network. È quindi il caso di riflettere con attenzione su come si formino queste "prove digitali" e su come vengano valutate. Insomma, l'identità digitale pesa sempre di più nella vita di ognuno, ma il dibattito resta ancora confinato nel ristretto ambito degli addetti ai lavori. Vorrei confutare quella sorta di teorema ormai accettato nelle aule di giustizia. Chiamia-

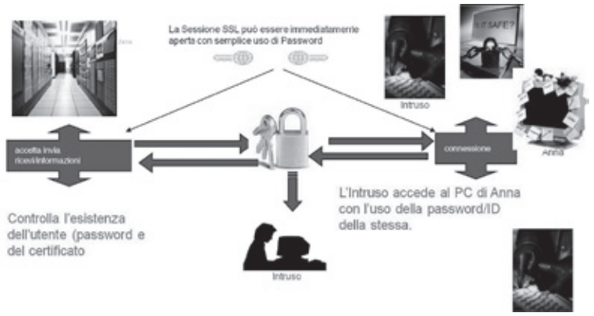
molo, per comodità, "Teorema della quattro P".
È invalsa la consuetudine - divenuta purtroppo prova in alcune sentenze ed investigazioni recenti (Garlasco, Perugia, Sarah Scazzi, il rapimento di Yara) – di considerare computer e cellulare elementi primari di indagine. Il proprietario di essi può così sostenere di aver lavorato in un certo giorno e ad una certa ora e, in alcuni casi (cellulare), affermare di trovarsi in un certo posto. Il teorema che la proprietà o il possesso di tali oggetti costituisca prova di averli usati è tutto da sfatare, soprattutto nel caso in cui l'identità dell'utilizzatore non sia più fisica, ma digitale. A maggior ragione, gli apparati localizzabili attraverso tecnologie (GSM o GPS). La proprietà o il possesso di un apparato usato per comunicare non certifica quindi:

- chi ne faccia uso;
- il luogo in cui si trovi;
- quando l'abbia usato;
- per quanto tempo l'abbia usato.

In sostanza, non è possibile stabilire che proprietà, possesso, uso, siano identificabili con una specifica persona fisica. Nessuna tecnologia è in grado di fornire queste certezze. Gli apparati digitali, quali computer, cellulari, smartphone, possiedono vita e personalità autonome, indipendentemente da chi li possieda e li usi. Come vedremo, anche le più recenti ricerche tecnologiche sulla sicurezza non sono riuscite a risolvere completamente questo importante tema. L'identità digitale rimane quindi un problema grave ed irrisolto. L'identità di chi opera con un computer/cellulare é nota solo a chi ne fa uso. L'operatore comunica, inserisce e riceve dati, sottoscrive digitalmente contratti, accetta clausole – interloquisce, insomma - con un'altra entità digitale, anch'essa sconosciuta. Neanche i più moderni sistemi di trasmissione dati (Posta elettronica Certificata, certificati con firma digitale) certificano chi riceve e trasmette un messaggio di posta elettronica. Facciamo un esempio banale, ma che evidenzia il problema: Bru-



no invia un messaggio ad Anna (che ha lasciato il PC incustodito). Davanti al PC di Anna potrebbe esserci chiunque, nonostante crittografia e firma digitale. Il certificato residente nel computer fa ritenere a Bruno che, dall'altra parte, ci sia Anna. In realtà, potrebbe esserci un'altra persona che millanta l'identità della donna ed intercetta i dati trasmessi. La stessa cosa accade se si usa una connessione sicura X509 (SSL), tipica dell'home banking: Anna lascia



il PC incustodito con il proprio certificato installato. Al posto di Anna potrebbe esserci chiunque. Il certificato residente nel computer fa sì che qualsiasi controllo del sistema non rilevi nulla di anomalo, poiché l'intruso impersona e sostituisce Anna. Scenario analogo se si scambiano messaggi con i cellulari. Quando si riceve un SMS da un numero noto, ciò non significa che "il pollice" sia della persona che si conosce. Non è il cellulare a stabilire "l'identità" dell'apparato, bensì la SIM, che può essere stata prelevata da un telefono ed introdotta in un altro. Clonare una SIM è facile. Basta uno scanner da pochi euro.

I tecnici di tutto il mondo si basano su questi concetti cardine:
1) something you have (qualcosa che solo tu hai)
2) something you know (qualcosa che solo tu conosci)
Sono gli assiomi dell'identità digitale. Le soluzioni fin qui adottate (user ID e password, sistemi biometrici, ecc.) non si sono dimostrate esaustive. La conoscenza dei nostri user ID e password, se abbinata ad un dato biometrico, offre un livello di sicurezza buono, ma non assoluto. La cinematografia ci ha proposto situazioni al limite, in cui una persona agisce sotto minaccia ed è costretta a rivelare user ID e password e, addirittura, si sottopone al controllo biometrico. Il sistema di sicurezza è così tratto in inganno dalla

falsa identità digitale. Ci sono anche altri stratagemmi per bypassare la barriera biometrica.
I sistemi di difesa possono essere di due tipi:
1) controlli a distanza;
2) controllo accessi.
I controlli a distanza prevedono l'uso di PIN, per attivare, ad esempio, il telefono cellulare, prelevare denaro dal bancomat, effettuare operazioni di home banking, accedere ad un server via FTP, ecc. Il controllo accessi comprende l'ingresso in un particolare edificio, oppure la verifica del passaporto alla frontiera. Negli Stati Uniti, i funzionari prelevano anche le impronte digitali e scattano una foto a chi entra nel Paese.

I due sistemi hanno in comune la ricerca continua di soluzioni che rendano le procedure semplici e veloci. È il caso dell'evoluzione dal passaporto tradizionale a quello biometrico. La direzione di marcia è la cosiddetta autenticazione multipla, basata cioè sull'acquisizione di informazioni che possano essere incrociate e verificate all'istante. Con buona pace della privacy. Lo sa bene chi si è recato di recente negli Stati Uniti. Innanzitutto, prima di partire, ci si deve registrare nel sito web dedicato.

All'arrivo, poi, è obbligatorio (e si pagano anche 14 dollari) farsi fotografare e sottoporsi al prelievo multiplo delle impronte digitali. C'è poi la recente introduzione (non dappertutto) del body scanner. La banca dati del servizio di immigrazione si arricchirà dunque di queste informazioni personali:

- dati anagrafici completi;
- luogo in cui si andrà a risiedere negli Stati Uniti;
- dati biometrici da confrontare con il passaporto elettronico;
- foto;
- compagnia aerea, scopo del viaggio e altro ancora.

Nel prossimo futuro (ma in alcuni casi è già realtà) è previsto:
1) lo scanning di tutto il corpo, con particolare attenzione a caratteristiche principali ed eventuali malformazioni;
2) l'esame minuzioso del contenuto di ogni oggetto contenuto nella valigia imbarcata e nel bagaglio a mano;
3) la creazione di una cartella personale del viaggiatore, che verrà riesaminata ad ogni ingresso successivo negli Stati Uniti.

CONCLUSIONI:
Allontanarsi da Internet? Questa è una delle domande che mi pongono spesso. Certo che no! Abbiamo ignorato per troppo tempo ogni forma di prudenza nell'uso della rete. Ora, direi che il segreto consiste in questa massima: "Nel mondo digitale la prudenza deve essere eguale a quella usata nella vita reale".

Creative Commons: il copyright nell'era digitale

Le nuove licenze alternative al copyright: nell'ambiente universitario è nato un progetto innovativo finalizzato a descrivere le diverse modalità per rendere fruibile a tutti in modo gratuito la propria opera d'ingegno.

Nel 2001, negli Stati Uniti, nasce un organismo no profit denominato Creative Commons. Lo scopo è quello di favorire ed incrementare la condivisione e l'utilizzo da parte di terzi di opere creative tutelate da diritto d'autore. Se ne offre una protezione più flessibile attraverso una serie di licenze diverse che dichiarino gli intendimenti degli autori. A seconda della tipologia scelta, il titolare limita il diritto d'autore parzialmente o totalmente. Specifichiamo che, a partire dal 1976, ed a pieno regime dal 1988, ogni opera d'ingegno è automaticamente protetta, dalla nascita, dal copyright. L'autore che desideri non avvalersi delle tutele di legge deve dichiarare la propria intenzione in modo esplicito. "Common" è ciò che non appartiene ad un singolo individuo, ma alla collettività. Con "The Tragedy of the Commons", Garnett Hardin (Università della California, San Diego) avanza, nel 1968, profonde perplessità sulla reale utilità dei Common. Sostiene che, in un ambiente ristretto, in cui le risorse sono scarse, gli individui tendono ad utilizzare maggiormente il bene comune, fino ad esaurirlo. Tuttavia, se The Tragedy of the Commons appare realistica nello sfruttamento comune delle risorse materiali, fisiche, effettivamente consumabili, non sembra poter applicarsi anche ai beni immateriali, la cui replicazione e la cui condivisione non ne determinano l'esaurimento e non ne ledono la qualità. Ne "La Fabbrica dell'Immateriale", il noto economista Enzo Rullani avvalora ulteriormente tale concetto, illustrando come i costi propri dell'informazione siano strutturalmente differenti rispetto a quelli relativi ai beni materiali: produrre informazione è molto oneroso, la replicazione o la condivisione presentano, invece, costi prossimi a zero.
Le Creative Commons Public Licenses (CCPL), introdotte per la prima volta in Italia nel 2004, si articolano in sei tipologie:

BY: con menzione del nome dell'autore. È consentito effettuare copie delle opere e diffonderle, ma solo citando i credits.

non commerciale. È vietato il fine di lucro.

= senza modifiche o rielaborazioni. L'opera può essere utilizzata, ma non come base o come parte di un'altra opera.

alle stesse condizioni. Sono consentite la commercializzazione dell'opera scaricata da Internet e la produzione di opere derivate, ma la nuova opera deve essere a sua volta condivisa con le stesse modalità di quella originaria.

pd pubblico dominio. Opera di tutti, fruibile liberamente senza limitazione alcuna.

© immagine protetta da copyright. Chi svolge l'attività professionalmente, vive dei proventi maturati sui diritti.

Viviamo in un mondo in cui tutto è percepito come "copia a costo zero". Assistiamo ad una lotta continua tesa ad arginare il fenomeno della pirateria, ma abbiamo anche maturato la sensibilità che la produzione di cultura non è più riservata esclusivamente alle case editrici. Le nuove licenze sopra descritte sostengono chi desidera condividere le proprie opere ed hanno il pregio di fare chiarezza nella regolamentazione della materia. Costituiscono un progetto intelligente, interessante, culturalmente corretto.

Mauro Volpatti

1 *Il data mining è una tipica applicazione informatica (solitamente fa parte di un sistema esperto), usata per rintracciare (ed accorpare) dati significativi sepolti sotto una montagna di informazioni irrilevanti. Il termine inglese mining fa proprio riferimento al lavoro di estrazione nelle miniere.*

Roberta Bruzzone
Psicologa Forense e Criminologa
Perfezionata in Scienze Forensi e Psicologia e Psicopatologia Forense
Presidente Accademia Internazionale di Scienze Forensi

Tutti pazzi per Facebook

Dalla bacheca di Facebook alla scena del crimine, in alcuni casi, il passo può essere terribilmente breve: come in ogni medaglia che si rispetti, ci sono sempre due lati da considerare... ed ecco affacciarsi prepotentemente il lato più oscuro di questa epoca digitale.

Facebook fa "impazzire" gli Italiani sempre più: in pochi mesi è diventato il social network più diffuso nel nostro Paese, con oltre 16 milioni di utenti, ed il trend è in crescita costante. In base ad una ricerca pubblicata dal Sole 24 Ore, ritrovare amici e fare nuove conoscenze è l'uso primario dichiarato da oltre la metà dei 2.500 utenti interpellati. Non manca, però, il rovescio della medaglia, ovvero i falsi profili, i cosiddetti fake, che sfruttano i personaggi famosi per le finalità più disparate. È capitato di recente anche al notissimo giornalista Bruno Vespa. Qualcuno ha aperto un account con il suo nome e molti hanno abboccato. Persino la candidata alla Presidenza della Regione Piemonte, Mercedes Bresso, si è ritrovata una richiesta di amicizia da parte del "falso" Vespa. Quello "vero" ha dichiarato: "Ho denunciato l'abuso alla polizia postale... Non ho la più pallida idea di chi, a mio nome, scriva a chi". Miracoli e aberrazioni dell'universo Internet. E non si tratta certo di un pericolo da poco. Ci sono anche altri personaggi famosi che si sono ritrovati su Facebook a loro insaputa. Di tali furti d'identità si è occupata anche Striscia la Notizia, inviando Capitan Ventosa nella sede londinese del social network. Purtroppo, però, la missione dell'intrepido inviato non ha sortito alcun effetto. Si rende quindi necessario un intervento ad hoc teso a fermare questi furti di identità. Altrimenti, resterà valido quanto scritto su Il Giornale da Gaia Cesare, che ha "clonato" Monica Bellucci: "Nulla di più facile. Sono bastati pochi minuti. Se noi siamo la sessantottesima Monica Bellucci in circolazione, quel Silvio Berlusconi diventato nostro amico è solo uno dei 42 (quarantadue!) che viaggiano nel magico mondo di Facebook". Potere dei social networks. E che dire di una star di Hollywood del calibro di Angelina Jolie? Sarà perché sono in molte a desiderare di giocare con quattro taglie in meno e venti centimetri di più che la bella di Hollywood è già arrivata a quota 21 profili aperti a suo nome? Una star nostrana superimitata è poi il pluricampione del mondo Valentino Rossi. Tra omonimi e mitomani, lui è a quota 26 profili "fake". Ma il social network più famoso a livello internazionale sembra possedere doti ancora più inquietanti, come testimonia la "resurrezione" dell'ex Presidente USA Ronald Reagan, che ha ormai superato gli 80 profili. Non è tutto. Questo è solo l'aspetto più edulcorato del cosiddetto "lato oscuro" che tanto contraddistingue il social network americano. Dalla bacheca di Facebook alla scena del crimine, infatti, in alcuni casi il passo può essere terribilmente breve. Del resto, come in ogni medaglia che si rispetti, ci sono sempre due lati da considerare... ed ecco affacciarsi prepotentemente il lato più oscuro di quest'epoca digitale travagliata: i valori condivisi, quelli che contano davvero, sono solo quelli diffusi e promossi dalla "rete delle reti". E gli esempi "sinistri" non mancano. Pensiamo alla spaventosa diffusione dell'anoressia, mitizzata in molteplici blog giovanili o ai siti che propugnano il suicidio come unica soluzione ai mali del mondo reale. Per non parlare, poi, del notevole incremento tra i giovani di gravi disturbi di matrice psicopatologica. Ma quest'epoca ha visto anche la nascita di veri e propri nuovi eroi. Modelli positivi o negativi, viene considerato determinante il possesso di competenze tecnologiche straordinarie, in grado di trasformare i "nuovi eroi" in esseri onnipotenti. O quasi. Insieme a loro sono nate nuove forme di devianza, come il cyberstalking ed il cyberbullismo e reati caratterizzati da alta tecnologia. Ma anche i reati per così dire più "tradizionali", come la diffamazione o la calunnia, hanno conosciuto una nuova "età dell'oro" attraverso la "rete delle reti". Ma davvero «in Democrazia un cittadino deve avere il diritto di dire le sciocchezze più grandi che crede», come teorizzò, nel 2003, l'allora Ministro della Giustizia Roberto Castelli? Considerata l'enorme mole di vera e propria immondizia che trabocca online, il Ministro dell'Interno Roberto Maroni pensa di no. E, a mio modesto parere, ha ragione. Se è vero che la nostra libertà finisce dove inizia quella degli altri, anche la libertà di parola, il bene più prezioso in una Democrazia degna di considerarsi tale, ha un limite. Che non è solo quello del buon senso, per molti un vero e proprio sconosciuto: si tratta del limite fissato dal nostro codice penale. Ci sono delle leggi e bisogna rispettarle. Nessuno escluso, nemmeno in forma di avatar o profilo "fake su facebook". Come ha spiegato Antonio Roversi nel libro «L'odio in Rete», il lato oscuro del web «è popolato da individui e gruppi che, pur nella diversità di accenti e idiomi utilizzati, parlano tutti, salvo qualche rara, ma importante, eccezione, il linguaggio della violenza, della sopraffazione, dell'annientamento». Tomas Maldonado l'aveva già intuito anni fa: «In queste comunità elettroniche cessa il confronto, il dialogo, il dissenso, e cresce il rischio del fanatismo. Web significa rete, ma anche ragnatela. Una ragnatela apparentemente senza ragno, dove la comunicazione, a differenza della tivù, sembra potersi esercitare senza controllo». Colpire Internet, dicono gli avvocati di Google, denunciata per certi video infami su YouTube, dello stesso infimo livello di quello che mostrava un disabile pestato e irriso dai compagni, «è come processare i postini per il contenuto delle lettere che portano». Ed eccolo, il lato oscuro, emergere in tutto il suo macabro fascino ed in tutta la sua terrificante diffusione. Il problema vero è che l'odio e la distruttività albergano in ciascuno di noi, anche quando il computer è spento.

Andrea Zapparoli Manzoni
CEO iDialoghi srl

Sofia Scozzari
COO iDialoghi srl

Il business dei social networks

Gli strumenti di social networking più diffusi, Facebook e Twitter, sono ormai considerati la piattaforma di incontro ed espressione delle masse. Tutto questo, solo 5 anni fa, sarebbe stato considerato fantascienza, e certamente non è stato valutato con la dovuta attenzione.

La rivoluzione dei social networks

Quanto avvenuto recentemente in Tunisia ed Egitto è particolarmente indicativo del rapidissimo emergere di nuove dinamiche politiche e socioeconomiche, veicolate e rese possibili dalla diffusione dei Social Networks. Per quanto non sia l'argomento di questo articolo, una ricapitolazione di quanto avvenuto nei giorni scorsi può essere utile ad introdurre le considerazioni che svolgeremo più sotto. In Nord Africa, il mix tra crescente disponibilità di connettività, un'età media della popolazione intorno ai 25 anni e le tecnologie di social networking, si è dimostrato dirompente, unito allo scontento causato da decenni di malgoverno e dall'attuale crisi economica globale. Questo mix ha contribuito in modo significativo al successo della rivoluzione tunisina, al punto da spingere il governo egiziano a compiere un atto mai accaduto da quando esiste Internet: scollegare l'intero Paese dalla rete, in un goffo tentativo di impedire alle folle di coordinarsi ed al mondo di ricevere notizie non filtrate sull'evolversi della situazione. Inevitabilmente, questo tentativo, per quanto tecnicamente riuscito, non ha sortito gli effetti sperati e le informazioni sono continuate a fluire per mille canali alternativi. Lo sdegno e la preoccupazione planetaria provocati da questa azione repressiva da parte egiziana hanno dimostrato che Internet, ed in particolare gli strumenti di social networking più diffusi, Facebook e Twitter, sono ormai considerati LA piattaforma di incontro ed espressione delle masse. La possibilità di accedervi senza vincoli è ritenuta fondamentale, tanto quanto lo sono l'accesso a telefono, radio e televisione, se non di più, data la loro natura di strumento di comunicazione "peer to peer". Tutto questo, solo 5 anni fa, sarebbe stato considerato fantascienza, e certamente non è stato valutato con la dovuta attenzione da parte degli analisti internazionali, colti di sorpresa dagli eventi nordafricani. Occorre dunque fermarsi un attimo a riflettere sulla velocità e sulla pervasività di questi fenomeni per poter cogliere appieno la dimensione del cambiamento epocale in corso ed inquadrarlo nell'ambito specifico del tema di questo articolo. A titolo di esempio, riportiamo quindi alcuni dati in merito alla stella più luminosa della galassia di servizi "social" basati su Internet, Facebook.

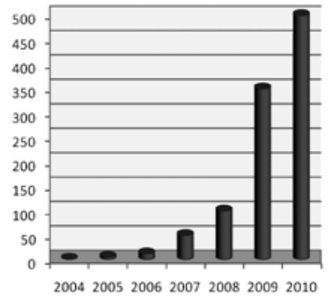
Il fenomeno Facebook

Facebook è una società privata nata nel 2004 ed è oggi valutata 50 miliardi di dollari. Vanta 600 milioni di utenti al mondo, di cui oltre 17 in Italia. Con una crescita di circa il 3,5% su base mensile, nel 2010 l'Italia è diventata il Paese con il tasso di aumento più rapido al mondo. L'utente medio ha 130 amici, è connesso a 80 gruppi e pagine di community e trascorre oltre 55 minuti al giorno navigando all'interno del sito. Di conseguenza, ogni mese nel mondo vengono spesi 700 miliardi di minuti su Facebook (corrispondenti ad oltre 1 milione di anni uomo!). Di questi 600 milioni di persone (che rappresentano, per popolazione, la terza Nazione della Terra, dopo Cina ed India), 150 milioni di utenti accedono a Facebook da dispositivi mobili e sono due volte più attivi rispetto agli utenti tradizionali, essendo tipicamente sempre connessi.
Questi numeri sono straordinari. Eppure, queste piattaforme non rappresentano alcuna rivoluzione, quantomeno dal punto di vista tecnologico, rispetto a quanto visto negli ultimi 15 anni. Qual è dunque la ragione della forza assunta dai social network?

Uno spazio sociale illimitato: qui, ora ed ovunque

È sufficiente una connessione Internet (anche lenta), un qualsiasi terminale con un browser web (anche un telefono) perché chiunque possa essere istantaneamente in contatto con chiunque altro, ed inizi a condividere contenuti con il resto del mondo. Gossip, tifo sportivo, politica, moda, fino all'organizzazione del prossimo sabato sera o della prossima rivoluzione, tutto viene postato, discusso, inoltrato, commentato e fatto circolare alla velocità del pensiero, ovunque si trovino le persone coinvolte.
L'aspetto rivoluzionario è dunque questo: la facoltà che, grazie ad una connessione spesso always-on ed ai social networks, chiunque ha di poter raggiungere uno "spazio sociale" ormai privo di confini, popolato in ogni momento da centinaia di milioni di persone in tutto il mondo, e di interagire in tempo reale potenzialmente con ciascuna di esse.
Tutti questi aspetti sono sicuramente positivi, ma deve essere considerato anche il lato oscuro dei social media, che inevitabilmente attirano le attenzioni e gli interessi di malintenzionati di ogni genere e possono diventare il veicolo di minacce anche molto gravi. Questi rischi vanno definiti ed affrontati quanto prima, date le dimensioni del fenomeno, in particolare quando l'uso dei social media avvenga in ambito business.

Facebook nel mondo
(in milioni di Active Users)



I rischi dei social media

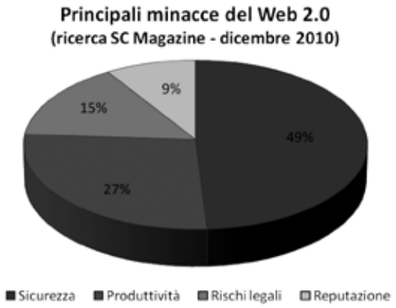
I rischi sono di due ordini, uno generale, legato alle tecnologie ed al loro utilizzo, l'altro specifico, relativo cioè all'uso in ambito business o comunque all'interno di scenari di utilizzo non privato (tra i quali rientrano anche la PA, le Istituzioni, le scuole, le PMI, gli studi professionali, ecc). Le minacce generiche derivanti dall'uso dei social media si possono riassumere in:

- Infezioni da malware (trojan, worms, rootkits, ecc) veicolate via browser tramite le pagine dei social network (Sophos ha re-

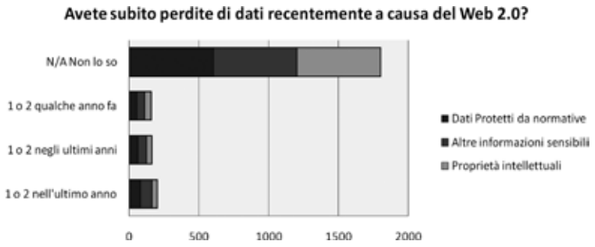
centemente sostenuto che il 40% degli utenti Facebook viene in contatto con qualche genere di malware diffuso tramite il sito);
- Esecuzione di applicazioni di terzi (apps) non affidabili, se non addirittura volutamente dannose;
- Spam (spesso in combinazione con malware);
- Phishing & Whaling (raccolta di informazioni a fini fraudolenti, tramite tecniche di social engineering), sia attuando forme di "pesca a strascico" (phishing), sia attaccando soggetti ben precisi, tipicamente vip (whaling);
- Furto di identità;
- Danni alla privacy;
- Diffamazione;
- Stalking.

Oltre alle minacce generiche, le minacce specifiche derivanti dall'uso dei social media in ambito business si possono riassumere in:
- Danni all'immagine ed alla reputazione dell'azienda;
- Perdita o diffusione incontrollata di dati riservati, proprietà intellettuale, informazioni sensibili protette da normative specifiche;
- Possibilità di diventare oggetto di Open Source Intelligence (OSInt) da parte di concorrenti e nemici;
- Possibilità di arrecare danni a terzi (liabilities/responsabilità);
- Frodi e Social Engineering;
- Minore produttività dei collaboratori.

Va inoltre segnalato, per le complicazioni che comporta, un ulteriore trend in atto: la cosiddetta consumerization dell'informatica, in cui gli utenti portano sul posto di lavoro propri computer, tablet e smartphone e ne fanno un uso misto, connettendosi alla rete ed alle risorse aziendali. Le motivazioni sono molteplici e vanno dall'interesse dell'azienda a risparmiare sulla gestione del parco macchine al fatto che gli utenti comunque utilizzano i propri device in ambito lavorativo per connettersi al proprio spazio sociale privato, senza dimenticare che, ormai, tali device sono spesso tecnologicamente più avanzati di quelli messi a disposizione dall'azienda. Questo fenomeno, unito alla prevista ulteriore diffusione dei Social Media nel prossimo futuro, determinerà un aumento esponenziale dei dispositivi e degli utenti connessi, con una crescita corrispondente dei rischi di sicurezza, in particolare a causa della proliferazione di dispositivi mobili e della diffusione di servizi cloud-based che rendono controlli e contromisure più difficili. In una recente ricerca, Cisco stima che nei prossimi 3 anni (entro il 2014) le minacce raddoppieranno e i rischi aumenteranno in modo più che proporzionale.



Prima di introdurre le possibili soluzioni, volte ad eliminare o mitigare i rischi sopra elencati, è opportuno mettere a fuoco i principali ostacoli ad un utilizzo sicuro dei Social Media in ambito business:
- un numero crescente di minacce si realizza a livello semantico, impossibile da monitorare e gestire con strumenti tradizionali;
- Consumerization of Enterprise IT: gli utenti utilizzano strumenti propri ed eterogenei rispetto all'IT aziendale;
- per vari motivi, è "vietato vietare" (particolarmente in Italia);
- la normativa tutela (giustamente) la privacy e la libertà dei collaboratori, complicando le attività di monitoraggio;
- la consapevolezza dei problemi è ancora molto bassa, a tutti i livelli;
- le tecnologie di mitigazione non sono ancora al passo con le problematiche (ma si evolvono a grande velocità);
- e policies ed i comportamenti virtuosi sono sempre in ritardo rispetto alla tecnologia. Recenti ricerche dimostrano inoltre che le aziende non possiedono strumenti adeguati per monitorare e misurare la perdita di dati. Il fenomeno sfugge quindi al controllo in oltre il 90% dei casi (ricerca Securosys del 2010, su un campione di 2.000 aziende a livello globale). Ciò dimostra quanto lavoro ci sia ancora da fare, e l'urgenza di mettere mano a rimedi e soluzioni adeguate.



Le Soluzioni

Il problema è complesso e non esistono bacchette magiche. Le variabili coinvolte sono moltissime e le problematiche vanno affrontate su piani diversi, non solo su quello tecnologico, perché i rimedi possano avere efficacia. Per delineare soluzioni consistenti ed applicabili nel mondo reale vanno considerati aspetti strategici e di budget, organizzativi, tecnologici e legali.

In un'ottica complessiva di Gestione del Rischio, le strategie da perseguire contemporaneamente sono quattro:
- rimediare alla mancanza di procedure standard, policies, strumenti organizzativi, piani di rientro e, in generale, di cultura aziendale in materia;
- implementare strumenti tecnologici efficaci di monitoraggio e controllo, considerando che firewall, proxy ed antivirus non servono (quasi) più a niente;
- responsabilizzare gli utenti e le strutture aziendali coinvolte, a qualsiasi titolo, sull'uso dei Social Media. Non è un problema (solo) dell'IT o dei responsabili legali;
- ridurre attivamente i comportamenti a rischio contrari alle policies aziendali: secondo Cisco, solo il 10% degli utenti le rispetta, mentre il 50% non le conosce ed il restante 40% le aggira! (Cisco connected world report - novembre 2010)

Conclusioni

Limitarsi a vietare non è solo impossibile, ma anche controproducente: social è il nuovo paradigma di comunicazione del Web 2.0, indietro non si torna. Nei prossimi anni si deciderà se il Web 2.0 diventerà una sorta di far west, insicuro ed insidioso, oppure un potente catalizzatore di nuovi business, dinamiche umane e lavorative e, soprattutto, di sviluppo socio-economico. Noi crediamo che gestire i nuovi scenari di sicurezza derivanti dall'utilizzo dei social media in ambito business sia una necessità ed insieme un'opportunità: selezionare le tecnologie più adatte, formare le persone, individuare le policies ed i controlli più efficaci in ogni contesto specifico ed integrarli nei sistemi di Governance esistenti è una sfida che, in qualità di addetti ai lavori, accettiamo con piacere... È tempo di aprire un dibattito serio tra istituzioni, imprese ed organizzazioni da un lato, ed esperti di sicurezza, marketing e questioni legali dall'altro, per definire obiettivi comuni: non gestire il fenomeno social media in modo organico, con una visione di medio-lungo termine, valorizzandone gli aspetti positivi e mitigando quelli negativi, è un errore oggi ancora evitabile. Ricordando, però, che la finestra temporale a disposizione si sta chiudendo rapidamente.

Roberto Setola
Direttore del Master in Homeland Security dell'Università CAMPUS BioMedico di Roma
Segretario della Associazione Italiana esperti Infrastrutture Critiche (AIIC)

Il futuro di WikiLeaks

Nei prossimi anni vedremo sempre più spesso exploit di informazioni più o meno veritiere sbandierate come segreti carpiti a questa o quell'organizzazione. Alla fine, le informazioni saranno protette non tanto dalle barriere dietro le quali verranno conservate, ma dalla difficoltà di determinare quale fra le diverse fonti sia attendibile e quali informazioni, da essa diramate, siano vere, false o astutamente manipolate.

Tutti gli organi di informazione hanno prestato grande attenzione al fenomeno WikiLeaks. Ne hanno evidenziato l'eccezionalità, quasi rappresentasse una "rivoluzione" nel campo della protezione delle informazioni. Qualcuno si è anche spinto a dire che, dopo WikiLeaks, nessuna informazione è più al sicuro e che avremo presto accesso a tutte le informazioni "riservate" generate, raccolte o conservate da chiunque. Questa visione molto giornalistica è, per fortuna, poco realistica, sebbene WikiLeaks rappresenti ugualmente un evento epocale per coloro che si occupano della protezione delle informazioni. Per capire questo apparente paradosso, dobbiamo analizzare meglio il significato effettivo di WikiLeaks. Sintetizzando in termini minimi, si può affermare che Julian Assange è entrato in possesso di alcune informazioni riservate (non certo quelle segrete o segretissime) e le ha pubblicate sul suo sito web. Il furto, o comunque l'acquisizione, delle informazioni dell'avversario è una strategia di politica estera comune a tutti i Paesi del mondo, ma anche a realtà industriali e commerciali. Non da oggi, potremmo dire da sempre. Conoscere in anticipo le mosse del "nemico" è sempre stato un obiettivo strategico, declinatosi nelle varie e molteplici forme dello spionaggio, dell'intelligence e, più di recente, della business intelligence. Per proteggersi da queste azioni, i diversi Stati e le aziende si sono attrezzati con strategie di contro-spionaggio anche molto raffinate, che non si limitano alla sola protezione delle informazioni, ma favoriscono anche la diffusione di informazioni volutamente false o fuorvianti. Il fatto che qualcuno sia riuscito ad entrare in possesso di alcuni documenti riservati non costituisce quindi una novità. Ciò che di peculiare possiede WikiLeaks è invece legato a due aspetti, evidenziati solo in parte dai media. Il primo è rappresentato dall'enorme quantità di informazioni che Assange è riuscito a carpire. Ciò è frutto della diffusione pervasiva delle tecnologie informatiche, le quali, da un lato hanno favorito un aumento esponenziale dello scambio di informazioni (quante mail riceviamo ed inviamo ogni giorno? Confrontiamo questo numero con i nostri scambi epistolari di cinque o dieci anni fa) e dall'altro hanno permesso di maneggiare, conservare e riprodurre con estrema facilità quantità anche enormi di dati. Oggi, su una mini pen-drive della dimensione di un francobollo, possono essere memorizzate tante informazioni quante quelle contenute in 300 metri di scaffalature! (e la pen-drive è certamente più facile da trasportare o nascondere rispetto alle tonnellate di carta delle scaffalature). L'altro aspetto colto da pochi è che Assange ha agito nel mondo dell'intelligence "violando" la prima regola, la riservatezza. Tutte le azioni di spionaggio sono sempre state improntate al più assoluto riserbo, dovuto al fatto che il valore di un'informazione "segreta" è tale solo fino a che la stessa mantiene, appunto, la sua segretezza: se so che il mio nemico conosce le mie mosse, per prima cosa cambierò strategia, è evidente. Così, anche il potere "ricattatorio" legato al possesso di informazioni scottanti è tale fino a che queste non divengano di dominio pubblico. Il modello di business di Assange è esattamente contrario a quanto previsto dall'intelligence: viene offerta la massima diffusione delle informazioni riservate di cui è entrato in possesso. E ciò è possibile, ancora un volta, grazie al progresso delle tecnologie ICT e del WEB in particolare. Oggi, infatti, il WEB permette una diffusione delle notizie/informazioni in modo assolutamente inarrestabile: non esistono strumenti per bloccare o limitare un'informazione immessa in rete. Il dopo WikiLeaks si contraddistinguerà quindi non tanto e non solo nel prevenire le fughe di notizie (impresa al limite dell'impossibile), ma nel limitare la capacità di diffusione delle stesse. Non tanto con la censura (che sul WEB ha poco successo), ma con la strategia esattamente opposta: rendendo meno attraenti le notizie, superate da altre del medesimo tono, costruite magari ad arte. Nei prossimi anni vedremo sempre più spesso exploit di informazioni più o meno veritiere sbandierate come segreti carpiti a questa o a quell'organizzazione. Alla fine, le informazioni saranno protette non tanto dalle barriere dietro le quali verranno conservate, ma dalla difficoltà di determinare quale fra le diverse fonti sia attendibile e quali informazioni, da essa diramate, siano vere, false o astutamente manipolate. Non è altro che il vecchio gioco dello spionaggio e del contro spionaggio. Il caro, vecchio, "grande gioco" dei tempi di Kipling, svolto, però, a carte scoperte, in modo tale che tutti possano guardare attoniti. In fondo, non c'è nulla di più nascosto di ciò che viene lasciato bene in vista.

Davide Giacalone
Politico, giornalista e scrittore italiano

Wikiflop

La faccenda dei files pubblicati è gravissima non tanto sotto il profilo del contenuto, ma del fatto stesso che cada il segreto diplomatico, fissato dal Congresso di Vienna (1815). Senza riservatezza diplomatica, non ci sono negoziati. Solo alleanze o guerre. Si provi ad immaginare.

Non appartengo a quanti si sono emozionati per i documenti pubblicati da WikiLeaks. Prima ancora che fossero pubblicati, sostenni che non ci si sarebbe trovato nulla che già non sapessimo. Con il senno di poi, almeno fin qui, non posso che confermare quell'opinione. Ciò non significa, però, che la fuoriuscita di materiale diplomatico sia insignificante. La reale natura della falla deve però essere cercata nelle guerre interne al mondo politico e all'amministrazione statunitense. Se ne è messa in piazza la vulnerabilità, mentre un Presidente non più in attesa di collaudo fatica a dominare lo scenario internazionale ed a trovare un ruolo credibile per gli Stati Uniti. Il Paese che ha svolto un ruolo di guida e di garante occidentale, quello che ha vinto la guerra fredda ed ha annientato l'impero sovietico, non ha mostrato solo la vulnerabilità dei propri archivi, ma, subito dopo, ha dovuto subire due smacchi impressionanti: il presidente cinese, Hu Jntao, prima di salire sulla scaletta dell'aereo che lo portava a colloquio con il collega americano, ha annunciato che avrebbe rifiutato ogni accordo valutario, mentre la crisi dell'intera fascia mediterranea dell'Africa, culminata nelle proteste contro il presidente egiziano Hosni Mubarak, ha messo in crisi equilibri di cui gli Stati Uniti erano garanti. A cominciare dalla sicurezza d'Israele, che costituisce, non lo si dimentichi mai, un avamposto democratico ed occidentale che sarebbe pericolosissimo abbandonare. Queste sono le partite che contano, il resto è contorno. Ciò che abbiamo letto, e molte polemiche di casa nostra, fanno, invece, tenerezza. Mi riferisco a quelli che hanno passato una vita a sfilare urlanti contro l'imperialismo americano, maledicendo la satanica macchina diplomatica che pretendeva di guidare le politiche altrui, screditando quanti non si piegavano agli ordini a stelle e strisce, e ora si ritrovano a biascicare moralismi da beghine affrante, lamentando che "gli Americani" ci giudicano male. Spulciano la documentazione di WikiLeaks e, non attendendo neanche che arrivi la parte succosa, posto che ci sia, s'accasciano sul pettegolume. S'accontentano della formula da barzelletta: ci sono un Francese, un Tedesco e un Italiano, il primo ha pretese napoleoniche, il secondo è ottuso, ma disciplinato, il terzo crapulone. Fin qui, la faccenda dei files pubblicati è gravissima non tanto sotto il profilo del contenuto, ma del fatto stesso che cada il segreto diplomatico, fissato dal Congresso di Vienna (1815). Senza riservatezza diplomatica, non ci sono negoziati. Solo alleanze o guerre. Si provi ad immaginare. Non ho idea se fra quei documenti si troverà qualcosa di meno superficiale, relativo al dossier energetico, ma è questa la partita più significativa. E ci vogliono miopia ed ignoranza fuori dal comune per affrontarla solo sotto la luce dei rapporti fra Berlusconi e Putin, quasi si trattasse di questioni personali. È una partita che attraversa tutta l'intera storia repubblicana, a cominciare dall'Eni di Enrico Mattei, di cui non solo i petrolieri statunitensi dicevano peste e corna, ma in relazione al quale si giunse pure a questioni di "donnine". Anche in quel caso, naturalmente, non era una vicenda personale, tant'è vero che coinvolse per intero la politica estera italiana. La gestione dossettiana e filo araba non piaceva per nulla agli Americani, ma piaceva tantissimo a quelli che oggi gongolano per i giudizi di un loro diplomatico. Era l'Italia in cui la Fiat apriva lo stabilimento di Togliattigrad, quella in cui si trovavano ambasciatori statunitensi che inviavano rapporti durissimi contro il centro sinistra e contro Aldo Moro. Ma allora, gli odierni adoranti erano impegnati a chiedere: fuori la Nato dall'Italia e l'Italia dalla Nato. Fortunatamente, hanno perso. E dico "fortunatamente" da antico estimatore degli Stati Uniti, poco propenso, pertanto, a confondere per "americane" le cose scritte da un Americano. Perché, alla fine, conta la politica estera ufficiale, non lo smanacciamento cui è stata sottoposta nelle cucine. E, per dirne due, conta che a Pratica di Mare sia iniziato l'avvicinamento della Russia alla Nato, come conta che il gas italiano arrivi prevalentemente dall'Algeria, mentre i nuovi gasdotti non si prestano a rapporti compromissori con gli Iraniani. Ma che possono capirne quelli che si sono sempre prestati alla non autonomia energetica dell'Italia e che volevano riconoscere ad Ahmadinejad l'aspirazione ad assurgere a potenza regionale? E oggi pubblicano i dispacci in cui lo si definisce Hitler, accanto alle battute insulse sul lettone di Putin, senza neanche afferrarne il nesso. C'è una forza della geopolitica, un peso degli interessi indisponibili di un Paese, che attraversa il tempo e non cambia colore con i governi. Per capirlo, si deve studiare la storia, avendo in mente una cartina geografica, e saper far di conto. Se si corre dietro ai documenti in cui i diplomatici fanno il riassunto della rassegna stampa, se si perde di vista la sostanza e ci si butta sulla paccottiglia, va a finire che l'intero Paese è ai materassi. Uno sopra e gli altri sotto. Il mondo ha atteso di sapere se dagli archivi della Segreteria di Stato statunitense fossero uscite solo riproduzioni di chiacchiericci o notizie precise su come si sono articolati affari altrimenti a tutti noti. Il netto prevalere dei primi non deve indurre a sottovalutare la portata di quel che è accaduto.

Luca Sofri
Giornalista, conduttore radiofonico italiano

Io, Julian Assange

Da quattro giorni rincorro Julian Assange, che mi risponde puntualmente ad ogni mail confermandomi un'intervista, ma glissa ogni volta su tempi e modi. Non so dove chiamarlo, mi ha chiesto i miei numeri e contatti: sto per andare a cena quando ricevo da Skype questo messaggio:

hi luca
this is iceland
can you respond?

"Iceland?". È uno dei soliti spammers su Skype? E come fa a sapere come mi chiamo? E poi realizzo e mi ricordo i titoli "Iceland aims to become an offshore haven for journalists": l'Islanda mira a diventare un rifugio sicuro per i giornalisti. Faccio due più due: è Assange. Rispondo, e mi appare in video la faccia da attore e la chioma platino inconfondibile.
Ciao, come va?

Bene, grazie. Dove sei?
Sono in Islanda.

Per quel progetto?
Sì. Su quattro tappe, siamo alla due.

Ovvero?
Ovvero c'è una proposta di legge firmata da 19 parlamentari perché l'Islanda accolga tutta una serie di misure protettive della libertà di stampa e informazione che le consentano di diventare un equivalente dei paradisi fiscali per il giornalismo investigativo. In Islanda il parlamento ospita 63 deputati, quindi parliamo di un terzo di loro. E ora una commissione sta esaminando la proposta.

Cosa succede se la proposta diventa legge?
Che l'Islanda creerà un precedente e un modello per gli altri Stati, soprattutto quelli che hanno regole più severe contro il giornalismo d'inchiesta e la libertà di informazione. In Inghilterra guardano con molta preoccupazione a questo progetto: la rigidità delle sue corti ha creato un fenomeno noto come il "turismo della querela": da tutto il mondo si presentano cause contro i giornali in Inghilterra dove è più probabile vincerle. L'Inghilterra, ma anche la Francia, dove i conflitti sociali sono più aspri e i poteri economici più forti, hanno più interesse a limitare la libertà di stampa. In Islanda, soprattutto dopo il crack economico, c'è invece una grande attenzione verso una maggiore trasparenza.

WikiLeaks come è coinvolta?
Stiamo collaborando con i promotori della legge, condividendo la nostra esperienza di perseguitati da cause e tribunali. Alla fine dell'anno scorso WikiLeaks ha sospeso le operazioni ed è entrata in sciopero… No, non siamo mai stati in sciopero… Sono parole tue, le ho lette in un'intervista. Ok, abbiamo cercato di promuovere uno sciopero interno, diciamo. I costi per far funzionare WikiLeaks sono diventati insostenibili e abbiamo spinto i volontari che ci lavorano a concentrarsi solo sulla raccolta di fondi.

E a che punto siete? Il sito mi pare a mezzo servizio.
Siamo a metà strada nella raccolta dei contributi che avevamo stabilito (600.000 dollari, ndr), oltre metà strada: stiamo lavorando per rimettere tutto in piedi.

Adesso cosa funziona?
Abbiamo ripreso a pubblicare dei documenti e lavoriamo costantemente sulla protezione dei nostri server, dei nostri archivi e della sicurezza delle fonti. Abbiamo molti documenti che costituiranno le cose più importanti che abbiamo mai pubblicato. Video, database, elenchi.

Puoi dire che tornerete a pieno regime in qualche mese?
Stiamo già ripristinando diverse cose, torneremo gradualmente a pieno regime: questione di settimane.

Sei soddisfatto di come ha funzionato WikiLeaks in questi anni?
Il suo successo me lo aspettavo. Ma sul rapporto con i media tradizionali sono ancora insoddisfatto. Non riescono a pubblicare tutto quello che forniamo: solo i media tradizionali hanno il tempo e i soldi per coprire i costi di tutte le verifiche e la competenza per comprendere i documenti e le storie. Non è una cosa che possa fare "internet" o le persone normali. Ma i grandi media hanno sempre paura di non essere abbastanza presenti sull'attualità: ci dedicano spazio solo nel momento in cui facciamo notizia. Possiamo diventare notizia grazie al pubblico, ai cittadini. Che però, spesso, non hanno le capacità né le motivazioni per capire la notizia e possono "ammazzarla".

Da qui la soluzione delle esclusive?
Il sistema dei media genera dei paradossi. Più materiale c'è, più è diffuso e più è difficile che trovi spazio sui giornali: meno una cosa circola e più è facile che i giornali la pubblichino. Quindi trattiamo con alcuni di loro delle esclusive.

Ma diffidi dei dilettanti perché non hanno le capacità giornalistiche necessarie o perché non sono in grado di promuovere le notizie abbastanza?
Dobbiamo stare attenti. Se scrivono delle tue cose i dilettanti, ci sono più rischi che non le capiscano, le divulghino male e chi è citato faccia causa o protesti. Su questo non ho dubbi: il giornalismo investigativo è roba da professionisti, solo loro possono venire a capo delle enormi quantità di documenti che mettiamo a disposizione.

Però, scusami: WikiLeaks vuole smontare i meccanismi perversi dei poteri politici ed economici, attaccandone la segretezza. E però con i meccanismi perversi dell'informazione sceglie invece di venire a patti. Non c'è una contraddizione?
Ok. Non mi faccio illusioni sui media: la maggior parte della stampa è spazzatura e andrebbe riformata. E l'unica via per riformarla forse sarebbe distruggerla. Però noi non le vendiamo l'anima, come sostieni tu. Le nostre esclusive sono a tempo, ed è una strada che vorremmo non scegliere. Ma la nostra lealtà prioritaria è nei confronti della verità e delle nostre fonti a cui dobbiamo ogni sforzo per divulgare ciò che ci hanno affidato.

Cambierà qual…
E comunque siamo contenti di collaborare con i bravi giornalisti.

Cambierà qualcosa nel funzionamento di WikiLeaks?
Avremo un sistema nuovo di pubblicazione.

Solo tecnologia, o anche nuovi criteri?
Soprattutto una cosa interna: prima l'accesso era uguale per tutti su ogni tipo di documento, dai verbali del liceo agli scoop giornalistici. Ora stiamo creando delle gerarchie di accesso.

Tornerà on-line anche la possibilità di commentare i documenti?
Stiamo lavorando ad un sistema di commenti nuovo, ma siamo ancora indietro. Abbiamo capito che un sistema alla Wikipedia – un wikisistema di commenti – è un'idea pessima: arriva sempre qualcuno che non capisce niente, o scrive cose che non c'entrano. Una bella tecnologia, accessibile, ma sbagliata per noi. La riformeremo.

WikiLeaks ti impegna al 100%?
Salvo scrivere degli articoli, sì.

Osservi cautele personali particolari?
Nei Paesi occidentali non ho preoccupazioni sulla mia vita. In Kenya c'è stato un raid nel mio ufficio, e gente che è stata uccisa in relazione alla storia sulla corruzione dell'ex presidente. In Occidente mi spiano di certo, ma non temo per la mia vita. Quando non fornisco il mio numero, è per cautele di segretezza e per proteggere le nostre fonti.

Sei soddisfatto di quello che avete fatto?
Sì. Ma avremo completato la nostra missione solo quando ogni tecnico informatico, ogni bambino dell'asilo, ogni burocrate di un ministero saprà di poter pubblicare quello che vuole senza correre rischi.

Ma la vostra battaglia è contro la segretezza in sé o contro le sue corruzioni?
Il nostro obiettivo è combattere le ingiustizie. Io non sono contro la segretezza in sé, ma succede sempre, prima o poi, che la segretezza corrompa. Che ci siano persone con molto potere non è di per sé pericoloso: il pericolo è che ci sia segretezza nelle cose che fanno con quel potere e che questa segretezza incentivi a fare cose sbagliate. C'è un limite nel grado di civiltà che una società può avere, ma l'antidoto è una maggiore trasparenza sui documenti storici che raccontano come funziona questa società.

Ci vediamo a Perugia?
Senz'altro. E seguite l'Islanda. Seguite l'Islanda. E ******* Berlusconi!

Per gentile concessione della rivista WIRED

L'aggiramento di un vincolo

La censura è come un danno

"The Net interprets censorship as damage and routes around it". (John Gilmore, attivista digitale).

Nel novembre scorso, WikiLeaks è assurto ad indiscussa notorietà globale con la pubblicazione di una vasta collezione di comunicazioni diplomatiche riservate del governo americano. Ha mostrato in modo eclatante la forza dirompente della rete in materia di circolazione delle informazione e loro resistenza ai tentativi di censura. Sebbene WikiLeaks esista on-line sin dal 2006, e già in passato abbia reso disponibili informazioni di natura segreta, riguardanti in particolare gli Stati Uniti, è solo con gli oltre 250.000 documenti della diplomazia americana messi in rete a novembre che ha ottenuto l'attenzione dei più. Ad essere sinceri, la maggior parte del materiale immediatamente rigurgitato dai media tradizionali possiede più i connotati del pettegolezzo che della scomoda verità: vizi e nomignoli del gotha della politica internazionale, giudizi poco edificanti sulle Nazioni alleate e pure peggiori su quelle antagoniste, ecc. Qualcosa di davvero segreto e pericoloso potrebbe effettivamente celarsi tra quella gran mole di dati, ma al popolo della rete e a quello dei media tradizionali è stato offerto il solito fritto misto di banalità pruriginose, buone per ogni occasione di conversazione spicciola, ma ben poco adatte per una riflessione a tutto campo sulla libertà di informazione. In un certo senso, WikiLeaks rappresenta l'attuazione più evidente ed immediatamente percepibile del concetto di libera circolazione delle informazioni e può svolgere un ruolo importante per la diffusione della libertà d'espressione. L'impressione è però che la fenomenizzazione delle ovvietà non giochi a favore della diffusione di una cultura basata sulla collaborazione e sulla condivisione della conoscenza volta al progresso collettivo. Nonostante la reazione piuttosto forte del governo americano e l'azione di boicottaggio operata da alcune importanti realtà commerciali, le quali si sono schierate contro WikiLeaks ostacolandone la presenza on-line e l'afflusso dei finanziamenti, i siti che replicano e rendono accessibili i contenuti si sono moltiplicati. In diverse parti del mondo si stanno inoltre organizzando reti di informazione simili a WikiLeaks finalizzate a continuare ad offrire la possibilità di accesso a dati e notizie altrimenti destinati a rimanere sepolti negli archivi per decenni. WikiLeaks ed i suoi emuli e successori poggiano la loro attività sull'uso combinato di diversi software a sorgente aperta, realizzati in tempi diversi, ed in alcuni casi finanziati addirittura dalla ricerca militare della Nazione maggiormente attaccata. L'obiettivo principale è la protezione dell'anonimato in rete: l'elemento è importantissimo per garantire la libertà d'espressione e proteggere dagli abusi a danno della privacy che la tecnologia rende attuabili con estrema facilità. Allo stesso tempo, la materia è controversa e di difficile trattazione per le sue implicazioni sociali. Se si resiste alla tentazione di lasciarsi fuorviare dai pettegolezzi del e sul potere che, come ogni forma di gossip, assolvono alla funzione di distrarre dagli argomenti davvero importanti per l'umanità tutta, quali sviluppo sostenibile, superamento equilibrato della crisi economica globale, accesso a cibo, acqua, riparo e cure mediche decenti per quella larga parte della popolazione mondiale che ne è ancora esclusa, si può abbracciare con sguardo più ampio l'orizzonte delineato dal fenomeno WikiLeaks. Attraverso la contrapposizione dinamica tra le esigenze di reciproca trasparenza nel rapporto tra amministrazioni di governo e cittadini, e la necessità di consentire a tutti gli attori in gioco l'anonimato e la segretezza laddove le condizioni li rendano necessari ed opportuni, sarà possibile una forma diversa di partecipazione alle istituzioni democratiche. Ed è un fatto che, anche dove l'accesso ad internet è regolato o sottoposto a censure, si determina una maggiore spinta sociale verso l'adozione di pratiche democratiche di governo. WikiLeaks e gli accesi dibattiti che lo contornano, se intesi in questi termini, possono allora essere considerati simboli dell'imponente cambiamento di mentalità che l'avvento della rivoluzione digitale ha portato a tutti i livelli sociali. È grazie a questo caso eclatante ed al battage mediatico che lo sta accompagnando che temi quali la censura, l'anonimato, la privacy, il diritto all'informazione, finora all'attenzione solo di nicchie di attivisti e di quanti sono impegnati nella tecnologia e nell'adeguamento delle norme al progresso che il digitale determina, hanno raggiunto un pubblico più vasto ed attento.

Yvette Agostini
Ingegnere, consulente in ambito informatico e energie rinnovabili

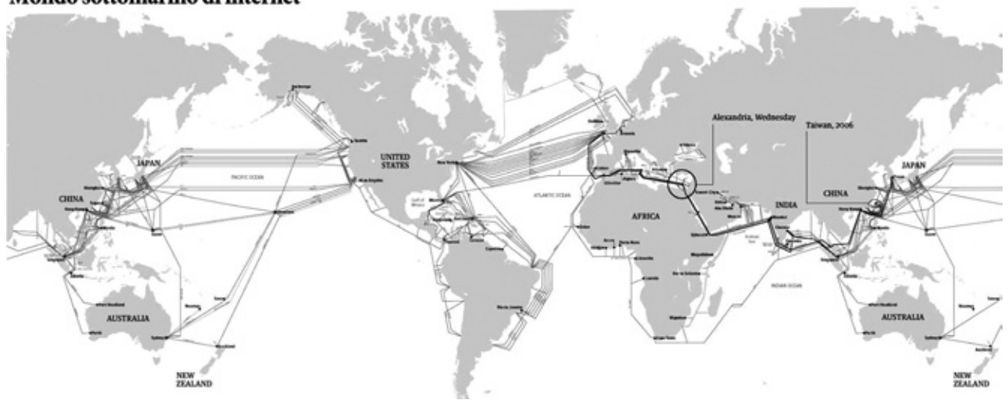
Walter Paolicelli
Avvocato, Presidente World Wide Crime

L'era dell'homo cyber

La maggior parte delle norme relative ai crimini informatici è il frutto di abbozzi veloci e per nulla innovativi. Si è legiferato con riferimento a un qualcosa di troppo instabile e sfuggente utilizzando "la vecchia maniera".

Da diversi anni mi occupo di cyber crime e diritto delle nuove tecnologie in qualità di avvocato e come presidente dell'associazione WorldWideCrime. Mi stupisco ancora quando, alla domanda "cos'è un computer?", ottengo solo risposte che implicano ulteriori chiarimenti. Se ci provate, senza troppo indagare su quali parole possano essere utilizzate per sviscerare un simile misterioso oggetto, vi rendete conto di non riuscire a spiegare la parola computer senza utilizzare espressioni con tutt'altro significato. È un apparecchio, una macchina, un elaboratore, un calcolatore... Queste sono, in genere, le parole utilizzate. Lasciamoci soccorrere. Con il termine computer, mutuato dalla lingua inglese, si fa riferimento al calcolatore elettronico o a particolari categorie di calcolatori che, per le dimensioni ridotte, la discreta seppur limitata capacità elaborativa e il prezzo contenuto, sono adatti all'uso tecnico-scientifico o aziendale di studiosi, professionisti, uffici, piccole imprese (come il personal computer), o sono destinati alle famiglie (home computer) per la contabilità domestica e per servizi vari o a scopo ricreativo. La definizione appena riportata è dell'edizione del Vocabolario della Lingua Italiana Treccani del 1986. Appare chiaro come in quegli anni difficilmente si sarebbe potuto pensare al computer negli stessi termini dei tempi che stiamo vivendo. In quegli anni, il computer appariva come un'enorme calcolatrice, che ben poco avrebbe potuto fornire alle attività quotidiane di ogni singolo cittadino. Nessuno, o quasi, avrebbe mai immaginato che, dal 1986 a pochi anni, questo straordinario apparecchio avrebbe modificato radicalmente la vita di ciascuno di noi. Dalla stesura di questo articolo ai siti web, dalla cartella clinica digitale alla telemedicina, il computer è ormai radicato in maniera imprescindibile in tutte le attività lavorative e ricreative dell'essere umano. Persino il rivenditore di pneumatici al quale mi rivolgo non è più in grado di indicarmi quale modello si adatti meglio alla mia auto senza consultare il PC. Le edizioni aggiornate dello stesso Vocabolario della Lingua Italiana Treccani riportano il significato di computer in questi termini: complesso di dispositivi in grado di effettuare operazioni matematiche e logiche su un insieme di informazioni, in modo da produrre altre informazioni, secondo le istruzioni di un programma che determina le regole di derivazione dei risultati a partire dai dati iniziali. La definizione aggiornata dello stesso Istituto è cambiata radicalmente, con nostro elevato stupore. Com'è possibile che il significato di una parola si modifichi quasi del tutto a distanza di pochi anni? Termini quali telefono, citofono, televisore, stampante, pur essendo riferiti a strumenti assoggettati all'evoluzione tecnologica – poiché di essa sono figli –, hanno conservato il significato attribuito all'epoca della loro creazione. Il computer si è invece evoluto parallelamente alla sua definizione. Una tale considerazione apre la mente a tutta una serie di conseguenze che, come cittadino e come professionista, non posso ignorare. La giurisprudenza si arricchisce di giorno in giorno di massime relative alla definizione di controversie e reati che coinvolgono le nuove tecnologie. Tuttavia, si assapora un certo imbarazzo quando, il più delle volte, ci si accorge che la soluzione del singolo caso viene ad essere ricercata nella sentenza di altro giudice oppure nell'articolo di qualche professionista. È una cosa naturale!, esclamerebbe ognuno di noi. Se solo pensiamo che in pochi anni la lingua italiana ha dovuto mutare la definizione relativa al computer, figuriamoci quali effetti si possono produrre sulle norme e sulla giurisprudenza. Ma non siamo in un Paese di Common Law! Proviamo ad immaginare un soggetto il quale, dopo aver commesso un crimine informatico, venga poi assoggettato ad uno dei tipici processi penali all'italiana. Decine di rinvii, testimonianze assunte a distanza di anni e, per completare, perizie, contestazioni e dissertazioni di natura tecnica completamente oscure al giudicante di turno. La tecnologia si evolve, si sa, e l'Italiano deve starle dietro come di consueto... Ma la norma? In effetti, la maggior parte delle norme relative ai crimini informatici è il frutto di abbozzi veloci e per nulla innovativi. Si è legiferato con riferimento a un qualcosa di troppo instabile e sfuggente utilizzando "la vecchia maniera". Basti pensare al reato di accesso abusivo a sistema informatico (art. 615 ter c.p.), il quale testualmente punisce chiunque abusivamente si introduce in un sistema informatico o telematico e al suo antenato di violazione di domicilio (art. 614 c.p.) che, invece, punisce chiunque si introduce nell'abitazione altrui... Riesco a immaginare i commenti che suscita una tale valutazione, ma è la realtà! Nel mondo digitale, non esiste una vera e propria intrusione, ma un'interrogazione dei sistemi. Quindi, in teoria, l'accesso abusivo non esiste, poiché un criminale informatico che preleva informazioni da un sistema non si introduce in alcun luogo. La discussione, tuttavia, non verte sulle parole (benché in diritto siano tutto), ma sul processo produttivo della norma in esame! Come ben sapete, per condurre un mezzo quale un motociclo, un motoscafo oppure un'autovettura, occorre, in Italia come nel resto del mondo, un brevetto, una patente o

Mondo sottomarino di internet



una speciale abilitazione. Questo perché il cattivo utilizzo dei mezzi appena citati potrebbe provocare un reato, una condotta civilmente illecita oppure, al contrario, potrebbe causare danni al soggetto che li utilizza. Sono sicuro che nessuno degli utenti che acquista un PC si sia mai chiesto come mai, all'interno della confezione appena aperta, non siano stati allegati manuali di istruzione. Ma come, mi direte, i manuali ci sono, e spiegano anche bene come utilizzare il pacco batteria, come usufruire della garanzia, ecc. Io mi riferisco però ad altro genere di manuale. Un manuale che ponga l'utente al corrente delle conseguenze penali e civili che derivano dall'uso del computer, dei rischi che i bambini corrono ad essere lasciati dinanzi al PC collegato in rete a tutte le ore del giorno e della notte, del fatto che i dati personali sono sacri e che prima di fidarsi del primo sconosciuto incontrato in rete occorre accertarsi della sua identità! Insomma, un riassunto dei consigli che intere generazioni di genitori hanno fornito ai propri figli, solo riadattati ai tempi moderni. Si dice – e ritengo fermamente sia così – che l'anello debole della catena informatica e telematica sia l'uomo. Le macchine non sbagliano, eseguono alla lettera ciò che viene loro ordinato... dall'uomo! A tutto questo va ad aggiungersi il fatto che, nel ricambio generazionale, è andato perduto qualcosa di importante. Coloro i quali ci hanno preceduto, avendo vissuto i periodi peggiori della storia dell'uomo, hanno cercato di non farci rivivere quei momenti. Purtroppo, è accaduto che i giovani hanno sì ricevuto quanto ai loro genitori era stato negato, ma non hanno ricevuto quanto i loro genitori avevano invece avuto. Parlo di valori e consigli utili a convivere, non sopravvivere, nella società. Con la smaterializzazione e deterritorializzazione dei documenti, dei beni e anche delle persone, l'informatica ha inesorabilmente dileguato anche la cognizione del mondo circostante, aggravando quanto appena detto. Dai numerosi studi effettuati con l'associazione World Wide Crime (www.worldwidecrime.it), è emerso un dato realmente allarmante: l'85% dei giovani utenti della rete, di età compresa tra i 15 e i 19 anni, ritiene internet una zona franca attraverso la quale poter far transitare ogni genere di file. Dai files tutelati dal diritto d'autore ai capi d'abbigliamento acquistati nei Paesi orientali e poi rivenduti in Italia, dalle minacce postate sulla bacheca del blog più in voga all'esibizione del proprio corpo in cambio di una ricarica telefonica. Il pensiero è: cosa faccio di male e tanto chi mi vede? I miei sono a letto e nella mia stanza faccio ciò che voglio, ci sono solo io e il mio PC. La nascita della nostra associazione si è ispirata proprio a questo. World Wide Web e World Wide Crime, non a caso. I criminali e le vittime si stanno uniformando a livello mondiale. Mentre anni addietro la notizia di un reato o la tecnica utilizzata venivano "importate" dopo alcuni mesi, se non addirittura anni, oggi le notizie ci appaiono in tempo reale ed attirano la curiosità degli utenti più giovani e dei malintenzionati. La conseguenza si legge nelle statistiche dei crimini informatici, che di anno in anno stanno lievitando. Il motivo è questo: i malviventi old style investono nell'innovazione, gli utenti comuni, non ritenendo illecita la condotta posta in essere in digitale, sono sempre più spinti a prelevare, diffondere, acquistare e vendere, ignorando gli effetti delle proprie azioni. I governi tentano affannosamente di adeguarsi e lo fanno male e a macchia di leopardo. Nonostante i numerosi tentativi di uniformare le norme, di instaurare una maggior collaborazione tra le forze di polizia e di consentire indagini sempre più snelle, non riescono ad accordarsi. Forse perché impegnati in problemi di ben altra natura o forse perché neanche conoscono le potenzialità devastanti della rete. L'esempio più eclatante lo ha dato, come di consueto, l'Italia, quando ha ratificato la Convenzione sulla Criminalità informatica di Budapest del 2001 con legge del 2008! Per chiudere, vorrei riferire quanto accadutomi la scorsa settimana. Dinanzi ad un ATM per prelevare denaro, leggo: prelievo non disponibile. La medesima frase era riportata anche da altre postazioni. Decido di recarmi ugualmente in un ipermercato onde poter pagare direttamente con carta. Tuttavia, la commessa di turno mi conferma l'assenza di linea nell'apparato e, quindi, la conseguente impossibilità di effettuare acquisti. Di sera, dopo aver ormai rinunciato a preparare qualcosa in casa, mi reco con amici in pizzeria e, sorpresa, anche qui non è possibile pagare con carta. Sono sicuro che a ciascuno di voi sarà balzata la pressione a mille almeno una volta nella vita, quando il cassiere di turno vi avrà detto che la vostra carta non è funzionante! Forse dovremmo cominciare a ripensare le nostre vite, abitudini, azioni e... i nostri politici, anche alla luce di quanto appena detto e di quanto si verifica quotidianamente in Italia e nel mondo, sotto lo sguardo indifferente di tutti. Indifferente perché occupato a capire come mai quella dannata carta non funziona...
Forse, all'interno del portafogli, si sarà smagnetizzata?

Gabriele Marra
Professore Associato di Diritto Penale Università di Urbino "Carlo Bo"

Una linea sottile

La politica ha incluso il contrasto alla criminalità informatica nell'agenda delle sue priorità. Gli ordinamenti giuridici nazionali hanno provveduto ad aggiornare il catalogo dei reati per colmare le lacune svelate dalla realtà tecnologica. Sul piano sovranazionale sono state intraprese iniziative di semplificazione dei rapporti tra le diverse giurisdizioni nazionali.

Sicurezza informatica, libertà della rete e diritto penale dopo il caso WikiLeaks.

1. L'utilizzo dei sistemi informatici per finalità illecite esprime una poliedrica offensività. Sul piano qualitativo amplia le modalità di aggressione ad interessi già ritenuti meritevoli di tutela (danneggiamento; danneggiamento informatico). Su quello quantitativo moltiplica le possibilità realizzative di violazioni ad interessi altrui proporzionalmente alle capacità di funzionamento delle risorse informatiche (phishing). Tale diffusività frustra le capacità di contrasto delle agenzie di controllo, apportando note di ulteriore offensività, come chiarito dalla Corte europea dei diritti dell'uomo: apparati di enforcement inefficaci minano la tenuta dei diritti fondamentali. Limitazioni indotte anche da un altro segno caratteristico della criminalità informatica, la transnazionalità che l'utilizzo illecito delle risorse informatiche mutua dalla rete di cui si avvale.

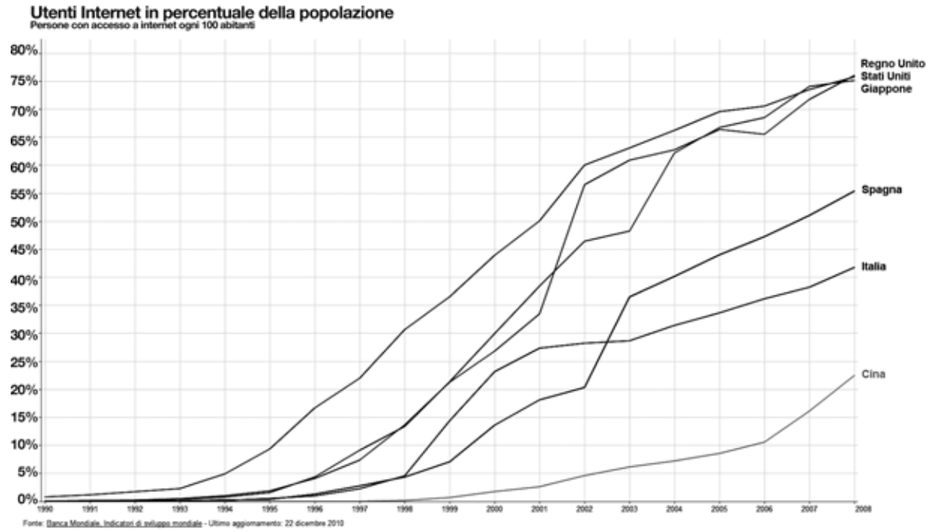
2. Su questi problemi si è lavorato molto. La politica, ad ogni livello, ha incluso il contrasto alla criminalità informatica nell'agenda delle sue priorità. Gli ordinamenti giuridici nazionali hanno provveduto ad aggiornare il catalogo dei reati per colmare le lacune svelate da una realtà tecnologica in tumultuoso progresso. Sul piano sovranazionale sono state invece intraprese iniziative di armonizzazione finalizzate ad indirizzare l'impegno nazionale senza trascurare le esigenze di semplificazione dei rapporti tra le diverse giurisdizioni nazionali e di adeguamento degli istituti processuali coinvolti. Spiccano, tra queste, la Convenzione del Consiglio d'Europa del 2001 e la Decisione quadro europea del 2005. Inputs che hanno innescato un circolo virtuoso, sollecitando ulteriori cambiamenti e significative convergenze nazionali sul piano della prevenzione e della repressione.

3. Molto resta però da fare. Non solo per gli inevitabili ritardi che l'apparato regolamentare sconta rispetto ai progressi giornalieri delle tecnologie informatiche. Il problema è più profondo, specie quando a venire in rilievo è l'uso illecito di Internet. Qualunque disciplina deve infatti fare i conti con la strutturale duplicità delle possibilità di utilizzo della rete. Risposte adeguate richiedono, quindi, capacità selettive che la legge, con i suoi caratteri di generalità ed astrattezza, non è sempre in grado di soddisfare. Solo un'inedita classe di strumenti disciplinari duttili e concreti può utilmente discriminare tra i costi (criminali) e i benefici (sociali) di Internet, garantendo così la collettività con un rete sicura, ma non imbrigliata da limitazioni illiberali.

4. Il caso WikiLeaks sintetizza al meglio quanto in precedenza osservato. Dimostra che non esistono significative lacune nell'arsenale di risorse penalistiche poste a presidio dell'integrità dei sistemi informatici: da questo punto di vista, l'intera vicenda può essere degradata a caso di ordinaria criminalità informatica. I soli dubbi che affliggono l'interprete riguardano le situazioni in cui WikiLeaks ha recitato il ruolo passivo di content provider di informazioni da altri acquisite, assumendo formalmente la responsabilità per l'avvenuta intrusione captativa al dichiarato scopo di proteggere le proprie fonti. Non è infatti scontato che tale rivendicazione possa superare il rigoroso vaglio imposto dai criteri liberali che sovrintendono all'operatività del diritto penale (art. 27/1 Cost.).
Attesta, al contempo, il basso livello di efficacia del reticolo sanzionatorio e preventivo messo in campo per dare corpo a quella che ai più appare, nonostante l'acribia impiegata, poco più di una chimera: la sicurezza informatica.

5. Insoluto è anche il quesito sulla giustificabilità, in nome di superiori interessi di trasparenza democratica, dell'operato diffusivo di WikiLeaks quale veicolo di 'lotta' ai segreti, di Stato e non. L'interrogativo svela infatti l'esistenza di un altro nodo problematico nei rapporti tra sicurezza informatica, libertà e diritto penale: l'assenza o la non chiara messa a fuoco dello statuto "costituzionale" della rete, delle libertà che consente e veicola e degli interessi collettivi che espone a rischio. L'istintiva preferenza a favore di soluzioni che risolvono l'intera vicenda in un caso di libertà di manifestazione del pensiero, esercitata attraverso la più grande arena democratica che l'umanità abbia mai conosciuto, deve fare i conti, oltre che con la disciplina nazionale in tema di segreto (artt. 256; 616 c.p. e 39 L.134/04), anche con le suggestioni originate dal principio di garanzia dell'integrità e riservatezza dei sistemi informativi. Concetto di recente espresso dalla Corte costituzionale tedesca, il cui perimetro operativo non risente della diversa natura (pubblica vs privata) dell'utilizzatore del sistema informatico, a fronte di una dimostrata pari capacità di intaccare l'integrità della rete da parte di soggetti pubblici ed agenti privati. In senso contrario, non varrebbe osservare che quel diritto, nella sua originaria declinazione, soddisfa un'esigenza di protezione della sfera privata rispetto ad invadenze pubbliche. Tacendo il fatto che l'utilizzo delle risorse informatiche per scopi pubblicistici non differisce sostanzialmente dall'utilizzo delle stesse per finalità comunicative tra privati, è vero, infatti, come dimostra la più recente proposta di direttiva europea in materia (2010), che l'interesse collettivo ad un'efficace prevenzione di tali forme di criminalità si giova anche della funzionalizzazione a fini pubblici di diritti individuali. È il caso della privacy. Il rafforzamento dell'effettività di tale diritto è qui considerato strumento di garanzia della reale integrità dei sistemi informatici. Condizione altresì essenziale per decretare l'illiceità di prassi intrusive e per attivare le risorse punitive del diritto penale, come dimostrano, a livello nazionale, la decisione del caso "Google-Vividown" e, prima, l'art. 169 D.lgs 196/03.

6. Il richiamo al principio di integrità dei sistemi informatici



consente di sviluppare ulteriori considerazioni in tema di sicurezza degli stessi. L'integrità non è, almeno in prima battuta, concetto di valore. È nozione dotata di un evidente spessore empirico, pregna di contenuti tecnologici. La sua garanzia è, d'altra parte, condizione essenziale per un'efficace protezione dei beni finali (patrimonio, onorabilità, sicurezza nazionale): chi desidera la tutela di questi ultimi non può quindi lesinare l'impegno nel predisporre tutti gli strumenti allo scopo necessari. L'esigenza di fissare l'insieme delle condizioni tecniche idonee a garantire il maggior grado possibile di invulnerabilità dei sistemi informatici si impone così all'attenzione dei policy makers. Come si legge in alcuni documenti comunitari, per "creare una società dell'informazione sicura" occorre migliorare "la sicurezza delle infrastrutture dell'informazione" (Decisione-quadro 2005). Trasformata in un interesse dotato di spiccata autonomia funzionale, la sicurezza reclama, nonostante la problematicità del connubio, l'intervento del diritto penale a garanzia della sua effettività. Segue una marcata anticipazione delle soglie di intervento (art.617-bis c.p.), la moltiplicazione delle fattispecie incriminatrici (artt.615-ter e ss. c.p.) e dei soggetti potenzialmente responsabili (art.24-bis Dlgs 231/01). Valorizzando l'innervatura empirica delle istanze sottese alla tratteggiata nozione di sicurezza, si prefigura una trama di protagonisti i cui nodi sono rappresentati da quanti controllano uno o più fattori di rischio. In questa prospettiva, utenti, intermediari e fornitori di servizi della più varia natura divengono partners necessari della pluralità di istituzioni pubbliche impegnate a salvaguardare la sicurezza dei sistemi informatici. La lettura della citata proposta di direttiva, con i suoi plurimi riferimenti all'indifferibile esigenza di implementare la cooperazione tra pubblico e privato, è, sul punto, assai istruttiva: conferma l'avvenuto consolidamento di un orizzonte '"costituzionale" che, relativizzata la preminenza imperativa dei pubblici poteri, si sviluppa secondo cadenze dettate da più duttili istanze cooperative. I tentativi intrapresi per disinnescare la mina WikiLeaks agendo sui fornitori dei servizi di connessione o sui gestori dei servizi necessari al suo sostentamento finanziario lasciano invece intuire le risorse preventive che i provider sono in grado di mettere efficacemente in campo, se richiesti od obbligati.

7. È uno scenario caratterizzato da un denso sistema di controlli ad alta intensità e senza lacune: pienamente giustificato in termini di efficacia preventiva, ma certamente bisognoso di un più profondo vaglio alla luce di tutti gli interessi in gioco. Il richiamo alla sicurezza non può infatti essere il Trojan Horse utilizzato per aggirare l'integrità dei sistemi di tutela dei diritti individuali in nome dell'onnivora razionalità di scopo a quella sottesa. Si ripropone, come ineludibile, l'esigenza di mettere ordine nel mosaico dei principi che sovrintendono agli sviluppi della disciplina di Internet. Una miglior comprensione dei contenuti e della portata dell'idea di neutralità può costituire un buon viatico in questa direzione. Fornisce una 'piattaforma' di dialogo tra diritto ed informatica. Il primo beneficia della spinta libertaria che deriva dall'originaria caratura tecnologica del principio in parola. L'architettura tecnologica della rete, invece, dei contenuti sociali propri di una sua declinazione in termini di ragionevolezza normativa. Operando sinergicamente, possono disinnescare il rischio che reticoli securitari superficiali soffochino le ragioni della libertà della rete, senza però disarmare i primi, nei limiti della necessità. Echi d'oltreoceano attestano che anche di ciò si continuerà a parlare dopo il caso WikiLeaks.

Nanni Bassetti
Consulente esperto di indagini informatiche; Caine Project Manager

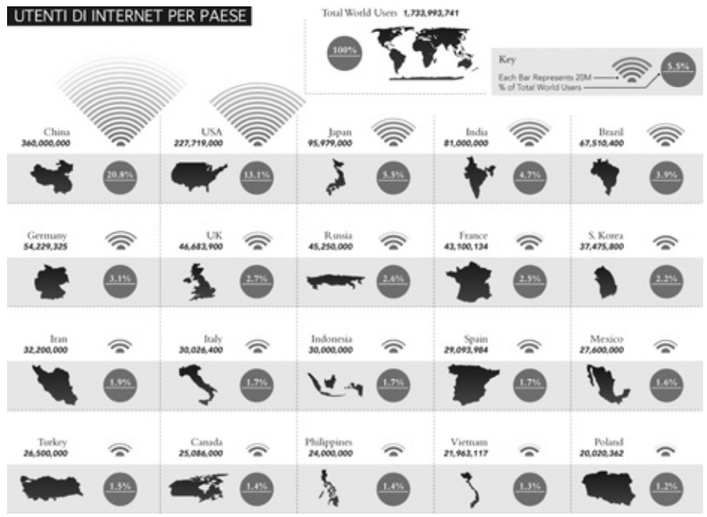
L'eterno gioco di "Guardie e Ladri"

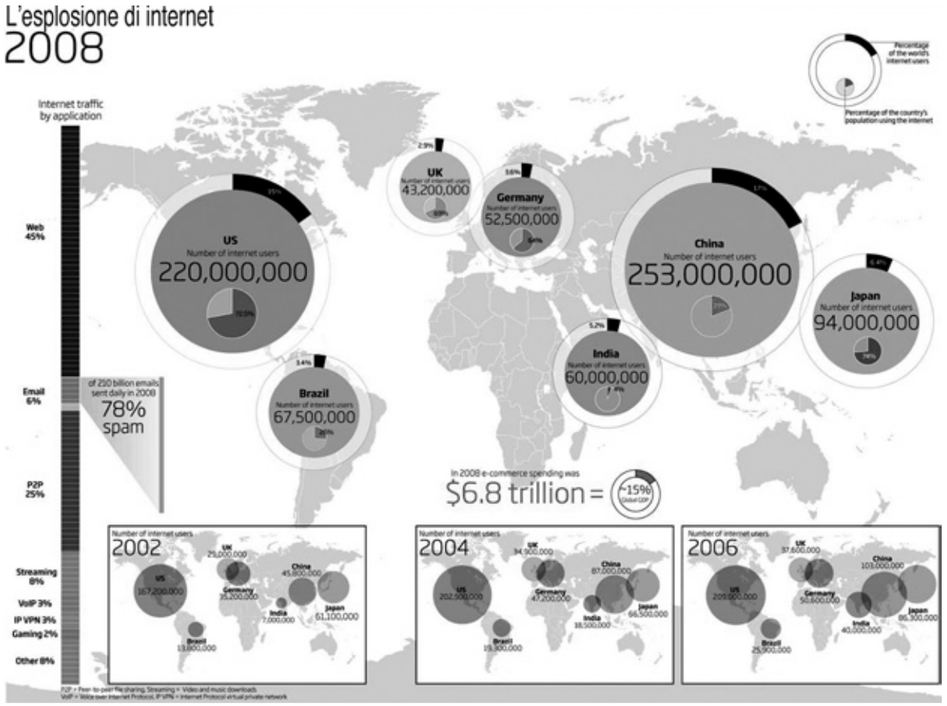
L'ignoranza di chi deve informare sulla sicurezza informatica e sulla computer forensics consente piena libertà d'azione ai criminali. La più grande falla non è quindi legata a super apparati di sicurezza, mega firewall o password e codici, ma all'ignoranza.

Informatica, ultima frontiera. Parafrasando l'inizio del famoso telefilm Star Trek, si potrebbe fissare lo stato temporale attuale. Ma applicare la parola "ultima" è un grosso errore. L'informatica non smette mai di evolversi e più si evolve più è in grado di generare nuove e più potenti applicazioni. A loro volta, queste serviranno a progettare altri programmi maggiormente sofisticati e performanti, i quali entreranno nelle nostre vite in modo sempre più profondo. Già oggi, gran parte della nostra esistenza ha a che fare con le applicazioni informatiche, le reti, le memorie digitali. Anni fa, quando la cultura informatica era meno diffusa, esisteva la barzelletta del cliente "ingenuotto", che chiedeva all'informatico se i virus dei computer potevano infettarlo, come se si trattasse di influenza. Allora faceva sorridere... ma oggi? Fortunatamente, non è ancora così. Possiamo però affermare che un'anomalia informatica assume oggi un impatto molto più significativo sulla vita di qualcuno rispetto a venti o anche solo dieci anni fa. Anche se ne siamo spesso inconsapevoli, le nostre vite sono regolate, monitorate e registrate nel mondo digitale in maniera massiccia. Come? Pensiamo ai social networks, a cui affidiamo notizie sulle nostre abitudini, i ricordi, i momenti felici e le delusioni, le foto ed i filmati, all'home banking, tramite il quale movimentiamo i nostri conti correnti, all'e-mail, il veicolo principale delle comunicazioni, alle pendrive ed agli hard disk, i contenitori di tutti i nostri vizi e virtù, a DVD, CD, memory cards, custodi delle immagini della nostra vita, ai telefonini, ormai mostri multimediali che raccolgono tutto ciò che è stato appena descritto. E non è finita qui, anzi. Disponiamo ovunque di memorie digitali: in tasca, pendrive da svariati gigabytes, altri gigabytes nei telefonini, orologi con memoria, navigatori satellitari che memorizzano i nostri spostamenti... Siamo, insomma, una massa ambulante di dati. Tutto questo ci porta a prevedere un'integrazione tra uomo e mondo digitale sempre più invasiva. Conosciamo, quindi, le nuove "guardie", gli investigatori informatici, ed i nuovi "ladri".

Chi è l'investigatore informatico?

Dal 2005 ho cominciato ad occuparmi di "computer forensics", informatica forense. Le condotte penalmente rilevanti attuate tramite i computers erano in costante aumento e si cominciava a capire che l'investigazione digitale non riguardava solamente il crimine informatico (cybercrime), ma anche la raccolta di informazioni utili alla soluzione di casi non strettamente legati all'informatica. Il mondo digitale consentiva di evincere se qualcuno aveva stilato un contratto fasullo o presentava documenti riferiti ad appalti truccati, evidenziava i tradimenti coniugali, gli alibi informatici, il riciclaggio di denaro. La corrispondenza virava sull'utilizzo dell'e-mail. L'errore commesso da alcuni inquirenti e da alcuni avvocati era quello di analizzare i dispositivi digitali solamente nel caso di reato di tipo esclusivamente informatico. Considerando, invece, la liason tra le nostre vite ed il mondo dei bit, il campo d'applicazione si espande a 360 gradi. In Italia, l'informatica forense è ancora in fase di assestamento e non esiste un protocollo che detti l'operatività in fase di repertazione, analisi e valutazione. Nel 2008 fondai una mailing list (CFI - Computer Forensics Italy) che oggi conta quasi 1000 membri ed è in costante aumento. In essa confluiscono diverse figure professionali, fra le quali forze dell'ordine e legali. Tutti desiderano crescere professionalmente e condividere le esperienze, con il fine di elaborare delle linee di condotta scientifiche, che preservino il lavoro investigativo da eventuali errori. Si, errori: nessuno si sognerebbe mai di raccogliere una pistola da una scena del crimine a mani nude; diversamente, quando si tratta di repertare materiale informatico/digitale, l'ignoranza conduce spesso a commettere errori che compromettono la futura fonte di prova, come accendere un computer spento, operazione che altera le timelines, o peggio. Come detto, l'Italia non possiede un protocollo specifico, ma il metodo scientifico risulta sempre il sistema migliore per garantire l'integrità





e l'inalterabilità dei dati, nonché la tracciabilità dei passaggi tecnici. Non tutti sanno che, allo stato attuale, le distribuzioni Gnu/Linux ad hoc per le indagini informatiche gratuite più usate dalla polizia e dai consulenti di tutto il mondo sono italiane ed una di quelle è CAINE, gestita dallo scrivente. Mai sentita? Ecco la prova che un settore così delicato è ancora completamente ignorato dai media ed è spesso inquinato da "tuttologi" che hanno il solo pregio di avere le conoscenze giuste, ma che non possono definirsi esperti della materia.

Chi sono i "ladri"?

L'ignoranza di chi deve informare sulla sicurezza informatica e sulla computer forensics consente piena libertà d'azione ai criminali. La più grande falla non è quindi legata a super apparati di sicurezza, mega firewall o password e codici, ma all'ignoranza. Procediamo per gradi. "La forza di una catena si misura dalla forza del suo anello più debole". Chi sarà mai l'anello più debole? Facile, l'uomo! L'uomo è ingannabile, ricattabile, soggetto a debolezze, sentimenti contrastanti. Insomma, una bomba ad orologeria, nitroglicerina da trattare con cautela. L'uomo è tutto ciò che non si può controllare al 100%. Spesso si pensa alla sicurezza informatica puntando tutto sulla tecnologia e sulle politiche aziendali. Giustissimo, ma se un dipendente vuole divulgare un'informazione, può farlo in tanti modi che non coinvolgono la tecnologia. Può copiare dei dati su un "pizzino" e nasconderlo, può imparare a memoria dei numeri o, più semplicemente, può sfruttare le sue amicizie o persuadere altri a collaborare. Il caso WikiLeaks insegna. Julian Assange non si è comportato da hacker o cracker, ma da semplice giornalista: ha offerto l'opportunità a chiunque di "uplodare" (inviare dal sito) dei documenti senza tracciarne l'indirizzo IP (il numerino che identifica il computer sulla rete). Ad esempio, un ufficiale dei Marines decide, per un motivo qualsiasi, di sfruttare i bachi nelle policies di sicurezza, chiedendo di poter inserire una chiavetta usb nel PC. Da lì riversa i dati che andrà poi a fornire a WikiLeaks. Ciò dimostra che i media non distinguono tra hacker, cracker, pirata informatico, cybercriminale ed un semplice giornalista (anche se con un passato da hacker). Fare i "cattivi" e proteggersi on-line è molto semplice: i sistemi delle "guardie" sono sempre in difetto rispetto ai metodi di data hiding (occultamento dei dati). Con un semplice proxy come TOR, un browser, i DNS non nazionali, la navigazione anonima o, meglio, da macchina virtuale o da sistema operativo live e, dulcis in fundo, connessi con la rete di qualcun altro, si scompare letteralmente dalla rete. Le tracce sono completamente inutilizzabili, come la crittografia dei dati: non è mai come nei film: decriptare un documento può richiedere decenni di elaborazione continua. Ma allora, come fanno i cyberpoliziotti? Semplice, usano armi informatiche d'indagine, ma sfruttano anche loro l'ignoranza, l'ingenuità, la pigrizia ed altre amenità umane. Spesso, il lavoro di ricerca delle prove digitali è facilitato proprio in questo modo. E cosa sfruttano i cybercriminali? Le stesse debolezze umane di cui sopra. Nel film "Totòtruffa '62", il grande comico vendeva ad un turista la fontana di Trevi. Oggi, i truffatori via e-mail ed altri sistemi vendono di tutto, ti fanno credere di aver vinto soldi, di essere la tua banca, ti convincono a cedere i tuoi dati con tecniche di ingegneria sociale. E l'immaginario collettivo demonizza il mezzo, la rete, i computers. Ma Totò non usava il computer... Per concludere, la miglior difesa è la cultura, la consapevolezza, lo spirito critico, l'attenzione ed una buona profilassi. Computer sanus in mente sana.

Luca Bovino
Responsabile Area Legale "Anti-Phishing Italia"

Frodi digitali

Il 4% degli Italiani è stato derubato della propria identità: ha, cioè, riscontrato l'indebito utilizzo dei propri dati personali, ad opera di terzi non autorizzati, al fine di compiere operazioni commerciali, o di altra natura, a sua completa insaputa e senza aver rilasciato alcun consenso.

L'utilizzo delle tecnologie informatiche e telematiche è caratterizzato, con sempre maggiore frequenza, dal verificarsi di frodi nei sistemi di pagamento elettronici. Secondo uno studio realizzato nel 2004 dalla Commissione Europea (COM, 2004, 679), già nell'anno 2000 la portata delle sole frodi concernenti le carte di pagamento era pari a 600 milioni di euro, circa lo 0,07% del fatturato del settore nel periodo considerato all'interno dell'Unione. Oggi il dato sembra ancor più preoccupante: secondo lo studio Internet Security Threat Report XV (riproposto in un recente resoconto della Polizia Postale Italiana), nel 2009, il valore dei dati sottratti attraverso furti informatici (identità personali, numeri di carte di credito e di conti correnti, ecc.) avrebbe raggiunto il trilione di dollari. Si stima l'esistenza di un vero e proprio mercato nero di questi dati, con un giro d'affari di circa 210 milioni di euro. In media, un "furto" di questo tipo costa alle imprese circa 5 milioni di euro, ed i tentativi di "effrazione" di tale natura sarebbero aumentati vertiginosamente negli ultimi anni, passando dal 22 al 60% delle minacce complessive tra il 2008 e il 2009. Secondo l'ultima relazione annuale della Banca d'Italia, pubblicata il 31/05/2010 con riferimento all'anno 2009, il rapporto tra transazioni fraudolente e totale delle operazioni con carte (di debito, di credito e prepagate) sarebbe assestato, in Italia, attorno allo 0,05%, a fronte del picco dello 0,07% del 2006. Nel 2009, il numero delle operazioni con strumenti alternativi al contante è stato pari a 4 miliardi. Ciò significa che 20.000 di queste operazioni erano fraudolente. Secondo il CRIF, invece, nel 2009 sarebbero stati riscontrati 25.000 casi di frodi con sistemi informatizzati di pagamento, con un aumento dell'11% rispetto al 2008, per un importo di 145 milioni (fonte Adiconsum, rapporto "Furto D'Identità"). Numerosi altri studi ritraggono un quadro non certo entusiasmante del fenomeno cybercriminale nel nostro Paese. Secondo un recente resoconto pubblicato dalla Polizia Postale e dall'azienda Symantec (che hanno, tra l'altro, stipulato un accordo di collaborazione per la prevenzione dei reati informatici) i reati informatici in Italia sarebbero costantemente in crescita, specialmente nel settore del commercio elettronico. In tale ambito sarebbero state denunciate alla Polizia Postale circa 800 persone (di cui 37 arrestate) soltanto nei primi mesi del 2010. Il Norton Cybercrime Human Impact Report 2010, pubblicato da Symantec, registra come il 69% degli Italiani sarebbe stato vittima di veri e propri attentati informatici, a fronte di una media mondiale del 65%. Ma di che tipo di "attacchi" si tratta? Secondo lo studio, il 51% dei nostri concittadini ospiterebbe, probabilmente a sua insaputa, virus ed altri codici fraudolenti all'interno del proprio computer. I nostri pc diventano degli inconsapevoli complici di attacchi sferrati dai cybercriminali mediante operazioni in rete con altri elaboratori che si trovino vittime della stessa "infezione". Si creano così veri e propri eserciti di computer robot (usualmente denominati Botnet) utilizzati per il compimento di attività telematiche delittuose come, ad esempio, l'accesso simultaneo a portali commerciali, azione che provoca il blocco degli stessi eseguito per finalità estorsive. Circa il 10% degli utenti è stato vittima di truffe on-line perpetrate mediante attacchi di phishing: cliccando su link presenti su e-mail ricevute nella propria posta elettronica che simulano comunicazioni istituzionali provenienti da portali bancari, gli utenti vengono indotti a fornire i dati d'accesso ai propri conti correnti o a rilasciare informazioni riservate. Il 4% degli Italiani si è visto derubato della propria identità: ha riscontrato l'indebito utilizzo dei propri dati personali ad opera di terzi non autorizzati, al fine di compiere operazioni commerciali, o di altra natura, a sua completa insaputa e senza aver rilasciato alcun consenso. Secondo un altro interessante studio realizzato da Adiconsum, il furto d'identità sarebbe misurabile economicamente ed avrebbe un'incidenza media di circa 500 euro, con picchi che, nel 10% dei casi, arriverebbe a superare quota mille euro. Ma quali sono le cause principali di tali fenomeni? Secondo lo studio, alla base del problema, più che la recrudescenza dei criminali, vi sarebbe proprio la disattenzione degli utenti, i quali, nel 22% dei casi (seppur in calo di 4 punti percentuali rispetto al 2009) rimangono vittima del furto di identità. Il 60% dei nostri concittadini, infatti, lascia memorizzate le proprie password sul pc o getta via estratti conto o altri documenti sensibili senza averli prima distrutti o resi illeggibili. Quali sono le principali insidie? Il furto d'identità deriva più frequentemente dalla sottrazione o dallo smarrimento dei documenti e dalla clonazione delle carte di credito (fenomeno definito skimming), mentre sarebbe abbastanza contenuto (14%) il numero di chi è caduto nella trappola del phishing. Nel 59,7% dei casi, la vittima di tali illeciti apprende di essere tale grazie alla consultazione dell'estratto conto bancario e dà così il via alle denunce, le quali riescono ad essere tanto più proficue quanto più tempestiva è la segnalazione. In rari casi, l'informazione proviene direttamente dagli inquirenti o dalla propria banca. Gli esperti invitano ad aumentare costantemente le difese della propria identità digitale per evitare di rimanere vittime di attacchi informatici. Ecco alcuni esempi:

- irrobustire le proprie password munendole anche di caratteri numerici e segni d'interpunzione;
- aggiornare sempre i propri antivirus;
- dotarsi di un firewall;
- eseguire costantemente l'aggiornamento dei propri programmi e dei propri sistemi operativi;
- evitare di navigare in rete (ed in generale di eseguire operazioni, ove possibile) dalla modalità "amministratore" e prediligere account "guest" o comunque modalità con privilegi limitati, al fine di evitare l'installazione automatica di software scaricati a propria insaputa durante la navigazione;
- prudenza nell'uso della carta di credito agli sportelli pubblici mediante un continuo controllo "manuale" dell'apparecchiatura nella quale viene strisciata (verificando accuratamente che non presenti laschi o altre sospette superfici traballanti). Ma, soprattutto, diffidenza verso comunicazioni bancarie recapitate via mail direttamente nella nostra casella di posta personale perché le banche veicolano la maggior parte delle comunicazioni elettroniche tramite e-mail create appositamente da loro stesse. Solo aumentando progressivamente le difese sarà possibile raggiungere un livello di sicurezza accettabile in grado di fronteggiare le numerose minacce presenti nel mondo digitale.

Massimo Condemi
Capo Dipartimento Ministero per le Pari Opportunità

Pedopornografia on-line

L'osservatorio acquisisce e monitora i dati e le informazioni relativi alle attività svolte da tutte le pubbliche amministrazioni nella prevenzione e nella repressione dell'abuso e dello sfruttamento sessuale dei minori. La legge prevede l'istituzione, presso tale organismo, di un'apposita banca dati per il monitoraggio del fenomeno.

Da cinque anni è attivo l'Osservatorio per il contrasto alla pedofilia ed alla pornografia minorile, istituito con legge 6 febbraio 2006, n. 38, recante "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet". Attualmente, l'Osservatorio opera presso il Dipartimento per le pari opportunità. La legge affida all'Osservatorio un ruolo di monitoraggio sull'abuso e sullo sfruttamento sessuale dei minori. In questi anni, tali condotte stanno assumendo un rilievo sempre maggiore: si stima che, in Europa, un bambino su cinque venga abusato, mentre in Italia, negli ultimi 3 anni, Telefono Azzurro ha rilevato più di 550 casi di abuso. Uno ogni due giorni. L'Osservatorio acquisisce e monitora i dati e le informazioni relativi alle attività svolte da tutte le pubbliche amministrazioni nella prevenzione e nella repressione dell'abuso e dello sfruttamento. La legge prevede l'istituzione, presso tale organismo, di un'apposita banca dati per il monitoraggio del fenomeno. Attualmente, essa è in fase di realizzazione. Raccoglierà informazioni che consentiranno di comprendere le caratteristiche dell'emergenza sotto il profilo sia qualitativo, sia quantitativo. I dati assunti rappresenteranno una preziosa base per individuare strategie ed ambiti di intervento per la prevenzione del fenomeno e per il recupero ed il sostegno delle vittime e dei condannati per questo tipo di reati. L'Osservatorio partecipa costantemente alle attività degli organismi europei ed internazionali competenti in materia di tutela dei minori nei fenomeni di abuso e sfruttamento. Il coinvolgimento nelle attività delle Nazioni Unite e dell'Unione Europea riflette il ruolo particolarmente rilevante che l'Osservatorio riveste in materia e la credibilità acquisita negli anni. In particolare, in ambito internazionale, l'Osservatorio collabora nell'elaborazione del rapporto periodico destinato al Comitato delle Nazioni Unite sui diritti dei minori relativo all'attuazione italiana della Convenzione ONU in materia di diritti del fanciullo e sull'implementazione del Protocollo Opzionale sulla vendita dei bambini, la prostituzione minorile e la pedopornografia. Nel rapporto, vengono illustrate le politiche nazionali di prevenzione e repressione dei reati di sfruttamento sessuale dei minori e vengono forniti i dati aggiornati sul fenomeno a livello nazionale. L'Osservatorio rappresenta inoltre l'Italia nel progetto del Consiglio d'Europa (COE) "Costruire un'Europa per e con i bambini", volto a garantire il riconoscimento ed il rispetto dei diritti dei minori nei 47 Stati membri del COE. Nell'ambito di tale progetto, l'"Osservatorio ha contribuito alla redazione di un rapporto sulle politiche nazionali di prevenzione della violenza nei confronti di bambini ed adolescenti. Ha inoltre partecipato attivamente alla stesura delle Linee Guida Europee per le strategie nazionali di protezione dei minori dalla violenza. Insieme a Norvegia, Portogallo e Romania, l'Italia, tramite l'Osservatorio, ha accettato di far parte del gruppo dei Paesi pilota che per primi hanno fornito un contributo concreto al progetto stesso. Di grande rilievo è stata poi la partecipazione dell'Osservatorio al negoziato per la redazione della Convenzione del Consiglio d'Europa sulla protezione dei minori nello sfruttamento e nell'abuso sessuale, aperta alla firma il 25 ottobre 2007 a Lanzarote. L'Osservatorio è risultato essenziale nell'organizzare in Italia, lo scorso 29-30 novembre, il lancio della campagna del Consiglio d'Europa contro la violenza sessuale a danno dei minori, fortemente sostenuta dal Ministro per le pari opportunità. Nelle numerose attività dell'Osservatorio, particolare attenzione è riservata al rapporto tra i minori e le nuove tecnologie e a come queste ultime, oltre a rappresentare strumenti di grande utilità, possano celare rischi per gli utenti più giovani e trasformarsi addirittura in pericolosi mezzi per perpetrare i crimini dell'abuso e dello sfruttamento. Per questa ragione, l'Osservatorio partecipa al Programma europeo Safer Internet, il piano d'intervento attuato dalla Commissione Europea in materia di nuovi media e tutela dei minori. Nell'ambito di tale progetto, ogni anno vengono organizzati il Safer Internet Day ed il Safer Internet Forum, a cui partecipano più di 50 Paesi in tutto il mondo. L'obiettivo è quello di promuovere un utilizzo sicuro e responsabile di internet e delle nuove tecnologie. Nell'ottava edizione del Safer Internet Day, celebrata lo scorso 8 febbraio, l'Osservatorio ha presentato sul sito internet www.sicurinrete.it un importante progetto al quale sta lavorando già da alcuni mesi: un portale internet rivolto principalmente alle famiglie, agli educatori e a tutti coloro che si occupano di tutela dei minori. Si tratta di un mezzo efficace il quale, utilizzando strumenti di comunicazione innovativi ed un linguaggio particolarmente vicino all'utente, offrirà informazioni complete sul fenomeno attraverso articoli, video interviste, un blog e molti altri contenuti aggiornati quotidianamente e viralizzati sui principali social network, come Twitter e Facebook. Il fine è quello di informare e sensibilizzare il pubblico sui molti temi che riguardano la violenza sui minori, dall'abuso sessuale alla violenza fisica e psicologica, dalla tratta alla prostituzione minorile. Ma la vera novità del portale è che, per la prima volta in un sito istituzionale, ci sarà la possibilità per gli utenti di partecipare attivamente, postando commenti sia nel blog, sia sui social network. Gli utenti potranno inoltre reperire nel portale le risposte alle domande più frequenti in tema di abuso e sfruttamento dei minori, avranno immediatamente a disposizione riferimenti utili in caso di necessità, potranno accedere alla più completa documentazione, nazionale ed europea. Il portale conterrà anche la possibilità di creare una comunità di pratica, attraverso una sezione dedicata ai professionisti i quali, a vario titolo, si occupano del fenomeno. Verranno raccolti esperienze e contributi e verranno condivise le "buone prassi", nate dall'esperienza nazionale ed internazionale nella tutela dei minori. Sono infine previste piattaforme di e-learning con corsi on-line disponibili 24 ore su 24, rivolti a pubblici specifici, dai genitori ai professionisti che lavorano nell'ambito della protezione dei minori. I corsi verteranno su temi di volta in volta diversi, come l'utilizzo dei social network o gli strumenti di sicurezza in rete. Attraverso il portale, l'Osservatorio intende inoltre aprire un proficuo e costante dialogo con i principali stakeholder europei ed internazionali sul tema della protezione dei minori dalla violenza, mettendo a disposizione contenuti informativi e formativi ed offrendo visibilità ad esperienze e buone prassi sulla materia realizzate dagli altri Paesi e dai principali organismi internazionali con cui intende collaborare. Tale azione consentirà al portale di trasformarsi in un punto di riferimento riconosciuto in ambito nazionale ed internazionale. La piattaforma rappresenterà dunque un ulteriore e fondamentale tassello da aggiungere alle numerose attività che l'Osservatorio pone in essere contro tutte le forme di abuso e sfruttamento di bambini ed adolescenti.

Marco Pingitore
Psicologo Criminologo Presidente AIPSI - Associazione Italiana di Psicoanalisi

Vittime e carnefici

Internet è una realtà virtuale in cui manca l'emotività. Se un utente scarica l'ultima versione del sistema operativo Microsoft o un film appena uscito nelle sale cinematografiche, ha la percezione di non commettere nulla di male. Siamo sicuri che è così?

Un decennio fa, commettere un crimine su internet significava soprattutto effettuare un download, tramite Napster, di un brano musicale in formato .mp3 con una velocità di 56 K. Si impiegavano circa 15 minuti per completare lo scarico. Oggi si impiegano circa 15 secondi per scaricare un intero album. Tempi che passano, tecnologia che avanza. Ricordo provocò grande clamore Napster ed il suo successivo passaggio alla versione commerciale. Gli utenti, spaesati, iniziarono a guardarsi intorno per cercare valide alternative, come, ad esempio, WinMx. Si basava sullo stesso principio di Napster, il peer-to-peer. Questo concetto ha fornito un imprinting fondamentale alla rete: scarichi se condividi. Dunque, chi accedeva ai programmi di file sharing per scaricare materiale senza condividere i propri film e la propria musica non riusciva nel suo intento. Alcuni utenti poco esperti condividevano l'intero hard disk del pc. Bastava inserire come termine di ricerca ".dbx" ed ecco che tra i risultati usciva la posta di Outlook Express dell'ignaro soggetto, oppure foto e filmini compromettenti. Personalmente, ricordo di aver scaricato fotografie di una festa di laurea di una ragazza residente a Pisa. Da questo episodio iniziai a comprendere che internet è un veicolo molto utile e pratico, ma può anche rappresentare uno strumento di controllo e di minaccia per la sicurezza personale. Non solo. Pensiamo alla diffusione delle caselle di posta elettronica: in principio, gli utenti (sempre quelli poco esperti e pratici), per pigrizia o inesperienza, erano soliti inserire una password molto debole, come il proprio nome o la data di nascita. Niente di più facile per i curiosi intenzionati a rovistare tra le e-mail delle ex fidanzate o degli amici in maniera del tutto indisturbata. Oggi, invece, gli strumenti di sicurezza a disposizione sono maggiori, come ad esempio la funzione "ultimo accesso" che indica il giorno e l'orario dell'ultima visita alla casella e la valutazione dell'efficacia della password in fase di creazione della casella e-mail. Tuttavia, sono ancora molti coloro i quali prestano poca attenzione a questo pericolo decidendo di utilizzare una password debole e facile da ricordare, magari uguale a quelle delle altre e-mail. Quasi tutti possediamo più di una casella di posta elettronica ed utilizziamo numerosi servizi (forum, social network, banca on-line), per cui, spesso, accade di effettuare "economia mnemonica" usando una sola password identica per tutto. Niente di più semplice. Ma, allo stesso tempo, niente di più pericoloso perché basta scoprire il codice segreto e si ha accesso a tutto ciò che riguarda virtualmente una persona. Spesso, il ragionamento che l'utente comune compie è "tanto a me non accade nulla". A livello psicologico, si attua una distorsione percettiva secondo la quale il soggetto sottovaluta il rischio per se stesso ed il danno a terzi. In termini di sicurezza personale, questo comportamento si trasforma in scarsa tutela dei propri dati e delle proprie informazioni su internet. La privacy diventa un concetto astratto, perdendo il valore che di solito le si attribuisce al di fuori del mondo virtuale. Nell'interazione con altri utenti, la distorsione percettiva permette che si verifichino fenomeni illegali, quali il download selvaggio e crackare siti, forum e caselle di posta elettronica. Internet è una realtà virtuale in cui manca l'emotività. Se un utente scarica l'ultima versione del sistema operativo Microsoft o un film appena uscito nelle sale cinematografiche, ha la percezione di non commettere nulla di male. Il file è accessibile con pochi click e il vantaggio, in termini economici – ma anche energetici – è decisamente consistente. Perché acquistare una copia di Office se la si può ottenere in pochi minuti? Perché acquistare un cd se in pochi istanti si riesce a scaricare l'intera discografia di un artista? Da un certo punto di vista, non fa una piega. Sarebbe quasi da invogliare e, infatti, spesso accade di essere additati come "poco furbi" se effettuiamo i nostri acquisti negli stores piuttosto che servirci dei canali peer-to-peer o torrent. Bisognerebbe riflettere su come sia possibile reperire un film su internet ancor prima della sua uscita nelle sale o scaricare un brano musicale ancor prima della sua incisione su cd. Sarebbe anche interessante comprendere come mai circolino nella rete files compressi contenenti interi album musicali con tanto di copertina scannerizzata pronta per essere stampata ed applicata sulla custodia del cd o interi libri in formato .pdf, come, ad esempio, il best seller "Uomini che odiano le donne" di Stieg Larsson. Oggi, la sicurezza è notevolmente aumentata. Ma ciò è avvenuto perché sono aumentati i reati informatici. È risaputo che un utente è al sicuro solo se ha il computer spento (forse!). Il caso WikiLeaks ha svegliato le coscienze di tanti, portando alla ribalta il concetto di sicurezza informatica e l'intera vicenda ha messo in mostra vulnerabilità e criticità di tanti Stati, fornendo solo un assaggio di ciò che potrebbe accadere in una guerra mondiale virtuale. Nel momento in cui ci colleghiamo ad internet, entriamo in un mondo in cui possiamo diventare vittime o carnefici. Alcuni esempi inquietanti del primo caso: quanti di noi si sono mai connessi ad una rete wi-fi libera, magari quella del vicino di casa? E quanti pensano che quella linea sia stata lasciata volutamente aperta per captare i dati scambiati dal nostro pc? Quante volte chiediamo consiglio nelle comunità virtuali per ricevere informazioni su un acquisto di un oggetto come un telefonino o una fotocamera? E quanti sono a conoscenza del pericolo che i suggerimenti ricevuti siano pilotati da "falsi" utenti esperti che in realtà altro non sono se non persone pagate da alcune aziende che producono quel telefonino o quella telecamera? È il fenomeno dell'"undercover marketing", quasi del tutto sconosciuto. Quanti sanno che il nostro pc potrebbe essere "posseduto"? Si chiamano computer zombie quei pc controllati da terzi senza che il proprietario ne sia consapevole. Gli hacker/cracker commettono reati attraverso il pc infetto facendo ricadere le responsabilità (ovviamente) sull'ignaro proprietario. E che dire delle vittime di stalking e di cyber-bullying? Se un utente desidera, invece, diventare carnefice, può spaziare in una vasta gamma di reati: diffamazione, truffa su eBay, vendita di organi umani, spionaggio industriale, violazione della privacy, pedopornografia. Quest'ultimo fenomeno è molto diffuso sul web e lo sarà

sempre di più con il futuro “cloud computing” attraverso cui utilizzeremo servizi e software da remoto: non avremo più computer con programmi installati, ma ci collegheremo ad un sito per disporre di Office, e-mail, Contatti, Rubrica, Photoshop, Antivirus, ecc. Tutto ciò semplificherà l'uso degli strumenti, ma aumenterà notevolmente il pericolo di essere intercettati e controllati. Un esempio di “cloud computing” sarà il nuovo sistema operativo di Google, mentre Skype, attualmente, rappresenta una delle tecnologie preferite dalla criminalità organizzata grazie alla crittografia delle conversazioni. Tutti questi e problemi critici che il Diritto segue a fatica, anche perché il legislatore, attualmente, tende a sottovalutare (distorsione percettiva?) i problemi giuridici connessi all'utilizzo di internet. Poniamo solo alcuni quesiti, forse in parte provocatori, ma contenenti problematiche evidenti: se si inserisce come parola chiave “lolita” in un motore di ricerca, uscirà qualche risultato che condurrà ad un sito pedopornografico. Il motore di ricerca ha svolto egregiamente il suo lavoro ed apparentemente non compie alcun reato. Sta solo rispondendo ad una domanda: dove posso reperire materiale pedofilo? Poniamo che un utente voglia inserire i medesimi links illegali nel proprio blog. Sicuramente, riceverebbe, dopo qualche giorno, una visita a domicilio della Polizia, alle 5 del mattino. Due pesi e due misure. Altra provocazione: diffamo una persona su Facebook con un account che possiede 10 amici. Da un punto di vista normativo, sarebbe più grave - in termini di quantificazione del danno subito - se quell'account possedesse 4000 amici? Ultima provocazione: carico un filmato protetto da copyright su YouTube. Successivamente, lo condivido su Facebook nella bacheca di un mio amico. Quanti e quali sono i responsabili? Ambiguità che favoriscono l'idea che la rete sia una zona franca in cui tutto è possibile. Tanto, quando si spegne il computer, il mondo virtuale non esiste più. Apparentemente, non si osservano/subiscono le conseguenze immediate. Come per le frodi. È percettivamente diverso rubare un dvd in un negozio piuttosto che truffare un utente su internet, così come è vissuto in modo emotivamente differente se in un concorso pubblico una persona si spaccia per un'altra piuttosto che rubare l'identità di qualcuno on-line, ad esempio su Facebook. Internet sostituirà la vecchia (attuale) concezione della tv ed il futuro sarà sempre più on-line. Basti pensare agli smartphone di ultimissima generazione, tramite i quali si può anche pagare il conto al ristorante. La privacy assumerà sempre più un significato aleatorio, le case disco-cinematografiche dovranno una volta per tutte fare i conti con il fenomeno del download facile, il legislatore dovrà necessariamente svegliarsi, aggiornando e rivedendo qualche legge obsoleta o mal fatta e crearne di nuove. Gli utenti dovranno invece muoversi in un campo virtuale minato e sempre più pericoloso. Ma, allo stesso tempo, suggestivo e ricco di risorse. Il fascino del paradosso.

Un fenomeno dell’era moderna

L’internet meme

Il termine "internet meme" si riferisce ad uno slogan o ad un concetto che si diffonde rapidamente attraverso internet, e-mail, blog, forum, imageboard, social network e instant messaging. Si comporta come un virus: funge da unità di trasporto culturale di simboli, idee o pratiche, che possono essere trasmesse da una mente all'altra attraverso la scrittura, le parole, i gesti, i rituali o altri fenomeni imitabili. Quando le persone vedono un meme, non importa quanto sciocco sia, lo trovano divertente per una qualsiasi ragione e lo fanno conoscere ai propri amici: ben presto, grazie alla velocità con cui le informazioni si diffondono on-line, milioni di persone ne vengono a conoscenza. L'assenza di confini fisici nella rete tende a favorire la rapida diffusione di idee e novità, specialmente se queste possiedono contenuti umoristici o bizzarri. Un internet meme può evolversi e diffondersi con estrema rapidità, raggiungendo, a volte, popolarità a livello mondiale per poi svanire in pochi giorni. 4chan è un sito di imageboard, utilizzato quindi principalmente per la pubblicazione di immagini e per la discussione di manga e anime giapponesi, i cui utenti sono responsabili di aver fatto nascere numerosi fenomeni di internet come lolcat, Rickrolling, Pedobear e molti altri. Il Rickrolling è un fenomeno che riguarda il video musicale della canzone del 1987 "Never gonna give you up", interpretata da Rick Astley. Il fenomeno si basa su un meccanismo "ad esca": un utente internet pubblica su un sito un link aggiungendo una descrizione particolarmente accattivante. Il collegamento rimanda però al video della canzone di Astley. In questo caso, si dice che il lettore ha subito un "rickroll". Con l'aumento del fenomeno, ad oggi, il video di Rickrolling più cliccato ha avuto più di 40 milioni di visite. Un altro fenomeno di recente successo in internet è “Forever Alone”. Si tratta di un fumetto reso popolare sempre da 4chan, che ha lo scopo di descrivere l'inadeguatezza sociale delle persone che passano troppo tempo su internet. Il meme “Forever Alone” ha iniziato a frequentare tutti gli abituali siti meme, come Tumblr, 4chan e FunnyJunk, diventando la carta di autocommiserazione di tutti quegli adolescenti che postano commenti patetici su Internet, ridicolizzandoli. Il web ha accorciato le distanze e aumentato drasticamente le probabilità di trasformare un’apparizione in un caso cliccato a ripetizione, fino ad eleggerlo ad icona degli anni 2000. Nato per diffondere video musicali e per promuovere prodotti commerciali, YouTube è diventato, col tempo, anche una vetrina per gli utenti “privati”, che lo utilizzano come uno dei principali mezzi per la self-promotion. Uno dei volti più noti e cliccati è quello di Laura Scimone, palermitana di 21 anni che si dilettava nel ballo e nel canto di fronte alla telecamera, per poi sparire nel momento in cui il suo personaggio stava diventando un vero e proprio tormentone del web. Nel 2009, è diventata, in poco tempo, un fenomeno sociale, citata da radio e televisione. Al suo posto è arrivata GemmaDelSud, ballerina, cantante, opinionista, che è diventata una vera e propria star senza eguali, con oltre 200 video caricati e quasi 22 milioni di visualizzazioni totali. Diventare un internet meme può essere profittevole oppure disastroso, come nel caso di Ghyslain Raza, quindicenne canadese protagonista del meme “Star Wars Kid”. Ghyslain si videoregistrò per un progetto scolastico mentre imitava le movenze dei cavalieri Jedi di Star Wars, ma al posto della spada laser brandiva una mazza da golf. La registrazione fu trovata da un compagno di scuola che la diffuse fra gli studenti e fu infine pubblicata su Internet, diventando in poco tempo uno dei video più condivisi della rete, con oltre 900 milioni di visualizzazioni. Ghyslain dovette lasciare la scuola per lo stress e ricorrere alle cure di uno psicologo, mentre i genitori fecero causa alle famiglie dei compagni che avevano caricato il filmato su Youtube. Un meme può essere invece profittevole, come nel caso in cui professionisti di pubbliche relazioni, pubblicità e marketing lo utilizzino come forma di marketing per creare “buzz”, l'insieme di operazioni non convenzionali volte ad aumentare il numero ed il volume delle conversazioni riguardanti un prodotto o un servizio e, conseguentemente, ad accrescere la notorietà e la buona reputazione di una marca. Gli internet meme vengono utilizzati anche per creare interesse in film che altrimenti non godrebbero di recensioni positive tra i critici. Il film del 2006 Snakes on a plane è stato molto pubblicizzato con questo metodo. Inoltre, anche gli attivisti politici hanno spesso usato gli internet meme per modulare l'opinione. Il successo di un meme dipende da fattori diversi, quali persuasione, accettazione, moda, pressione del gruppo, intensità del messaggio. Se prendiamo, per esempio, un gene, il suo successo e la sua diffusione sono legati alla sua utilità nella sopravvivenza dell'organismo che lo accoglie. Possiamo quindi definire il meme culturale analogo al gene biologico? A quanto pare, si, dal momento che entrambi sfruttano la mimesi replicativa, ovvero si propagano, si diffondono e si replicano attraverso l'imitazione. Ciò significa che l'internet meme è destinato a non essere un fenomeno passeggero? Che l'umanità non potrà farne a meno? Se la risposta è affermativa, e potremo saperlo solo in futuro, qualcuno, in qualche modo, dovrà spiegare il fenomeno a Charles Darwin!

Sara Crisnaro
Dottoressa in LISAO Giapponese

Fabio Ghioni
Fondatore di Hacker Republic. Esperto in sicurezza e tecnologie non convenzionali, consulente strategico per diversi organismi governativi e internazionali

La cyber guerra

Come i virus naturali, anche il virus informatico Stuxnet elimina difficilmente proprio tutti i suoi bersagli. Pensare di utilizzarlo per colpire solo l'Iran è sbagliato, perché il rischio che si rivolti contro è altissimo.

Non c'è nulla di più insidioso ed ignoto, oggi, della guerra cibernetica. Mentre la situazione socioeconomica si fa sempre più critica, la minaccia di attacchi informatici si intensifica e diventa sempre più concreta e meno virtuale. Dietro ad ogni attacco rimane sempre un'ombra asimmetrica e la perenne incertezza sul volto dell'autore. Certo, esistono comunità di hacker che combattono da sempre contro l'establishment e si fanno sentire con azioni clamorose: il recente caso WikiLeaks ha suscitato l'appoggio del gruppo di attivisti celato dietro il nome Anonymous. Ma la vera novità di questi ultimi anni è che i governi stessi si sono dotati di cybereserciti. Con ogni probabilità, rientrano in quest'ultimo caso gli attacchi DoS che paralizzarono i sistemi informatici dell'Estonia nel 2007 (proprio dopo che dalla capitale Tallin fu rimosso un monumento ai caduti sovietici durante l'invasione nazista), quelli dell'Azerbaijan e della Georgia nel 2008 (in corrispondenza dell'invasione russa) e le intrusioni degli hacker cinesi contro Google scoperte proprio un anno fa. Ancora, il virus Stuxnet, che ha messo in seria difficoltà il programma nucleare iraniano. In ogni caso, di fronte all'evidenza del danno subito, i veri mandanti rimangono nell'ombra. E, spesso, anche gli esecutori materiali. È una guerra 'sporca', sempre sul punto di ritorcersi contro i suoi stessi autori. Bisogna infatti ricordare che l'hacker è per definizione una figura ribelle e difficile da ricondurre ad un ordine prestabilito: anche se accetta di essere stipendiato dal sistema, lo fa solo per studiare i segreti del suo 'nemico'. Con questi segreti preziosissimi, disporrà di tutte le chiavi d’accesso alle vulnerabilità della tecnologia venduta al pubblico e delle infrastrutture vitali di una Nazione. Gli hacker sono autogestiti, agiscono per se stessi, per un eventuale uso futuro. Poi, se ciò coincide con gli obiettivi di un Paese o di una grossa compagnia, possono anche mettersi a disposizione. Insomma, gli stessi autori di attacchi condotti per conto di governi potrebbero, poi, con gli stessi strumenti e le stesse conoscenze acquisite, celarsi dietro attacchi terroristici. D'altro canto, il caso Stuxnet ha dimostrato che la guerra informatica non è più limitata al furto di informazioni: tramite un virus si può bloccare o far saltare in aria una centrale nucleare, oppure far partire un missile. A questo riguardo, è bene ricordare due episodi molto recenti: lo scorso 23 ottobre, per 45 minuti, gli specialisti della base di Warren (Wyoming) hanno perso le comunicazioni con 50 missili nucleari intercontinentali ospitati nei silos sotterranei; l'8 novembre, al largo della costa della California Meridionale, è stata avvistata la scia di un missile. Malgrado il Dipartimento della Difesa abbia chiamato in causa l'illusione ottica, la spiegazione non ha convinto molti esperti, tra i quali l’ex vice segretario alla Difesa Robert Ellsworth ed il generale in pensione Tom Mclnereney, il quale, a Fox News, ha dichiarato che si trattava di un missile lanciato da un sottomarino. Naturalmente, stiamo ragionando solo su ipotesi. Ma è un dato di fatto che un virus informatico sarebbe perfettamente in grado di spiegare entrambi gli episodi. E siccome operazioni di questo tipo non possono essere opera di hacker dilettanti, si può supporre che la responsabilità sia di una grande organizzazione o di uno Stato. Del resto, negli ultimi anni, i rapporti di intelligence sulle intrusioni nei sistemi informatici del Pentagono non si contano più. E gli indizi puntano tutti verso la Cina. Comunque sia, condurre azioni di guerra attraverso virus è un'arma a doppio taglio per gli stessi Stati: i malware possono essere poi rivenduti sul mercato nero e finire a disposizione di gruppi terroristici. È quello che potrebbe essere già successo – lo dicono rapporti di intelligence - proprio con Stuxnet, che per la sua complessità e la sua sofisticatezza è stato definito 'il miglior malware di ogni tempo'. Stuxnet è uno vero strumento di guerra, un’arma di nuova generazione. Ma come i virus naturali, è improbabile elimini proprio tutti i suoi bersagli. Pensare di utilizzarlo per colpire solo l'Iran è sbagliato, perché il rischio che si rivolti contro è altissimo. Quante Nazioni usano gli stessi sistemi Siemens colpiti dal virus per i loro sistemi critici? I Paesi più industrializzati sono ancora più a rischio dell'Iran, che dipende da quei sistemi solo per il 5%. Noi, invece, siamo completamente legati ad essi, inclusi i trasporti. Ora, quindi, che il confine tra guerra e guerriglia si confonde, probabilmente non sapremo da chi arriverà il grande attacco. Sappiamo però che arriverà, è pronto. E forse, conoscerne l'autore diverrà un dettaglio superfluo. Negli ultimi anni, numerosi rapporti di intelligence hanno evidenziato che gli hacker - russi, cinesi, iraniani, o cani sciolti - hanno mappato dettagliatamente le infrastrutture vitali degli Stati Uniti e dell'Europa, dalle reti elettriche a quelle idriche, dal sistema fognario alle telecomunicazioni. Tutto ciò che è connesso ad una rete ed ha un indirizzo IP è stato disseminato di virus pronti ad esplodere non appena giunga il comando. Nel caso di un conflitto, o semplicemente nel momento in cui uno dei Paesi mandanti volesse mettere in ginocchio l’Occidente, non dovrebbe far altro che risvegliare gli zombie. Proprio per l'accumularsi di queste minacce, il danno maggiore potrebbe verificarsi anche nel caso in cui un attore come gli Stati Uniti decidesse di difendersi adottando misure drastiche. Obama ha già chiesto al Congresso la facoltà di “spegnere” internet, ovvero di far saltare la Rete con l'ipotesi “kill switch”. Il problema è che, se si preme l’interruttore, salta anche il 70% del business mondiale. Ma gli Stati Uniti – o chi per loro – potrebbero avere anche altri interessi per spegnere o militarizzare la rete, e qui occorre riflettere proprio sul fenomeno WikiLeaks. Possiamo credere che il sito di Assange sia davvero uno strumento di libertà, ma – visto il tenore delle ultime rivelazioni – abbiamo anche ragioni sufficienti per ritenere che WikiLeaks sia ormai uno strumento nelle mani del potere per far uscire "miratamente" informazioni riservate. In entrambi i casi, è molto probabile che chi tiene davvero le redini del gioco – e non è sicuramente Assange, almeno non più – abbia interesse a scatenare il caos. Vuoi per far saltare un ordine mondiale non più tollerato, vuoi per risolvere una crisi economica che non ha sbocchi alternativi ad un conflitto a livello mondiale. Crisi che in passato è sempre stata il prologo di un conflitto di vaste proporzioni, perché l’economia di guerra è un solvente che ricompone tutti gli equilibri. Invece di avere una nuova Sarajevo, con un incidente traumatico come un omicidio o un atto terroristico, la battaglia può cominciare con la diffusione di informazioni e generare gli stessi effetti. Un'altra faccia del conflitto cibernetico e un altro possibile sbocco dal virtuale al reale.

Fabio Pietrosanti

Hacker per passione dal 1995. Attivista per la privacy in rete del PWS (Progetto Winston Smith)
Gestore di nodo TOR di anonimato in rete. Imprenditore dedito alla protezione della cifratura delle telefonate cellulari

Siamo pronti al cambiamento?

In rete stanno nascendo sempre più "leak sites", i quali propongono soluzioni organizzative e tecnologie volte ad incoraggiare il "fenomeno del leaking". La diffusione di informazioni segrete, ma di interesse pubblico, è destinata a divenire una pratica innovativa di esercizio delle libertà civili e dei diritti individuali, secondo un percorso analogo a quello intrapreso dalla crittografia.

Nell'esprimere un giudizio sul tema "WikiLeaks", molti hanno considerato solo gli aspetti superficiali del fenomeno, senza comprendere l'"ecosistema" di pensieri filosofici e politici da cui proviene. Allo stesso modo, molti sono convinti che gli Stati Uniti siano contro WikiLeaks, benché gli USA stessi siano fra i principali promotori di iniziative "radicali" condivise dal pensiero WikiLeaks e dal suo ecosistema filosofico e politico. Senza pretesa di esaustività, elencheremo qui di seguito alcuni fra i principali elementi di supporto - diretto od indiretto - da parte degli USA ad un nuovo modo di concepire la Democrazia ed i diritti che la compongono, i medesimi di WikiLeaks.

Anonimato in rete

TOR è il principale strumento di comunicazione anonima in rete ed è alla base anche di WikiLeaks. Permette di garantire l'anonimato delle fonti di informazione. TOR è finanziato da dieci anni dalla Naval Research Laboratory della marina militare statunitense (che ha inventato il GPS) e dal DARPA (che ha inventato Internet). È il principale strumento di anonimato in rete che permette anche ai cittadini di Paesi che applicano mezzi di censura (Cina, Iran, Thailandia, Tunisia, Egitto, Arabia Saudita, Italia inclusa) di accedere liberamente ad internet senza filtri. Mentre in Italia siamo ancora orientati a contrastare l'anonimato, negli Stati Uniti "colpiti" da WikiLeaks, la Corte Suprema dichiarava già nel 1995, in merito alla libertà d'espressione, "Anonymity is a shield from the tyranny of the majority". Organizzazioni come TOR, sponsorizzate dai militari USA, combattono contro i sistemi di censura di Paesi quali Iran e Cina in una corsa agli "armamenti digitali" quotidiana, volta a garantire a tutti la libertà di espressione e l'accesso all'informazione.

Collaborazione in rete ed efficienza

WikiLeaks è basato sui medesimi principi organizzativi dei programmi di Government 2.0. Gli Stati Uniti sono i principali promotori del Govern-ment 2.0, un cambiamento generale e profondo nel modo di concepire la Democrazia, l'organizzazione dello Stato e la relazione con il cittadino, informata a principi di trasparenza, efficienza e collaborazione. Le linee strategiche dei programmi di Govern-ment 2.0 sono:

- Trasparenza, tramite l'apertura di gran parte dei database della pubblica amministrazione messi gratuitamente a disposizione per consultazione, manipolazione, analisi e riutilizzo;
- Partecipazione, coinvolgendo, tramite "crowd sourcing", tutti i cittadini nei processi decisionali ed operativi in cui questi possono contribuire, inclusa la definizione di quali dati rendere pubblici;
- Collaborazione, invitando la comunità civile a collaborare per lo sviluppo di programmi di e-govern-ment sulla base delle informazioni e dei database pubblici messi a disposizione.

Piani nazionali di Govern-ment 2.0 sono già una realtà anche in Inghilterra ed Australia. Nella UE, fra le priorità per il 2015, viene fissato l'obiettivo che "European Govern-ments will be recognized for being open, flexible and collaborative in their interaction with citizens". Considerato l'ancora ridotto livello di informatizzazione della pubblica amministrazione italiana, sarà un obiettivo difficile da raggiungere, soprattutto perché questi modelli di gestione contrastano in modo fenomenale forme corruttive. La collaborazione distribuita del Govern-ment 2.0 è nel DNA organizzativo di WikiLeaks e delle decine di iniziative simili che stanno nascendo nel mondo, come Openleaks, Globaleaks, Balkanleaks, ecc.

Trasparenza nelle informazioni dello Stato

Il motto di WikiLeaks è: "We Open Governments". Tutti i programmi di Government 2.0 sono basati sul concetto radicale di OpenData, la divulgazione di gran parte delle informazioni grezze e dei database della pubblica amministrazione ed il suo funzionamento interno a tutti i livelli. Lo Stato e tutte le sue agenzie centrali e locali mettono a disposizione i dati grezzi. La comunità civile li analizza, li migliora e li elabora sviluppando applicazioni utili per creare un valore aggiunto a favore del cittadino. Esempi di iniziative governative OpenData:

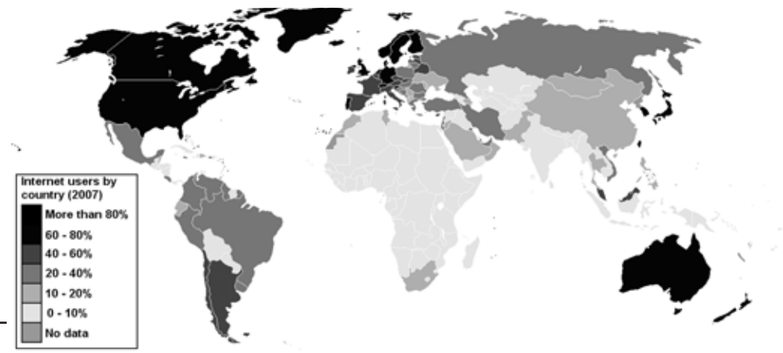
- US http://data.gov;
- UK http://data.gov.UK;
- AU http://data.austrialia.gov.au;
- World Bank Open Data initiative.

Lo stesso modello è stato implementato da WikiLeaks con il cablegate, in cui il rilascio dei dati grezzi clonati su oltre 2.000 siti di volontari nel mondo ha portato alla nascita di decine di siti per l'analisi distribuita, la ricerca, la valorizzazione e la correlazione del database dei cable diplomatici americani. Esattamente quello che accade con i database delle iniziative OpenData succitate, dove addirittura i governi promuovono concorsi per lo sviluppo di nuove idee e "Apps for Democracy", al fine di valorizzare le informazioni dello Stato rese pubbliche. Non parliamo di utopia annunciata da filosofi della società dell'informazione, ma di interventi concreti volti ad aumentare la competitività e la trasparenza della società in cui viviamo. E non stiamo nemmeno parlando del futuro, visto che alcuni di questi progetti sono già stati realizzati da grandi Democrazie. In ambito italiano, l'iniziativa di pubblicare le dichiarazioni dei redditi effettuata da Bersani può essere considerata un goffo, seppur filosoficamente apprezzabile, tentativo di guardare al Government 2.0. Ahinoi, lo sviluppo di linee strategiche di Government 2.0 richiede una profonda comprensione dei nuovi metodi di governance basati sulla collaborazione e non un semplice rilascio di dati pubblici "all'italiana". Microsoft è uno dei principali player di questo cambiamento con la sua Open Govern-ment Data Initiative finalizzata alla promozione dei nuovi modelli organizzativi pubblici basati sulla totale apertura dei database e sulla trasparenza governativa. In Germania, la leader dei programmi di innovazione di governo della Microsoft è la moglie di Daniel Berg, l'ex-fondatore di WikiLeaks assieme a Julian Assange, e ora suo concorrente con la nuova iniziativa Openleaks. Tutto ciò non ci dice niente sulle relazioni fra Government 2.0 ed il fenomeno WikiLeaks?

Un fenomeno destinato a cambiare tutte le Democrazie

WikiLeaks è solo una dimostrazione pratica che il percorso di apertura e trasparenza nell'azione di governo attraverso modelli di Government 2.0 e OpenData è inevitabile. Un percorso obbligato per ogni Democrazia. Se non sarà intrapreso autonomamente, verrà imposto dalla società civile con iniziative di questo tipo. È già accaduto con la liberalizzazione della crittografia alla fine degli anni '90, una forma di cambiamento originatasi nella società civile con azioni di forza pragmatiche tese ad eliminare i limiti di distribuzione ed esportazione dei sistemi crittografici forti. In rete stanno nascendo sempre più "leak sites", i quali propongono soluzioni organizzative e tecnologie volte ad incoraggiare il "fenomeno del leaking". La diffusione di informazioni segrete, ma di interesse pubblico, è destinata a divenire una pratica innovativa di esercizio delle libertà civili e dei diritti individuali, secondo un percorso analogo a quello intrapreso dalla crittografia. Anche chi scrive è uno dei proponenti del progetto www.GlobalLeaks.org, finalizzato a condurre il modello di leaking a livello regionale e locale. Il proposito è quello di amplificare l'azione mediatica anticorruttiva del leaking anche laddove i grandi media internazionali o nazionali non arrivino. In un'accezione così moderna di Democrazia, libertà d'espressione, trasparenza dell'operato dello Stato e collaborazione attiva con il cittadino, la domanda "chi controlla il controllore?" ha una risposta. È la cittadinanza stessa che partecipa in modo attivo all'analisi ed al funzionamento della macchina dello Stato, la rende più efficiente, trasparente e meno corrotta, in grado di competere su una scala planetaria in un mondo nel quale, ormai, chi rimane indietro rispetto alla capacità di apportare innovazioni organizzative sistemiche è destinato a perdere. E tutto ciò è dietro, davanti e a fianco del "fenomeno WikiLeaks", una forma di pensiero politico ed organizzativo profondamente orientato all'efficienza, alla condivisione, alla collaborazione ed alla trasparenza, destinato a cambiare il mondo e che vede proprio gli USA fra i primi attori.

Utenti di internet nel 2007



Il mondo hacker

Non è facile essere un hacker. Non è facile rischiare di essere giudicati come criminali, essere considerati quelli che inviano virus attraverso internet, quelli che entrano impunemente nei computer degli altri, rubano informazioni, distruggono sistemi. La gente questo pensa. Eppure... I veri hacker non propagano virus, non danneggiano siti internet, non interrompono le connessioni. Per essere hacker, bisogna innanzitutto essere curiosi. I principi fondanti dell'etica hacker comprendono creatività, ricerca della perfezione, sfida ai limiti, perseguimento del consenso attraverso il merito. Occorrono impegno e duro lavoro, ma anche un'intelligenza al di sopra della media e priva di condizionamenti. Nessuno può scegliere a priori di essere un hacker. Estremizzando il concetto, si capisce come esso non sia riferibile soltanto all'informatica. Chiunque si riconosca in questi valori, in qualsiasi campo operi, può sentirsi hacker. L'hacking esiste da sempre. Le differenze vanno ricercate con altre due categorie, i lamer ed i cracker: lamer è un dispregiativo, indica colui il quale si ritiene un grande esperto di informatica, ma che in realtà sfrutta solo quanto già fatto da altri. Cracker identifica invece il vero pirata informatico, chi possiede la stessa conoscenza tecnica e gli stessi strumenti degli hacker e li utilizza per violare la sicurezza di un sistema. La storia degli hacker potrebbe iniziare nel 1959, al Massachussets Institute of Technology (Mit), Boston. Alcuni studenti cominciarono a frequentare il primo corso di informatica rivolto allo studio dei linguaggi di programmazione, all'epoca elaborati su macchine IBM a schede perforate. Il desiderio di conoscenza di questi ragazzi non aveva limiti. La generazione successiva passò attraverso vari gruppi, spesso all'interno di facoltà universitarie prestigiose. Il gruppo degli Yippie, riconducibili ad un movimento anarchico, univa ad una forte lotta ai valori borghesi tradizionali e ad un rifiuto assoluto delle guerre la messa a punto di tecniche di pirateria informatica in grado di evitare gli addebiti delle chiamate telefoniche o di ricevere gratuitamente gas e corrente elettrica. Con la fine della guerra del Vietnam, il movimento di dissenso radicale degli Yippie si dissolse. Subito dopo, negli anni '60-'70, nacque il gruppo degli Homebrewers. Focalizzò la sua attività sullo studio delle caratteristiche dell'elaboratore per spingerne il funzionamento al massimo delle sue potenzialità. Va ricordato che il primo personal computer, l'Altair, trovò il suo mercato proprio fra gli hacker. Molti di essi acquistarono il kit per costruirselo da soli. Assemblare pazientemente quella macchina significava inserirsi nel mondo logico dei computer. Poco importava che si costruisse solo una scatola di luci lampeggianti con 256 byte di memoria. L'Homebrew computer club divenne il mezzo per scambiarsi informazioni e condividerle in maniera globale. Più importante era il segreto, più grande il piacere di rivelarlo. L'etica hacker insegna la libertà e la condivisione a qualunque livello, ma già allora cominciò a scontrarsi con uno dei temi più scottanti del mondo informatico: la proprietà dei programmi. Negli anni '80 comparve la terza generazione di hacker, quella dei Software superstar, i maghi dei giochi, gli artisti della programmazione. Si era realizzato il sogno hacker di un computer per la gente comune, ma era nato il problema di mantenere libero il flusso delle informazioni. Ormai i pc erano entrati nelle abitazioni, erano dotati di modem e, tramite le linee telefoniche, comunicavano tra loro. Si apriva l'era della telematica e nasceva il cyberspace, lo spazio virtuale nel quale chiunque possedeva gli strumenti e rispettava le regole poteva comunicare e socializzare a velocità mai sperimentate e senza barriere spaziali. Ma proprio nel raggiungimento di questo traguardo trae origine l'assalto ai sistemi informatici e telematici. Nasce la connotazione negativa del termine hacker, che da allora identifica chiunque utilizzi illecitamente le proprie capacità informatiche e si comporti da trasgressore digitale. Nella percezione comune, una vera forza del male. Circa vent'anni dopo, compare l'hacking italiano, contemporaneamente all'arrivo nelle case dei primi microcomputer (Commodore, Atari, ecc.). Ci si ritrovava di frequente negli sgabuzzini dei primi negozi di computer, si scambiavano giochi, ma si condividevano anche informazioni. I giovani "smanettoni" italiani ebbero le prime esperienze in rete attraverso i videotel della SIP, i quali misero a disposizione degli utenti, quale servizio aggiuntivo, una casella di posta elettronica che permetteva di scambiare breve corrispondenza. Si utilizzarono poi le connessioni alle BBS straniere e, quindi, i primi nodi Fidonet. Alcuni hacker diventarono gestori di un nodo, amministrarono una parte del cyberspazio, migliorarono i contatti, configurarono nuovi programmi. Molti però tendevano a non riconoscere le regole della policy che governava il funzionamento dei nodi, la sorveglianza dei contenuti, la responsabilità sui messaggi e sulle azioni degli utenti. Alcuni utenti dell'area Cyberpunk si staccarono e fondarono Cybernet. Qui origina la fondamentale devianza del movimento hacker, rappresentata dall'accesso abusivo ai sistemi informatici. Per tutti i veri hacker, le informazioni sono patrimonio dell'umanità, come ogni altra risorsa naturale. Servono a migliorare le condizioni di vita di tutti. L'informatica deve diffonderle rapidamente e capillarmente. Ma, in nome di questi nobilissimi ideali, è giustificabile l'intrusione nei sistemi informatici? Pensare che alcuni governi, certe istituzioni, le grandi imprese commerciali siano responsabili della manipolazione delle informazioni, può legittimare l'introduzione abusiva in tali sistemi allo scopo di liberalizzare i dati, anche solo come forma di protesta? L'etica hacker, anche nella più corretta buonafede, può diventare una discriminante per un comportamento socialmente più pericoloso di ciò che potrebbe sembrare?

Antonio Irlando
Dirigente medico Ass n°4

Luca Sileni
Avvocato, membro dell'associazione Wikimedia Italia e amministratore di Wikipedia

La cultura di Wikipedia

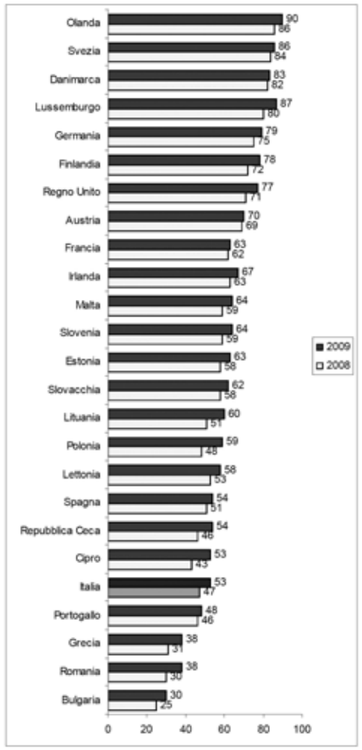
Wikipedia deve necessariamente possedere il requisito della libera modificabilità per raggiungere pienamente il proprio scopo. Ciò perché un'enciclopedia non è un'opera statica, ma è un'entità in continuo divenire, che si modifica senza soluzione di continuità e che necessita di aggiornamenti costanti.

La società moderna è ormai inesorabilmente permeata di tecnologia. Le interazioni fra real life e web life sono così strette da rendere a volte quasi inscindibile l'una rispetto all'altra. Ciò è vero soprattutto per coloro i quali hanno fatto del web la propria professione. Ma anche per quelli che, come me, hanno trovato in rete interessi, passioni e spunti di riflessione così forti da ripercuotersi inesorabilmente sulla vita reale. Oggi, i media si interessano più che mai al rapporto che lega l'uomo alla rete, ed in particolare a tutta una serie di fenomeni con la rete nati e sviluppatisi. Fenomeni quali social network, blog ed il cosiddetto web 2.0 interessano giornali, radio e tv, a volte per un'esaltazione del fenomeno, altre per una sua demonizzazione. Personalmente, sono convinto che nessuno strumento in sé sia negativo o positivo. È il suo utilizzo ad avere, eventualmente, connotazioni positive o negative. Come per altri fenomeni legati al web, anche quello della cultura libera ha pagato – e continua a pagare – un pesante scotto nei confronti dell'informazione generalista, quella della scarsa conoscenza del fenomeno da parte di chi ne scrive. Per comprendere meglio il punto saliente di questa riflessione, ritengo importante portare ad esempio la mia esperienza personale con Wikipedia e con il mondo del web 2.0 in generale. Wikipedia è un'enciclopedia on-line redatta da utenti volontari e non retribuiti i quali, in modo collaborativo, apportano il proprio contributo alla crescita del progetto mettendo a disposizione di tutti i fruitori le proprie conoscenze. Io sono approdato sulle pagine di Wikipedia nell'estate del 2005 (il progetto, in realtà, è nato nel gennaio del 2001) con delle modalità – ho scoperto poi – del tutto analoghe a quelle di molti altri miei futuri colleghi, tramite una normalissima ricerca sul web. Sono da sempre un grande appassionato di musica rock e metal e, spulciando le pagine di Wikipedia, mi resi immediatamente conto che alcune delle pagine riguardanti i miei beniamini erano scarne o, addirittura, del tutto inesistenti. A quel punto, notai che esisteva la possibilità di modificare i testi già presenti e quella di crearne di nuovi. Decisi così di aggiungere parte delle informazioni che non erano presenti in quelle pagine, contribuendo a rendere più completa l'enciclopedia. Rimasi letteralmente folgorato dallo spirito dell'iniziativa. In fin dei conti, si trattava di redigere un'enciclopedia in modo totalmente libero ed indipendente, e la cosa più affascinante era la possibilità di offrire il proprio sapere a favore di qualcun altro. Ognuno di noi possiede un suo bagaglio di conoscenze, esperienze, nozioni ed informazioni che può condividere con gli altri. Wikipedia non fa altro che creare un'immensa rete sociale, formata da milioni di piccole nozioni apportate da milioni di persone diverse, che formano – globalmente - un lavoro unitario e continuamente in divenire. Questa concezione appare a tratti realmente utopistica. Mi affascinava. E mi affascina tremendamente anche oggi. A mio avviso, il concetto di cultura libera risiede in due elementi principali ed imprescindibili: la libera fruizione e la libera diffusione. Qualcuno tende ad inserire fra questi elementi anche la possibilità di libera modificazione. Personalmente, non lo ritengo elemento essenziale, ma un mero quid pluris. Questo perché un'opera d'arte, per essere definita libera, deve essere soprattutto fruibile o, se vogliamo, "godibile" da chiunque e, allo stesso tempo, comunicabile – senza eccessive limitazioni – a soggetti terzi. Non è strettamente necessario che chiunque possa anche apportare delle modifiche. Wikipedia, invece, deve necessariamente possedere anche il requisito della libera modificabilità per raggiungere pienamente il suo scopo. Ciò perché un'enciclopedia non è un'opera statica, ma è un'entità in continuo divenire, che si modifica senza soluzione di continuità e che necessita di aggiornamenti costanti (elemento, questo, che ha evidenziato uno dei grandi limiti delle enciclopedie cartacee).

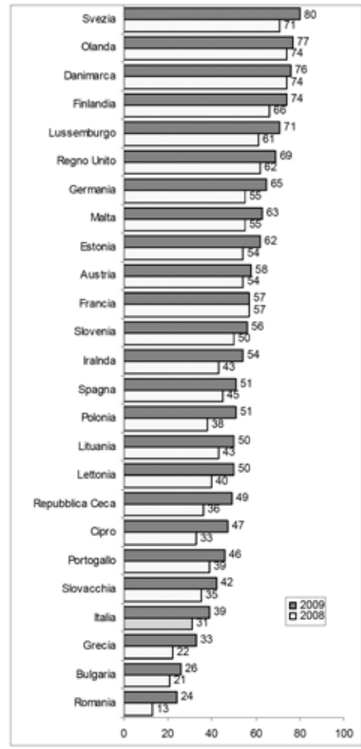
Un'opera d'arte, come un dipinto, un brano musicale o un'opera fotografica, non necessita in modo imprescindibile del requisito della modificabilità per essere definita libera. Basta che chiunque possa goderne in maniera libera, potendo poi condividerla con altri. Libero accesso e libera diffusione, quindi. Al fine di consentire un più agevole accesso ai contenuti liberi, ed al fine di garantire una maggiore chiarezza nei termini di utilizzo delle opere libere, si sono sviluppate – in tempi relativamente recenti – le cosiddette "licenze libere" o "licenze copyleft". Queste non sono altro che contratti con i quali l'artista (detentore di tutti i diritti sulla propria opera grazie alla legislazione nazionale ed internazionale sul copyright) concede all'utilizzatore finale tutta una serie di facoltà altrimenti precluse. Le licenze oggi maggiormente diffuse ed utilizzate sono le licenze creative commons, redatte – appunto – dall'associazione no-profit "Creative Commons" a partire dal 2002/2003. La fortuna di questi strumenti si deve soprattutto alla loro semplicità di applicazione e comprensione anche da parte di chi non ha dimestichezza con testi giuridici. Le licenze creative commons sono costituite da una struttura modulare: data una licenza base, l'autore può scegliere quali clausole ulteriori inserire nella licenza con cui intende rilasciare la propria opera. Ad ogni clausola corrisponde una maggiore ristrettezza nelle facoltà dell'utilizzatore finale. A titolo meramente esemplificativo, un autore può scegliere di rendere la propria opera liberamente fruibile da chiunque, ma non modificabile e non utilizzabile per finalità commerciali, utilizzando la licenza "Cc-by-nc-nd". Tale sigla identifica la licenza creative commons (Cc) che consente all'utilizzatore finale di divulgare liberamente l'opera a patto di indicare l'autore originale della stessa (by) e lo obbliga a non modificare l'opera (nd=no opere derivate) e a non sfruttarla commercialmente (nc=no sfruttamento commerciale). Sempre a titolo esemplificativo, Wikipedia è invece rilasciata con la licenza Cc-by-sa 3.0 (il 3.0 è semplicemente la versione della licenza) che, rispetto alla Cc-by-nc-nd dell'esempio precedente, non prevede l'obbligo di non modificare l'opera, né quello di non trarne profitto, ma aggiunge la clausola "Sa" chesta per share alike, ossia – molto semplicemente –, con tale licenza si concede all'utilizzatore finale ogni facoltà, compresa quella di modificare integralmente il testo dell'enciclopedia e, addirittura, quello di stamparla e venderla, ma si richiede l'indicazione obbligatoria degli autori originali ed il rilascio di ogni eventuale opera derivata sempre con la medesima licenza. Risulta quindi evidente come la grande forza di Wikipedia sia intimamente insita anche nella licenza che utilizza. Questo perché le normali enciclopedie cartacee non sarebbero oggi in grado di garantire lo stesso livello di crescita e divulgazione. A detta di molti, ciò in realtà non è un fatto del tutto negativo: per alcuni, infatti, la libera modificabilità dell'enciclopedia più famosa del web è - alla fine - anche il suo tallone d'Achille. Molti sostengono che un'enciclopedia cartacea sia in grado di offrire garanzie precluse a Wikipedia, quali autorevolezza dei redattori e controllo capillare dell'opera finale. A mio avviso, però, molte delle critiche portate a Wikipedia sono dovute soprattutto alla scarsa conoscenza dei meccanismi interni al progetto. Wikipedia, rispetto ad un'enciclopedia cartacea, offre un aggiornamento costante, la virtuale assenza di limiti di spazio e, soprattutto, la completa gratuità dell'opera, elementi che non possono certo essere sottovalutati. Al contempo, negli ultimi anni sono stati sviluppati diversi strumenti volti alla verifica delle informazioni inserite:

- il lavoro di vigilanza degli amministratori, i quali, benché non retribuiti, trascorrono buona parte del proprio tempo libero sulle pagine dell'enciclopedia per rimuovere violazioni di copyright, moderare le discussioni più accese e bloccare utenze vandaliche o problematiche;
- il lavoro dei volenterosi "patroller", i quali si occupano di controllare in tempo reale le singole modifiche apportate all'enciclopedia. Lavoro assolutamente prezioso, soprattutto contro i vandalismi più evidenti;
- strumenti di controllo successivo, come gli "osservati speciali", una pagina riepilogativa in cui ogni utente può inserire una serie di voci che vuole tenere sotto controllo. All'interno di tale pagina saranno riportate tutte le ultime modifiche effettuate negli ultimi giorni alle voci che si stanno monitorando;
- non vanno infine dimenticate le policy di base di Wikipedia, le quali richiedono sempre e comunque di citare la fonte delle informazioni inserite sulle pagine dell'enciclopedia. Ciò al fine di verificare agevolmente l'origine di quanto è riportato in una determinata voce biografica. È quindi sbagliato affermare che Wikipedia sia un progetto senza controllo e, di conseguenza, non affidabile. In ogni caso, abbiamo sempre affermato – e continueremo a farlo – che è consigliabile (nonché auspicabile) il ricorso a più fonti nella ricerca di notizie sul web. Questa regola non vale solo per Wikipedia, ma per qualunque fonte di informazione. Spesso, i giovani studenti approdano sulle pagine della nota enciclopedia on-line e prelevano "di peso" (il classico copia-incolla) tutto ciò che trovano, senza soffermarsi a leggere, ponderare e – soprattutto – capire ed approfondire quello che stanno copiando. La base di una buona ricerca è la varietà delle fonti bibliografiche, per cui, accanto ad un'analisi di una voce enciclopedica (questo vale per Wikipedia ma – a mio avviso – dovrebbe valere per tutte le enciclopedie, Treccani compresa) deve sempre esserci un approfondimento delle informazioni attraverso altri siti, testi, articoli ed altre fonti di informazione. Questo per permettere a chi legge di attingere ad una pluralità di nozioni e punti di vista differenti, che consentano di giungere ad una conoscenza personale di ciò che si sta ricercando. Concludendo, la mia esperienza personale mi ha portato più volte a riflettere sul fenomeno della cultura libera e su quello del web 2.0. Tali riflessioni mi hanno convinto che questi fenomeni sono semplicemente delle mere possibilità. Possibilità importanti, ma sta a noi saperle sfruttare ed utilizzare al meglio. Una cultura che viaggia libera dentro e fuori dal web potrebbe finalmente condurre ad una visione maggiormente etica del sapere. Una visione che tenga conto delle differenze sociali che – purtroppo – ancora oggi esistono e permeano la nostra società. Una visione che tali differenze potrebbe, in parte, abbattere. Una cultura che si estranei – anche parzialmente – da un sapere strutturato e costruito solo in virtù di finalità commerciali, potrebbe portare ad un concetto di conoscenza quale bene che non debba subire limitazioni in funzione di lingua, luogo di nascita, convinzioni ideologiche e possibilità economiche. È l'idea di una cultura che possa fluire libera attraverso un'immaginaria connessione fra miliardi di menti ed anime sparse in tutto il mondo.

Famiglie con almeno un componente tra i 16 e i 64 anni che possiedono un accesso ad Internet. Anni 2008 e 2009 *(per 100 famiglie con almeno un componente tra i 16 e i 64 anni)*



Famiglie con almeno un componente tra i 16 e i 64 anni che possiedono un accesso ad Internet da casa a banda larga. Anni 2008 e 2009 *(per 100 famiglie con almeno un componente tra i 16 e i 64 anni)*



"INTERNET: DALL'USO ALL'ABUSO"

@uxilia
Onlus per la tutela dei soggetti deboli

IL PROGETTO

Promuovere iniziative per prevenire forme di disagio minorile e giovanile significa realizzare interventi a sostegno dei soggetti in età evolutiva ed adolescenziale. La nostra esperienza nasce dall'analisi dei nuovi strumenti di comunicazione sociale, "internet e nuovi media", degli aspetti positivi e negativi che ogni grande innovazione si porta dietro e che si manifestano quando l'uso diventa abuso. Nuove forme di dipendenza si stanno facendo strada, in particolare, fra le fasce deboli della società ed in particolare tra i giovani, che sono i maggiori consumatori di nuove tecnologie. Attraverso interventi di formazione e sensibilizzazione mirati e di immediata applicabilità, intendiamo proporre ai giovani, ai loro familiari, agli insegnanti, percorsi di prevenzione del disagio, di partecipazione sociale e di integrazione giovanile.

A CHI SI RIVOLGE:

Giovani compresi tra i 14 e i 25 anni; insegnanti; genitori

OBIETTIVI:

Promuovere iniziative di prevenzione delle forme di disagio minorile e giovanile.
Sviluppare esperienze educative, di partecipazione sociale e di integrazione giovanile.
Sensibilizzare i giovani sui rischi delle nuove dipendenze.
Coinvolgere genitori ed insegnanti nella prevenzione e nel riconoscimento di possibili patologie da dipendenza.

REALIZZATO DA:

Auxilia Onlus

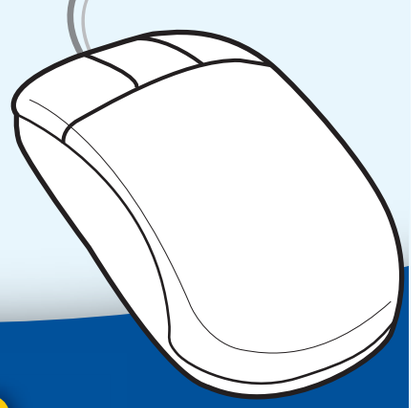
FINANZIATO DA:

Fondo dell'Osservatorio Nazionale per il Volontariato – Ministero del Lavoro, della Salute e delle Politiche Sociali

RISULTATI ATTESI

- *maggiore consapevolezza sull'uso e sull'abuso di internet da parte dei giovani;*
- *incentivare il ricorso alla rete per la ricerca di contenuti educativo-culturali;*
- *educare i giovani ad un uso proficuo, prudente e consapevole dei nuovi mezzi di comunicazione e socializzazione;*
- *partecipazione attiva dei giovani nelle associazioni di volontariato;*
- *maggiore coinvolgimento dei genitori sui temi affrontati;*
- *interazione tra docenti e familiari su eventuali anomalie del comportamento dei giovani.*

www.auxiliaitalia.it



Aiutaci ad Aiutare...

Iscriviti anche tu ad @uxilia onlus, editore di Social News

www.auxilia.fvg.it info@auxilia.fvg.it tel. 3476719909

La tessera d'iscrizione annuale ad @uxilia onlus come socio sostenitore costa solo 20 euro! Potrai contribuire anche tu ad aiutare i bambini italiani e quelli dei Paesi in via di sviluppo. L'iscrizione prevede:

1. la spedizione gratuita a domicilio ogni mese della rivista SocialNews;
2. la possibilità di richiedere via e-mail e di ricevere gratuitamente specifiche su argomenti medici, giuridici e psicologici da parte del comitato scientifico dell'associazione (avvocati, medici, psicologi);
3. iscrizione gratuita a corsi e convegni organizzati dall'associazione.

Bollettino postale
C/C 61925293

Bonifico bancario
IBAN: IT15H0760102 2000 0006 1925 293