

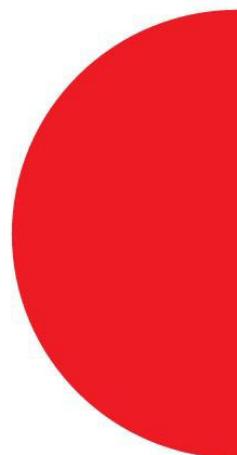
CORECOM
LAZIO

NICOLA DI STEFANO
FEDERICO GIANNONE

**MANUALE
SULLA
WEB** **REPU
TATI
ON**

**DALL'IDENTITA' DIGITALE
ALL'ECONOMIA
DELLA REPUTAZIONE**

**PREFAZIONE DEL COMMISSARIO AGCOM
ANTONIO PRETO**



INDICE

PREFAZIONE DEL COMMISSARIO AGCOM, DOTT. ANTONIO PRETO	3
<i>LA PERSONA IN RETE, CARDINE DELLA WEB REPUTATION</i>	
CAPITOLO I: LA STORIA DI INTERNET E LA CRESCITA ECONOMICA E CULTURALE	17
<i>1.1 GLI INIZI - LA STORIA DI INTERNET: UNA RIVOLUZIONE NATA IN SORDINA</i>	
<i>1.2 LE PRIME RETI DI INTERCONNESSIONE</i>	
<i>1.3 I BBS, IL PROTOCOLLO UUCP</i>	
<i>1.4 L'INTERNET 1.0</i>	
<i>1.5 II CERN DI GINEVRA: L'INTERNET EUROPEA</i>	
<i>1.6 LA BIBLIOTECA MONDIALE: DA GOPHER AL WEB</i>	
<i>1.7 DIFFUSIONE DEL WORLD WIDE WEB</i>	
<i>1.8 LA NASCITA DEL WEB 2.0</i>	
<i>1.10 LA CRESCITA ECONOMICA E CULTURALE DI INTERNET</i>	
<i>1.11 INTERNET E LE IMPRESE</i>	
<i>1.13 L'AFFERMAZIONE DELLA WIKINOMICS</i>	
<i>1.12 DATE PRINCIPALI DELLA STORIA DI INTERNET</i>	
CAPITOLO II LA RADICE DELL'IDENTITA' DIGITALE: L'IDENTITA' PERSONALE	57
<i>2.1 IL CONCETTO DI PERSONA</i>	
<i>2.2 IL DIRITTO ALL'IDENTITA' PERSONALE</i>	
<i>2.3 DALL'IDENTA' PERSONALE ALLA REPUTAZIONE</i>	
<i>2.4 IL WEB MARKETING</i>	
<i>2.5 L'EVOLUZIONE DEL MARKETING 2.0</i>	
<i>2.6 IL PERSONAL BRANDING</i>	
<i>2.7 L'ECONOMIA DELLA REPUTAZIONE</i>	
CAPITOLO III: LA DISCIPLINA DEI DATI PERSONALI SU INTERNET	86
<i>3.1 LA DIFFUSIONE DEI SOCIAL NETWORK</i>	
<i>3.2 IL PROBLEMA DELLA PRIVACY NEI SOCIAL NETWORK</i>	
<i>3.3 LE NUOVE FRONTIERE DI TUTELA DELLA PRIVACY</i>	
<i>3.4 DATI PERSONALI E NATURA GIURIDICA DI INTERNET</i>	
<i>3.5 LE MINACCE ALLA PRIVACY CHE VENGONO DAL WEB</i>	
CAPITOLO IV: WEB REPUTATION E IDENTITA' DIGITALE	114
<i>4.1 E'POSSIBILE RINUNCIARE AD ESSERE DIGITALI</i>	
<i>4.2 LA REGOLAMENTAZIONE DELL'IDENTITA' DIGITALE</i>	
<i>4.3 LA VIA EUROPEA E LA VIA STATUNITENSE</i>	
<i>4.4 LE DUE ANIME DELLA PRIVACY</i>	
<i>4.5 DALLA PRIVACY ALLA WEB REPUTATION</i>	
<i>4.6 IL CONCETTO DI REPUTAZIONE</i>	
<i>4.7 LE RECENSIONI ONLINE</i>	
<i>4.8 I MECCANISMI CHE STANNO ALLA BASE DI UNA BUONA REPUTAZIONE</i>	
CAPITOLO V: ASPETTI LEGISLATIVI DELLA WEB REPUTATION	138
<i>5.1 LA NOVITA'DI INTERNET 2.0 NELLA VITA DI RELAZIONE</i>	
<i>5.2 I PROFILI PENALI</i>	
<i>5.3 LA TUTELA IN SEDE CIVILE</i>	
<i>5.4 LA TUTELA TRADIZIONALE</i>	
<i>5.5 IL CODICE DELLE COMUNICAZIONI ELETTRONICHE</i>	
<i>5.6 LA RESPONSABILITA' DEL PROVIDER</i>	
CAPITOLO VI: DALLA TEORIA ALLA PRATICA: MONITORARE LA WEB REPUTATION	172
<i>6.1 LA CAPACITA' DI ASCOLTARE LA RETE</i>	
<i>6.2 FASI DI UN'ATTIVITA' DI MONITORAGGIO DELLA REPUTAZIONE IN RETE.</i>	
<i>6.3 TIPOLOGIE DI MONITORAGGIO</i>	
<i>6.4 GESTIRE UNA CRISI</i>	
<i>6.5 IL WEB REPUTATION MANAGER</i>	
CONCLUSIONI	183

Prefazione del Commissario AGCOM, Antonio Preto

La Persona in Rete, cardine della web reputation

Se la Rete è divenuta il centro delle attività umane sotto il profilo economico, lo è divenuta anche – e, forse, soprattutto – da quello sociale.

È nell'ambito dei rapporti sociali che gli studi mostrano come Internet sia un fattore di profondo cambiamento. Non solo tecnologico, ma relazionale. Essa ridefinisce i rapporti tra singoli, cambia i metodi di comunicazione personale, promuove l'economia della condivisione e della distribuzione.

Nella dinamica relazionale, entra in gioco, oltre a molti altri aspetti della vita consociata, la dimensione complessiva della persona.

In tale contesto, il volume scritto da Nicola Di Stefano e Federico Giannone ha il pregio di partire dalla prospettiva generale che ho cercato di tracciare. Gli Autori, infatti, partono dall'assunto che la "reputation" sia, in senso lato, un'attività di raccolta di ogni cosa detta, all'interno di Internet, su una certa persona, prodotto, servizio o evento.

Se, oggi, assume preminenza la dimensione personalistica della tutela, è altrettanto vero – altro pregio del volume – che anche servizi economici o di diversa natura possono essere più facilmente monitorati e valutati attraverso l'uso critico delle informazioni circolanti in Rete. Del resto, la connessione con la dimensione economica è evidente sotto tutti i profili considerati.

In aggiunta, è da evidenziare come nel testo si differenzino le attività compiute in modo continuativo, a testimonianza che l'attenzione può essere focalizzata non solo come processo generale, ma anche come indagine su uno specifico evento che può colpire il singolo. In questo senso, è di rilievo anche la differenziazione, ulteriormente compiuta nel volume, circa la differente attitudine – e impatto – di soggetti come personaggi pubblici, opinion leader e appartenenti al mondo della stampa, rispetto a quella degli individui 'anonimi' – che forse, proprio perché tali, presentano un elevato interesse a limitare, se necessario, l'uso delle informazioni circolanti al loro riguardo.

Il volume è l'occasione per riflettere ulteriormente su un tema che presenta numerosissime sfaccettature, e che va compreso con attenzione, nei suoi dettagli, nei suoi risvolti. Solo attraverso una differenziazione e una misurazione capillare dei concetti si può cercare di affrontare problemi ed equilibri delicatissimi come quello della manifestazione delle idee, dei suoi limiti e dell'uso dei dati che anche noi stessi immettiamo in Rete.

Un tema in espansione e costante movimento, come visto, su cui è doverosa l'attenzione dei soggetti istituzionali coinvolti, *in primis* i poteri indipendenti di vigilanza e regolazione.

Il volume, nell'insieme, rende possibile agganciarsi a temi di ordine generale, che tratterò nell'ordine: dimensione della persona, *privacy* e nuovi strumenti di protezione, come il diritto all'oblio, la sicurezza generale in rapporto con la *privacy*, la tutela dei minori, la posizione degli *Over-the-top* (Ott) e l'asimmetria regolatoria. Sono tutti temi apparentemente slegati, ma in realtà intimamente connessi alla dimensione della persona in Internet – e dunque anche alla sua reputazione – che cercherò di illustrare di seguito.

La nostra persona si manifesta continuamente nella Rete, è immersa nel suo universo, vive di essa e con essa. L'identità, come ho altrove sostenuto¹, diviene digitale. E, dal mondo *online* passa direttamente a quello *offline*², sancendo un percorso circolare, in cui i due aspetti divengono inseparabili e testimoniano una profonda comunicazione dall'uno all'altro lato.

Tale processo – questo l'aspetto che più reputo di rilievo – avviene secondo un canale umanistico, e non solo tecnico. È la dimensione intera della storia e dei valori della persona che si forma insieme al mezzo. La prospettiva è, in altri termini, olistica: la persona diviene qualcosa di nuovo perché va oltre le singole parti che la compongono nella vita reale.

¹ Sia consentito richiamare quanto scritto nel volume *In principio è la rete. Suggestioni comunicative per una società connessa*, Venezia, 2014.

² In questa specifica accezione, si v. H. MASUM, M. TOVEY, C. NEWMARK, *The Reputation Society: How Online Opinions Are Reshaping the Offline World*, Cambridge MA, MIT Press, 2012.

Tutto questo offre straordinarie possibilità. Ma è anche fonte di notevoli rischi, come si comprende immediatamente, o come forse ciascuno ha sperimentato, con immediatezza, nella prassi.

Le problematiche, complesse e sconfinata – come lo sono le regole chiamate a risolverle, e che presidiano un mezzo globale come Internet³ – non hanno infatti tardato a manifestarsi. L'interazione di un numero vastissimo di utenti, come quelli connessi, genera evidentemente problemi relazionali e interferenziali.

E, come sempre accaduto nella Storia, i diritti di alcuno possono limitare quelli degli altri. Ecco la necessità di doveri. E di limiti, di regole. Che non devono comprimere, limitare, frenare le possibilità offerte dalla tecnologia, o essere punitive. Devono invece spingere a un uso equilibrato del mezzo, cercando di perseguire gli interessi di tutti, nei limiti del possibile (è noto come sia difficile il raggiungimento dell'ottimo paretiano).

La necessità di un equilibrio non deve tendere a una *over-regulation*. La disciplina giuridica deve essere "sana", al passo con i tempi. Né deve essere chiusa e unilaterale, deve aprire i propri canali di comunicazione con gli interessati, esperti e singoli, in modo da poter arricchire le prospettive e le conoscenze della materia.

Senza minare le libertà, in altri termini, occorre rendersi conto che il pericolo maggiore che corriamo è la messa in pericolo dei diritti connessi alla persona. Che possono essere minacciati da un uso distorto della Rete, o dai malintenzionati che a volte si celano dietro di essa. Non è un rischio secondario, se la *Global Commission on Internet Governance* (Gcig), istituita nel 2014, ci parla di orizzonti nuovi, in cui si stagliano nuovi diritti, caratterizzati dall'essere *fondamentali* – proprio perché vi sono rischi della violazione di sfere intime della persona. "*Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to*

³ È d'obbligo il richiamo a M.R. FERRARESE, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Roma-Bari, 2006.

these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation”⁴.

A volte, dunque, servono diritti nuovi. Oltre al caso appena citato, vorrei ricordare l’iniziativa *NetMundial*, momento importante di fissazione di principi e diritti all’interno di Internet con pretesa di universalità. Essa, in linea con la *Gcig*, afferma il carattere fondamentale della *privacy* e, al suo interno, riconosce che essa *“includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data”* – così confermando la centralità del tema dei dati, del loro utilizzo (come avviene con la reputazione) e del loro effetto sulla persona.

Si aggiunge, naturalmente, la Carta dei diritti in Internet, promossa dalla Camera dei Deputati italiana, che si è svolta con un’ampia e interessante consultazione pubblica e che recita, all’art. 4 (nel testo risultante dalla prima bozza, che presto sarà sostituito da quello definitivo), che *“[o]gni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza”* e che *“[i] dati possono essere raccolti e trattati solo con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge”*. È di rilievo, però, soprattutto l’art. 8, per il quale *“[o]gni persona ha diritto alla rappresentazione integrale e aggiornata della propria identità in Rete”* e che *“[l]’uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano”*.

Altre volte (molte, a dire il vero), i diritti *offline* possono essere applicati anche al mondo *online*, come ci insegna chiaramente il Consiglio d’Europa, con la sua *Guida ai diritti umani per gli utenti di Internet*⁵.

⁴ *Toward a Social Compact for Digital Privacy and Security*, Statement by the GLOBAL COMMISSION ON INTERNET GOVERNANCE, Wednesday, April 15, 2015, core element no. 1 – testo disponibile all’indirizzo <https://www.ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security/>.

⁵ RECOMMENDATION CM/REC(2014)6 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON A GUIDE TO HUMAN RIGHTS FOR INTERNET USERS (*Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers’ Deputies*), disponibile all’indirizzo <https://wcd.coe.int/>.

In alcuni casi vi è la necessità di scrivere diritti nuovi, come accade con l'accesso, oppure di stimolare l'utilizzo di strumenti, come avviene con la promozione della domanda verso reti e servizi a banda ultra-larga⁶.

In ogni caso, preme evidenziare la circolarità, cui già si è fatto un accenno, tra diritti *online* e diritti *offline*, per affrontare in modo complessivo e coerente i delicati temi che un mezzo di comunicazione globale solleva.

Il mercato è in continua evoluzione. Le istituzioni sono chiamate a prendere atto dell'incessante cambiamento, favorendone i benefici e frenandone gli eccessi. L'Autorità non può più occuparsi soltanto di accesso alla rete.

Se cerchiamo di scendere nelle strutture giuridiche basilari dello scenario vigente, vediamo il modo in cui la persona trova uno scudo protettivo.

Lo sviluppo della persona, a ben vedere, deriva direttamente dal testo Costituzionale, per cui essa è riconosciuta e tutelata, e prende vita nelle formazioni sociali che la promuovono (art. 2). In tale scenario, anche una dinamica sociale, come quella che prende vita nella Rete, necessita di forme di protezione – e promozione – effettiva. Per rispondere a quel dettato fondamentale che, altrimenti, potrebbe essere infranto.

Soffermiamoci sulla *privacy*, oggetto di riqualificazione, in termini – si noti – di *diritto fondamentale*, da parte della Gcig, all'interno della dichiarazione prima richiamata.

Come rileva il *Global Privacy Enforcement Network*, appena il 15% delle "app online" fornisce un'informativa realmente chiara. In Italia, una ricerca condotta da *Federprivacy* ha dimostrato che il 67% dei siti italiani tratta i dati degli interessati in violazione al *Codice della Privacy*.

⁶ Cardine della regolazione pro-concorrenziale di cui si sta occupando l'Autorità per le garanzie nelle comunicazioni (AGCOM). Si v. sia l'analisi di mercato 2014-1017, sia l'indagine conoscitiva sulle reti *ultra-broadband* condotta congiuntamente con l'Autorità garante della concorrenza e del mercato (AGCM). Il tema della domanda è al centro anche della Strategia del Governo Italiano per la Banda Larga, adottata all'inizio del 2015 e in corso di attuazione.

Nessuno è in grado di controllare i contenuti, una volta immessi in rete. Servono strumenti concreti, che possano offrire tutela in un ecosistema in continua trasformazione come quello attuale.

Uno degli strumenti utilizzabili è senz'altro una corretta – seria e non strumentale – applicazione del diritto all'oblio.

Il tema è molto noto. La Corte di Giustizia, con il "*right to be forgotten*", ha fatto un passo in avanti coraggioso. L'unica "pecca" della sentenza è di aver addossato l'onere della scelta a un privato (nella specie, *Google*). È stata una soluzione affrettata, anche se sul piano applicativo, sia a livello europeo (con il Wp 29), sia in Italia, si è poi affermato un ruolo forte del Garante per la protezione dei dati personali, che così assicura (riesaminando "in secondo grado" le richieste non accolte) il rispetto del diritto da parte dell'operatore.

Del resto, ciò è in linea con la natura di alcune fattispecie, vale a dire i casi in cui sono coinvolti personaggi pubblici. Se c'è l'interesse pubblico alla notizia, la libertà di informazione non può subire compressione. Solo se tale interesse pubblico non sussiste, si pone un problema di *privacy* – e, nella specie, di possibilità di esercizio del diritto all'oblio.

Il tema è connesso a quello della sicurezza e della sorveglianza di massa.

Viviamo in tempi di attacchi informatici, terroristici, di vere e proprie guerre informatiche. Da più parti si ricerca maggiore sicurezza. Ma la sicurezza mette a rischio la nostra riservatezza. Accanto alle ragioni di sicurezza, è necessario ricordare che le piattaforme devono restare neutrali anche rispetto al potere politico: i recenti fatti (che vengono alla luce costantemente) che hanno coinvolto i giganti del *web* e le agenzie di spionaggio (anche quelle private che vendono i propri costosissimi servizi di nascosto, e dunque illegalmente) confermano il rischio di derive antidemocratiche, che dobbiamo assolutamente contrastare.

In proposito, è stato affermato che la sorveglianza è “*nella sua essenza, un abuso della privacy*”⁷. Qual è il giusto equilibrio? Come assicurare la prevenzione dei crimini con la tutela del singolo? Quale il ruolo dell’Unione europea, che sta discutendo nuove norme sia su *privacy*, sia su sicurezza delle reti?

La soluzione è complessa, e per nulla facile. Si possono focalizzare alcuni punti fermi: i mezzi di tutela limitati al singolo (per i «propri dati») non sono sufficienti; serve, per converso, una regolazione omnicomprensiva, che parta dalle infrastrutture, e giunga a tutti soggetti interessati, operatori e utenti, prevedendone diritti ed obblighi.

Abbiamo un grande insegnamento: la pronuncia della Corte di giustizia dell’Unione europea nel caso *data retention*⁸. La Corte, infatti, ha annullato la Direttiva n. 2006/24/CE, che consentiva la raccolta, la conservazione e l’utilizzo di informazioni elettroniche private per motivi di sicurezza. Ebbene, in riferimento alla raccolta generalizzata consentita dalla direttiva, la Corte ha rilevato un’ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. L’ingerenza, infatti, è stata ritenuta *non proporzionata, generalizzata e indifferenziata*; inoltre, non offriva opportune *garanzie procedurali*⁹.

La Corte, con questa sentenza, ha dimostrato che è necessario ricercare – anche in questioni generali che riguardano l’intera società, come la sicurezza e la prevenzione del terrorismo – un corretto equilibrio tra sicurezza e *privacy* e non generare uno squilibrio che possa comprimere i diritti. E, con essi, la persona.

⁷ Così si è espressa Marietje Schaake, Deputata europea.

⁸ CGUE, sent. 8 aprile 2014, cause riunite C-293/12 e C-593/12, *Digital Rights Ireland Ltd (C-293/12) c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri*.

⁹ In particolare, non erano specificati *criteri certi e oggettivi* che giustificassero l’ingerenza nei casi più gravi; si stabiliva un termine di conservazione minimo (6 mesi) e massimo (24 mesi), senza criteri per differenziare la durata effettiva della *retention*, a seconda delle caratteristiche del singolo caso; conservazione e utilizzo dei dati avvenivano senza che l’utente fosse informato; infine, mancava l’obbligo di conservare i dati solo nel territorio dell’Ue.

L'Unione europea, in merito, ha un ruolo importantissimo, e può fungere da mediatore nelle diverse esigenze, equilibrando i diversi Stati membri. Essa può conciliare la protezione dei dati con operazioni efficaci di sorveglianza. Che però devono essere specifiche, non generalizzate e giustificate da ragioni obiettive – come insegna la Corte di giustizia. La sintesi di questo approccio «europeo» sembra essere presente nella nuova proposta di direttiva *Network and Information Security* – Nsi, che sarà un banco di prova notevole (ad esempio, si parla di controllare solo le “*infrastrutture critiche*”, come energia, mercati finanziari e trasporti, escludendo invece, correttamente, servizi della società dell'informazione come i *social network*).

Anche l'aggiornamento del nuovo regolamento dell'Unione in materia di *privacy* darà un notevole banco di prova. L'aggiornamento della normativa è necessario per allineare il testo alla realtà odierna (con meccanismi innovativi le definizioni di dato genetico e biometrico; la portabilità del dato, l'obbligo di notifica alle autorità competenti delle violazioni della *privacy*, o il problematico, perché assai dibattuto, *one stop shop mechanism*, che prevede la competenza dell'autorità dello Stato membro ove sussiste il cd. “stabilimento principale”).

Altro tema di grande centralità è la protezione dei minori.

Qui occorre trovare un difficile e delicato equilibrio, che si fonda sulla proporzionalità delle misure, sulla loro specificità in relazione al rischio da evitare. La tutela della *privacy* dei minori (che negli Usa trova da anni previsioni normative specifiche, come avviene con il Coppa) non può impedire il libero flusso dell'informazione.

In questo campo, a mio avviso, bisogna seguire due strade maestre. La prima è quella della imposizione, vale a dire della regolazione; la seconda della condivisione, ossia della *self-regulation* e della *coregulation*, congiuntamente a una efficace opera di educazione da parte dei soggetti competenti.

Quanto alla prima, occorre ripensare il tema in modo ampio, non solo come funzione regolatoria, ma come modifica della normazione primaria. Vista la

posizione di protagonismo dei minori, che spesso usano da soli la Rete, e li lasciano le loro tracce spesso in modo inconsapevole, la risposta normativa e regolatoria, in particolare, non può appiattirsi su concetti superabili e su posizioni concettuali "di comodo", ma ricalcare il terreno ondulato di cui è composta la Rete. Questo deve essere l'insegnamento: differenziare le situazioni, distinguere, acuire lo spirito critico.

Quanto alla *self* e *co-regulation*, essa va promossa per favorire una soluzione condivisa e virtuosa dei nuovi problemi sollevati da Internet (come accaduto, in ambito di media, con i codici di autoregolamentazione, che hanno visto come parte attiva gli stessi operatori e le associazioni degli utenti). Si può ricordare, in proposito, che l'Unione europea ha sostenuto questo sistema integrato di interventi proprio nell'ambito esaminato, all'interno della "*Strategia europea per un Internet migliore per i ragazzi*".

Sull'educazione, infine, ricordo come l'Ocse sottolinei, anche un questo caso, con la sua raccomandazione del 2012 sulla protezione dei ragazzi *online*, che tutti gli *stakeholders* hanno grandi responsabilità in merito. Devono creare un ambiente sicuro per i ragazzi, sostenere il ruolo delle famiglie nel ridurre i rischi legati a un certo (non tutto) utilizzo di Internet, creare e diffondere una cultura sana.

Se pensiamo a quelli che altrove ho definito "i padroni della Rete" – e su cui tornerò più diffusamente a breve – vediamo che hanno effettivamente un ruolo cruciale. Un attore come *Google*, in questo campo, può divenire un vero e proprio "attore istituzionale". Ma può farlo solo se orienta la propria condotta all'interesse della società, dei ragazzi in questo caso, e non solo dell'impresa.

Per i minori serve, concludendo sul punto, un approccio olistico, che tenga conto delle componenti nel loro insieme, e non in modo separato.

È in questa tematica che si colloca la reputazione *online*. Che non è un argomento nuovo. Il tema è stato studiato dal punto di vista economico, in

relazione alle dinamiche di impresa¹⁰, vale a dire delle informazioni utilizzate a fini lavorativi (è noto che singoli *post*, commenti o informazioni possono condizionare assunzioni).

Il tema della reputazione *online* ricade all'interno del quadro complessivo che stiamo delineando, tra *privacy*, minori, oblio... e tutto all'interno della dimensione della persona umana. La reputazione *online* caratterizza la persona. Ne determina i tratti. E, dunque, va protetta. Prima ancora, vanno compresi gli ambiti in cui si manifestano i suoi diversi risvolti.

Oggi, stando alle indagini più recenti, lo strumento più utilizzato per compiere ricerche sulle persone è *Google*. Assistiamo, ancora una volta, a un ruolo di predominanza degli Ott. Secondo il *World Economic Forum* i dati raccolti su Internet potrebbero diventare una nuova ideologia: perché nella società di oggi ogni cosa è misurata. Cito da un recente volume: «[I]a quantità di informazioni contenute negli archivi elettronici cresce quattro volte più in fretta dell'economia mondiale, mentre la capacità di elaborazione dei computer cresce nove volte più in fretta»¹¹.

Ancora una volta, emerge la necessità di introdurre regole: e non certo per limitarne l'innovazione, ma per disciplinarne gli eccessi e ricondurli, per quanto possibile, a normalità. L'applicazione di regole serve a creare un comune *level playing field* che generi una cooperazione virtuosa dei soggetti economici e non, stimolando innovazione, servizi innovativi e miglioramenti della situazione economica.

Se, per converso, questo complesso "ecosistema digitale" continuerà a vivere di una asimmetria regolatoria, allora persisteranno i rischi di posizioni privilegiate di alcuni, in posizione di superiorità tecnica e, quindi, di superiorità economica e sociale. Con il controllo dei dati e la profilazione dei singoli sempre più estensiva (e non sempre lecita o legittima), l'esigenza di regolazione si riverbera direttamente nell'ambito della persona e, dunque, della sua reputazione *online*.

¹⁰ R. FARMER, B. GLASS, *Building Web Reputation Systems*, O'Reilly Media Inc., 2010.

¹¹ V. MAYER-SCHÖNBERGER, C. KENNETH, *Big Data*, Milano, Garzanti, 2013.

Questa primazia deve essere, in qualche modo, regolata. Alla concentrazione di potere nelle mani di pochi "giganti", occorre dare risposte concrete.

Riprendendo le parole di Thomas Friedman, la globalizzazione ha quasi «appiattito» il mondo¹². Il carattere sconfinato della rete impone nuove e ulteriori sfide. Pensiamo alla territorialità di alcuni interessi. Con la citata sentenza *Google Spain*, la Corte di Giustizia non solo ha sancito, come visto, e come a tutti noto, il diritto all'oblio, ma ha anche riletto la libertà di stabilimento: per i Giudici di Lussemburgo, ormai conta molto il luogo dove si svolge l'attività, meno il Paese in cui il soggetto è stabilito. Questo principio introduce alcune importanti valutazioni. Pensiamo, ad esempio, alle conseguenze su materie come la tassazione: sono casi di preminente interesse pubblico, in cui i poteri nazionali si riappropriano di alcune prerogative. In generale, si arriva a regolare la "a-territorialità", definendo principi comuni (ed evitando le conseguenze più dannose del *forum shopping*). Non si tratta di ricreare confini ormai obsoleti, ma di definire in modo equilibrato diritti e libertà.

Il problema concerne non solo la regolazione, ma anche la normazione primaria. Infatti – come ho sostenuto in diverse occasioni – un nodo cruciale da sciogliere è la definizione di "fornitore di servizi di media audiovisivi" e la distinzione tra "servizi lineari e non lineari" previste dalla direttiva sui servizi media. Sono distinzioni ormai superate, e il "refit" in corso della direttiva n. 2010/13/UE dovrebbe tenerne espressamente conto. La stessa 'distorsione' avviene con l'esclusione di motori di ricerca e aggregatori dalla nozione di "responsabilità editoriale". Questi soggetti, infatti, forniscono servizi del tutto analoghi a quelli dei *broadcaster*, e non si comprende il motivo per cui non debbano essere sottoposti alle stesse regole. Anche qui, il *refit* della direttiva Smau sarà un banco di prova dell'attività normativa dell'Unione.

D'altronde, lo scenario sembra già aperto. La Commissione europea sembra muoversi, infatti, proprio in questa direzione, se la strategia per il *Digital*

¹² T.L. FRIEDMAN, *Il Mondo è piatto. Breve storia del ventesimo secolo*, Milano, Mondadori, 2007.

Single Market, annunciata a maggio dal Commissario Ansip, prevede anche la revisione della regolazione di questi servizi.

È da rilevare, infine, che negli ultimi anni è cresciuta anche l'attenzione delle Autorità *antitrust* verso i giganti del *web*: non solo *Google*, ma anche *Expedia* ed *eDreams*.

Così come in Rete si tutela, in generale, la *net neutrality*, così all'interno della raccolta dei dati – e della “reputazione” che può essere costruita attraverso di essi – occorre garantire una *platform neutrality*, per evitare che il potere di mercato delle piattaforme di intermediazione generi discriminazioni.

Gli Ott, comunque, costituiscono anche una risorsa. Un modello economico e organizzativo che può insegnare qualcosa anche agli altri operatori. Sono una sfida per migliorare. *Google* offre servizi generali (le email sono diffusissime), è promotore di progetti di valore, come *Google* per il *made in Italy*.

L'azione da intraprendere, in questo senso, deve richiamare la tesi di einaudiana memoria: “*conoscere per deliberare*”. Servono decisioni informate, non ideologiche e, per questo, occorre conoscere a fondo il contesto di riferimento, dialogando gli operatori in posizione di terzietà e indipendenza.

Vista la posizione dominante nel mercato del *search*, *Google* ha un accesso privilegiato ai cosiddetti *big data*. Occorrerebbe dunque chiedersi se la grande azienda di *Mountain View* non sia a tutti gli effetti un operatore verticalmente integrato; e, conseguentemente, se i *big data* maneggiati dall'impresa siano da considerarsi una *essential facility*.

In tal caso, sarebbe necessaria qualche formula regolatoria ulteriore, da intendere come forma di accesso ai dati. Eventualmente associata a una forma di remunerazione dell'utente finale che, di fatto, è il proprietario e “produttore” dei dati che tutti rincorrono.

Trattandosi di un fenomeno recente, è ancora presto per dare una risposta chiara e univoca. Certamente, però, possiamo intravedere una commistione di

strumenti: Ott e diritto alla *privacy* non sono più temi distinti, in quanto fanno parte di un quadro unico, e molto ampio.

In generale, si osserva come ai diritti (anche ai diritti che nascono con le nuove tecnologie), vanno correlati precisi doveri. In questo caso, da un lato ci sono i doveri dei soggetti privati – come motori di ricerca o *social network*: i giganti che ben conosciamo – chiamati a collaborare in maniera equa e paritaria. Dall'altra, vi è il dovere delle istituzioni di intervenire per riportare equilibrio in una situazione che rischia di svilupparsi in modo unidimensionale, "a una dimensione" per richiamare, *mutatis mutandis*, Foucault.

In un ambito soggetto a un dinamismo evolutivo così elevato, occorre ripensare anche il diritto chiamato a regolarne – se necessario – gli aspetti più delicati e a porre l'equilibrio degli interessi.

La tecnologia non ha solo bisogno di regole nuove. La tecnologia modifica le regole e modifica abitudini e comportamenti dei singoli. La reputazione ne è un palpabile esempio.

Il tema della reputazione solleva la necessità di definire i diritti applicabili in Rete. E, non lo si dimentichi, dei doveri correlati a tali diritti. Quando dell'utilizzo del mezzo viene fatto abuso, infatti, occorre una risposta certa, in termini regolamentari e aggiudicatori, e in termini di possibilità di difesa giurisdizionale. Di rispetto, in ultima analisi, di quei fondamentali precetti costituzionali, così semplici eppur così complessi, che prima ho richiamato.

Tutto ciò, nell'insieme, impone una riflessione continuata, documentata e approfondita su un argomento che tocca le vite di ciascuno di noi, ampliando il novero dei diritti e dei relativi doveri.

Ben venga, dunque, la pubblicazione e l'ampia diffusione di questo Volume, opera meritoria degli Autori, che ci aiutano a rinnovare un dibattito sempre attuale e su cui abbiamo, tutti, ancora molto da imparare.

Roma, 16 luglio 2015

Antonio Preto

CAPITOLO I

LA STORIA DI INTERNET: UNA RIVOLUZIONE NATA IN SORDINA

1.1 Gli inizi

Per affrontare il complesso tema della web reputation è necessario avere una visione globale del fenomeno internet. In questo senso appare opportuno ripercorrere le tappe fondamentali che hanno segnato la sua nascita e il suo sviluppo.

Sappiamo tutti che Internet è una rete telematica di portata mondiale. Il suo scopo originario era quello di garantire comunicazioni stabili ed efficienti tra le sedi delle forze armate statunitensi oltre che tra le università e i centri di ricerca che lavoravano a progetti di natura militare.

Con il passare del tempo, si è evoluta in una rete prettamente universitaria e dopo l'avvento dell'interfaccia grafica che ne facilita la navigazione, è diventato uno strumento di massa, aperto alla divulgazione di notizie e alla vendita di prodotti e servizi.

La possibilità di fruizione di tale risorsa si è poi estesa anche a utenti in movimento che dispongono di dispositivi cellulari o palmari.

L'avvento di Internet ha dunque cambiato i modi e le usanze di lavoro di molte persone, consentendo di avere rapidamente informazioni e notizie di qualunque tipologia e in qualunque campo.

Grazie alla sua rapida espansione e popolarità è divenuta essenziale in certi ambiti lavorativi nei quali la diffusione e la pubblicazione di informazioni è fondamentale. Spesso alcuni eventi vengono trasmessi esclusivamente attraverso Internet che consente di assistere in tempo reale a situazioni che finora era possibile diffondere solo attraverso la televisione.

La prima rudimentale apparizione di questa forma d'interconnessione risale al 1969 quando il Ministero della Difesa statunitense creò un'agenzia, Arpa,

preposta allo sviluppo di una rete che potesse reggere al bombardamento nucleare, garantendo la continuità di comunicazione tra località diverse.

Il progetto coinvolse centri di ricerca, università e qualche azienda privata, tutti in qualche modo legati all'attività militare e dotati di computer che all'epoca costituivano quanto di più moderno la tecnologia informatica americana potesse offrire.

Contestualmente i Bell Laboratories (famoso centro di ricerca americano di proprietà di AT&T) stavano lavorando allo sviluppo del sistema operativo Unix, che sarebbe diventato uno standard per il mondo accademico e della ricerca e anche per molte applicazioni militari.

L'unione di questi filoni avrebbe portato a quello che oggi è Internet, ma il percorso è contrassegnato da alcuni eventi che hanno lasciato il segno.

Il primo appalto per la costruzione della rete fu concesso alla società Bolt, Beranek and Newman (BBN) che collegò quattro università diverse: Stanford University, Ucla (University of California at Los Angeles), Ucsb (University of California at Santa Barbara) e la University of Utah, usando linee telefoniche e installò in ciascuna di queste un imp (Information Message Processor), ovvero un particolare computer che gestiva il traffico in rete.

L'impianto fungeva da intermediario tra linee di connessione e mainframe, i grandi elaboratori centralizzati su cui all'epoca risiedevano tutte le informazioni e tutti i programmi. Lo stesso divenne attivo il 2 settembre 1969 e così nacque Arpanet. Tutto il traffico che viaggiava su queste connessioni non era confidenziale e serviva prevalentemente a titolo di ricerca e sperimentazione.

All'inizio degli anni Settanta i sistemi per trasmettere messaggi da una località all'altra non erano molto efficaci e il primo obiettivo dei ricercatori fu proprio quello di trovare soluzioni funzionali per convogliare i pacchetti su Arpanet. Si decise così di adottare un modello il cui sviluppo era già iniziato in Europa (per opera del National Physics Lab inglese e della Società Internationale de Télécommunications Aeronatiques francese) e che sarebbe poi diventato comune in molti altri sistemi di comunicazione: la commutazione di pacchetto.

Attraverso questa tecnica, i messaggi e le informazioni vengono suddivisi in pacchetti di lunghezza fissa e ogni singolo pacchetto diventa un'entità a se stante, capace di viaggiare sulla rete in modo completamente autonomo perchè dotata al proprio interno dell'indirizzo sia di provenienza sia di destinazione.

Non era importante che tutti i pacchetti che componevano un determinato messaggio rimanessero uniti durante il percorso e non era nemmeno indispensabile che arrivassero nella sequenza giusta. Le informazioni che essi convogliavano al proprio interno erano sufficienti per ricostruire, una volta arrivati a destinazione, l'esatto messaggio originale, indipendentemente dal percorso seguito da ciascuno dei suoi frammenti.

Grazie a questo sistema si potevano avere due benefici immediati: qualunque fosse lo stato della rete, il pacchetto poteva sempre trovare una via alternativa per giungere alla propria destinazione. Ed era questa una caratteristica utile per gli obiettivi militari e per chiunque desiderasse avere un impianto il più possibile resistente ai guasti, anche a quelli accidentali. Inoltre i vari pacchetti provenienti da fonti diverse potevano essere convogliati tutti assieme su una singola linea ad alta velocità invece di dover ricorrere a tante linee separate, usate solo parzialmente.

Si riuscì in questo modo a convogliare il traffico su una linea collegata in permanenza che ripartiva dinamicamente la propria capienza tra i vari computer collegati e che, in ogni caso, era quasi sempre attraversata da qualche tipo di traffico e perciò giustificava il proprio costo. Se la linea veniva usata da una singola macchina o da poche macchine, sarebbe restata quasi sempre inattiva visto che anche l'utente più veloce avrebbe passato la maggior parte del tempo a lavorare in locale (leggendo quello che gli è arrivato dalla rete o preparando una risposta) e solo molto sporadicamente avrebbe trasmesso o ricevuto qualcosa. In effetti Internet usata con un modem su linea commutata, cioè la linea normale telefonica, non sembrò molto efficiente poichè esistevano numerosi tempi morti dovuti al nostro personale modo di lavorare e al ritardo di reazione dei server con cui chiedevamo di collegarci.

Il primo protocollo sviluppato per la commutazione di pacchetto su Arpanet si chiamava ncp (Network Control Protocol), ma non era particolarmente efficiente. Col passare del tempo i progettisti di Arpanet definirono un insieme di circa 100 protocolli per regolare il trasferimento dei pacchetti e questo insieme si è evoluto in quella che noi oggi conosciamo con il nome di Internet Protocol Suite: una raccolta di standard trasmissivi che verte su due protocolli primari, il Transmission Control Protocol (tcp) e l'Internet Protocol (ip), più molti altri secondari che consentono la comunicazione tra computer e reti molto diverse.

La prima definizione di tali protocolli risale al 1973 e nel 1974 Vincent Cerf e Robert Kahn ne definirono le caratteristiche su un documento intitolato IEEE Transactions on Communications. Quello stesso anno fu pubblicata la prima specifica per i protocolli da utilizzare su Internet. Si dovette però attendere fino al 1 gennaio 1983 per l'adozione ufficiale dell'intera Internet Protocol Suite.

Nel 1972 l'Università dello Utah realizzò un sistema per controllare un computer a distanza su Arpanet e divenne possibile trasferire file da un computer all'altro per mezzo del protocollo ftp (File Transfer Protocol). Combinando tcp/ip ed ftp si era raggiunto l'obiettivo tecnologico di Arpanet: trasferire dati da un punto all'altro della rete. Quel che ancora rimaneva da dimostrare era se i dati sarebbero potuti fluire tra due macchine di tipo anche diverso, utilizzando i tipi più disparati di collegamento (incluso l'etere).

L'esperimento chiave in questo senso fu condotto nel 1978: un computer che viaggiava a bordo di un camion su un'autostrada californiana inviò dati a un altro computer che si trovava a Londra. Il camion era collegato via radio con un terzo computer in California, il quale inoltrava le informazioni sulla rete, queste attraversavano l'intero continente nordamericano su linee terrestri e infine superavano l'Atlantico per mezzo di una connessione satellitare.

Già nel 1980 Arpanet si trasformò in uno strumento vitale per le università e per i centri di ricerca americani, che avevano un bisogno sempre maggiore di scambiare informazioni e di coordinare le proprie attività.

Nacque così la posta elettronica che si affiancava al semplice trasferimento di file, che aveva rappresentato la prima applicazione di Arpanet. Nel 1983 Internet divenne a tutti gli effetti la rete delle reti, utilizzando Arpanet come dorsale, ovvero una rete ad alta velocità che unisce tra loro altre reti locali. Tuttavia restavano ancora esclusi tutte le università americane che non avevano rapporti con il Dipartimento della Difesa.

Per risolvere questo problema e estendere l'accesso a tutti gli interessati, il Dipartimento della Difesa creò una propria rete alternativa, chiamata Milnet, per non dover più dipendere da Arpanet e lasciare campo libero al mondo accademico, mentre il governo americano istituì la National Science Foundation (NSF) con il duplice scopo di fornire risorse di elaborazione alle università, attraverso l'uso centralizzato di supercomputer, e favorire la crescita di un sistema di comunicazione veloce tra queste ultime.

Nei primi anni Ottanta la NSF costruì Cernet, una rete che univa le varie facoltà d'informatica statunitensi. Alla fine del decennio si costituì Nsfnet con lo scopo dichiarato di rimpiazzare Arpanet per mezzo di una rete dorsale alternativa. A posteriori abbiamo avuto modo di notare come la transizione sia stata relativamente lunga tanto che Arpanet è stata smantellata definitivamente solo nel 1990.

Nel 1991 il governo degli Stati Uniti ha emanato una legge, l'High Performance Computing Act, che decretava la nascita della National Research and Education Network (Nren - detta anche "autostrada elettronica") il cui scopo era quello di costituire reti ad alta velocità che avrebbero unito le varie università e i vari centri di ricerca americani, fornendo anche l'infrastruttura per eventuali attività commerciali.

Sempre quello stesso anno, il Cern (Consiglio Europeo per la Ricerca Nucleare) poneva le basi per una nuova architettura capace di semplificare enormemente

la navigazione di Internet, la World Wide Web. Nel 1993 è stato inventato il primo strumento grafico per esplorare Internet, il programma Mosaic.

A partire dal 1994 la World Wide Web ha trasformato Internet in un fenomeno di massa e oggi esistono dorsali alternative a Nsfnet che servono sia per aumentare la quantità di traffico che può circolare su Internet sia per consentire la presenza di servizi commerciali che sono vietati nel contesto accademico definito dalla National Science Foundation.

A differenza delle quattro università che parteciparono alla versione originale di Arpanet, l'Internet moderna si compone di migliaia di singole reti e ognuna raccoglie a sua volta un numero più o meno grande di host (macchine individuali).

Il termine non si riferisce ai singoli oggetti fisici al suo interno, bensì allo spazio complessivo che questo insieme di computer rappresenta e che può essere attraversato in lungo e in largo da chi cerca notizie, documenti, messaggi e file da scaricare. La natura dei protocolli tcp/ip è tale da consentire l'interconnessione dei network più eterogenei: dalle lan convenzionali (come Ethernet) alle reti geografiche che si spargono sul territorio attraverso l'impiego di linee telefoniche più o meno veloci, governate coi metodi trasmissivi più disparati. Non esiste computer al mondo che non possa dialogare con il tcp/ip e questo comprende i personal computer, i mini computer e i grandi mainframe (i mostri da centro di calcolo).

Il sistema fisico di connessione può essere il più vario: fibra ottica per le grandi distanze, cavo coassiale e doppino telefonico, satellite, onde radio, raggi infrarossi. Si tratta di un mondo in continua trasformazione, con pezzi che si aggiungono e pezzi che scompaiono, ma nel suo insieme lo spazio Internet è sempre disponibile, a qualsiasi ora, e la sua esistenza non dipende dall'iniziativa di una singola azienda oppure di un singolo governo. L'universalità di questa rete consente agli utenti di scegliere il computer e i programmi che preferiscono, di decidere liberamente il tipo di connessione da

utilizzare (modem su linea privata, linea isdn, rete locale con collegamento geografico ad alta velocità).

1.2 LE PRIME RETI DI INTERCONNESSIONE

Nella prima metà degli anni Ottanta, negli Stati Uniti esistevano svariate reti d'interconnessione, tutte finanziate dal governo, ma ciascuna indipendente dalle altre. La più importante storicamente era Arpanet, la precorritrice di Internet finanziata dal Department of Defense (Dipartimento della Difesa) ed estesa a tutte le università e i centri di ricerca che all'epoca lavoravano su progetti militari o federali.

La prerogativa primaria di Arpanet era quella di aver dimostrato, in vent'anni di attività, la possibilità di collegare tra loro sistemi diversi e reti diverse utilizzando un nuovo tipo di protocollo suddiviso in due componenti: tcp (Transmission Control Protocol) e ip (Internet Protocol).

Il grande difetto di Arpanet derivava dalla sua dipendenza da strutture burocraticamente complesse e poco agili. Finché la sua attività si era concentrata su quattro università-polo, come nella configurazione originale del 1969, o comunque era rimasta asservita a progetti militari, non erano emersi problemi. Tuttavia dal 1983 la componente militare si era separata (trasformandosi in Milnet) e Arpanet aveva assunto le caratteristiche e il nome di Internet, vale a dire uno strumento al servizio dei ricercatori e docenti universitari di qualsiasi genere e provenienza.

All'inizio del 1985 vi si collegavano già 100 reti diverse ed era già fortemente congestionata, all'inizio del 1987 questa cifra era salita a 200 e nel 1989 ce ne sarebbero state 500. Arpanet stentava a reggere il passo con una crescita esponenziale di questo tipo. Le università scoprivano le grandi potenzialità offerte dalla posta elettronica, dallo scambio di file a distanza e dall'impiego condiviso di supercalcolatori. I ricercatori non dovevano più viaggiare da una città all'altra oppure da una nazione all'altra per scambiare informazioni con i loro colleghi e potevano accedere a risorse di calcolo prima irraggiungibili.

Nel 1989 la National Science Foundation (un ente governativo creato per finanziare lo sviluppo della ricerca americana) aveva assegnato ad Arpanet uno stanziamento di 4 milioni di dollari al fine d'installare nodi in 40 nuovi college e università che dovevano collegarsi alla Rete. La Defense Communications Agency, che aveva da poco rilevato la gestione di Arpanet ereditandola da Darpa (Defense Advanced Research Projects Agency), impiegò ben cinque anni prima di far arrivare questi terminali a destinazione. Le apparecchiature erano diventate talmente vecchie che quando arrivarono a destinazione erano già obsolete e in alcuni casi furono installate e disinstallate nella medesima settimana perché il loro arrivo coincise con il varo della nuova dorsale ad alta velocità che li rendeva di fatto inutilizzabili.

La prima dorsale Nsfnet funzionava a 56 Kbit per secondo e collegava sei centri di supercalcolo in diverse regioni degli USA. A questi centri accedevano numerose università e centri di ricerca.

Nel periodo di massimo splendore solo il cinquanta per cento delle università primarie negli Stati Uniti erano collegate ad Arpanet.

Per colmare la forte richiesta di comunicazione e di servizi a cui l'arrivo di Arpanet aveva dato la stura, senza poi farvi fronte, erano nate altre reti parallele.

Nel 1981 la National Science Foundation aveva costituito una propria dorsale chiamata Csnet (Computer Science NETwork) che collegava tra loro ricercatori e ingegneri informatici e che aveva consentito dal 1983 in avanti il collegamento a Internet per molti centri di ricerca non raggiunti da Milnet o da Arpanet.

Con l'arrivo di MCI, IBM e Merit Network, fu costruita una nuova dorsale con linee da 1,5 Mbps. Questa dorsale usava i protocolli tcp/ip per affiancarsi ad Arpanet e progressivamente sostituirla.

Parallelamente esistevano anche una rete del Department of Energy, una rete della Nasa (National Aeronautics and Space Administration), Hepnet (High Energy Physics network) che riuniva i ricercatori della fisica delle alte energie,

Mfenet (Magnetic Fusion Energy Network), e Bitnet (Because It's Time NETwork) una rete creata nel 1981 con tecnologia IBM per lo scambio di messaggi tra le università. C'era ben poca integrazione tra tutti questi vari ambienti che utilizzavano anche talvolta protocolli diversi. Occorreva trovare un legante universale che fosse anche in qualche modo svincolato dagli obiettivi militari che avevano caratterizzato Arpanet (nata come sistema di comunicazione capace di resistere a un bombardamento nucleare). L'unificazione di queste varie risorse fu demandata alla National Science Foundation che nel luglio del 1986 costruì una dorsale che collegava sei città negli Stati Uniti dove risiedevano altrettanti centri di supercalcolo. La dorsale usava uno speciale software di gestione chiamato Fuzzball (dal nome di un fungo che esplose per disseminare i suoi semi) e funzionava a 56 Kbit per secondo, una velocità modesta secondo i nostri standard attuali, ma adatta per quell'epoca, dove ancora la grafica non era in uso.

I nodi erano il San Diego SuperComputer Center in California (<http://www.sdsc.edu>), il National Center for Supercomputing Applications a Urbana-Champaign nell'Illinois (luogo dove nel 1993 sarebbe nato il browser Mosaic antesignano di Netscape - <http://www.ncsa.uiuc.edu>), il Cornell Theory Center di Ithaca nello stato di New York (<http://www.tc.cornell.edu>), il Pittsburgh Supercomputing Center in Pennsylvania (<http://www.pscinfo.psc.edu>), il John von Neumann Supercomputer Center a Plainsboro nel New Jersey (vicino a Princeton) e il National Center for Atmospheric Research a Boulder nel Colorado (<http://http.ucar.edu>).

Lo sviluppo della rete era demandato al Cornell Theory Center e al Ncsa, col supporto tecnico di Dave Mills dell'Università del Delaware e di Hans-Werner Braun di Merit Network, un consorzio formato dalle università del Michigan e gestore di una rete Internet regionale (MichNet). Questa struttura già costituiva un'alternativa interessante ad arpanet come terreno di prova per la costruzione di una nuova dorsale più potente visto che dall'inizio del 1986 aveva già riunito intorno a sé un consorzio di 13 università statunitensi, interessate a fruire dei servizi offerti dai cinque centri di supercalcolo appena

menzionati.

Il consorzio comprendeva l'Università dell'Arizona (<http://www.arizona.edu>), la Brown University (<http://www.brown.edu>), l'Università del Colorado (<http://www.colorado.edu>), la Columbia University (<http://www.columbia.edu> - inventrice del noto protocollo di comunicazione Kermit), l'Harvard University (<http://www.harvard.edu>), l'Institute for Advanced Study (<http://www.ias.edu>), il MIT (Massachusetts Institute of Technology - <http://web.mit.edu>), la New York University (<http://www.nyu.edu>), la Pennsylvania State University (<http://www.psu.edu>), l'Università della Pennsylvania (<http://www.upenn.edu>), la Princeton University (<http://www.princeton.edu>), l'Università di Rochester (<http://www.rochester.edu>) e la Rutgers University (<http://www-n.s.rutgers.edu>).

A ciascuna di queste università si sarebbero poi collegate altre università e altri centri locali, formando una rete capillare dedicata interamente alla ricerca che partiva da una dorsale comune alla quale si sarebbero allacciate diverse reti regionali (successivamente identificate col nome di Regional Network Provider). Tra l'altro, mediante una di queste reti, la JvNCnet (John von Neumann Center network) abbinata al centro di supercalcolo di Plainsboro, la NSFnet aveva attivato già nel 1987 due connessioni verso l'Europa: Janet (Joint Academic NETWORK) in Gran Bretagna e NORDUnet per tutti i paesi Scandinavi a cominciare dalla Norvegia. La connessione transatlantica usava inizialmente una linea a 64 Kbps che sarebbe passata a 128 Kbps nel 1989.

Sempre mediante Jvncnet, quello stesso anno NSF aveva attivato una connessione diretta con Arpanet permettendo in tal modo il libero scambio di traffico tra quest'ultima ed Nsfnet, usando protocolli comuni. Per questi motivi il governo statunitense affidò all'NSF il compito di continuare lo sviluppo di Internet per i successivi cinque anni. D'altro canto la stessa NFS aveva bisogno

di migliorare il rendimento della propria rete che già nella prima metà del 1987 era arrivata alla saturazione.

Di conseguenza il 15 giugno 1987 NFS pubblicò un bando di appalto per la realizzazione di una nuova dorsale che recepisce i protocolli tcp/ip già impiegati in Arpanet, ma che modificasse l'architettura di quest'ultima trasformandola da una sola dorsale alla quale si collegavano le singole reti componenti Internet, a una serie di dorsali regionali da far confluire su una dorsale nazionale, distribuendo meglio il traffico e favorendo la diffusione dei nodi. La nuova dorsale si sarebbe chiamata Nsfnet, avrebbe usato linee ad alta velocità T1 (1,5 Mbit per secondo) e avrebbe collegato, tanto per iniziare, le tredici reti regionali e i centri di supercalcolo visti in precedenza. Nsfnet sarebbe stata al servizio di qualsiasi istituto universitario e di qualsiasi centro di ricerca, senza distinzione, ma sarebbe rimasta preclusa al traffico di tipo commerciale.

Queste regole furono definite in un documento passato alla storia con il nome di AUP (Acceptable User Policy). Le università avrebbero avuto voce in capitolo nella scelta delle soluzioni tecnologiche e implementative della rete, così da raccogliere il massimo consenso e la piena cooperazione di chi avrebbe dovuto promuoverne l'uso a livello locale (anche questo era un cambiamento importante rispetto all'impostazione di Arpanet). L'appalto quinquennale del valore di 57,9 milioni di dollari fu concesso a un pool di quattro aziende. IBM avrebbe fornito i sistemi di commutazione necessari per interconnettere i vari nodi (Nodal Switching Subsystem), MCI avrebbe provveduto alle linee fisiche di connessione organizzando anche un centro di gestione operativo. Merit Network si sarebbe occupata della gestione operativa dei servizi e del supporto agli utenti finali. Lo stato del Michigan contribuì anch'esso con uno stanziamento di 5 milioni di dollari che andava ad arricchire il budget a disposizione di NSF e che avrebbe favorito strategicamente lo sviluppo di know how e di risorse d'interconnessione. La linea di connessione da 1,5 Mbps

veniva suddivisa in diversi canali da 448 Kbps ciascuno, così da consentire la massima comunicazione simultanea tra i diversi nodi.

La rete entrò fisicamente in funzione nel luglio del 1988 e restò attiva fino al luglio del 1989 quando fu rimpiazzata da una nuova dorsale capace di fornire 1,5 Mbps pieni su ciascuna connessione. Furono anche aggiunti due nodi nuovi.

Nel 1990 IBM, MCI e Merit Network crearono un'organizzazione senza fini di lucro chiamata Advanced Network and Services (ANS) che aveva la missione di gestire e commercializzare i servizi di Nsfnet oltre che di potenziare, assieme a Merit Network, la dorsale già esistente. Nel gennaio 1991 entra in gioco un altro contendente, Sprint, a cui viene affidato il compito di sviluppare le connessioni con le reti della ricerca in Europa, e successivamente con l'Asia, attraverso quello che all'epoca si chiamava ICM (International Connections Manager).

Già nel 1992 gran parte delle istituzioni accademiche e di ricerca americane erano collegate a Nsfnet e la comunicazione con le reti Internet governative veniva garantita dalla presenza di speciali nodi di scambio (Federal Internet Exchange) sulle due coste: fix-East e fix-West. La connessione con l'Europa e con l'Asia veniva garantita da Sprint (<http://www.sprint.com>). Le organizzazioni commerciali, non potendo transitare su Nsfnet, avevano creato il CIX (Commercial Internet Exchange) a San Francisco e Sprint offriva la connessione tra la dorsale americana e le reti della ricerca in Europa e in Asia.

Nel novembre del 1992 fu attivata una terza versione della dorsale dotata di linee T3 a 45 Mbit per secondo. Questa sarebbe stata la versione finale di Nsfnet destinata a rimanere in funzione fino all'aprile del 1995, data in cui sarebbe stata rimpiazzata da una nuova architettura d'interconnessione. Nei sette anni di durata dell'appalto (se n'erano aggiunti due rispetto ai cinque previsti inizialmente) IBM, MCI e Merit Network collaborarono ricavando know how fondamentale per lo sviluppo futuro della propria presenza su Internet. Durante la sua vita, Nsfnet ha consolidato la crescita di grandi dorsali regionali,

ciascuna delle quali è diventata di fatto una piccola Internet che serve una particolare porzione degli Stati Uniti.

Nel maggio del 1993 lo staff tecnico della National Science Foundation ipotizzò una trasformazione nell'architettura di Nfsnet che avrebbe dovuto portare alla costruzione di una dorsale ad altissima velocità Vbns (very high-speed Backbone Network Service) e diversi Nap (Network Access Point) per consentire alle singole reti regionali di collegarsi alla dorsale servendosi e al tempo stesso di scambiare traffico tra loro. I Nap e la Vbns avrebbero continuato a ricevere sovvenzioni governative rispettivamente per quattro e cinque anni, mentre le reti regionali si sarebbero trasformate da Rsp (Regional Service Provider) in Nsp (Network Service Provider) fornendo i propri servizi a pagamento e ricevendo sovvenzioni pubbliche quadriennali solo se si fossero agganciate ad almeno tre Nap. In questo modo veniva garantita la connessione a Internet per tutte le università statunitensi e al tempo stesso si favoriva un'evoluzione commerciale dell'infrastruttura esterna alla dorsale così da svincolarla entro quattro anni dai finanziamenti governativi. Un'altra componente chiave dell'architettura era la creazione di un Routing Arbiter (RA) per gestire tabelle e database d'instradamento globali a beneficio delle varie reti periferiche.

La dorsale Vbns è entrata in funzione nell'aprile del 1995 e collega i cinque centri di supercalcolo statunitensi con linee ottiche a 155 Mbps gestite da MCI (tutti quelli già connessi da Nsfnet nel 1986 con la sola eccezione del John von Neumann Supercomputer Center).

L'accesso alla Vbns era consentito solo a quelle organizzazioni che dovevano eseguire applicazioni ad altissima velocità come il calcolo scientifico e la visualizzazione d'immagini in movimento. La gestione del Routing Arbiter fu invece affidata a Merit Network con uno stanziamento quinquennale iniziato nel luglio del 1994.

I Nap regionali furono gestiti da Pacific Bell a San Francisco (<http://www.pacbell.com>), Ameritech Advanced Data Services (aads) a

Chicago (<http://www.ameritech.com>), Sprint nel New Jersey, vicino a New York (<http://www.sprint.com>) e Metropolitan Fiber Systems (mfs) nella cittadina di Vienna in Virginia, nei pressi della capitale Washington (<http://www.mfsdatanet.com>).

La nuova Vbns costituiva la prima realizzazione della Nren (National Research and Education Network) che costituisce a sua volta il primo tassello della Electronic Information Infrastructure (infrastruttura informativa elettronica) che il presidente Bill Clinton ha definito in una legge del 1991 chiamata High Performance Computing Act.

Le singole università usavano i loro provider regionali per arrivare alla dorsale e ai Nap, in questo modo sono autonome nella scelta del servizio e del tipo di supporto che ricevono, e al tempo stesso viene garantito loro l'accesso privilegiato alle risorse della Vbns qualora le rispettive applicazioni lo richiedano.

MCI ha gestito una rete sperimentale ATM da 622,8 Mbps che unisce i poli di Reston (Virginia), Dallas e Pittsburgh, anch'essa costruita in collegamento con NSF. Infatti il programma governativo che NSF segue per la creazione di questa nuova infrastruttura dedicata alla ricerca che la dorsale Vbns arrivi a 2,5 Gbps (2,5 milioni di bit per secondo) vale a dire una velocità trasmissiva sufficiente a trasmettere l'intero contenuto di due biblioteche ogni secondo. Il programma si chiama hpcc (High Performance Computing and Communications) e viene coordinato dal NLANR (National Laboratory for Applied Network Research - <http://www.nlanr.net>) che riunisce tutti i cinque centri di supercalcolo americani.

Sono stati i tecnici del NLANR a curare tra il marzo e l'aprile del 1995 la posa della fibra ottica sia della tratta principale della Vbns sia della tratta secondaria di test e, successivamente, a realizzare il collaudo e le prove di rendimento della rete. Il Pittsburgh Supercomputing Center ha provato a collegare il proprio anello Fddi interno ai corrispondenti anelli del San Diego Supercomputer Center e del National Center for Atmospheric Research usando

la Vbns come intermediario e dimostrando che era possibile arrivare alla piena velocità di 100 Mbps su rete geografica.

Con l'avvento della Vbns, il primo passo verso la trasformazione della rete Internet americana è stata la creazione dei quattro Nap (Network Access Point) ciascuno incaricato di presidiare una porzione del territorio statunitense. Il primo di questi Nap che s'incontra venendo dall'Europa è quello di New York (in realtà nel New Jersey) gestito da Sprint, la società che dal 1991 costituisce l'interfaccia primaria tra le reti della ricerca sui due continenti. Le prime connessioni erano verso Stoccolma e Sophia Antipolis (polo tecnologico sulle telecomunicazioni costruito nei pressi di Nizza e che riunisce i centri di ricerca di svariate multinazionali americane), e si affiancavano alle linee verso il Regno Unito e verso la Scandinavia già create dalla JvNCnet. Successivamente le linee intercontinentali di Sprint sono state estese a Londra, Parigi, Tokyo, Bonn, Milano, la Cina, la Malesia, il Sud Africa e il Medio Oriente. Benché il ruolo non sia più ufficiale, questa presenza diffusa conserva a Sprint il ruolo di ponte verso gli altri continenti per la rete della ricerca statunitense, anche dopo lo scioglimento della Nsfnet.

Nel 1992 Sprint è stata la prima a lanciare un servizio di accesso per i privati, denominato SprintLink, con 320 punti di presenza nei soli Stati Uniti e con numerose ramificazioni in Europa e in Italia. La tipologia è a due livelli, con un primo livello dedicato ai clienti privati e un secondo livello costituito da una dorsale che interconnette i nodi della rete SprintLink. All'interno di ciascuno di questi ultimi viene impiegata una rete locale Fddi (Fiber Distributed Data Interface) in fibra ottica a 100 Mbps. La rete SprintLink si collega anche ai vari punti d'interscambio del traffico esterni alla dorsale per la ricerca: fix-East e fix-West per l'interconnessione con le strutture governative americane, cix (Commercial Internet Exchange) a Santa Clara e mae-East (Metropolitan Area Exchange) per il traffico commerciale. Proseguendo verso l'interno troviamo Ameritech Advanced Data Services responsabile del nodo di Chicago assieme a Bellcore (<http://www.belcore.com>) di cui è una controllata. Questo nodo serve tutti i Network Service Provider dell'area urbana di Chicago con

linee telefoniche dedicate a 45 Mbps oppure linee ottiche a 155 Mbps. Il protocollo trasmissivo è ATM. Oltre a garantire la connessione diretta per l'Università di Chicago (<http://www.uchicago.edu>), l'Università dell'Illinois (sempre a Chicago, <http://www.uic.edu>), il Fermi National Laboratory (<http://www.fnal.gov>) l'Argonne National Library (<http://www.anl.gov>), Ameritech si aggancia alla rete commerciale di Sprint negli USA (<http://www.sprintlink.net>), a MCI (<http://www.internetmci.com>), alla dorsale Vbns (<http://www.widdehren.reston.mci.net>) e al Routing Arbiter gestito da Merit (<http://www.ra.net>) più ad altri fornitori di accesso locali.

A Washington troviamo la MFS Communications Company che offre una copertura nazionale piuttosto ampia (più di quaranta città americane collegate direttamente in fibra ottica) che si estende anche a Londra, Francoforte, Parigi, Zurigo e Stoccolma, oltre che Città del Messico. Anche questo Nap è costruito su tecnologia ATM e si collega da una parte alla dorsale Vbns e dall'altra a una serie di fornitori di accesso regionali e locali che hanno il vincolo di agganciarsi a MFS con linee della velocità minima di 1,5 Mbps. Quest'ultima ha costruito e sta costruendo una propria rete di mae (Metropolitan Area Exchange) che coprono le città di Chicago, Dallas, Houston, Los Angeles (in cogestione con l'Information Sciences Institute), New York, San Jose, Parigi e Francoforte. Il Nap più remoto è quello di San Francisco dove Pacific Bell interconnette svariati Network Service Provider regionali usando linee ad alta velocità da 36 Mbps e 139 Mbps con tecnologia atm. Il valore è più basso della velocità nominale delle linee ds3 e oc-3 (45 Mbps e 155 Mbps) perché tiene conto dell'effettivo volume di traffico che riesce a convogliare su una di queste linee usando il protocollo atm. Non a caso Pacific Bell si sta specializzando nei test di ottimizzazione del traffico tcp/ip su dorsale ATM. Dovendosi collegare ai Nap per accedere alla dorsale della ricerca e dovendo al tempo stesso contare sulle proprie forze per la reciproca interconnessione, le singole reti regionali si sono riunite in diversi consorzi, oppure si sono attrezzate per presentarsi sul mercato per proprio conto. Uno dei primi consorzi creati allo scopo di far fronte all'imminente scioglimento della Nsfnet è stato il COREN (Corporation for Research and Enterprise Networking), nato nel 1992 su iniziativa di MCI per

riunire tutte le principali otto delle reti regionali attive all'epoca BARNET, CINET, MIDNET, NEARNET, NYSERNET, NORTHWESTNET, SURANET, WESTNET (con la sola eccezione di PCSNET). Il COREN, a cui successivamente si è aggiunta anche SEQUINET, aveva lo scopo di creare una dorsale comune per scambiare traffico al di fuori di NSFNET.

Ebone (European Backbone Network - rete dorsale europea)

Ebone è una dorsale Internet paneuropea creata nel 1991 e che collegava tra loro 52 Internet Service Provider in 27 nazioni, agganciandoli alla rete Internet statunitense. L'organizzazione che la gestisce non ha fini di lucro e si trova in Francia. Non esiste nessun vincolo sul tipo di traffico trasmesso, perciò può essere utilizzata anche per attività di natura commerciale. La dorsale ha il suo centro a Parigi, da qui si diramano a stella connessioni dirette verso Vienna (2 Mb per secondo), Monaco (1 Mbps), Stoccolma (4 Mbps), Ginevra (2 Mbps) e Amsterdam (4 Mbps) dove Ebone dispone di nodi propri a cui sono collegate altre reti nazionali. Al nodo di Parigi si collegano direttamente anche diverse reti italiane tra quella del CINECA e InterBusiness di Telecom Italia. La capacità trasmissiva globale all'interno dell'Europa è di 28 Mbps. Per la connessione transatlantica verso gli Stati Uniti vengono impiegate diverse linee ad alta velocità per un totale di 13 MBps. I costi di collegamento vengono condivisi da ciascuno dei partecipanti. L'indirizzo del sito Web è <http://www.ebone.net>, l'indirizzo di posta elettronica è info@ebone.net.

EUnet

Un grande fornitore di accesso olandese con 250 Point of Presence (punti di presenza) e con migliaia di siti collegati in tutto il continente, inclusi i paesi dell'Est. È nato come consorzio di svariati fornitori di accesso nazionali, ciascuno dei quali concorre al suo finanziamento.

Oltre a fornire servizi alle aziende, questa rete viene anche utilizzata nel mondo dell'istruzione e della ricerca. L'indirizzo del suo sito Web è

<http://www.eu.net>. Il nome della rete è InterEUnet. Serve come punto di accesso internazionale per il fornitore di accesso italiano IUnet, gestito da Olivetti.

La dorsale per la ricerca Nsfnet che gli Stati Uniti hanno utilizzato dal 1986 al 1995 serviva una serie di reti regionali che a loro volta portavano l'accesso alle università e ai centri di ricerca sul territorio. Dal 1995, con il taglio degli stanziamenti governativi e la necessaria chiusura di Nsfnet, tutte queste reti regionali (Regional Network Provider) si stanno trasformando in fornitori di accesso commerciali (Network Service Provider), potendo contare su uno stanziamento federale di quattro anni che favorirà la transizione e di cui possono usufruire solo a patto di continuare a fornire la connessione per le università pubbliche alla nuova dorsale che si chiama Vbns (very high-speed Backbone Network Service).

1.3 I BBS, IL PROTOCOLLO UUCP

L'altra origine di Internet si trova nel "BBS" (Bulletin Board System), un sistema di bacheca elettronica sorto alla fine degli anni settanta. Nel 1977 due studenti dell'Università di Chicago, Ward Christensen e Randy Suess, hanno scritto un programma battezzato MODEM.ASM, che permetteva il trasferimento di file tra i loro personal computer e nel 1978 hanno messo a punto anche il Computer Bulletin Board System, che consentiva al pc di trasmettere e archiviare messaggi. Entrambi i programmi sono stati distribuiti dai loro creatori, in forma open source.

Nel 1983 Tom Jennings ha ideato FIDO, un proprio programma per le BBS e che ha dato vita a una rete, FIDONET.

Per la comunicazione tra computer è fondamentale ciò che è emerso dalla comunità di utenti UNIX, nome di un sistema operativo sviluppato nei Bell Laboratories e rilasciato da Bell alle università nel 1974, con il codice sorgente e il permesso di implementarlo.

1.4 L'INTERNET 1.0

Nel 1978 è nato UUCP (Unix-to-Unix copy protocol), che consente ai computer la copia dei file. Basandosi su questo, nel 1979 nasce un programma di comunicazione per computer UNIX. Nascono così reti di comunicazione tra computer, chiamate Usenet News, al di fuori di ARPANET. Poi ARPANET e Usenet si sono unite creando Internet, a partire da un gruppo di laureati dell'Università di Berkeley, che hanno creato un ponte tra ARPANET e Berkeley, che era nodo della rete del governo.

Unix ha dato anche vita al movimento open source, che ha tentato di tenere aperto l'accesso a tutte le informazioni relative al software. Nel 1984, un programmatore del laboratorio di intelligenza artificiale del MIT, Richard Stallman, ha fondato la Free Software Foundation, introducendo il concetto di copyleft, opposto al copyright. Stallman sottintendeva a tutto questo che chiunque avesse utilizzato il software messo liberamente a disposizione in cambio avrebbe dovuto distribuire in rete il codice migliorato. Stallman creò un'alternativa a UNIX, il sistema operativo GNU e lo rese pubblico in rete, con la sola clausola di rispettare il copyleft.

Su questa base, nel 1991 Linus Torvalds, studente allora ventiduenne dell'Università di Helsinki, sviluppò un nuovo sistema operativo basato su UNIX, in modo da trovare qualcosa che "girasse" sulle sue macchine di poco costo, non potendosi permettere di meglio a livello hardware. Così è nato il kernel Linux.

1.5 Il CERN di Ginevra: l'Internet europea

Nel 1984 l'Europa cominciò l'aggiornamento della sua rete al protocollo TCP/IP. Il processo si concluse solo alla fine del decennio. La Cisco Systems, una piccola impresa all'epoca specializzata nella costruzione di router, venne incaricata dal CERN, l'istituto per la ricerca scientifica avanzata della Comunità Europea, di sviluppare la parte europea di Internet attraverso il passaggio dalla

rete UUCP esistente verso il nuovo protocollo. Nel 1989 il CERN aprì la sua prima connessione TCP/IP esterna.

Ciò coincise con la creazione del RIPE (Réseaux IP Européens, Rete degli IP europei), da parte di un gruppo di amministratori di reti IP. La rete venne ideata durante le riunioni periodiche del gruppo. Successivamente, nel 1992, il RIPE venne registrato ufficialmente come cooperativa.

Alla fine degli anni ottanta anche le università del continente australiano completarono la revisione tecnologica della rete, eseguendo il passaggio al protocollo TCP/IP. D'altra parte tecnologie come l'X.25 e la UUCP si erano dimostrate molto costose e questo ne aveva limitato la diffusione. È nel 1989 che le università australiane si uniscono alla rete TCP/IP creando la AARNet.

In quegli stessi anni Internet cominciava il suo ingresso nell'esteso continente asiatico. Il Giappone, che nel 1984 aveva fondato JUNET, una rete dentro la rete UUCP, si connetté alla NSFNet nel 1989. La città giapponese di Kobe fu scelta come sede del meeting annuale dell'Internet Society per l'anno 1992. Singapore sviluppò la sua rete TECHNET nel 1990; la Thailandia si unì alla rete mondiale nel 1992 grazie all'iniziativa dell'Università Chulalongkorn.

1.6 La biblioteca mondiale: da Gopher al Web

Archie e Wais

I ricercatori nel periodo che segue la creazione di internet cercarono di rendere l'utilizzo della strada più user-friendly in modo da raggiungere non solo studenti e ricercatori ma una vasta gamma di utenti. Già nel 1989 fu avviato il primo passo in questa direzione, quando Peter Deutch della Mc Gill University di Montréal, inventa Archie, un programma in grado di indicizzare il contenuto di molti archivi pubblici di file presenti su Internet e sino ad allora "sparsi" per la rete.

Poco tempo dopo fu sviluppato il primo sistema di "ricerca informazioni distribuito" il cosiddetto Wais (Wide Area Information Server). Wais era in

grado da un lato, di indicizzare enormi quantità di file, dall'altro, di effettuare ricerche su di essi. Si pensi che nel server Wais venne ospitato l'intero database delle RFC (Request For Comment). Vista la sua complessità, Wais venne ben presto abbandonato.

Gopher e Veronica

Il primo strumento (non si parla ancora di Browser) di "Interfaccia Universale" alle risorse di rete fu Gopher. Esso adottava menù descrittivi a struttura gerarchica e soprattutto si basava su un'architettura di tipo client-server. Al successo di Gopher contribuì enormemente un programma in grado di effettuare ricerche nel cosiddetto "Gopher-Space": Veronica (Very Easy Rodent Oriented Netwide Index to Computerized Archives).

Gopher fu inventato da Paul Lindner e Mark Mc Cahill. Il suo nome è dovuto alla mascotte dell'Università del Minnesota ed in inglese significa "marmotta": un simpatico roditore che scava gallerie nel terreno. Poiché (metaforicamente) il Gopher "scava" gallerie attraverso Internet, i suoi inventori decisero di affibbiargli questo nome.

Mentre Gopher raggiungeva l'apice del suo successo, nei laboratori del CERN di Ginevra veniva sviluppato però il World Wide Web (WWW), la grande ragnatela mondiale.

1.7 Diffusione del World Wide Web

Anche se Internet è nato nella mente e nelle utopie di tante persone nei primi anni sessanta, per la massa, per le imprese e per il mondo nel complesso, Internet nasce effettivamente nel 1995. È dall'ampia diffusione delle tecnologie del World Wide Web che si comincia a parlare sempre di più del commercio elettronico anche per gli utenti finali e non solo per le transazioni fra grandi imprese.

Nel periodo che va dal 1991 (anno in cui Il Web divenne pubblico) sino ai primi anni del 2000, gli utenti non esperti di informatica intrapresero la loro prematura esperienza con la rete Internet. Sino ad allora solo ingegneri informatici, esperti di linguaggi di programmazione e ricercatori potevano usare Internet con relativa praticità.

Gradualmente, dopo l'invenzione di T. Burnes Lee del linguaggio HTML (con il quale si creò il World Wide Web), la diffusione della posta elettronica e lo sviluppo dei browser, anche "l'utenza non esperta" cominciò a consultare documenti elettronici e ad utilizzare il Web per lavoro o altri scopi comunicativi. Tuttavia l'attività digitale "dell'utente comune" era comunque limitata e circoscritta a pochi usi interattivi con la rete, tra cui l'invio-ricezione dei messaggi di posta elettronica e la compilazione di moduli che richiedevano l'inserimento dei dati personali.

Successivamente comparvero altre forme di comunicazione digitale indiretta come i newsgroup e i forum ("salotti di discussione" digitali). Cominciò così a svilupparsi un'interazione di massa, mai avvenuta prima, tra "utenti inesperti". Questi si interessavano di argomenti specifici di loro gradimento, richiedendo pareri agli esperti o scambiando opinioni tra di loro.

Comunque, l'interazione non avveniva in tempo reale" e per avere corrispondenza nell'interlocuzione, l'utente, doveva aspettare che l'esperto o l'altro utente li rispondesse per poter continuare la comunicazione (come avviene nel meccanismo dei messaggi della posta elettronica).

Con l'invenzione delle "Chat" (ambienti digitali di conversazione in tempo reale) e di altri strumenti mediatici (come i social network), l'interazione tra gli utenti non è più una forma indiretta di comunicazione (come avveniva nei newsgroup e forum), ma diviene una "forma diretta" d'interazione (p. es: tra utenti di uno stesso gruppo di amici, che sono connessi ad un social network nello stesso momento), che consente una partecipazione immediata e in tempo reale tra gli utenti.

1.8 La nascita del Web 2.0

Tra il 2004 e il 2005, un grande editore americano, "O'Reilly Media", organizzò una serie di conferenze negli U.S.A. per spiegare le nuove opportunità che la Rete Internet e il Web, in particolare, metteva a disposizione degli utenti. In questi incontri venne coniato e ufficializzato il concetto di "Web 2.0". Vennero descritti e pubblicizzati i nuovi modi della comunicazione digitale e gli innovativi servizi di cui potevano usufruire anche gli utenti comuni, "non esperti di informatica". Durante questi convegni, si evidenziò la novità della partecipazione attiva dell'utente nella fase comunicativa e la gestione autonoma dei contenuti multimediali. Con queste conferenze, insomma, si inaugurò la "seconda fase di sviluppo del Web", che si lasciava ormai alle spalle i linguaggi e le programmazioni dei primi periodi, quando T. Burnes Lee propose al mondo il World Wide Web. Diciamo che il Web da bambino divenne adolescente. Nei nostri giorni, infatti, i contenuti del web (2.0) ruotano attorno a due concetti chiave: la condivisione dei contenuti multimediali e la partecipazione attiva dell'utente nella gestione degli stessi.

La Rete Internet non è più usata solo da esperti informatici, ricercatori, giornalisti o editori, ma, grazie allo sviluppo dei browser e delle innumerevoli applicazioni grafiche, è alla portata di tutti. I nuovi servizi gratuiti generano strumenti mediatici di una potenzialità unica. Il loro utilizzo, soprattutto, non richiede alcuna competenza specifica, al contrario di quanto avveniva in passato (web 1.0). Addirittura adesso alcuni di questi servizi vengono interamente sviluppati dagli utenti e non da esperti informatici. I "wiki", per esempio, sono modificati e sviluppati liberamente dagli utilizzatori. Il caso esemplare di questo tipo di servizi è rappresentato da "Wikipedia", un'enciclopedia libera e gratuita, interamente redatta dagli utenti che la utilizzano. Gli altri servizi più utilizzati nel Web 2.0 sono i CMS, gli RSS e i nuovissimi servizi Cloud.

I CMS (Content Management System), più maccheronicamente i Blog, sono dei sistemi di gestione dei contenuti multimediali. Più precisamente sono dei

modelli di siti web "pre-confezionati". Bisogna solo scegliere il tema grafico da utilizzare e riempirlo di contenuti appunto. Sono soluzioni user-friendly (di facile uso), ma dispongono anche di funzionalità avanzate come la gestione degli utenti iscritti al blog, dei loro commenti e degli articoli pubblicati da altri. Non bisogna necessariamente conoscere linguaggi di programmazione per realizzare un blog, lo può fare chiunque, anche se la conoscenza di qualche nozione di programmazione può far risultare più accattivante un blog nella sua omogeneità. Un altro strumento del web 2.0, molto diffuso e che si usa frequentemente anche per curare gli articoli che vengono pubblicati nei blog, è il lettore di feed o "Feed RSS".

Nel dettaglio i Feed RSS, sono aggregatori di notizie, di articoli su argomenti specifici, account di mail, di commenti agli articoli dei blog ecc., che provengono da siti diversi o blog differenti. C'è sono di diversi tipi, ma tutti funzionano da aggregatori, cioè: invece che cercare singolarmente in ogni sito ciò che ci interessa, basta memorizzare, in uno di questi programmi, gli indirizzi delle pagine web in cui cerchiamo informazioni, per estrapolarne poi quello che ci serve. Quando si avviano questi programmi o vengono aggiornati, le pagine web che ci interessano, già predisposte a tale uso, trasferiscono sul "lettore Feed RSS", una lista di articoli, della quale possiamo servirci per i nostri scopi.

I nuovi "servizi Cloud" o di "Cloud computing", sono invece, un insieme di tecnologie che ci consentono di memorizzare i dati su un archivio multimediale, esterno al nostro computer, che risiede su qualche server sulla rete Internet. Con questa tecnologia, tutti i documenti che elaboriamo vengono conservati su uno spazio web personalizzato, senza occupare memoria, per l'archiviazione dei dati, sul nostro sistema operativo.

Il Cloud permette di lavorare senza installare alcun software. Possiamo usufruire dei programmi e di altre risorse di cui abbiamo bisogno, direttamente usando la rete; se vogliamo usufruire di qualche servizio più completo (di quelli

offerti gratuitamente), lo possiamo ottenere pagando "a consumo", per intenderci, quello che ci serve.

Il Web 2.0 quindi, evidenziando la sua duttilità e semplicità d'uso, offre all'utente comune, non esperto, l'opportunità della libera espressione dell'individuo, che può: pubblicizzare la sua persona, la sua professione o attività e/o la sua competenza per un argomento specifico, in maniera semplice, veloce e gratuita.

1.9 IL WEB 2.0 E I SOCIAL NETWORK

Sin dalla loro introduzione, i social network (MySpace, Facebook, Twitter), hanno attratto milioni di utenti alcuni dei quali li hanno integrati addirittura nelle pratiche di tutti i giorni.

Esistono siti di nicchia virtualmente per ogni tipo di specialità e interesse; ci sono siti che consentono di condividere foto, video, aggiornamenti di stato e altri che permettono di conoscere nuove persone e ritrovare vecchi amici. (A. Pernici, *La storia e l'evoluzione dei Social Media*, 2009)

La storia dei social network inizia nel 1997, quando uno statunitense di nome "Ellison" lancia il sito SixDegrees.com. Questo sito è stato infatti il primo social network riconosciuto dagli studiosi odierni (il termine social network non era infatti stato ancor coniato all'epoca).

L'obiettivo era quello di creare delle relazioni fra persone, permettendo la creazione un proprio profilo e di catalogare i propri amici e, solo nel 1998 permise anche di poter navigare in quella stessa lista.

Nonostante un relativo successo, il sito chiuse i battenti nel 2000, comprato dalla YouthStream Media Networks per 125 milioni di dollari.

Da quell'anno fino al 2001, vi è stata una successione di "community tools" aventi uno scopo simile a SixDegrees.com, con varie combinazioni di profili con pubblicità o liste di amici in cui poter navigare.

AsianAvenue, BlackPlanet e MiGente permisero agli utenti di creare profili personali, professionali o di dating, dove si potevano identificare i propri amici nei profili personali senza bisogno di alcun tipo di approvazione. (Danah M. Boyd e Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 2008, p. 214).

Allo stesso modo si comportò anche LiveJournal's (1999), che instaurò un tipo di connessione unidirezionale tra gli utenti, a ragion del fatto che la novità era che le persone "marcavano i nuovi amici come followers" (un po' come il futuro Twitter) per seguire il loro Journal, mentre l'utente lo modificava personalmente nel tempo (B. Fitzpatrick, *Personal Communication*, 15 Giugno 2007).

Mentre Six Degrees permetteva agli utenti di creare un profilo statico, LiveJournal era un social costruito sull'idea di un continuo aggiornamento dei blog.

Sulla scia di queste tipologie di network, altre community furono tentate di emulare quelli che erano i tratti caratteristici dei Social Network Sites.

Ad esempio la web community svedese LunarStorm si "ristrutturò" negli anni 2000 come un SNS contenendo profili, liste di amici e anche pagine di diario (quelle che immetterà anche Facebook).

Anche il sito Coreano del mondo virtuale Cyworld (1999) applicò nel 2001 quelle che erano le caratteristiche di un social network, indipendentemente dagli altri siti.

Dopo questi primi tentativi di Social Networks, l'apertura di un'ulteriore ondata di creazioni di SNS si ha con Ryze.com (2001), di Jonathan Abrams, un social network dedicato ai professionisti (in particolare businessmen). Si sottolineò di come le persone dietro Ryze.com, Tribe.net, o LinkedIn e Friendster, erano strettamente intrecciate sia in ambito professionale che personale, in qualità del fatto che questi "users" credevano che si potessero fornire supporto reciproco senza cadere in competizione tra di loro (Festa, 2003).

Alla fine però, Ryze.com non acquistò mai abbastanza popolarità; Tribe.Net crebbe, ma solo per attrarre community di nicchia; LinkedIn divenne un potente servizio di Business (un social orientato al mondo del lavoro, dove il profilo diventa il curriculum vitae e le relazioni che si instaurano sono professionali) e Friendster divenne, come lo definì Chafkin nella prima pagina di un suo articolo (2007): "Una delle più grandi delusioni nella storia di internet".

Friendster fu inequivocabilmente il primo social network moderno di carattere generale, e nonostante la repentina caduta che ricevette, è tuttora un social network molto attivo, con più di 90 milioni di utenti registrati e più di 60 milioni di visitatori unici al mese. Il 90% dei visitatori di questo social arrivano dall'Asia.

L'obiettivo principale di Friendster è quello di permettere alle persone di scoprire i propri amici e conoscere gli amici degli amici in modo da permettere l'espansione della propria rete, allo scopo di essere un posto più sicuro e veloce per conoscere persone rispetto alla vita reale.

A differenza di molti SNS, che operavano facendo conoscere gli utenti in base agli interessi comuni di questi ultimi, Friendster aiutava a trovare amici di amici (formula friends-of-friends), perché gli amministratori contavano sul fatto che se fosse sbocciato qualcosa tra utenti già in amicizia tra loro, di sicuro sarebbe stato "molto più romantico che tra sconosciuti" (J. Abrams, personal communication, 27 Marzo, 2003). La popolarità di Friendster toccò il massimo con tre diversi gruppi: Gay Men, attendess of Burning Man e blogger (A. Pernici). Come definisce Valerio Novelli in un suo articolo, "Friendster era il primo social che mostrava le foto degli utenti ed il loro vero nome, permetteva di cercare persone e vedere li loro profilo per poi collegarsi alla loro rete..".

Questa visualizzazione era però limitata fino al quarto grado di amicizia (formula: friends-offriends-of-friends-of-friends).

Il Social Network ebbe sin dall'inizio un gran successo, anche se proprio questo successo fu un'arma a doppio taglio: vi era un così elevato numero di utenti e

di richieste, che Friendster non era "preparato a sopportarle", quanto i database non erano configurati alla necessità.

Le pagine, di conseguenza, erano molto lente nel caricamento, frustrando gli utenti che erano quindi costretti a mandare e-mail. Inoltre, questa crescita esponenziale provocò un collasso nel contesto sociale: gli utenti potevano ritrovarsi come amici i loro capi o i loro professori! (Boyd e Ellison). Dopo non molto vi fu l'inizio di creazione da parte degli utenti di profili falsi, tanto che si parlava addirittura di "Fakester", ovvero utenti che creavano questi profili allo scopo di acquisire più interazione con gli altri utenti. Questa azione "fake", era dovuta principalmente al fatto della limitazione di visualizzazione di utenti (formula relativa al requisito del quarto grado di amicizia).

Altre motivazioni che spingevano questa falsificazione di nuovi profili erano di tipo iconico: ci fu un'ondata di profili falsi riguardante persone famose, dal cinema alla musica. Fu un vero e proprio oltraggio per la compagnia, che bloccò dal social un gran numero di fake profiles, ed eliminò tutti i profili delle "Grandi Star".

Da questo punto di vista, si capì subito però che la compagnia di Friendster non era dalla parte degli interessi degli utenti. Molti utenti presto lasciarono il sito, sia per le difficoltà tecniche del social, sia per il collasso sociale esposto precedentemente. Il periodo "Fakster" segnò inoltre una rottura di fiducia tra gli utenti e il social network stesso.

Nonostante questa evanescenza di Friendster negli USA, il SNS continuò comunque ad essere attivo in altri paesi (Filippine, Singapore, Malaysia e Indonesia).

Proprio in quel periodo vi fu uno spostamento radicale da Friendster a un altro nuovo SNS: MySpace, nato da Tom Anderson e Chris De Wolfe (2003) con uno scopo preciso: dare ai giovani uno spazio dove poter fare ciò che volevano.

MySpace conteneva inizialmente un blog, dei giochi e l'oroscopo. Per colpa di un bug del sistema si poteva personalizzare ogni pagina a piacimento: quando in MySpace se ne accorsero videro anche che moltissimi utenti si divertivano

personalizzando le pagine, coinvolgendo altri utenti. MySpace stava prendendo la giusta piega soprattutto nei giovani, ed è per questo motivo che il bug risultò un aspetto positivo del social network, e quindi non fu mai eliminato.

MySpace venne poi venduto nel 2005 per 600 milioni di dollari alla News Corporation di Rupert Murdoch.

Arriviamo al 4 Febbraio 2004, data in cui nasce un nuovo Social Network: "The Facebook", creato da Mark Zuckerberg (a soli 19 anni), che chiese anche il supporto di alcuni colleghi di università (Andrew McCollum, Eduardo Saverin, Dustin Moskovitz, Chris Hughes). L'idea iniziale del giovane Mark era nata con facemash, un sito che permetteva agli studenti, tramite un confronto tra due fotografie prese da vari studenti, di votare quella più bella. Passò in seguito all'idea di un social network esclusivo (ai primi tempi era infatti riservato alle reti dei college, primo fra questi, Harvard, con l'indirizzo e-mail harvard.edu che si basava sui profili reali: un sistema per restare in contatto con la gente conosciuta, oppure per conoscerne di nuova.

Dal Settembre 2005 Facebook si espanse anche nelle scuole superiori, e successivamente, a chiunque. E' solo nel 2008 e nel 2009 che Facebook inizia a toccare picchi che superano quello che fino ad allora era stato il social network più famoso: MySpace.

All'inizio le opzioni e funzionalità di Facebook erano limitate, ma allora cos'è che a differenza di Friendster a permesso a Facebook di prosperare? Probabilmente furono, oltre che ad un database e una tecnologia migliore, le continue innovazioni: alcune funzioni che lo renderanno il social network più popolato al mondo saranno l'applicazione Foto con la funzione di tagging delle foto ed il news feed. Un altro punto di svolta per Facebook è stato quello di trasformare il Social in una piattaforma in grado di ospitare applicazioni di terze parti, come le applicazioni per iPhone o Android scaricabili.

Oltre a questo, creava anche delle applicazioni proprie, che permisero agli utenti di personalizzare il proprio profilo e sviluppare esperienze personali, come comparare un film con un altro o scrivere la propria "travel chart".

Sono moltissime le persone che utilizzano Facebook ogni giorno: il famoso social network è infatti secondo solo a Google in quanto a visite giornaliere. Seguito da circa un miliardo di utenti in tutto il mondo, Facebook è disponibile in ben 70 lingue diverse così da poter essere utilizzato in tutto il mondo senza problemi di barriere linguistiche! Ma in quanto a numeri, Facebook vanta anche un altro primato: il social network inventato e lanciato da Mark Zuckerberg, è infatti primo tra le reti sociali per numero di utenti attivi; sono infatti oltre un miliardo gli utenti che effettuano l'accesso a Facebook almeno una volta al mese! Insomma Facebook offre la percezione di nuovi e aumentati benefici, e consente di mettersi a contatto con vecchi amici o conoscenti che difficilmente senza questo strumento sarebbe stato possibile contattare.

Gli elementi che caratterizzano Facebook e ne hanno determinato il successo sono riassumibili in quattro parole chiave che sono:

Compatibilità: la sua struttura lo rende adeguato e compatibile con le esigenze della nuova generazione digitale, abituata alla comunicazione real time.

Semplicità: è di facile utilizzo ed è stato tradotto in moltissime lingue.

Testabilità (o triability): gli utenti non pagano assolutamente nulla. Ci si può iscrivere, provare e decidere se si è interessati o meno.

Visibilità: Facebook dà al singolo la possibilità di mostrarsi e di mostrare quello che vuole. Tra le nuove generazioni chi non è iscritto a FB rischia paradossalmente di vedere ridotta la propria vita sociale.

Dopo due anni, da Facebook, il 15 luglio del 2006, durante un brainstorming, nasce l'idea di un servizio che permette di mandare brevi messaggi a piccoli gruppi: è così che nasce Twitter, una piattaforma microblogging creata da Jack Dorsey. Il nome deriva dal verbo inglese to tweet, che significa "cinguettare", ma che è anche il termine tecnico degli aggiornamenti del servizio. Nel 2012 Twitter ha raggiunto i 500 milioni di iscritti, e 200 milioni di utenti attivi che fanno accesso almeno una volta al mese.

Negli ultimi anni ci sono stati altri due Social Network a prendere larghissimo campo: Google+, il Social network di Google, lanciato nel 2011 e Pinterest, nato nel 2012.

1.10 LA CRESCITA ECONOMICA E CULTURALE DI INTERNET

Negli anni più recenti abbiamo assistito ad una crescita senza precedenti di internet sia dal punto di vista dello sviluppo degli hostcount, degli utenti unici, degli accessi, del traffico globale che dei posti di lavoro legati alla rete. Tutto ciò ha portato un incremento del peso complessivo del settore digitale sull'economia mondiale e una crescente rilevanza del nuovo mezzo di comunicazione ai fini del pluralismo informativo.

E' facile constatare che Internet è il frutto di un processo evolutivo estremamente complesso che si è articolato su vari livelli nei quali può essere idealmente scomposta la filiera produttiva.

- A. Il primo stadio concerne le infrastrutture fisiche di rete, le apparecchiature e i protocolli che consentono la connessione mondiale delle reti di computer.
- B. Sono riconducibili al secondo livello, invece, le apparecchiature hardware (device) e i software che permettono all'utente di connettersi al web.
- C. Il terzo livello concerne, le applicazioni disponibili attraverso la rete ossia i servizi, prodotti e contenuti fruibili dagli utenti attraverso la navigazione, che possono essere divisi in due grandi categorie: servizi di tipo verticale tesi a soddisfare una specifica esigenza dell'utente e servizi di tipo orizzontale, diretti a rispondere a una pluralità di scopi indirizzando e soddisfacendo le varie richieste dell'utente (motori di ricerca, portali e social network).

Ciascun livello ha contribuito allo sviluppo del mezzo mediante processi di innovazione radicale che si sono succeduti nel tempo, sconvolgendo gli assetti di mercato, imponendo forme di "separazione" e di "apertura" di sistemi centralizzati e concentrati, seguiti da fasi di consolidamento dell'industria e di "chiusura" dei mercati, che almeno fino ad ora non hanno compromesso la

natura e le caratteristiche della rete internet, che prevedono la contemporaneità di un sistema aperto, flessibile, adattabile, privo di proprietari, alle quali è ascrivibile il successo del web a livello globale.

Questo ciclo evolutivo è stato seguito a più riprese dal settore nel corso degli ultimi cinquant'anni, prima con l'industria informatica dei mainframe, poi con l'avvento dei personal computer e dei relativi sistemi operativi, successivamente con le nuove applicazioni software (ed in particolare con i browser), con l'offerta di servizi web e infine con lo sviluppo di servizi sui dispositivi mobili.

Sotto il profilo economico, internet rappresenta un'industria a rete che si distingue da altri comparti industriali per la presenza ai diversi livelli produttivi di network platform, ossia di piattaforme che servono, agevolando lo scambio, le negoziazioni o l'incontro all'interno di reti di utenti, sistemi di nodi interconnessi costituiti da agenti indipendenti (imprese, inserzionisti, consumatori finali) che aderiscono alla piattaforma al fine di ottimizzare i contatti reciproci. Più piattaforme sono parte della stessa industria a rete quando i beni sono sostituiti.

Tali mercati sono caratterizzati dall'esistenza di fattori che tendono a determinare un incremento del livello di concentrazione fino a una situazione in cui, alle volte, un unico operatore rimane sul mercato, come del resto avviene nella teoria economica classica. Fra questi fattori, stante la capacità di influenzare la propensione attuale e futura degli utenti ad aderire ad una rete condizionando, altresì, gli esiti competitivi dell'industria nel suo complesso, acquistano un particolare rilievo gli effetti di rete che possono definirsi anche "esternalità di rete" o "economie dal lato della domanda".

Si parla di effetti di rete diretti (e positivi) quando il valore di un bene o servizio (e, quindi, l'utilità) per un individuo aumenta direttamente all'aumentare delle persone che posseggono il medesimo bene o aderiscono al medesimo servizio, come avviene nel caso di un social network. Si pongono quindi le basi per uno sviluppo della cosiddetta "sharing economy".

Gli effetti di rete indiretti si manifestano quando l'acquisto di prodotti o servizi complementari da parte di altri utenti aumenta il valore del bene principale, come avviene nel caso delle applicazioni sul valore di un sistema operativo. Infine, si parla di esternalità di rete incrociate in presenza di mercati a due o più versanti, consistenti nel beneficio o danno recato agli utenti del primo versante, derivante dalla partecipazione al sistema da parte dell'altro gruppo di utenti, nel secondo versante. Vale la pena di osservare che i motori di ricerca esibiscono forti effetti di rete incrociati dato che gli inserzionisti preferiscono piattaforme con un maggior numero di contatti, ma anche gli utenti ricercano attivamente reti in cui sono presenti una molteplicità di inserzionisti, a patto che offrano i prodotti oggetto della ricerca o comunque di interesse per l'utente.

I settori che presentano consistenti effetti di rete sono caratterizzati, sotto il profilo dinamico, da feedback positivi): in pratica, al crescere del numero di utenti che già utilizzano i servizi e prodotti di una piattaforma, un numero sempre maggiore di soggetti viene attratto. In tali contesti, la possibilità per un prodotto, servizio o sistema tecnologico di raggiungere la "massa critica" di utenti consente di innescare una dinamica particolare secondo cui un operatore tende ad affermarsi mentre gli altri escono gradualmente dal mercato.

Accanto ai consistenti effetti di rete, la presenza di elevati costi di multihoming (che aumentano il costo di utilizzo di due o più piattaforme), di rilevanti costi affondati (che innalzano barriere all'entrata), di rendimenti di scala (che comportano un'espansione della dimensione ottima minima di impresa fino al limite del monopolio naturale), nonché di preferenze omogenee dei consumatori (che riducono lo spazio per l'offerta di piattaforme in concorrenza) favorisce l'emergere della dominanza di un sola piattaforma in grado di servire (quasi) tutto il mercato.

1.11 INTERNET E LE IMPRESE

Le imprese hanno considerato internet in una prima fase come un mezzo nel quale essere presenti con le stesse modalità utilizzate nel marketing tradizionale.

I siti si presentavano come brochure online in cui affermare e consolidare la propria identità corporate e quella dei propri brand. A seguire si svilupparono nuove forme di comunicazione e, in alcuni settori in particolare, il sito venne considerato come un vero e proprio mercato in cui vendere i propri prodotti. Si ebbe quindi l'affermazione dell'e-commerce, di siti di aste online (ebay).

La terza fase, definita dell'engagement, ovvero dell'intrattenimento e partecipazione, vede brand importanti come Pepsi, HP, Dell e Nike fare leva sui nuovi trend del mercato e sulle diverse possibilità di interagire con i vari stakeholders. In particolare questi brand hanno cercato di coinvolgere individualmente ed emozionalmente i propri target audience, sviluppando e utilizzando strumenti in cui potevano dare vita a un'interazione diretta e disintermediata. I consumatori hanno iniziato a vivere il brand come modo di espressione di sé e alcune aziende hanno saputo percepire questa tendenza e trasformarla in un nuovo modo di approcciare il Web e non solo.

Internet quindi non rappresenta un nuovo paradigma di marketing in sé, ma la dimostrazione che è possibile, per le organizzazioni, usare strumenti trasversali che permettano di comprendere le esigenze della domanda e di soddisfare i bisogni dei consumatori in modo più puntuale, diretto e immediato, in una relazione "one-to-one".

In questo quadro si inserisce il concetto di Web 2.0, termine coniato da Tim O'Reilly – fondatore e CEO della O'Reilly Media, Inc. – per descrivere l'evoluzione dei siti e servizi nel Web come i siti wiki e i social network, in cui sono fondamentali l'interazione, la collaborazione e la condivisione dei contenuti da parte degli utenti.

Il concetto esprime e rappresenta l'era in cui le persone hanno compreso che non è tanto nel software l'importanza del Web, quanto nei servizi e nelle esperienze che sono offerti attraverso il Web stesso. In altre parole il web non è inteso come fine ma come mezzo.

I due principali assunti sui quali si fonda il web 2.0 sono: l'intelligenza collettiva e l'affermazione della rete come ecosistema in cui gli utenti creano valore tramite la condivisione e la creazione di esperienze nel Web che facciano leva sull'engagement e sulla partecipazione.

1.13 L'affermazione della Wikinomics

La collaborazione di massa in rete sta cambiando il mondo: "la rapida e universale diffusione di Wikipedia, l'enciclopedia online a cui tutti possono accedere e collaborare liberamente, è diventata la metafora di un nuovo modo di concepire l'economia e il business. È il mondo in cui milioni di persone interconnesse tramite e-mail, blog, network, community e chat usano Internet come la piattaforma globale di scambio, si autorganizzano e si trasformano in una forza economica di dimensioni globali, capace di modificare radicalmente la società e il business"

Dion Hinchcliffe scrive nel suo Web Services Journal: È molto importante il valore del web 2.0 perché:

- Potenzia la lunga coda: the Long Tail è un concetto espresso per la prima volta da Chris Anderson, redattore capo di Wired, in un omonimo articolo sulla rivista uscita nell'ottobre 2004. Amazon ed eBay hanno usato quest'idea per costruire società che valgono miliardi su miliardi: il web 2.0 fornisce sia il pubblico che i servizi.
- Fornisce piccoli pezzi, slegati: il monoblocco non esiste più, non è agile. Quello che si è costruito non si può aggregare, non si può distribuire, nè può sopravvivere a lungo.
- Agevola self service e partecipazione: incoraggiare questa visione permette di cogliere nuovi valori nelle applicazioni di web 2.0, 24 ore su 24, come ad esempio: tagging, ranking, trackback e reputazioni.
- Fornisce decentralizzazione radicale: le singole fonti di funzioni non forniscono nè la distribuzione nè il ritrovamento di contenuti di valore significativo.
- Sottolinea comportamento emergente: le funzioni del web 2.0 possono essere riutilizzate, remixate, aggregate, ricercate ed il valore che ne risulta può essere nuovamente reintegrato nelle varie applicazioni.

Secondo Tapscott e Williams la Wikinomics (Wikinomia o Economia nel nuovo mondo Wiki) può rappresentare un motore di innovazione e creazione di

ricchezza su una scala mai raggiunta prima, proprio per i principi fondamentali su cui si basa quali:

- apertura, concetto strettamente associato all'idea di trasparenza, libertà, flessibilità e coinvolgimento. L'azienda non dovrebbe più detenere/trattenere le informazioni, ma permettere ai clienti di poter verificare meglio il valore dei prodotti e ai dipendenti di conoscere meglio la strategia e le sfide che l'azienda deve affrontare.

Le aziende che hanno ripensato e rivalutato l'importanza dell'essere aperti verso idee provenienti dall'esterno della propria compagnia e che hanno valutato l'apporto di risorse estranee all'azienda come una fonte di innovazione e miglioramento, si sono dimostrate capaci di mantenere alta la competitività e rimanere su un mercato in continua evoluzione ed aggiornamento, oltre che informato e per questo esigente.

- Il concetto di "peering" invoca una nuova forma di organizzazione orizzontale che si oppone drasticamente a tutti i modelli gerarchici da sempre presenti presso le grandi istituzioni della società. Anche se lo sradicamento dei modelli piramidali largamente diffusi non può essere immediato, sta emergendo sempre più prepotentemente una forma di organizzazione orizzontale fondata sullo scambio di idee e strumenti fra i singoli. Un esempio di peering è Linux: Linus Torvalds creò una semplice versione del sistema operativo Unix, che chiamò Linux, e lo condivise apertamente con i programmatori attraverso un forum online. Dato il successo e l'utilità dell'iniziativa, Torvalds decise di brevettare il sistema operativo tramite una licenza pubblica generale (GPL, General Public Licence) in modo che chiunque potesse usarlo gratuitamente, a patto che condividesse apertamente con gli altri i cambiamenti apportati al programma. Con l'andar del tempo si è sviluppato un'organizzazione informale dedita alla gestione dello sviluppo del software, la quale continua ancora oggi a sfruttare gli input provenienti dagli organizzatori.

- La condivisione predicata nell'era Wiki si scontra con il credo generale, per cui ogni azienda, come ogni singolo, dovrebbe tentare quanto più possibile di proteggere e mantenere un certo controllo sulle proprie idee, sulle risorse interne e difendere i diritti d'autore. Il fatto di condividere il proprio know-how

e la propria competenza in determinati ambiti, ad oggi è il meccanismo alla base dell'innovazione e del miglioramento.

- L'azione globale, ovvero non circoscritta alle azioni dei singoli, risponde finalmente alla sempre più contingente esigenza del modello societario in vigore presso la maggior parte delle grandi compagnie. Non si possono infatti immaginare colossi multinazionali che rispondano separatamente alle esigenze del mercato, affidando strategiche operazioni di marketing alle proprie filiali locali. Le compagnie di successo, che si contendono il mercato con competitor internazionali, devono cominciare non solo a pensare in ottica globale, ma ad agire in modo globale, considerando il mondo come un unico paese.

L'impresa moderna si trova quindi a dover accogliere la sfida di rivoluzionare la sua struttura per vincere nel nuovo scenario competitivo. La gerarchia e la chiusura appaiono anacronistici se paragonati alle opportunità date dall'apertura e dalla condivisione che offre il mercato attuale.

Oggi è proprio ai mercati che viene affidato un ruolo attivo nella definizione della strategia aziendale, nella pianificazione e nell'esecuzione. Molte imprese come Hewlett-Packard, Siemens e Microsoft hanno e stanno ri-orientando la modalità di allocazione delle risorse, simulando un mercato interno all'impresa, creando competizione e collaborazione tra team eterogenei e interfunzionali con l'obiettivo di stimolare la nascita delle idee migliori. Il CEO

di Procter and Gamble, A.G.Lafley, conscio di non poter più contare esclusivamente sulla potenza numerica dei suoi dipendenti (circa 7500 chimici) per mantenere la leadership, ordinò ai Direttori di ogni unità di business di cedere in outsourcing il 50% dei nuovi prodotti e servizi. Il risultato è che oggi chiunque può lavorare per P&G senza timbrare il cartellino: è sufficiente iscriversi al network Innocentive, una comunità di 90 mila scienziati che collaborano per la risoluzione dei problemi nella R&S in cambio di una ricompensa indennario.

Il ruolo di Internet ha cambiato intere industrie e istituzioni, fino ad arrivare al mondo della salute: da un lato i cittadini usano internet come prima fonte di informazione medica, dall'altro la stessa organizzazione della ricerca biomedica

è cambiata grazie alla possibilità di organizzare sperimentazioni cliniche su scala globale.

Sempre facendo riferimento al mondo scientifico, lo stesso settore dell'astronomia vede una collaborazione di massa significativa: è diventata la norma, non l'eccezione in quasi tutte le scienze naturali.

Ad esempio il progetto GalaxyZoo, che permette agli utenti comuni di classificare le galassie sulla base della loro forma. Un giovane Dottorando, avendo un database di circa 50.000 immagini (grazie ai nuovi telescopi infatti ci sono più immagini di galassie di quante sia possibile analizzare), ebbe l'idea di pubblicare le immagini e chiedere al pubblico di aiutare a classificare le galassie basandosi sulla loro forma. Ha pensato che potessero esserci persone interessate a contribuire e che, se anche solo 200 persone avessero collaborato, questo avrebbe fornito una grossa spinta nell'analisi dei risultati. I ricercatori hanno poi verificato che, semplicemente dopo aver seguito un breve tutorial video, i partecipanti classificavano correttamente le galassie nel 95% dei casi. Dopo qualche giorno, il progetto fu raccontato dalla BBC, e nel giro di qualche giorno vi erano non 200 ipotizzati, ma ben 200.000 cittadini coinvolti nell'esperimento mentre (oggi hanno superato i 300.000) e l'analisi si sta allargando ad altri problemi più sofisticati. Si tratta non più solo di crowdsourcing, ma di creare veri e propri gruppi di collaborazione allargati.

I principali fattori che hanno decretato il successo dell'iniziativa sono stati:

- Un tema interessante e coinvolgente;
- L'attenzione ed il ruolo reale attribuito ai partecipanti;
- Alto grado di trasparenza e partecipazione degli scienziati coinvolti;
- La forza dei legami sociali fra i partecipanti

Anche nel contesto della PA, tutti i Paesi del mondo hanno sviluppato o stanno riflettendo su come coinvolgere i cittadini nei processi politici e nell'erogazione dei servizi pubblici. Un esempio tra tanti è rappresentato da Apps for Democracy, uno dei primi concorsi negli Stati Uniti, che fu lanciato nell'ottobre del 2008 da Viviek Kundra, all'epoca Responsabile dei sistemi informativi (CTO) del governo del Distretto di Columbia (DC). Kundra ha sviluppato il catalogo

dati del distretto, <http://data.octo.dc.gov/>, che includeva dataset quali feed sulla criminalità in tempo reale, risultati dei test scolastici, e indicatori di povertà. All'epoca era il più ampio catalogo al mondo per i dati locali. La sfida era di renderlo utile per cittadini, visitatori, imprese e agenzie governative di Washington, DC.

La soluzione creativa fu di crearci un contest Apps for Democracy. La strategia era quella di chiedere alle persone di costruire applicazioni utilizzando i dati del catalogo appena lanciato, i cui elementi distintivi erano: candidatura online delle applicazioni, molti premi di importo contenuto anziché pochi di grande ammontare e categorie differenti insieme ad un premio "Giuria popolare". La gara rimase aperta per 30 giorni e costò al governo del distretto federale della Columbia 50.000 dollari. In cambio, furono sviluppate in totale 47 applicazioni per iPhone e per il web, con un valore aggiunto per l'economia locale di 2.600.000 dollari.

1.12 Date principali della storia di Internet

1960: Avvio delle ricerche di ARPA, progetto del Ministero della Difesa degli Stati Uniti

1967: Prima conferenza internazionale sulla rete ARPANET

1969: Collegamento dei primi computer tra 4 università americane

1971: La rete ARPANET connette tra loro 23 computer

1972: Nascita dell'InterNetworking Working Group, organismo incaricato della gestione di Internet. Ray Tomlinson propone l'utilizzo del segno @ per separare il nome utente da quello della macchina.

1973: La Gran Bretagna e la Norvegia si uniscono alla rete con un computer ciascuna.

1979: Creazione dei primi Newsgroup (forum di discussione) da parte di studenti americani

1981: Nasce in Francia la rete Minitel. In breve tempo diventa la più grande rete di computer al di fuori degli USA

1982: Definizione del protocollo TCP/IP e della parola "Internet"

1983: Appaiono i primi server con i nomi per indirizzarsi ai siti

1984: La rete conta ormai mille computer collegati

1985: Sono assegnati i domini nazionali: .it per l'Italia, .de per la Germania, .fr per la Francia, ecc.

1986: Viene lanciato LISTSERV, il primo software per la gestione di una mailing list. Il 30 aprile, da Pisa, sede del Centro nazionale universitario di Calcolo elettronico (Cnuce)[1] viene realizzata la prima connessione Internet dall'Italia.

1987: Sono connessi 10 000 computer. Il 23 dicembre viene registrato "cnr.it", il primo dominio con la denominazione geografica dell'Italia; è il sito del Consiglio Nazionale delle Ricerche.

1989: Sono connessi centomila computer

1990: Scomparsa di ARPANET; apparizione del linguaggio HTML

1991: Il CERN (Centro Europeo di Ricerca Nucleare) annuncia la nascita del World Wide Web; il Crs4 (Centro di ricerca, sviluppo e studi superiori in Sardegna) crea il primo sito web italiano, secondo in Europa.[2][3]

1993: Apparizione del primo browser pensato per il web, Mosaic

1995: al CRS4 (Centro di ricerca, sviluppo e studi superiori in Sardegna) viene sviluppato il primo servizio di webmail[4]

1996: Sono connessi 10 milioni di computer

1999: Viene pubblicato Napster, il primo sistema di file sharing di massa. Gli utenti di Internet sono 200 milioni in tutto il mondo.

2008: Gli utenti di Internet sono circa 600 milioni in tutto il mondo.

2009: Gli utenti di Internet sono circa 1 miliardo in tutto il mondo.

2011: Gli utenti di Internet sono circa 2 miliardi in tutto il mondo.[5]

2014: Gli utenti di Internet sono circa 5 miliardi in tutto il mondo.

CAPITOLO II

LA RADICE DELL'IDENTITÀ DIGITALE: L'IDENTITÀ PERSONALE

2.1 IL CONCETTO DI PERSONA

Ma alla radice dell'identità digitale sta il concetto di identità personale che vale la pena di approfondire. Per identità personale in filosofia s'intende la capacità dell'individuo di avere consapevolezza del permanere costante del suo io che si manterrebbe sostanzialmente identico attraverso il tempo e le diverse e varie esperienze che hanno segnato la sua vita fino al momento presente.

Il problema dell'identità nel senso del mantenimento delle caratteristiche fondamentali dell'individuo era stato risolto dalla filosofia antica, e in particolare da Aristotele, con la teoria di una sostanza (*hypokeimenon*) che si manteneva identica a se stessa anche se variavano i suoi molteplici e mutevoli attributi.

Nell'età di John Locke (1632–1704) entra in crisi la vecchia idea della sostanza aristotelica che continuava ad essere nella concezione metafisica e religiosa dell'anima che permetteva di dare una caratteristica unitaria e trascendente ad un io contingente e di mantenere, nello stesso tempo, la permanenza della sua identità personale nel susseguirsi del tempo.

Queste concezioni verranno superate del tutto con l'avvento dell'empirismo moderno il quale negherà che si possa pretendere di conoscere

la sostanza o l'anima come una cosa in sé quando in realtà noi possiamo avere dell'oggetto soltanto le sue rappresentazioni in base alle nostre sensazioni.

Locke, quindi per primo metterà in discussione l'idea di sostanza rivelando come essa non fosse stato che un tentativo di risolvere il problema di rendere unitaria la molteplice realtà. Sulla base di questo dualismo gnoseologico, per cui il soggetto conoscente avrà semplicemente la rappresentazione fenomenica e sensibile dell'oggetto conosciuto, Locke nega possa pensarsi ad una sostanza che accompagni, mantenendone l'identità, la storia dell'io.

Innanzitutto, dice Locke, bisogna distinguere i concetti di uomo e persona, apparentemente sinonimi ma in vero molto diversi: per uomo si può intendere un corpo materiale vivente strutturato dove si evidenzia la «partecipazione alla stessa vita continua di particelle sempre fuggevoli di materia, unite allo stesso corpo organizzato in una successione vitale.» È dunque questa costituzione materiale vivente che caratterizza l'uomo e non più la sua essenza razionale: «Chiunque infatti veda una creatura fatta come lui, anche se in tutta la sua vita non avesse più raziocinio di un gatto o di un pappagallo, lo chiamerebbe ancora uomo; e chiunque sentisse un gatto od un pappagallo discorrere, ragionare, filosofare, lo chiamerebbe tuttavia e lo considererebbe null'altro che un gatto o un pappagallo».

La persona invece è nell'uomo quando egli sia in grado tramite la coscienza e la memoria di credere nella sua identità tale da differenziarsi da tutti gli altri così che «fin dove questa coscienza può essere estesa indietro ad una qualsiasi azione o pensiero del passato, fin lì giunge l'identità di quella persona».

Ma per mantenere viva questa memoria di noi stessi, aggiunge Locke, dobbiamo continuamente riportare alla primitiva nitidezza quelle idee che si sono sbiadite col passare del tempo. È un continuo lavoro di manutenzione della nostra memoria che ci assicura la nostra identità che inevitabilmente si annebbia con la perdita del ricordo delle nostre esperienze passate.

David Hume

L'elemento della memoria per la percezione dell'identità personale, secondo David Hume (1711–1776), è ampiamente insufficiente: «Chi può dirmi

che cosa pensava e faceva il 1 gennaio 1715, l'11 marzo e il 3 agosto del 1733?». Ma a parte la difficoltà di mantenere una memoria del passato che sia priva di falle e amnesie, Hume sostiene che ogniqualevolta riflettiamo sulla nostra identità personale ci troviamo di fronte a una serie di percezioni che ci appartengono ma tra le quali non possiamo mai isolare quella distinta percezione del nostro io: «Non riesco mai a sorprendere me stesso senza percezione e a cogliervi altro che percezione». La ragione che giunge al sapere sulla base delle percezioni nel caso della conoscenza dell'io si trova di fronte al vuoto, l'idea dell'io è un feticcio che costruiamo per poter credere in un'immagine di noi stessi ma in realtà le nostre impressioni ed idee ^[6] sono instabili e mutevoli: pensare sia possibile avere un'idea permanente del nostro io è un'illusione: «Noi non siamo altro che fasci o collezioni di differenti percezioni che si susseguono con una inconcepibile rapidità, in un perpetuo flusso o movimento». Ma la ragione, che non è quindi in grado di darci un riferimento sicuro e costante del nostro io, viene superata da quelle passioni e sentimenti che si sviluppano nella vita sociale, nei nostri rapporti con gli altri: a questo punto infatti interviene l'immaginazione che, per una specie di "inclinazione naturale", in quella serie di percezioni isolate che riaffiorano nel nostro lacunoso ricordo, stabilisce, sulla base dei principi di somiglianza e di causalità, una relazione costante tale che la memoria «non soltanto scopre l'identità, ma contribuisce anche alla sua produzione, producendo fra le percezioni il rapporto di somiglianza» e quello di causa-effetto tra le impressioni e le nostre idee.

Ai fini della identità personale occorre quindi un collegamento tra la memoria del passato, che collega le percezioni tramite la somiglianza e la causalità, e l'immaginazione che le unifica e in più estende la nozione del nostro io nel futuro.

2.2 IL DIRITTO ALL'IDENTITÀ PERSONALE

Il diritto di ciascuna persona a non vedersi attribuite la paternità di condotte, di dichiarazioni o più in generale di azioni non proprie corrisponde ad una recente acquisizione giurisprudenziale.

Si tratta dell'ultima evidenza interpretativamente ricavata nell'ambito dei diritti della personalità. Il diritto all'identità personale viene fondato sulla base dei diritti di libertà costituzionali, che implicherebbero la pretesa di ciascun soggetto di essere rappresentato con la sua vera identità e di non vedere alterato, contestato o mistificato il proprio patrimonio intellettuale, nelle varie forme in cui si può estrinsecare.

Il fondamento di questa tutela viene rinvenuto più specificamente nell'articolo 2 della Costituzione della Repubblica Italiana che recita: "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale". E' stato detto, con riferimento a questa norma, che, lungi dall'essere connotata da una funzione semplicemente riassuntiva dei diritti espressi e tutelati nella costituzione o di quelli previsti dal codice civile e concernenti la persona umana, svolge un ruolo di riferimento fondamentale al centro dell'intero ordinamento costituzionale in relazione ai valori della persona, costituendo una clausola aperta e generale di tutela del libero e integrale svolgimento dei diritti fondamentali dell'uomo.

Ogni nuovo interesse umano emergente come riflesso dei diritti della personalità, quale appunto quello in esame, rinverrebbe motivo della propria tutela nel disposto della norma in questione.

Il diritto all'identità personale in definitiva deve essere inteso quale autonomo diritto, ulteriore ed indipendente rispetto al diritto al nome ed a quello all'onore, consistendo per l'appunto nel diritto a che non venga stravolta, alterata la propria identità, intesa come complesso di atteggiamenti etici, politici, comportamentali, indipendentemente dall'ingiuriosità delle espressioni (Cass. Civ. Sez. I, 3769/85).

La giurisprudenza ha posto in evidenza tre distinti aspetti dell'identità

personale:

1. La sua natura onnicomprensiva della personalità del soggetto, ovverosia rappresentativa del suo patrimonio culturale, politico, morale ecc.;
2. La sua oggettività, intesa nel senso di corrispondenza fra comportamenti esterni del soggetto rilevabili e rappresentazione della personalità; in altri termini l'identità personale tutela quel che il soggetto risulta essere, non quel che crede di essere; la figura viene in tal modo ancorata alla verità, intesa non in senso assoluto, bensì di realtà conoscibile secondo i criteri "della normale diligenza e della buona fede soggettiva";
3. La sua exteriorità, in quanto l'identità caratterizza un soggetto in una comunità; la sua lesione pertanto può avvenire solo attraverso un mezzo di comunicazione che alteri nei consociati la loro percezione della persona.

E, infatti, nei casi sottoposti all'esame dei giudici l'illecito è commesso, generalmente, con un manifesto, un volantino, una trasmissione televisiva, un articolo di giornale o un inserto pubblicitario.

Molto delicato è il contemperamento tra diritto all'identità personale e l'esercizio del diritto di cronaca (Cass. Civ. Sez. I, 978/96). La disciplina può essere dedotta, per analogia, dalla normativa prevista per il diritto al nome (art. 7 cod. civ.), essendo tale figura la più affine al diritto in considerazione. Pertanto il soggetto che subisce ad opera di un terzo una lesione pregiudizievole alla sua immagine sociale, potrà ben chiedere in sede giudiziale la cessazione del fatto lesivo ed il risarcimento del danno, in quanto di questo ne sussistano i presupposti soggettivi ed oggettivi per la sua risarcibilità, nonché ottenere dal giudice l'ordine di pubblicazione della sentenza (oltre la pubblicazione di una sua rettifica se la lesione è arrecata a mezzo della stampa: art. 42 della legge 5 agosto 1981, n. 416).

Il diritto all'identità personale va, inoltre, ben distinto dagli altri diritti della personalità, nei confronti dei quali presenta caratteri di differenza e di affinità. Con riguardo al nome, si deve sottolineare la non modificabilità di quest'ultimo (tranne che si segua una complessa procedura), mentre l'identità personale ben può subire un'evoluzione. Lo stesso elemento di staticità si rileva anche nell'immagine, la quale, oltre a essere trasmessa in una forma visivamente percepibile, è fortemente determinata dai tratti somatici del soggetto; prevalgono, in tal modo, gli aspetti materiali, di contro a quelli chiaramente intellettuali dell'identità personale.

Quanto alla riservatezza, essa mira ad impedire che altri conoscano. Viceversa, l'identità personale tende a che questi conoscano correttamente. La prima prescinde dalla verità (anzi, più è vera la notizia del fatto intimo, più essa è lesiva), all'opposto dell'identità di cui la verità costituisce elemento essenziale.

Inoltre, l'identità si differenzia dall'onore, poiché questo attiene ad un momento soggettivo, la percezione della propria personalità, mentre l'identità si collega ad un aspetto oggettivo, la percezione esterna che altri hanno del soggetto.

Infine, l'identità si distingue dalla reputazione, poiché riguarda il rapporto di conoscenza fra il soggetto ed una comunità. La reputazione, invece, attiene ad un momento successivo alla conoscenza e consiste in un giudizio di valore. Pertanto, mentre perché ci sia lesione dell'identità è sufficiente una alterazione nella rappresentazione, per la reputazione è necessario che da ciò consegua una diminuzione nella stima dei consociati

2.3 DALL'IDENTITÀ PERSONALE ALLA REPUTAZIONE

La reputazione di una organizzazione è il giudizio complessivo dato da coloro che in modo diretto o indiretto ne influenzano l'operato. La consapevolezza del valore che la corporate reputation ha per un'azienda negli ultimi anni è aumentata vertiginosamente. Comportamenti etici, trasparenza, qualità dei processi e delle relazioni, oggi più che mai, dovrebbero essere alla base di qualsiasi piano di marketing e rappresentare asset strategico per costruire vantaggio competitivo sui mercati globali. Un costante monitoraggio e un'attenta gestione della propria reputazione rappresentano attività importanti per costruire, mantenere o rafforzare il consenso dei diversi interlocutori sociali.

Molti imprenditori hanno potuto verificare sulla loro pelle come l'entità del danno che un comportamento errato può apportare alla reputazione di un'azienda è tanto più alto quanto il suo settore di riferimento o le sue caratteristiche fanno leva su valori immateriali, quali l'immagine, la fiducia e la creatività.

Oggi, per parlare al mondo, non è più necessario lavorare all'interno dei media mainstream, avere particolari licenze o chiedere permessi. Basta pubblicare il proprio pensiero in un angolo dell'immensa Rete sperando che, qualora accettato e condiviso, ottenga risonanza e produca risultati. La reputation 2.0, ovvero le conversazioni che hanno luogo sulla Rete, devono essere tenute costantemente sotto controllo.

Che si tratti di mondo virtuale o reale i consumatori si scambiano continuamente idee, esperienze e storie, vissute in prima persona o raccontate loro da qualcun altro. Il valore riconosciuto alle parole pronunciate da persone comuni e soprattutto disinteressate, è sempre maggiore di quello attribuito alle comunicazioni aziendali. Il passaparola è un virus e si propaga in tempi e luoghi imprevedibili. Controllarlo e gestirlo è un "dovere" del brand: nell'arco di poco tempo potrebbe apportare all'azienda enormi benefici, quanto disastrose perdite.

La reputazione è un processo in continua evoluzione, alla cui formazione partecipano diversi soggetti, alcuni più incisivamente, come giornalisti e opinion leader, altri meno, come i consumatori passivi. La reputazione non può quindi, per sua natura, essere semplicemente costruita a tavolino dagli esperti della comunicazione e divulgata attraverso i media.

Pianificare unacorporate reputation, per un'azienda, significa decidere cosa e come comunicare ai propri pubblici di riferimento. Conoscere il posizionamento del brand nella mente dei consumatori e seguire standard di Corporate Governance sono punti di partenza importanti per pianificare una comunicazione efficace. L'insieme dei messaggi inviati dal brand saranno infatti pretesto di dialogo per i pubblici esterni che pian piano andranno a delinearne, più o meno direttamente, la reputazione.

Pianificare una corporate reputation è quindi possibile, ma importante sarà monitorarla ed evolvere con essa. Solo attraverso un costante impegno comunicativo e relazionale si otterranno buoni risultati.

Il sociologo Steven Nock definisce la reputazione come *una condivisa, o comune, percezione rispetto una persona*. Avere una buona reputazione significa avere maggiori possibilità di intrecciare rapporti, umani o lavorativi che siano.

Siamo quello che comunichiamo, ma soprattutto siamo quello che gli altri, entrando più o meno direttamente in contatto con noi, pensano.

Su Internet, dove le interconnessioni tra individui sono maggiori e il mondo diventa davvero piccolo, questo discorso si amplifica, tanto che in America si parla già distress da web reputation.

Nel villaggio globale le informazioni disponibili sono molte e spesso poco controllate o controllabili: tutte messe per iscritto, permangono nel tempo e possono riaffiorare quando meno te lo aspetti.

Attraverso blog e social network informazioni personali vengono postate quotidianamente, a velocità prima impensabili.

Proprio per questo, al giorno d'oggi, uno degli strumenti più utilizzati per conoscere una persona è Google. *Googlare*, verbo nato dal famoso motore di ricerca, significacercare informazioni su qualcuno all'interno della Rete. Questo sistema, facile e veloce, viene utilizzato nelle occasioni più disparate, con partner commerciali, clienti, datori di lavoro ma anche più semplicemente con amici e conoscenti, magari incontrati proprio sul Web. All'interno del mondo virtuale le informazioni viaggiano a velocità inaudite e una volta sparse per la Rete non sono più cancellabili. Parlare di una persona può quindi rivelarsi micidiale.

E le aziende?

Un costante monitoraggio e un'attenta gestione della propria corporate reputation rappresentano attività importanti per costruire, mantenere o rafforzare il consenso dei diversi interlocutori sociali.

Comportamenti etici, trasparenza, qualità dei processi e delle relazioni, oggi più che mai, dovrebbero essere alla base di qualsiasi piano di marketing e rappresentare asset strategico per costruire vantaggio competitivo sui mercati globali.

Secondo uno studio condotto da Laura Pasotti la ricerca di lavoro (e, dall'altra parte, di candidati) si sta sempre più spostando sui social network. Ma se, a livello globale, i social media giocheranno un ruolo sempre più rilevante nel processo di ricerca e selezione, la loro efficacia nell'incontro tra domanda e offerta in Italia, pur se in crescita, è ancora scarsa. È quanto emerge da una ricerca condotta da Adecco nel 2014 insieme all'Università Cattolica di Milano, che ha coinvolto 17 mila candidati e 1.500 selezionatori in 24 Paesi del mondo da cui emerge che, nel 2013, più della metà delle attività di selezione è avvenuta su Internet (53%) e si prevede che nel 2014 raggiunga il 61%.

Nel nostro Paese l'indagine è stata condotta su 269 selezionatori e su 7.597 candidati, in maggioranza uomini (54%), nati dopo il 1965 (45% dal 1965 al 1980 e il 39% dopo il 1981), diplomati (49%). Tra chi cerca lavoro, quasi 6 persone su 10 hanno dichiarato di usare anche i social network e più di 5 su 10 hanno diffuso il proprio curriculum tramite i social media. Solo il 7%, però, ha trovato lavoro proprio grazie ai social (erano il 2% nel 2013). La ricerca conferma, inoltre, l'importanza della "web reputation": un recruiter su 4 ha, infatti, ammesso di aver escluso dalla selezione potenziali candidati a causa dei contenuti o delle foto pubblicate sul suo profilo social.

Per i selezionatori, tra gli elementi più attrattivi dei candidati sui profili social ci sono le esperienze professionali, la presenza di informazioni personali e riconoscimenti professionali. Tra quelli negativi, la partecipazione ad attività in violazione di regolamenti universitari o del posto di lavoro è quella che riceve più disapprovazione da parte dei recruiter, segue la presenza di foto in comportamenti poco consoni, ad esempio in stato di ebbrezza.

Il report, nel complesso, è strutturato in quattro aree: l'utilizzo dei social media a fini professionali, la loro efficacia nell'incontro tra domanda e offerta, la "web reputation" e il suo impatto nella ricerca di lavoro, il capitale sociale dei candidati.

In generale, il 67 per dei candidati italiani usa i social media per cercare lavoro, un dato in linea con quello registrato tra i selezionatori, e il più utilizzato è LinkedIn (41%, sale al 59% tra i selezionatori). Le donne usano i social media più degli uomini, sia per la ricerca di lavoro che in generale. Il loro uso cresce in modo significativo al diminuire dell'età degli intervistati. Il 75% dei più giovani fa uso di almeno un social network per la ricerca di lavoro. Anche il grado di istruzione risulta un fattore determinante: si passa da un utilizzo al 67% fra chi ha la licenza media all'86% di chi ha un'istruzione post-universitaria. Inoltre, l'uso dei social è

più alto tra coloro che sono alla ricerca del primo impiego (80%) e tra gli occupati (75%) che cercano un posto migliore, mentre è più contenuto tra i disoccupati.

Ovviamente, l'uso dei social è correlato al livello di competenza digitale dei candidati. Rispetto alla loro efficacia, dal report emerge che, anche se il 56% degli intervistati li ha utilizzati per distribuire il cv, solo il 23% è stato contattato almeno una volta da un selezionatore e il 7% ha trovato lavoro. Inoltre, la maggior parte dei candidati dichiara di utilizzare Facebook più come canale di comunicazione riservato agli amici che come strumento per creare e mantenere rapporti di lavoro. Vero è, però, che la reputazione online può influenzare i recruiter, ma in Italia gli elementi che possono giocare un ruolo negativo (foto in atteggiamenti controversi su tutto) hanno un indice di presenza molto basso. Un altro aspetto significativo è rappresentato, poi, dalle relazioni online: chi ha una rete più ricca ottiene risultati migliori nei contatti con i selezionatori e ha più possibilità di essere assunto.

Quanto ai selezionatori, sono soprattutto le grandi aziende a essere presenti sui social (il 79 per cento di quelle con più di 250 dipendenti ha un profilo social) e le piccole (il 64 per cento di quelle tra 10 e 50 lavoratori). Solo un intervistato su quattro però ha seguito sessioni formative sull'uso dei social e le ha valutate positivamente. I recruiter, infine, ritengono che i social media siano "scarsi" nel far incontrare domanda e offerta, a parte LinkedIn, eppure in molti intendono utilizzarli nei prossimi 12 mesi.

Un aspetto che indubbiamente contribuisce alla reputazione e all'immagine di un'organizzazione è la discussione che si attiva sulle diverse piattaforme online sulle diverse caratteristiche di un'azienda e sui suoi prodotti e servizi. Come noto il fenomeno delle recensioni e dei commenti degli utenti è in crescita esplosiva e viene da molti seguito, studiato e anche temuto. A volte in maniera poco razionale si cerca di combattere questa espansione senza, spesso,

comprenderne bene gli effetti e le reali possibilità di presa sul pubblico. Lungi dall'essere una novità, guide, commenti e critiche sono da sempre state pubblicate e discusse su tutti i mezzi di informazione, il fenomeno ha assunto un gran peso oggi per l'utilizzo capillarmente diffuso di Internet e del Web. Una rassegna di quanto si conosce a oggi in questo campo, e su quanto soprattutto il mondo accademico ha studiato, è stata pubblicata di recente (Baggio, 2010). La rassegna analizza principalmente il settore del turismo, ma non solo, vista la diffusione del fenomeno, e porta alcune conclusioni interessanti che val qui la pena ripetere.

Innanzitutto l'abitudine a commentare ed esprimere pareri su prodotti e servizi di vario genere sembra ormai abbastanza consolidata e non si vedono rallentamenti nella crescita del numero di utenti che ne fanno uso. La qualità e numero delle recensioni hanno certamente un impatto sugli affari delle strutture interessate, ma le scelte del consumatore sono influenzate in maniera diversa a seconda del suo livello di coinvolgimento: il numero di recensioni influenza i meno coinvolti, la qualità i più consapevoli.

Le recensioni si polarizzano, in genere valutazioni medie sembrano non valere il tempo e le risorse necessarie a scriverle. I commenti negativi, se ben gestiti, possono essere rovesciati nei loro effetti, ma se ignorati o snobbati possono avere conseguenze abbastanza pesanti. In ogni caso, positive o negative che siano, le recensioni online sono indicatori molto affidabili e utili per una migliore conoscenza del mercato e della concorrenza. Inoltre, cosa non secondaria, possono essere fonte essenziale per azioni di miglioramento dell'offerta. Infatti, come dimostra un recente lavoro (Cunningham et al., 2010), la valutazione espressa nelle recensioni pubblicate su TripAdvisor migliora nel corso del tempo, segno che gli hotel interessati traggono beneficio dai commenti dei visitatori e si impegnano nel miglioramento della qualità del servizio.

L'idea che molte recensioni, soprattutto quelle negative, siano infondate o in mala fede è falsa, in ogni caso cominciano a esistere metodi e tecniche per isolarle, anche se, per ora almeno, di non facile applicazione. In ogni caso il

lettore è molto più sensibile di quanto non si creda ed è in grado, attraverso la consultazione di fonti diverse, di farsi un quadro abbastanza neutrale.

Eccessi di positività, come di negatività, nei commenti vengono (intuitivamente) identificati come poco affidabili e scartate nella formazione del giudizio.

Ovviamente queste sono indicazioni non sempre facilmente generalizzabili, anche se costruite su metodologie solide, collaudate e verificate e inevitabilmente si tratta di risultati medi e casi estremi non sono del tutto improbabili. Ma, in definitiva, il quadro che sembra emergere è quello di strumenti che se ben utilizzati possono rivelarsi estremamente utili ed efficaci per il miglioramento e la crescita del settore.

Per essere davvero riconosciuto come tale, l'influencer ha bisogno di parlare al suo pubblico in modo diretto e specifico. Può costruirsi un personaggio a tavolino, oppure può scavarsi una nicchia in un certo settore e farsi strada in quello, o ancora può essere semplicemente sè stesso, e se gli va bene non deve fare altro, perché è già brillante e interessante così. Di solito però è nazionalpopolare, cioè si occupa trasversalmente di tutto ed è percepito come uno che potenzialmente potrebbe dire la sua sia sulle caldaie a induzione che sull'ultimo fidanzato di Selvaggia Lucarelli. Dire cose interessanti, esserci da molto tempo e mantenere alta la credibilità sono tre caratteri fondamentali di questo "lavoro" e fanno sì che l'influencer sia molto seguito da un pubblico che è trasversale quanto gli argomenti che tratta. Certo, se è brillante, attira il pubblico con la sua simpatia; se è preparato, lo attira con l'autorevolezza; se è particolarmente fotogenico, lo attira per la bellezza, gli outfit, ecc. Insomma, metà del merito rimane suo. Ma l'etichetta di influencer gli arriva da chi lo segue: sono i suoi followers a decretare se veramente l'opinione di questo utente "Premium", se così vogliamo chiamarlo, traina le coscienze, trasforma le idee, crea un desiderio. E se sposta opinioni, che succede? Parte l'attività di marketing, che lo incorona a pseudo testimonial e gli affida un prodotto, un evento, un lancio, un libro, un aspirapolvere, un pacco di noccioline, dei preservativi. L'opinione porta a fatturato per l'azienda che coinvolge l'influencer? In certi casi sì, in altri (quasi sempre) no; nel primo caso l'azienda

è contenta e acquista fiducia nel mezzo web. E nel secondo caso? È la popolarità dell'influencer che aumenta: l'azienda X o l'agenzia di PR Y nota la sua attiva partecipazione con il brand Z e lo coinvolge nuovamente, in un circolo vizioso che aumenta i suoi followers e sigilla il suo essere "*uno che influenza*" le masse, anche se non è mica poi tanto vero.

Un'altra cosa fondamentale della figura dell'influencer è che ha bisogno, almeno una volta nella sua vita di opinion leader, di litigare con un'altra persona del suo settore, rigorosamente online. Sono ammessi tweet, commenti sul blog, frecciate anonime che vengono lanciate su Facebook senza mittente e che vengono subito intercettate dalla controparte che ha la coda di paglia, e così via. Di solito gli influencer veterani vedono come una minaccia i novellini che pure hanno seguito con passione tutti gli step per arrivare sul podio dell'influenza, e allora millantano supremazia e metodo, in una guerra senza esclusione di colpi che rimane circoscritta alla cerchia dei followers dell'uno e dell'altro. E nel resto del mondo, che succede? Niente, perché se c'è una cosa autoreferenziale, sono proprio le guerre clandestine tra crew del web.

Quando entri nella mailing list delle agenzie di PR, non ne esci più. È come un buco nero senza fine dal quale riemergi dopo anni di mail non lette e cestinate senza pietà. C'è da dire che a volte però i Brand si inventano cose carine a cui non si può dire di no: viaggi, prove prodotto hi-tech e così via. Eppure, l'influencer bravo non acchiappa a scrocco tutto quello che gli viene proposto: l'influencer bravo prende solo quello che è nelle sue corde e poi modella quella che, a conti fatti, è una marketta, trasformandola in una segnalazione. Cosa vuol dire? Ecco un esempio:

Influencer A riceve un dono dall'Agenzia X, che ha come obiettivo quello di promuovere quel dono attraverso un network ben consolidato. Poniamo il caso che sia un deodorante per auto e che il brand che lo produce abbia bisogno di "attaccarsi" ai followers dell'Influencer A, che lo seguono a occhi chiusi qualsiasi cosa faccia. A questo punto, Influencer A ha davanti tre strade: 1) rifiuta: i suoi lettori non lo seguono perché parla di deodoranti per auto, ci tiene alla sua reputazione online e dunque non accetta il dono né l'eventuale

gettone di partecipazione. Influencer A è dunque coerente, oppure semplicemente è talmente in alto che può permettersi di rifiutare progetti piccolini in attesa di quelli molto grossi.

2) accetta e promuove: la marketta si nasconde dove meno ve l'aspettate, ma a volte è talmente palese che casca davanti agli occhi. Prima o poi ci cadono tutti (e probabile che ci sia caduta anche io, chi è senza peccato scagli la prima pietra). L'influencer A presenta il deodorante per auto come fosse uno spot, in modo neanche poi tanto originale e in un flusso di post che sono tutti uguali agli altri. Influencer A è dunque (secondo me) un accattone scroccone.

3) accetta e promuove a modo suo: questo riescono a farlo in pochissimi, solo se si è particolarmente brillanti, o seguiti perché molto autorevoli, o decisamente originali. Andare a un evento e descriverlo come "Amazing", senza aggiungere uno straccio di parola dedicata alla situazione è facile e indolore, ma porta sicuramente meno che mettere dentro un tocco personale a quello che sì, è a tutti gli effetti una promozione. Influencer A è dunque in questo caso uno che sa fare il suo mestiere (qualsiasi cosa voglia dire).

Chi sono gli haters? E' un gruppo di persone che vi odia (o odia quello che fate). I followers sono invece persone che vi seguono e, se lo fanno per lungo tempo, vi apprezzano anche (altrimenti userebbero l'Unfollow, o vi ignorerebbero). Esser influencer con un gran numero di followers implica una grande esposizione e dunque maggiore possibilità di essere preso di mira, ma anche questo fa parte del gioco. Insomma, se a Belén dicessero: "Bella mia, ti promettiamo che nessuno parlerà mai più male di te sui giornali, sotto le foto di Instagram o sui siti di gossip, ma non sarai più famosa e cadrai nell'anonimato" sapete cosa risponderebbe Belén? Direbbe no con quel suo adorabile accento spagnolo, e ve lo dico io perché: perché il gioco vale la candela. Anche essere un influencer (se è riconosciuto dalla rete come tale) ha i suoi privilegi, sebbene in minor proporzione e con guadagni meno ingenti. E quindi avere gli haters, sebbene non si capisce bene perché la gente debba prendersela così tanto con qualcuno che non conosce, fa parte del gioco.

Ci sono gli influencer che si autoetichettano. Cioè, nella bio, scrivono "Web influencer", come se qualcuno li avesse investiti del ruolo. In alcuni casi è vero

- perché magari st'influencer ne ha le prove - in altri casi millanta solo perché sa venderci particolarmente bene. Buon per lui.

In certi casi, uno influencer ci si sente solo, in altri casi lo usa come job title sui bigliettini da visita. Non sono a conoscenza di particolari eventi, in Italia e nel mondo, in cui utenti del web vengono investiti di onorificenze e agghindati con una fascia come Miss Italia, quindi sono certa di dire il vero, affermando che influencer non è tanto un titolo, quanto uno status guadagnato sul campo.

2.4 Il Web Marketing

L'epoca che stiamo vivendo è un'era nella quale l'informazione, la conoscenzascientifica e le avanzate tecnologie creano la «società a Rete», un network, nuovo villaggio globale, dove i rapporti cambiano, evolvendo verso nuove forme di interconnessione e socialità. In particolare, la globalizzazione dei mercati ha prodotto un radicale cambiamento nei rapporti tra l'impresa ed il consumatore: quest'ultimo non è più, infatti, solo il fruitore di un prodotto finale, ma, più informato, consapevole e sicuro, tende a divenire partner attivo dell'impresa. Parallelamente, l'irrompere delle nuove tecnologie ha prodotto un accrescimento nelle cognizioni di ogni individuo, permettendogli, come mai prima d'ora sarebbe potuto avvenire, di produrre conoscenza, risolvere problemi, creare soluzioni, in una logica simultanea, sincronica, atemporale, dove tempi e spazi si comprimono notevolmente.

Tali evoluzioni hanno di sicuro convogliato gran parte del potere contrattuale, a livello di mercato, nelle mani del consumatore finale: egli non è più, infatti, quel soggetto passivo di un tempo, a cui indirizzare e vendere la grandissima quantità di merce prodotta dall'industria, ma un attore attento, informatissimo e capace di scegliere tra una miriade di alternative, in tempi relativamente brevi (e definito, non a caso, da Fabris come «consumATTORE»).

Un'impresa virtuosa dovrebbe essere in grado di sfruttare a proprio vantaggio tale evoluzione del consumatore; infatti, negli ultimi anni, la distribuzione organizzata, di grandi dimensioni, sta scavalcando le imprese di produzione in merito al rapporto con la clientela finale, grazie alla possibilità di godere di

evidenti asimmetrie informative: un tipico caso è quello dell'utilizzo di "carte fedeltà", utili per analisi di mercato anche approfondite.

Grazie al fatto che il consumatore, ora, più consapevole, possa esprimere le proprie opinioni e condividerle con una "comunità", l'impresa può ribaltare a proprio favore i rapporti di forza con gli altri agenti del mercato consolidando una partnership, un'alleanza con tale soggetto.

In questo percorso, sicuramente il Web è destinato ad assumere il ruolo di protagonista: grazie all'interattività, il flusso di comunicazione tra impresa e consumatore diviene bidirezionale, con una possibilità di dialogo e condivisione in tempo reale, in ogni parte del globo.

Finora, l'advertising su Internet si è servito quasi esclusivamente dei banner; facendo così, ha in pratica riprodotto, più o meno fedelmente, la tipologia offline senza scandagliare tutte le enormi potenzialità che la Rete offre: ci riferiamo soprattutto a motori di ricerca, blog, social network ed altri siti "virali" che prevedono una fruizione attiva, con efficaci possibilità di feedback, dei messaggi comunicativi.

Tutto questo rientra in un nuovo tipo di comunicazione "2.0" orientata a raggiungere i vari segmenti di pubblici, intercettandone identità, valori e linguaggi; il culmine di tale evoluzione consiste in quello che molti esperti considerano il passaggio dall'entertainment (o info-tainment) all'engagement, ovvero l'integrazione della mission istituzionale dell'advertising, e cioè creare una favorevole propensione al consumo, con l'esigenza di creare condivisione, partecipazione e coinvolgimento del pubblico.

Tale strategia di integrazione migliorerà la comunicazione, creando al contempo un'identità di marca forte e coerente; perseguire tale strada può consentire, tra l'altro, di risparmiare risorse, ottenendo maggior efficacia anche rispetto ad investimenti molto più gravosi in termini assoluti. Inoltre, vista la debolezza, finora riscontrata, da parte delle maggiori imprese ad implementare queste nuove strategie all'interno della propria organizzazione, chi per primo dovesse avviarsi con convinzione e capacità lungo questo sentiero, ne

trarrebbe un importante vantaggio competitivo difficilmente scavalcabile, soprattutto nel breve termine.

In questo contesto, risulta necessario anche ridiscutere il ruolo del marketing all'interno dell'azienda e, più in generale, del sistema economico. L'evoluzione della figura del consumatore implica un ribaltamento, nelle società contemporanee, dei ruoli consolidati: la produzione non è più al servizio del consumatore; è il consumatore, oggi, al servizio della produzione.

In questo, il ruolo del marketing dovrebbe, secondo logica, uscirne rafforzato: esso è da sempre visto, infatti, come quella fondamentale funzione aziendale destinata a soddisfare i bisogni dei consumatori tramite la fornitura di un adeguato sistema d'offerta, e quindi, l'unica a mettere al centro del proprio mondo proprio il consumatore.

Una conseguenza molto evidente di tale evoluzione è riscontrabile nel superamento della definizione storica kotleriana, basata sul paradigma delle 4 P. Una prima trasformazione si è comunque già registrata in questi decenni, nei quali il concetto di Marketing, fondandosi sempre di più sulla centralità del consumatore, è cambiato, passando dal marketing di massa al marketing personalizzato, via via fino ad arrivare ai più recenti micromarketing e marketing one-to-one.

L'evoluzione finale, però, sta in quello che diversi studiosi, tra i quali Fabris (2008), hanno indicato col termine di «Societing», neologismo che mette insieme marketing e sociologia, e che va sviluppandosi secondo molteplici direttrici, tutte focalizzate sulla figura centrale del consumatore/cliente.

Si passa perciò dall'antico approccio transazionale, secondo il quale il fine ultimo dell'impresa era solo quello di vendere, a quello, moderno, relazionale, inteso come rapporto paritario tra azienda e consumatore, basato sulla condivisione di opinioni, esperienze e sul coinvolgimento; rapporto che, perciò, non sarà più di tipo gerarchico, ma di partnership, basato sulla co-creazione di valore da entrambe le parti.

Passa la mano, poi, anche l'individualismo nei rapporti, tipico del marketing tradizionale, per passare al concetto di individuo come parte di una comunità

(o tribù) con la quale identificarsi; viene infine portata all'estremo la personalizzazione della comunicazione, sempre più "a 2 vie" e rivolta a segmenti il più "narrow" possibili, fino ad arrivare, se possibile, ad una comunicazione prettamente individuale.

2.5 L'evoluzione del Marketing 2.0

Possiamo considerare il Marketing 2.0 come la naturale conseguenza di un'evoluzione delle leggi del mercato, che si è osservata negli ultimi decenni. La vecchia impostazione prevedeva, infatti, l'esistenza di un mercato di massa, dove la domanda era caratterizzata da richieste fondamentalmente omogenee, e la visione era "global" tout court, con il mondo visto come un unico mercato uguale: ciò implicava l'implementazione di grosse campagne comunicative, di immenso impatto rivolte ad una clientela di massa, indifferenziata, dove poco (o nulla) veniva lasciato alla personalizzazione. Tali campagne prevedevano un costo molto elevato e, spinte soprattutto dalla necessità di imporsi nella mente dei consumatori attraverso il ricordo, venivano veicolate indistintamente tramite tutti i mezzi di comunicazione.

Questo è quello che si definisce il vecchio Marketing 1.0, attuato in una logica "1-to-many", dove l'obiettivo era quello di raggiungere la maggior parte di utenza/clientela possibile, da colpire con un messaggio impersonale, senza possibilità di feedback da parte dei clienti stessi. In questa fase, Internet veniva semplicemente visto come uno strumento tramite il quale creare siti, sviluppare portali e piattaforme di servizi web nel quale gli utenti si limitavano a "navigare", o al massimo si spingevano ad operare acquisti on-line tramite la pratica dell'e-commerce.

Il simbolo di tale sistema era il sito internet aziendale, che consentiva sì ai clienti di entrare nel sito, sfogliare il catalogo virtuale dei prodotti e magari anche acquisire il prodotto on-line, ma che non prevedeva un rapporto di condivisione delle idee tra i due lati della domanda e dell'offerta; infatti, le possibilità di feedback erano praticamente nulle e l'approccio al marketing era

più basato sulla comunicazione pubblicitaria tradizionale, mirante a colpire il target dell'azienda, che su un approccio partecipativo alla creazione dei messaggi e dei contenuti da proporre al pubblico di riferimento.

Negli ultimi anni, però, le imprese si sono accorte che qualcosa è cambiato: il consumatore è diventato, come abbiamo visto prima, sempre più esigente e selettivo nelle sue scelte, e sempre più insoddisfatto verso le tecniche di mass marketing indifferenziato. Questo ha spinto la maggior parte delle aziende a mutare radicalmente la propria politica strategica, avviandosi sempre più lungo il sentiero del marketing personalizzato; da una parte, esse si sono rese conto di come non fosse assolutamente profittabile investire ingenti quantità di denaro per campagne indistinte, che potevano anche non incontrare i desiderata della clientela. Dall'altra parte, unitamente a ciò, diventa per le aziende sempre più necessario considerare il cliente come partner dell'impresa, co-creatore di valore, le cui opinioni ed istanze devono necessariamente essere recepite all'interno.

Nasce così il «Marketing 2.0», secondo una logica dapprima definita "1-to-1", e poi, ancor più correttamente, "many-to-many". Il primo paradigma, infatti, può facilmente trarre in inganno e riportarci alla mente le ultime, evolute, forme di Marketing 1.0, dove la segmentazione della clientela, attuata su basi socio-psicodemografiche, era un cardine decisivo. Qui, però, ci si spinge ben oltre: le istanze, le opinioni, gli atteggiamenti viaggiano con tempi e spazi sempre più compressi, ed è la condivisione di esperienze da parte di tutti gli utenti del mondo a far viaggiare rapidamente il "virus" dell'informazione; è proprio qui, allora, che l'impresa deve essere attenta e presente, per detectare il maggior numero di messaggi e migliorare, o conservare il più a lungo possibile, un sistema d'offerta realmente efficace e coerente con il volere dei suoi target di riferimento.

Nasce allora un nuovo mercato, dove global è sostituito da "glocal", neologismo che sta ad indicare come il globale è in realtà la somma di tanti mercati locali, nei quali le richieste dei singoli individui che compongono la domanda sono sempre più specifiche.

Il marketing è rivolto alla conoscenza approfondita delle molteplici esigenze dei consumatori e si pone l'obiettivo di sviluppare relazioni stabili con i clienti: verso di loro, oggi, infatti, è sempre più impensabile poter pensare di inviare una generica email, o pensare che possa bastare il sito istituzionale dell'azienda, informale e senza possibilità d'interazione, o ancora che basti indirizzare loro una pubblicità televisiva nel peak-time sperando che la vedano e, soprattutto, che la ricordino.

Il consumatore oggi si aspetta ben altro: si aspetta che le imprese adattino il proprio sistema d'offerta alle sue mutevoli esigenze, e, così, che non sia più bombardato da una miriade di messaggi indifferenziati. Per questo nascono campagne nelle quali, ad esempio, un'impresa invita il consumatore a creare lui il prodotto più adatto alle sue esigenze: l'esempio tipico, qui, è quello di Nike, che permette, tramite il suo sito, all'utente di scegliere la scarpa a lui più congeniale mediante la combinazione di diverse parti (colore, forma, ecc...); o ancora, i clienti spingono le aziende stesse ad istituire comunità, in rete, grazie alle quali le persone possano condividere esperienze e scambiarsi opinioni.

Deve risultar chiaro, comunque, che questo passaggio epocale non implica necessariamente la fine delle grandi campagne indifferenziate o, ancor più, la "detronizzazione" della pubblicità: è però chiaro che un'impresa, che opera in un settore altamente tecnologico, o che ha un target giovane, attivo e consapevole, non può assolutamente esimersi dall'acquisizione, nelle proprie scelte strategiche, delle nuove leve del marketing.

La pubblicità, dal canto suo, rimane sempre il mezzo più utilizzato da parte delle imprese per creare soprattutto "brand awareness"; ciò nonostante, circa il 70% degli utenti si dimostra irritato da un eccesso di pubblicità in televisione, ed un segmento di non minor entità sarebbe disposto a pagare pur di ricevere advertising coerente con i propri interessi, bisogni ed esigenze informative.

Senza soffermarsi troppo sull'argomento, che esula dagli obiettivi principali del presente scritto, si può dire che l'affermazione, ormai in tutto il mondo, della TV satellitare o digitale, con i suoi canali tematici, in contrapposizione con quella generalista, potrebbe divenire ben presto un ottimo canale tramite il quale veicolare pubblicità distinta a seconda delle diverse aree d'interesse.

Come dice il nome stesso, il Marketing 2.0 deve la sua nascita al grande, recente, sviluppo delle tecnologie del c.d. Web 2.0, che può essere definito come quell'insieme di piattaforme caratterizzato dall'assenza di mediazione per l'accesso, la creazione, la fruizione e la modifica dell'informazione e dei contenuti.

Grazie alla dimensione di dialogo che sta promuovendo, esso offre alle aziende l'opportunità di conoscere sempre meglio il proprio pubblico di riferimento, di imparare dalle persone stesse e consente loro di migliorare quindi il proprio servizio, in accordo e in armonia con i propri clienti. Questo significa poter ridurre i budget di pubblicità tradizionale, volta per lo più a imporre stili e creare bisogni, in favore di una sorta di co-progettazione dei servizi serena e conviviale con il proprio pubblico, la propria clientela.

Oggi il Web 2.0, pur basandosi sempre sulla medesima tecnologia Internet presente anche negli anni del «Marketing 1.0», si caratterizza per il fatto di aver modificato un approccio che non guarda più agli aspetti meramente tecnici e commerciali nell'utilizzo della Rete: il nuovo corso del Web si basa sulla "cultura della partecipazione" piuttosto che sulla sola capacità di connessione da parte degli utenti.

Le tre direttrici fondamentali del Web 2.0 risultano perciò essere: l'interconnessione, ovvero la possibilità di avere persone collegate sempre ed ovunque; l'informazione, sempre più facile da reperire e produrre, e la disintermediazione, la quale implica la caduta di limiti e barriere in Rete.

Riassumendo, possiamo vedere l'evoluzione dal Marketing 1.0 a quello 2.0 come il passaggio dal concetto di unidirezionalità a quello di bidirezionalità, contemplando quest'ultimo il fondamentale momento del ritorno di informazione, tramite feedback, dal cliente all'impresa. Ci si potrebbe spingere anche fino a identificare un concetto di multidirezionalità (many to many).

Si parla poi di rapporto non più impersonale tra le due parti, ma, al contrario, altamente personalizzato, dove il cliente viene messo al centro di tutte le relazioni aziendali; infine, la possibilità di veicolare messaggi indirizzati, con una possibilità di "reach" elevatissima, consente alle imprese di risparmiare ingenti risorse, in particolare ottimizzando quelle (talvolta scarse, soprattutto

in momenti di recessione come quello attuale) fornite dalla direzione generale alla divisione marketing.

Secondo diversi operatori nel campo del marketing, si assiste ad una rivoluzione copernicana che abbandona il classico paradigma delle 4 P di Kotler (Product, Price, Promotion, Point of sale) ed evolve verso un modello più snello, ribattezzato delle "3 P": delle prime, sopravvive solo la Promozione, vista come il fine di ogni azione di marketing; accanto ad essa si affermano i concetti di Piattaforma e di Partecipazione.

Per Piattaforma intendiamo l'ambiente digitale in cui l'interazione è visibile a tutti gli utenti, in maniera persistente nel tempo, e lo strumento attraverso cui l'impresa crea un sistema omnicomprensivo nel quale, tramite conversazione, si possa trovare risposta a bisogni informativi, sociali ed economici diversi.

Partecipazione, invece, come già accennato in precedenza, è uno dei concetti chiave dell'evoluzione di cui stiamo discutendo, che permette alle persone di non essere più dei semplici fruitori passivi dell'informazione, ma di diventare veri e propri "interattori" attivi nella produzione dei contenuti.

Alcuni contenuti prodotti nelle nuove piattaforme tendono addirittura ad essere considerati più autorevoli dei media tradizionali, in quanto espressi da persone che condividono relazioni ed interessi comuni e che non hanno interesse a fare pubblicità. Chiunque può avviare conversazioni con altri individui su uno stesso argomento: queste conversazioni si intrecciano tra loro attraverso parole chiave e link, costruendo così un ecosistema nel quale l'informazione iniziale si dipana in mille rivoli distinti ma in qualche modo coordinati ed ordinabili.

Nasce così un mondo dove gli utenti creano contenuti, si scambiano opinioni e condividono idee in modo semplice ed informale, favorendo la fiducia reciproca.

In sintesi, possiamo tracciare la strategia del "nuovo" marketing nel modo seguente: il Marketing Manager attua la propria campagna di Web Marketing tramite i vari social media, cercando di raggiungere un target preciso e selezionato; l'ideale in questa fase sarebbe rivolgersi, innanzitutto, a coloro che hanno già avuto esperienze (positive) con l'azienda in questione, in modo che, nel loro ruolo di "opinion leader", possano favorire lo scambio di commenti

e relazioni con altri gruppi di persone a loro collegate (ad esempio, tramite una pagina su Facebook).

Grazie a questi "prosumer", allora, i messaggi si diffonderanno rapidamente, trasmettendosi a molteplici soggetti formanti quella che abbiamo in precedenza definito tribù (o comunità); in questo modo, l'azienda sarà riuscita a veicolare il proprio messaggio ad un pubblico molto più ampio di quello di partenza, e di sicuro rilevante per il proprio business, dato che presenterà caratteristiche affini al target di partenza.

Ovviamente, l'impresa deve essere sempre presente in queste fasi, anche se all'apparenza sembrerà defilarsi "dietro le quinte": essa dovrà continuamente monitorare i vari social media e partecipare a scambi di idee e giudizi con gli altri utenti, così da recepire, o addirittura anticipare, le istanze ed i desiderata della clientela.

Se ben attuata, questa strategia potrà portare importanti risultati sinergici, tra cui quella che molti indicano come la "coda lunga della comunicazione" nel Web 2.0.

Secondo tale teoria, mentre nel sistema tradizionale dei media è presente un numero ristretto di emittenti che generano ciascuna un numero elevato di spettatori, nel nuovo panorama il rapporto si rovescia: grazie alle piattaforme del Web 2.0, miriadi di utenti producono contenuti rivolti ad altri individui che fanno parte del loro piccolo network personale; questi, relazionandosi tra loro, creano una "coda lunga" di tante piccole audience che, sommate nel loro complesso, possono arrivare a superare il numero degli spettatori legati ai media classici.

Il mercato si trasforma così, grazie all'utilizzo dei flussi di comunicazione partecipativi veicolati dalle nuove piattaforme, in un percorso di informazione che ogni giorno può arricchirsi di nuovi elementi.

I problemi possono sorgere qualora le informazioni che viaggiano sul Web, attraverso una comunità, risultino essere di discredito per una determinata azienda; bisogna considerare, infatti, che la velocità con cui commenti ed informazioni viaggiano in Rete, facendo diventare ogni utente un potenziale "veicolo di Marketing", alle volte può rivelarsi un micidiale boomerang per

l'impresa, qualora quest'ultima immetta sul mercato un prodotto assolutamente scadente.

È questo il caso della vicenda che vide, nel 2004, protagonista la Kryptonite, una famosa azienda produttrice di lucchetti. Tutto nacque da un post pubblicato su un forum di discussione, in cui si diceva che un particolare tipo di lucchetti per bicicletta prodotti da tale azienda si poteva aprire semplicemente con una penna bic: il primo video dimostrativo era, infatti, appena apparso su YouTube, e fu rapidamente seguito da altri amatori che si cimentavano in tale "impresa".

La notizia si diffuse rapidamente nel mondo web attraverso i post pubblicati su altri blog; l'azienda inizialmente era convinta che i propri clienti (per lo più distributori e venditori) nemmeno leggessero i blog, ma rapidamente capì che si stava sbagliando e fu costretta a correre frettolosamente ai ripari: dovette infatti spendere 10 milioni di dollari per sostituire gratuitamente 380.000 lucchetti difettosi in tutto il mondo.

Le considerazioni finora svolte ci hanno dimostrato come il Web 2.0 sia un mercato potenzialmente molto redditizio per le imprese che vogliono fare Marketing stando al passo coi tempi, sfruttando le nuove tecnologie per avvicinarsi sempre più al proprio target di riferimento.

Recenti ricerche dimostrano, infatti, come, pur in un momento di grave crisi come quello attuale, il "medium" Internet risulti essere quello che ha avuto il tasso di crescita più elevato in termini di investimenti pubblicitari tra il 2007 ed il 2008 (+15,6%).

La stessa ricerca ha poi dimostrato come, all'interno del WWW, i mezzi più utilizzati per fare pubblicità, a fine 2008, risultino ancora essere banner e button – strumenti tradizionali di comunicazione tipici del Web 1.0; per questo motivo, ritengo certamente che le imprese debbano fare ancora una lunga strada prima di avviarsi pienamente lungo il sentiero del Marketing 2.0, ma anche che una puntuale analisi delle caratteristiche delle nuove piattaforme, accompagnata da una piena condivisione degli obiettivi all'interno della propria

struttura, possa aiutarle a comprendere le enormi potenzialità che in futuro le si potranno aprire per una strategia di marketing sempre più personalizzato.

Tom Peters, CEO di FastCompany, lo aveva capito già in un insospettabile 1997, quando pubblicò un fantastico articolo intitolato *The Brand Called You*, "La marca chiamata te". Peters suggeriva che, qualsiasi sia la propria estrazione sociale o età, si è di fatto il presidente, amministratore delegato e responsabile Marketing dell'azienda chiamata "Io Spa". La propria reputazione e la propria credibilità si definiscono tramite la qualità del proprio lavoro attuale e passato e determinano la qualità del lavoro futuro.

La qualità del lavoro passato, determina il posizionamento per quello futuro. Questo è ancora più importante vista la direzione che sta prendendo l'economia del lavoro moderno: gli impiegati sono sempre più visti come consulenti freelance, fornitori e prestatori d'opera, anche da lontano, all'interno di un'organizzazione flessibile e remotizzata.

Il fiorire di aziende quali eLance.com⁹ e Odesk.com, dove chiunque può proporsi come sviluppatore per progetti informatici, design e altro, sembra confermare tale tendenza. Il segreto allora sta nella differenziazione e nella specializzazione. Se si è un programmatore, magari anche bravo, come si può riuscire a farsi distinguere dalla miriade di programmatori là fuori e convincere un'azienda o un cliente ad assumerti?

2.6 IL Personal Branding

Peters, con il suo articolo, ha coniato il termine *Personal Branding*, l'arte di costruire il proprio Brand, la propria marca personale. Il *Personal Branding* riguarda il modo particolare con cui tu fai Marketing di te stesso.

Il Brand personale potrebbe essere definito come quello che collettivamente le persone dicono, provano e pensano su di te e sui tuoi servizi nei vari contesti della tua vita. Fare *Personal Branding* significa influenzare quelle persone rispetto alla percezione del tuo Brand. La definizione di *Personal Brand* è la seguente: Il tuo *Personal Brand* è il motivo per cui qualcuno ti assume o richiede i tuoi servizi/prodotti.

Occorre anche tenere presente che il Branding è una cosa completamente inevitabile: appena le persone interagiscono con te in qualche modo, ti etichetteranno e ti faranno rientrare in una delle loro personali categorie. E' il modo con cui funziona il nostro cervello, disegnato per riconoscere schemi, somiglianze e differenze: comunque vada, le persone identificheranno coloro che incontrano con un Brand.

2.7 L'economia della reputazione

L'economia del Web2.0 si basa sull'entusiasmo dei suoi utenti di produrre servizi e contenuti di ogni genere. Se i grandi business, situati nella grande testa delle statistiche delle vendite, seguono un'economia regolata dal guadagno, le motivazioni di coloro che sono giù in fondo alla lunga coda sono senza dubbio differenti: prestigio, contatti, conoscenze e soprattutto reputazione.

La vera moneta del Web2.0 è la reputazione. Del resto la reputazione si può scambiare in fama, richieste di consulenza, offerte di posti di lavoro e soprattutto in soldi.

E ciò non è una novità. Come sanno bene i professori e i ricercatori universitari, pubblicare un articolo su una rivista di fama significa ottenere un incarico, finanziamenti e successo.

Ma il Personal Brand non è solo Reputazione.

Personal Brand non coincide con il solo concetto di reputazione. Quest'ultima è solo una delle dimensioni del tuo marchio. Altre dimensioni sono ad esempio la propria Rete Sociale e gli strumenti che si usa per comunicare l'identità (logo, slogan, colori, bigliettini, etc), la fiducia che si è in grado di generare nel Pubblico e, soprattutto la competenza. Senza competenza ed efficienza non esiste Personal Brand. Se quello che si fa non risolve i problemi dei clienti o non genera dei solidi benefici, il proprio Personal Brand non può rimanere forte a lungo.

Il proprio Brand non rimane forte a lungo se non viene sostenuto dalla competenza.

Uno potrebbe anche riuscire a creare un'immagine online fittizia ed improvvisarsi il massimo esperto su un determinato argomento, ma prima o poi, grazie ad Internet, verrebbe scoperto e smascherato (e massacrato).

Come nasce un Personal Brand?

Come scritto in precedenza tutti abbiamo già un Personal Brand. Magari solo offline, magari non proprio perfetto, ma in qualche modo esiste ed è percepito.

La vera domanda è: funziona?

Ma come diventa forte ed efficace un Brand?

Ci sono varie maniere e strategie, alcune più complesse richiedono il lavoro di professionisti specializzati, ma la più semplice è sicuramente quella di essere i primi. Considera ad esempio quello che hanno fatto le seguenti aziende:

- Coca Cola: la vera bevanda gasata colorata con caramello.
- Google: il motore di ricerca per definizione.
- Skype: il servizio di telefonia via Internet.
- Rimmel: il Mascara per antonomasia.

Cosa hanno in comune tutti questi Brand?

Sono stati i primi a offrire una soluzione particolare ed innovativa ad un problema noto:

- Coca Cola, la prima bevanda della sua categoria.
- Google, il primo motore di ricerca
- Skype, il primo sistema di telefonia online
- Rimmel la prima azienda a lanciare il mascara con la spazzola.

Questi Brand sono così noti che il loro marchio è utilizzato per far riferimento all'intera categoria di servizi o prodotti, proprio perché sono stati loro ad inventarla!

Essere i primi è un ottimo modo per creare un Brand, per essere ricordati.

Questo perché tutti si ricordano dei primi. Pochi ricordano le medaglie d'argento, i vice-campioni d'Italia o il secondo uomo sulla Luna. La gente ama i primi allo stesso modo in cui ama essere prima lei stessa. Pensa a quello che è avvenuto con Facebook. Inizialmente tutti ad iscriversi e a parlarne perché a classificare i siti sulla base dei link faceva tendenza. Adesso che fa meno tendenza ci vanno tutti lo stesso, ma non lo ammettono neanche sotto tortura!

Per gli stessi motivi spesso i primi finiscono sui giornali, sulla televisione e sugli altri media, aumentando ulteriormente le loro possibilità di successo.

Il modo migliore di specializzarsi è quello di fare qualcosa in una maniera diversa da tutti gli altri, perché, come diceva Lévi Strass: "non può esserci identità se non c'è differenza".

Vi sono vari modi per farlo. Talvolta significa semplicemente aggiungere uno o più termini alla parola chiave che identifica la tua attuale categoria, magari identificando l'ambito, il luogo, la modalità o lo stile.

Ad esempio un Designer potrebbe avere un metodo particolare o dedicarsi ai bicchieri o identificarsi con un colore o una forma particolari.

Ma sentito parlare di "Nero Armani"? Pensa che il celebre Designer Karim Rashid si è identificato con il colore rosa, tanto da vestirsi solamente in bianco e rosa!

Altre volte specializzandosi si compie una vera e propria piccola rivoluzione, magari associando le tue competenze con una delle tue passioni. Invece di essere "semplicemente" un architetto uguale a tanti altri, potresti aver la passione per l'impegno sociale e per l'ambiente. E' quello che ha fatto Camillo Magni, Professore presso la facoltà di Architettura a Milano e Presidente dell'associazione Architetti senza Frontiera Italia, un caro amico con il sogno di costruire case con meno di 2500 euro per le popolazioni più disagiate.

Essere specializzato ha inoltre ulteriori vantaggi:

- significa essere considerato automaticamente un esperto
- concentri i tuoi sforzi e le tue esperienze diventando sempre più competente
- ottimizzi i tuoi servizi e intanto fai quello che più ti piace.

Nell'era di Internet crescono le opportunità e aumentano i vantaggi per la specializzazione. Se ti specializzi e crei così una tua categoria, diversa da tutti gli altri, ti distingui e sei il primo. Tutti ti identificheranno chiaramente e il tuo Brand sarà forte ed efficace rispetto ai tuoi obiettivi.

CAPITOLO III

LA DISCIPLINA DEI DATI PERSONALI SU INTERNET

3.1 La diffusione dei social network

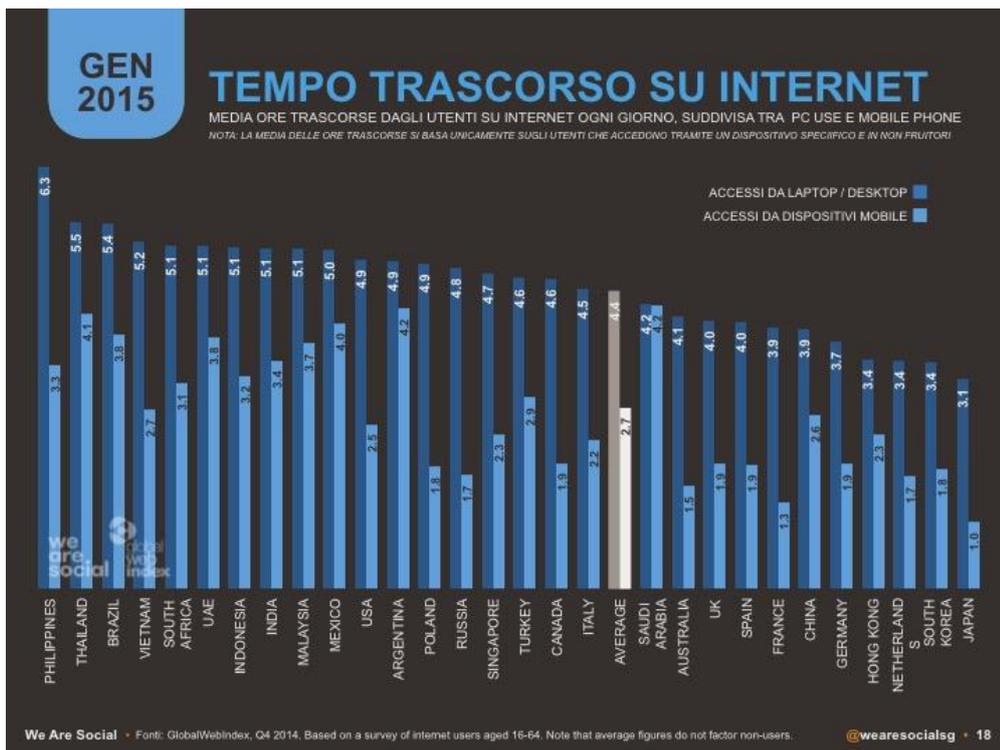
Prima di affrontare la complessa questione della privacy all'interno dei social network vale la pena di dare uno sguardo ai dati riguardanti la loro diffusione. Dal report annuale Digital, Social e Mobile 2015 sappiamo che il 2014 è stato un anno di crescita a tutti i livelli per quanto riguarda l'utilizzo dei canali social, sia in termini di volume, sia di modalità di interazione delle persone

A fronte di una popolazione mondiale passata da 7 a 7.2 miliardi di persone il numero di utenti internet attivi ha superato i 3 miliardi di utenti. Erano 2.5 miliardi 12 mesi fa (con una penetrazione che ha raggiunto il 42% dell'intera popolazione mondiale).

Gli account attivi sui social media sono oggi più di 2 miliardi (penetrazione 29%), con una crescita del 12% in 12 mesi. Per quanto concerne i dati relativi al mobile, è interessante notare come a fronte di un incremento della diffusione del 5% di utenti mobile, sia cresciuto invece del 23% il numero di persone che usano attivamente social media dai propri smartphone (313 milioni di persone in più).



La crescita di tutti questi indicatori è un fenomeno assolutamente globale. Ma l'Italia? Se a livello di penetrazione il dato è superiore alla media (60% vs 42% della media mondiale), osservando il tempo speso online ci accorgiamo che quello relativo all'accesso a internet da desktop è – di poco – superiore alla media – mentre quello legato alla navigazione da mobile è decisamente inferiore (2.2 ore al giorno, contro una media di 2.7 ore).

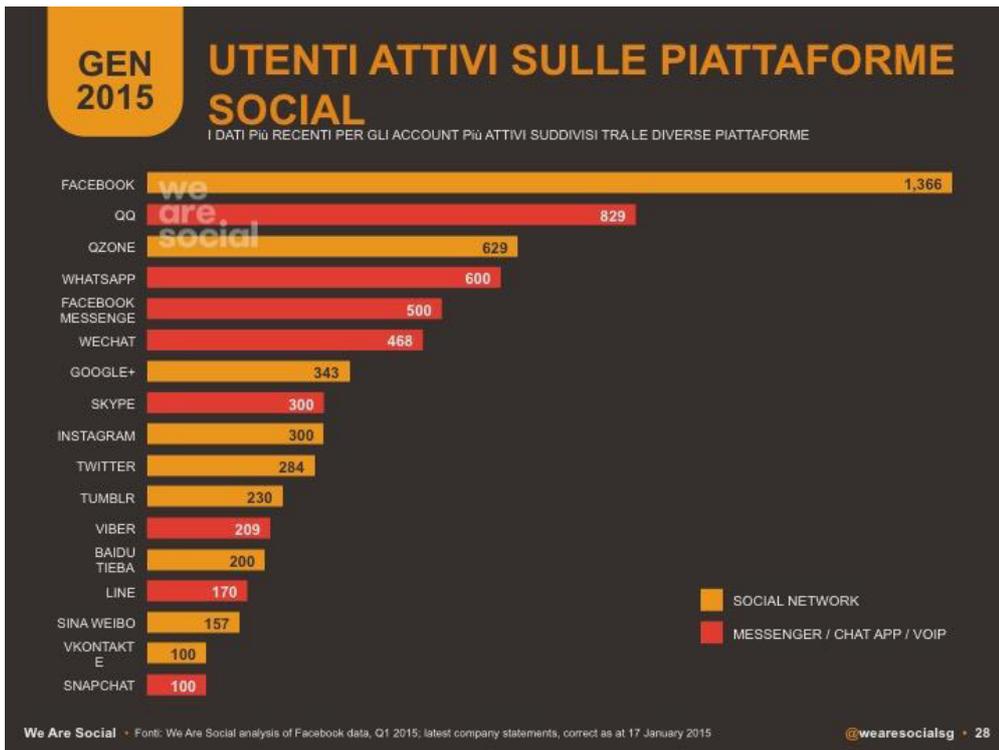


Insomma, sembra che gli italiani prediligano molte sessioni, ma di durata inferiore rispetto a quanto accade in altri paesi: a livello globale il numero di pagine visitate da desktop è diminuito del 13%, mentre è aumentato del 39% da smartphone (e 17% da tablet).

L'analisi relativa all'utilizzo dei canali social evidenzia come anno dopo anno risulti sempre più determinante permettere alle persone di interagire, e di trovare le informazioni che cercano: oggi sono più di 2 miliardi gli account attivi su piattaforme social (con una penetrazione del 29% sul totale della popolazione): in Italia la penetrazione è del 46% (il valore più alto è quello registrato a Singapore – 66% – mentre in Francia, ad esempio, è 45%, e in Germania 35%).

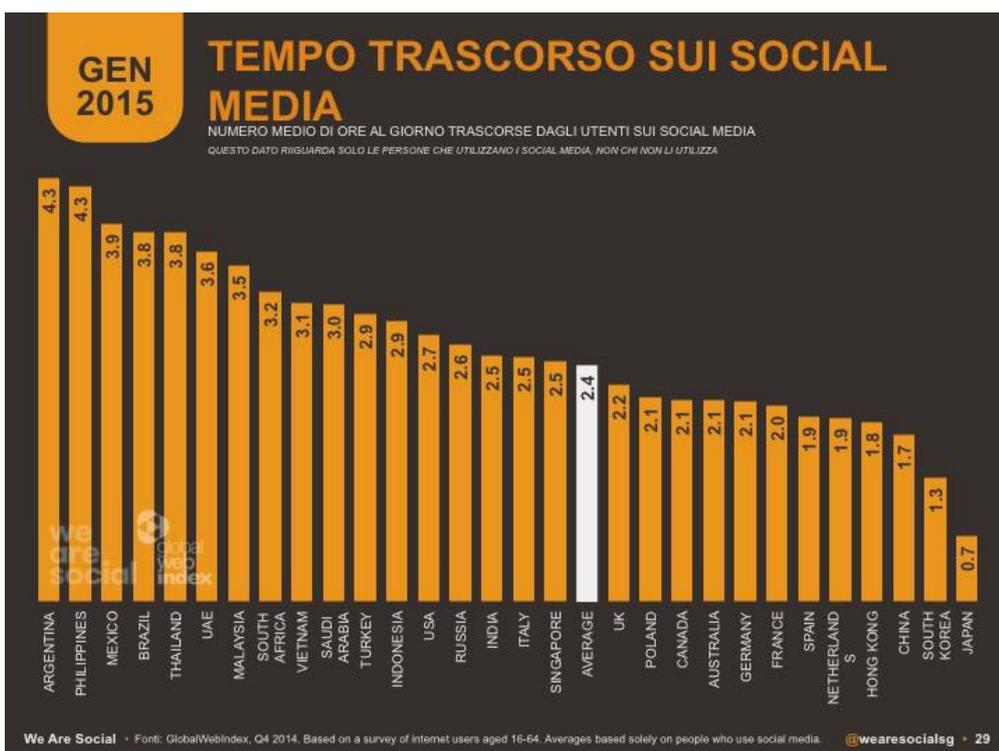


La piattaforma – largamente – più usata rimane Facebook (1.36 miliardi di utenti attivi), ma è interessante osservare come continui il trend di crescita dei servizi di instant messaging (WhatsApp ha superato i 600 milioni di utenti, contro i 400 milioni di 12 mesi fa, e Facebook Messenger è usato oggi da più di 500 milioni di persone; WeChat ha quasi raddoppiato la sua user-base, raggiungendo oggi i 468 milioni di utilizzatori).



La grande new entry in questa classifica è Instagram, che è oggi utilizzato da più di 300 milioni di persone.

Gli italiani trascorrono 6.7 ore al giorno su internet (tra mobile e desktop), e 2.5 ore sono dedicate all'utilizzo di canali social: contro una media mondiale di 2.4 ore (2 ore in Francia e 1.9 in Spagna – per offrire dei termini di paragone).



Ecco, invece, com'è cresciuto – negli anni – il traffico da dispositivi mobile a livello globale:



Ma scendiamo ora nel dettaglio, e osserviamo da vicino la situazione relativa all'Italia.

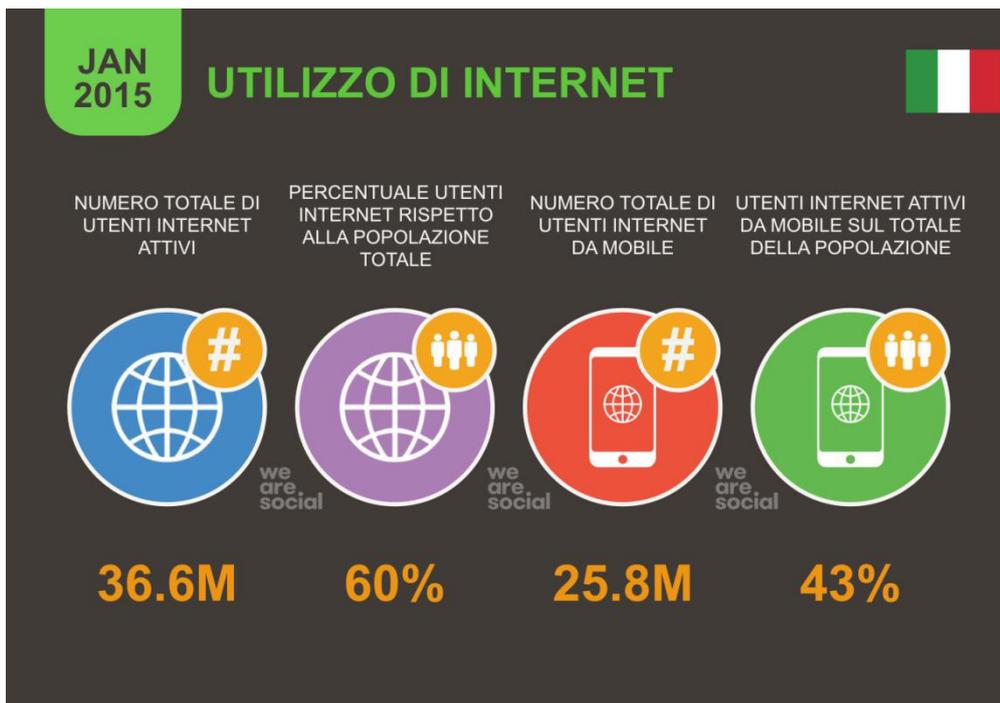
Il 60% degli italiani accede regolarmente a internet, e gli account attivi sui canali social sono oggi 28 milioni (22 milioni accedono da dispositivi mobile): quest'ultimo (accesso a canali social da mobile) è il dato che ha visto il maggior incremento negli ultimi 12 mesi (+11%), a dimostrazione di una sempre maggior propensione di interagire in mobilità e in maniera attiva con i contenuti a cui è possibile accedere online.



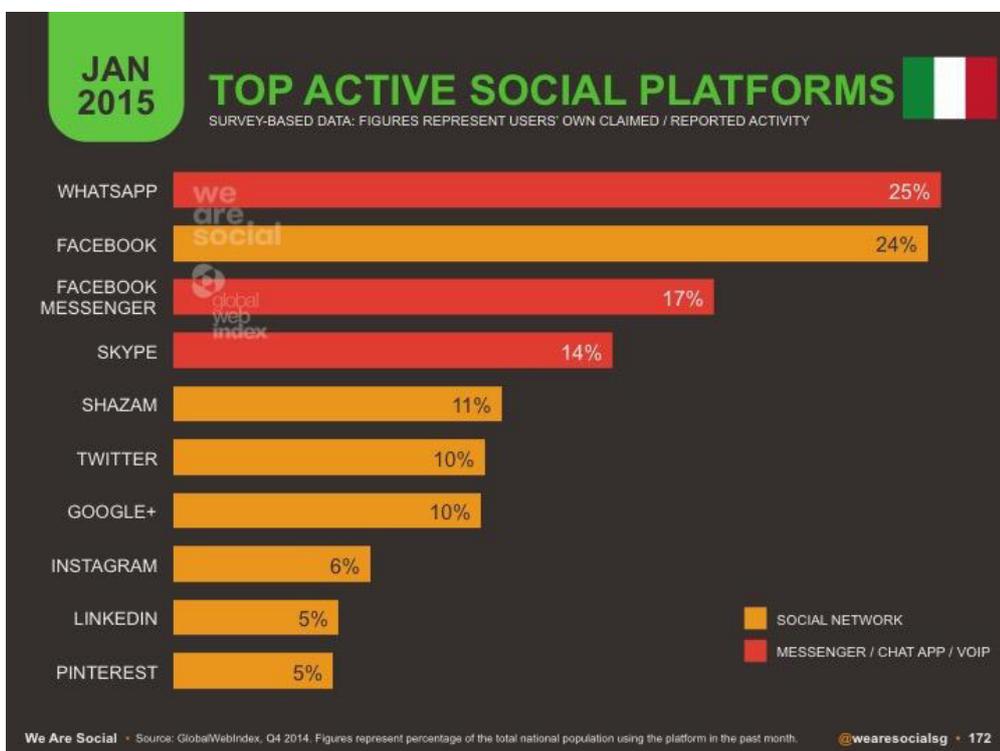
Ed ecco invece cosa emerge osservando il tempo speso su diversi media:



Di seguito invece i dati che abbiamo visto relativamente a ciò che accade a livello globale, calati sulla nostra popolazione:



Abbiamo visto come WhatsApp e – in generale – le piattaforme di messaging siano sempre più usate in tutto il mondo, ma in Italia questo è ancora più vero, tanto che – rispetto al totale della popolazione – sia proprio WhatsApp il servizio più usato ogni mese (ancor più di Facebook):



Quindi, anche in Italia, il mobile è sempre più il mezzo attraverso cui accedere a piattaforme di relazione e conversazione online. Gli italiani infatti usano i propri smartphone per svolgere diverse attività, un tempo delegate a schermi più grandi: la fruizione di contenuti video è sempre maggiore, così come l'uso di applicazioni legate a piattaforme social.

È interessante poi osservare come le percentuali relative a chi cerca informazioni su prodotti da acquistare, e di chi poi finalizza effettivamente l'acquisto da desktop siano identiche (39%), mentre c'è un piccolo discostamento tra chi cerca da smartphone, e chi finalizza poi dallo stesso dispositivo (20% vs 19%), perché – probabilmente – preferisce approfondire da desktop prima di concludere la transazione.



3.2 IL PROBLEMA DELLA PRIVACY NEI SOCIAL NETWORK

Attualmente i social network stanno vivendo un periodo di intenso sviluppo commerciale, dominato dalla necessità di catturare l'attenzione e l'interesse di nuovi utenti: questo si traduce, spesso, in una scarsa attenzione verso le problematiche relative alla sicurezza ed alla privacy.

Partendo da una ricerca dell'Enisa (agenzia europea per la sicurezza delle reti e delle informazioni), i principali rischi che, allo stato attuale, le piattaforme di social network pongono con riferimento ai dati personali degli utenti possono essere classificati in:

- rischi relativi alla riservatezza dei dati;
- rischi concernenti le identità digitali;
- rischi di natura tecnologica;
- rischi di natura sociale.

Ci soffermiamo sui rischi del primo tipo che, generalmente, hanno come presupposti la mancanza, la scarsa trasparenza o l'ambiguità delle politiche di trattamento dei dati e delle condizioni di utilizzo dei servizi, ma anche la possibilità di associare immagini ai profili oppure di etichettare le immagini con particolari metadati.

In questo contesto esistono dunque delle pericolosità specifiche:

- creazione di dossier digitali ed aggregazione di dati secondari;
- tecniche di riconoscimento facciale;
- content-based image retrieval;
- metadati associati o relativi alle immagini;
- problemi nella cancellazione dei dati degli utenti.

Sul primo punto c'è poco da aggiungere salvo che chiunque abbia accesso ad un qualsiasi servizio (l'accesso è libero, basta registrarsi, ed i controlli previsti in fase di registrazione sono spesso carenti) può acquisire e raccogliere i dati degli utenti, all'insaputa di questi ultimi, ed utilizzarli per le finalità più disparate (spam, pubblicità, attacchi diretti alla persona, discriminazione, ecc....) che, raramente, corrispondono a quelle per le quali è stato prestato il consenso.

Questo inconveniente non può ritenersi superato nemmeno in virtù dei tanto sbandierati controlli di accesso, sia perchè a volte i dati personali, apparentemente non visibili, risultano accessibili mediante una semplice ricerca, sia per la debolezza intrinseca di molte impostazioni predefinite (pochi utenti si preoccupano di modificarle!), sia perchè, in realtà, è molto facile diventare "amici" di tutti ed avere così accesso ai dati.

Considerazioni analoghe le possiamo fare anche per i dati di natura, per così dire, secondaria (indirizzi ip, data e durata delle connessioni, profili visitati, messaggi scambiati, ecc.): questi sono di regola accessibili ai fornitori per asserite finalità miglioramento dei servizi ma, in realtà, non esistono di fatto adeguate garanzie di protezione e, soprattutto, di trattamento per le finalità consentite.

In relazione al secondo punto, l'enorme progresso tecnico raggiunto nel campo degli algoritmi rende tutt'altro che teorico il rischio di una correlazione tra i profili, di cui gli utenti sono spesso titolari su servizi o piattaforme differenti, proprio per effetto del riconoscimento delle relative immagini. Lo stesso livello di rischio deriva dalla possibilità di utilizzare tecniche di content-based image recognition (CBIR), originariamente sviluppate nel settore della digital forensic, per dedurre informazioni utili alla geolocalizzazione degli utenti attraverso il riconoscimento delle caratteristiche degli oggetti o dei luoghi raffigurati nelle immagini associate ai profili.

La questione dei metadati abbraccia due evenienze diverse: da un lato c'è l'eventualità, offerta da alcune piattaforme, di associare alle immagini delle etichette contenenti informazioni personali relative alla persona ritratta (nome, cognome, indirizzo di posta elettronica, ecc...), senza prima aver ricevuto il consenso da parte di quest'ultima.

L'inclusione, invece, di particolari metadati nelle immagini digitali che vengono caricate sulle piattaforme, in particolare il numero seriale della fotocamera, può costituire una minaccia per la privacy dell'utente a causa della

associazione con i dati relativi al suo indirizzo riportati nella cartolina di registrazione della garanzia.

Infine una ulteriore questione da non sottovalutare è quella relativa alla eventuale cancellazione dal servizio: raramente, infatti, l'eliminazione dei dati principali si accompagna ad una completa rimozione di tutti i contenuti generati dall'utente (post, commenti, contenuti audio-video, ecc...).

Questa ambiguità è ulteriormente esasperata quando, a fronte di una richiesta di cancellazione, c'è soltanto una disattivazione del profilo, con conseguente mantenimento di una copia "nascosta" dei dati: entrambe le ipotesi costituiscono una violazione palese della direttiva 95/46/CE essendo gli individui privati di un mezzo efficace con il quale controllare la diffusione dei propri dati.

Su questo tema vale la pena di riportare la Risoluzione sulla tutela della privacy nei servizi di social network emessa in occasione della Trentesima Conferenza internazionale delle Autorità di protezione dei dati, tenutasi a Stasburgo dal 15 al 17 ottobre 2008.

Ecco il contenuto della Risoluzione:

“I servizi di social network sono divenuti estremamente popolari negli ultimi anni. Fra l'altro, si tratta di servizi che offrono agli abbonati la possibilità di interagire attraverso profili personali generati autonomamente, il che favorisce la comunicazione di dati personali relativi agli abbonati, ma anche a soggetti terzi, in una misura che non ha precedenti. I servizi di social network offrono una gamma del tutto nuova di opportunità comunicative e di interazione in tempo reale attraverso ogni possibile tipologia di informazioni, ma l'utilizzo di questi servizi può comportare rischi per la privacy sia degli utenti sia di terzi. I dati personali divengono infatti disponibili pubblicamente e in modo globale, secondo schemi qualitativi e quantitativi che non hanno precedenti, anche attraverso enormi quantità di foto e video digitali.

C'è il rischio di perdere il controllo dell'utilizzo dei propri dati una volta pubblicati in rete. Il fatto che si tratti di servizi operanti attraverso una

"comunità" di utenti può far pensare che la situazione non sia molto diversa dal condividere informazioni con un gruppo di amici nel mondo reale; in realtà, le informazioni contenute nel proprio profilo possono raggiungere l'intera comunità degli abbonati al servizio – talora in numero di diversi milioni.

Attualmente non vi sono che scarse tutele rispetto alla riproduzione dei dati personali contenuti nei profili-utente; possono essere copiati da altri membri della rete, o da terzi non autorizzati esterni alla rete, e quindi venire utilizzati per costruire profili personali oppure essere ripubblicati altrove. Talora risulta assai difficile, o addirittura impossibile, ottenere la totale cancellazione dei propri dati da Internet una volta che essi siano stati pubblicati. Anche dopo la cancellazione dal sito originario (ad esempio, un servizio di social network), possono esistere copie in mano a soggetti terzi o ai fornitori del servizio di social network. Inoltre, i dati personali contenuti nei profili possono "filtrare" dalla rete se sono indicizzati da un motore di ricerca, mentre alcuni fornitori di questi servizi consentono a terzi di accedere ai dati relativi agli utenti attraverso API (interfacce di programmazione applicazioni), cosicché tali soggetti terzi sono liberi di disporre dei dati in questione. Fra gli esempi di utilizzo ulteriore dei dati, possiamo citare la prassi invalsa presso molti uffici del personale di varie aziende di ricercare i profili-utente relativi a candidati all'assunzione o singoli dipendenti. Secondo quanto riferito dalla stampa, un terzo dei responsabili delle risorse umane ammette di utilizzare informazioni tratte da servizi di social network, ad esempio per verificare o completare le informazioni fornite dai candidati all'assunzione.

Le informazioni contenute nei profili-utente e i dati di traffico sono utilizzati anche dai fornitori di servizi di social network per l'invio di messaggi mirati di marketing ai rispettivi utenti.

E' molto probabile che in futuro si manifestino altre modalità di utilizzo dei dati contenuti nei profili-utente. Fra gli altri rischi specifici per la privacy e la sicurezza già oggi individuati, possiamo ricordare l'incremento del rischio di furti di identità favorito dalla diffusa disponibilità dei dati personali contenuti nei profili-utente e dalla "cattura" di tali profili ad opera di terzi non autorizzati.

La 30ma Conferenza Internazionale delle autorità per la protezione dei dati e della privacy ricorda che tali rischi hanno già formato oggetto di analisi nel documento "Relazione e Linee-Guida sulla Privacy nei Servizi di Social Network ("Memorandum di Roma")" adottato durante la 43ma riunione dell'International Working Group on Data Protection in Telecommunications (3-4 marzo 2008), nonché nel Position Paper n. 1 dell'ENISA dedicato a "Security Issues and Recommendations for Online Social Networks" (ottobre 2007).

Le Autorità per la protezione dei dati e della privacy riunitesi in occasione della Conferenza Internazionale sono convinte, in primo luogo, della necessità di condurre un'approfondita campagna informativa che investa tutti i soggetti pubblici e privati: dalle autorità di governo alle istituzioni scolastiche, dai fornitori di servizi di social network alle associazioni di utenti e consumatori, nonché le stesse autorità, al fine di prevenire i molteplici rischi associati all'utilizzo dei servizi di social network.

Raccomandazioni

Tenuto conto della particolare natura dei servizi in oggetto, e dei rischi per la privacy delle persone nel breve e nel lungo periodo, la Conferenza sottopone le seguenti raccomandazioni agli utenti ed ai fornitori di servizi di social network:

Utenti dei servizi di social network

I soggetti interessati al benessere degli utenti dei servizi di social network, ivi compresi i fornitori di tali servizi, i governi, e le autorità per la protezione dei dati, dovrebbero contribuire ad educare gli utenti alla tutela dei dati personali che li riguardano, trasmettendo i messaggi di seguito indicati:

1. Pubblicazione delle informazioni

Gli utenti di servizi di social network dovrebbero valutare con attenzione se e in quale misura pubblicare dati personali in un profilo creato su tali servizi. Occorre tenere presente che le informazioni o le immagini pubblicate potrebbero riemergere in tempi successivi – ad esempio, in occasione della

presentazione di una domanda d'impiego. Soprattutto, i minori dovrebbero evitare di fornire l'indirizzo o il numero telefonico di casa.

Sarebbe opportuno valutare se utilizzare nel profilo uno pseudonimo anziché il nome reale. Tuttavia, gli utenti devono ricordare che la tutela offerta dall'utilizzo di pseudonimi è piuttosto limitata, in quanto altri potrebbero individuare chi vi si cela dietro.

La privacy degli altri

Gli utenti devono rispettare la privacy altrui. Occorre particolare attenzione se si pubblicano dati personali relativi a soggetti terzi (comprese foto con o senza didascalie o etichette) senza il consenso di tali soggetti.

Fornitori dei servizi di social network

I fornitori dei servizi di social network sono tenuti ad operare nell'interesse delle persone che utilizzano i loro servizi. Oltre a rispettare la normativa in materia di protezione dei dati, dovrebbero mettere in pratica anche le raccomandazioni di seguito indicate:

1. Norme e standard in materia di privacy

I fornitori devono rispettare gli standard in materia di privacy vigenti nei Paesi ove operano. A tale scopo, dovrebbero consultarsi, se necessario, con le autorità per la protezione dei dati.

2. Informazioni relative agli utenti

I fornitori dei servizi di social network devono informare gli utenti in merito al trattamento dei dati personali che li riguardano, secondo modalità trasparenti e corrette. Inoltre, devono fornire informazioni veritiere e comprensibili sulle conseguenze derivanti dalla pubblicazione di dati personali in un profilo, nonché sugli altri rischi in materia di sicurezza e sulla possibilità che soggetti terzi (comprese, ad esempio, le forze dell'ordine) accedano legalmente a tali

dati. L'informativa deve indicare anche le modalità per una corretta gestione dei dati personali relativi a terzi che siano contenuti nei singoli profili-utente.

3. Controllo da parte degli utenti sui dati che li riguardano

E' necessario che i fornitori potenzino ulteriormente la capacità degli utenti di decidere l'utilizzo dei dati contenuti nei rispettivi profili per quanto riguarda i membri della comunità. Devono consentire agli utenti di limitare la visibilità dell'intero profilo, nonché di singoli dati contenuti nel profilo o ottenuti attraverso funzioni di ricerca messe a disposizione della comunità. Inoltre, i fornitori devono consentire agli utenti di decidere sugli utilizzi ulteriori dei dati di traffico e dei dati contenuti nei rispettivi profili – ad esempio, per quanto riguarda attività di marketing. Come minimo, devono offrire la possibilità di negare il consenso (opt-out) rispetto all'utilizzo dei dati non sensibili contenuti nel profilo, e prevedere un consenso previo (opt-in) rispetto all'utilizzo di dati di natura sensibile contenuti nel profilo (ad esempio, dati relativi ad opinioni politiche o all'orientamento sessuale) nonché rispetto ai dati di traffico.

4. Impostazioni di default orientate alla privacy

Inoltre, i fornitori devono prevedere impostazioni di default orientate a favorire la privacy degli utenti per quanto riguarda le informazioni contenute nei singoli profili. Le impostazioni di default sono essenziali ai fini della tutela della privacy; è noto come solo una minoranza degli utenti che aderiscono ad un determinato servizio si preoccupi di modificare tali impostazioni. Le impostazioni in oggetto devono essere particolarmente restrittive se il servizio di social network è destinato o rivolto a minori.

5. Sicurezza

I fornitori devono continuare a potenziare e garantire la sicurezza dei sistemi informativi, impedendo accessi abusivi ai profili-utente, utilizzando standard riconosciuti per quanto concerne la programmazione, lo sviluppo e la gestione delle rispettive applicazioni, e ricorrendo a verifiche e certificazioni indipendenti.

6. Diritti di accesso

I fornitori devono riconoscere alle persone (siano esse membri del servizio o meno) il diritto di accedere e, se necessario, apportare modifiche a tutti i dati personali detenuti dai fornitori stessi.

7. Cancellazione dei profili-utente

I fornitori devono permettere agli utenti di recedere facilmente dal servizio, cancellando il rispettivo profilo ed ogni contenuto o informazione da essi pubblicato attraverso il servizio di social network.

8. Utilizzo di pseudonimi

I fornitori devono consentire la creazione e l'utilizzo, in via opzionale, di profili basati su pseudonimi e promuovere il ricorso a tale modalità opzionale.

9. Accesso da parte di soggetti terzi

I fornitori devono prendere misure atte ad impedire che soggetti terzi possano raccogliere attraverso dispositivi di spidering e/o scaricare (o raccogliere) in massa i dati contenuti nei profili-utente.

10. Indicizzazione dei profili-utente

I fornitori devono garantire che i dati relativi agli utenti siano navigabili da parte dei motori di ricerca soltanto con il previo consenso espresso ed informato da parte del singolo utente. Deve essere prevista per default la non indicizzazione dei profili-utente da parte dei motori di ricerca.

Il Contributo del Consiglio d'Europa

Il Consiglio d'Europa ha pubblicato un contributo in occasione del Forum delle Nazioni Unite sulla Governance di Internet, organizzato dal 3 al 6 dicembre 2008 a Hyderabad, in India.

Con lo slogan «Internet - una risorsa essenziale per tutti», il contributo attribuisce particolare importanza ai diritti degli utenti. Diritti che sono oggetto dell'attenzione anche delle Autorità per la privacy che si sono riunite in conferenza a Strasburgo e che hanno deciso di adottare severi provvedimenti per difendere la privacy degli internauti.

Il problema, infatti, è che i siti di social networking come Facebook e MySpace sono pieni di dati sensibili immessi dagli stessi utenti e che non di rado finiscono nei motori di ricerca. Come è accaduto alla figlia di Sarah Palin, candidata vicepresidente per i repubblicani nelle elezioni USA, la cui gravidanza doveva rimanere segreta e invece è finita su tutti i mezzi di informazione, a causa della confidenza fatta dal suo ragazzo a un amico proprio tramite Facebook.

Secondo quanto concordato dalle Autorità dei 78 paesi che si sono dati appuntamento a Strasburgo, i social network dovranno adottare misure per rendere inaccessibili ai motori di ricerca tutti i dati sensibili dei propri utenti, a meno che questi ultimi non diano il proprio assenso. In secondo luogo, i provider responsabili del funzionamento dei vari aggregatori sociali virtuali dovranno fornire ai netizen informazioni trasparenti e approfondite sui rischi derivanti dalla diffusione dei propri dati personali e limitare la visione completa dei profili degli utenti solo ad altri utenti iscritti allo stesso social network.

3.3 LE NUOVE FRONTIERE DI TUTELA DELLA PRIVACY

Il diritto alla privacy, teorizzato dalla dottrina giuridica statunitense alla fine dell'Ottocento, nel corso di più di un secolo, ha mostrato la capacità di modellarsi in relazione all'evoluzione dei costumi ed al frenetico progresso tecnologico.

Il cosiddetto "right to be let alone", così come definito dal giudice americano Cooley, grazie anche alla originale giurisprudenza nord-americana, è divenuto "one theme that pervades the entire constitutional structure", non solo negli Stati Uniti d'America, ma in tutti i Paesi con un regime democratico.

Nel processo di affermazione della privacy come diritto fondamentale, è stato essenziale il ruolo delle convenzioni internazionali in materia di diritti umani: il riferimento va alla Dichiarazione Universale dei Diritti dell'Uomo, del 1948 (art.12), alla Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, del 1950 (art.8), alla Dichiarazione dei Diritti dell'Uomo in relazione ai mezzi di comunicazione di massa, del 1970 (art.1).

Con il tempo, direttamente collegata alle innovazioni tecnologiche, alla concezione di "privacy intimacy" che si riscontra nei documenti prima citati, si associa il concetto di "informational privacy", quale diritto dell'individuo di limitare e controllare la raccolta, la registrazione e l'utilizzazione, in particolar modo da parte di terzi, dei dati di carattere personale. Su questo filone si sono mossi l'Unione Europea con la Direttiva 95/46, il Consiglio d'Europa con la Convenzione Dati del 1981 e i singoli Stati, questi ultimi per lo più in attuazione degli impegni transnazionali.

Grazie alla corposa normativa comunitaria sulla privacy degli ultimi anni, l'Unione Europea è oggi la regione con il più alto livello di protezione dei dati personali al mondo.

Tuttavia lo sviluppo esponenziale dei mezzi di comunicazione telematica e, particolarmente, della rete mondiale Internet, sta via via mettendo in crisi gli strumenti normativi, messi a punto a livello nazionale e internazionale per tutelare il trattamento dei dati personali.

E' sotto gli occhi di tutti il fatto che Internet è una rete telematica planetaria, costituita da milioni di computer interconnessi tra loro attraverso le normali reti di telecomunicazione. E' utilizzata quotidianamente da milioni di utenti, che trasmettono una quantità enorme di dati. In altre parole siamo di fronte a una realtà globale, alla quale con molta difficoltà possono essere riferiti i parametri territoriali e giuridici ai quali siamo stati sin qui abituati.

Se vogliamo analizzare le principali caratteristiche del web notiamo che siamo in presenza di:

- mancanza di un sistema di gestione dei dati telematici centralizzato;

- libero accesso da ogni parte della Rete con strumenti e procedure di facile uso.

Appare ovvio che a queste condizioni, non può esservi nessuna forma di controllo complessivo delle innumerevoli operazioni che ogni giorno vengono compiute con internet e attraverso internet.

La Rete consente a milioni di individui di comunicare in tempo reale tra loro, al di fuori dei tradizionali mezzi di comunicazione e dei controlli insiti in questi. A queste condizioni essa è divenuta ben presto "uno spazio sociale, uno spazio politico, uno spazio economico, uno spazio altamente simbolico, che permette nuove forme di rappresentazione del sé, incide sulle identità, consente nuove forme di espressione e di esperienza artistica".

3.4 DATI PERSONALI E NATURA GIURIDICA DI INTERNET

Le opinioni sulla natura giuridica di internet sono varie e contrastanti:

secondo alcuni, Internet sarebbe un sistema, fondato su regole tecniche, che consentirebbe il collegamento tra un numero indefinito di soggetti che si trovano nelle stesse condizioni. Internet si configura dunque come un meta - territorio, dove i confini tra i vari Stati non sarebbero fisici ma logici.

Questa teoria però non spiega come i comportamenti di coloro che operano in Internet producano degli effetti concreti e tangibili nel mondo reale.

Secondo altri Internet sarebbe una realtà sovranazionale, più che transnazionale, dal momento che coinvolge e riguarda tutte le Nazioni dotate di infrastrutture di telecomunicazioni.

In base a tale teoria sono da tenere in conto le responsabilità dell'Internet Service Provider, del proprietario delle infrastrutture di rete, del gestore del sistema informatico. Tuttavia non viene affrontata la problematica della natura giuridica della Rete.

Secondo altri ancora, Internet sarebbe un sistema di telecomunicazione al livello planetario, che va al di là degli attuali termini di riferimento politico quali

lo Stato nazionale, la sovranità limitata dal territorio, la definizione dei confini e degli attributi di potere tra Stato e Stato.

Tale teoria tratteggia una rappresentazione realistica della Rete, dal momento che coglie la sostanziale novità di un fenomeno che difficilmente può essere regolamentato ricorrendo unicamente alle categorie giuridiche tradizionali.

Va ricordata infine la teoria, secondo cui Internet sarebbe un luogo di infinita libertà, in cui gli utenti potrebbero navigare nella più totale autonomia rispetto ad ogni autorità.

Tale teoria appare eccessivamente utopistica e fuori dalla realtà dal momento che dimentica come negli ultimi tempi i veri beneficiari della libertà di Internet non sono stati i singoli individui, ma le grandi multinazionali e gli apparati di controllo sociale dei governi.

In ogni caso, qualunque sia la teoria giuridica per la quale si propende appare evidente che Internet necessita di una regolamentazione per contenere gli abusi e soprattutto per identificare il foro competente in caso di conflitti d'interesse nell'ambito della Rete.

Numerosi sono i diritti che meritano di essere tutelati sul web ma certamente uno dei più importanti è il cosiddetto diritto all'autodeterminazione informativa, ossia la possibilità di controllare i processi di comunicazione che ci riguardano.

Nel sistema di circolazione planetaria delle informazioni, la privacy costituisce il "centro di gravità" attorno al quale si impernia il corretto utilizzo della Rete e il suo potenziale sviluppo.

Infatti, per usufruire di tutti i servizi che mette a disposizione Internet, dalla posta elettronica al commercio online (tanto per fare degli esempi concreti), è necessario che l'utente possa utilizzare i propri dati personali con la sicurezza che essi non vengano raccolti e rielaborati per costruire un profilo personale, suscettibile di future probabili invasioni della sfera privata.

In tale ottica, da strumento di isolamento dagli altri, da diritto ad essere lasciato solo, quale era la sua antica nozione, la privacy diventa strumento di comunicazione.

Afferma, a tal proposito, il giurista Stefano Rodotà:

"A me serve avere tutela dell'anonimato, a me serve la tutela della riservatezza, della privacy, non per isolarmi ma per partecipare. Solo se sono certo del mio anonimato potrò partecipare senza timore di essere discriminato o stigmatizzato a gruppi di discussione in Rete su temi politicamente sgraditi al potere dominante in un certo momento. Solo se avrò la certezza di non essere discriminato, potrò denunciare gli abusi, magari nel luogo dove io stesso lavoro.

Ecco allora che la riservatezza non è un problema di silenzio, di isolamento dagli altri, ma è uno strumento di comunicazione. Allo stesso modo, nell'area del commercio elettronico, la riservatezza diventa lo strumento attraverso il quale, con fiducia, io accedo all'acquisto di beni o di servizi, avendo ad esempio la sicurezza che quelle mie informazioni non saranno ulteriormente utilizzate, fatte circolare, elaborate per costruire profili della mia personalità che potrebbero avere anche effetti discriminatori".

3.5 LE MINACCE ALLA PRIVACY CHE VENGONO DAL WEB

Da anni le nuove tecnologie informatiche applicate alla Rete permettono con grande facilità l'acquisizione e l'elaborazione dei dati concernenti le persone e consentono un'utilizzazione dei dati stessi qualitativamente diversa dalla mera somma aritmetica che i vecchi strumenti consentivano, determinando una capacità di incisione della sfera giuridica del soggetto al quale le notizie si riferiscono, tale da non essere immaginabile in passato.

Per passare dalla teoria alla pratica basti pensare al caso in cui Tizio risulta iscritto a due gruppi di discussione (c.d. newsgroups), gestiti da soggetti diversi, di cui uno dedicato ad auto sportive, e l'altro al diritto.

Lo stesso soggetto ha pubblicato su un sito web di annunci economici gratuiti la ricerca di un'abitazione di lusso ed anche l'offerta di vendita di un'automobile di media cilindrata, indicando soltanto il proprio recapito telefonico.

La ricerca dell'abitazione di lusso attira l'attenzione degli specialisti dell'ufficio marketing di una società che propone investimenti finanziari di una certa consistenza i quali, individuate le generalità di Tizio tramite il suo numero del telefono, lanciano una ricerca in Rete.

Scoprono così che tale soggetto appartiene a due liste di discussione, sulla base di queste controllano velocemente gli Albi degli esercenti una professione legale e scoprono che Tizio è un avvocato, che ha raggiunto una buona posizione economica e che quindi gli può essere proposto un certo investimento.

E tutti questi dati possono essere incrociati e confrontati in pochissimi secondi permettendo di avere un identikit definito di una persona a cui poter vendere eventuali prodotti o servizi commerciali.

In questo caso, l'utilizzo delle informazioni è stato effettuato per fini di direct marketing, ma si comprende benissimo che lo stesso tipo d'indagine (peraltro legittima, essendo stata effettuata con strumenti ordinari di ricerca, senza compiere alcuna criminale forzatura dei sistemi informatici altrui) potrebbe essere compiuta per fini meno commendevoli.

Se poi dalla "normalità" si passa alla "patologia", ci si accorge che i rischi per la privacy sono molto più grandi di quanto si possa pensare.

Per effettuare un'indagine accurata in ordine ai nuovi modi in cui, tramite Internet, si può effettuare una violazione della altrui privacy, si deve avere riguardo ai vari tipi di dati circolanti, che possono essere così classificati:

Dati concernenti gli abbonati ad un provider

Premesso che un "provider" è un fornitore di accesso ad Internet, ogni provider dispone sia dei dati identificativi dei propri abbonati, sia dei dati concernenti il traffico degli stessi, i cosiddetti transactional data.

I "transactional data" sono equiparabili sostanzialmente al traffico telefonico e rientrano nella normativa dettata dalla Direttiva CEE 97/66 e dalle norme nazionali attuative (in Italia, il D. Leg.vo n.171/1998). Pertanto vanno mantenuti nel log (specie di registro elettronico del provider) per il tempo strettamente necessario per esigenze di fatturazione.

I dati identificativi degli abbonati costituiscono invece una vera propria banca dati, assoggettata alla disciplina di cui alla direttiva 95/46/CE ed alle norme nazionali attuative di questa (in Italia, la L. 675/1996).

Riuscire ad esaminare il traffico sul nodo di un provider consente di individuare tutti i siti cui un determinato utente si è collegato e, conseguentemente, di ricavare con un'elevata precisione tutte le sue preferenze ed i suoi interessi siano essi economici, politici, morali, professionali.

La posta elettronica

La trasmissione dei messaggi di posta elettronica (e-mail) è oggi l'attività più diffusa di Internet e, nello stesso tempo, uno dei punti più vulnerabili del sistema.

A livello giuridico la posta elettronica va assimilata alla posta tradizionale circa le forme di tutela, basti pensare alla tutela della corrispondenza.

Ora sappiamo che nei sistemi privati di posta elettronica i messaggi vanno direttamente al server e vi rimangono, fino a quando vengono letti.

Invece su Internet i dati passano da un server all'altro, fino a quando giungono a destinazione, il che espone i messaggi al rischio di essere intercettati lungo il loro cammino.

Poiché tutti i messaggi di posta elettronica, anche se cifrati, contengono in chiaro l'indirizzo del mittente e quello del destinatario, si è pensato di

approntare delle reazioni difensive, attivando gli "anonymous remailers", particolari server dotati di uno specifico programma, che consente di inviare la posta elettronica in maniera anonima.

In realtà, neanche il sistema dei remailers anonimi è del tutto sicuro in quanto, esaminando il traffico del remailer, è possibile stabilire una correlazione tra i messaggi in arrivo e quelli in uscita, così individuando l'effettivo autore del messaggio in uscita.

La tutela dei gruppi di discussione

Con gli anni, accanto ad Internet, si è sviluppata una rete parallela (Usenet), che viene utilizzata dai gruppi di discussione (newsgroups).

Chi partecipa ad un gruppo di discussione, invia dei messaggi, nei quali sono indicati il mittente, l'origine geografica del messaggio, la sua data ed ora, il suo contenuto.

Poiché i messaggi dei gruppi di discussione hanno natura di messaggi pubblici, essi possono essere tranquillamente letti da chiunque abbia interesse di vedere cosa fa e cosa pensa un determinato un soggetto o un determinato gruppo.

Negli Stati Uniti tali dati vengono elaborati da apposite società, che poi vendono i risultati delle indagini a fini commerciali.

La vulnerabilità della privacy di coloro che partecipano ai gruppi di discussione è stata l'oggetto principale dell'esempio concreto riportato al paragrafo precedente.

I servizi gratuiti

Esistono in Rete molti servizi come la distribuzione di programmi, la fornitura gratuita di pagine Web che vengono proposti all'utente come gratuiti, ma che tali non lo sono, perché, per consentire l'accesso, viene richiesta ad ogni utente la cessione di informazioni personali, che in questo modo diventano una vera e propria merce di scambio.

I documenti forniti dai server web sono poi generalmente composti da numerosi frammenti, ognuno dei quali è scaricato separatamente, potenzialmente anche da siti diversi.

In genere, nelle pagine web sono contenuti anche dei messaggi pubblicitari, scaricati da server appositi, che pagano il gestore della pagina per inserire gli annunci.

Nel momento in cui, nell'esaminare una pagina, l'utente "clicca" su un messaggio pubblicitario, generalmente scarica nel proprio computer e manda in esecuzione delle applet (piccoli programmi) java. Grazie a tale operazione, il gestore del server nel quale è memorizzato il messaggio pubblicitario è in grado di conoscere sia il tipo di client (programma che consente all'utente di navigare in Internet) utilizzato dall'utente, sia l'indirizzo IP del server tramite il quale l'utente si è collegato ad Internet, sia l'indirizzo del sito Web tramite il quale è stato letto il messaggio pubblicitario.

Se si visita un sito Web, può accadere che il server di questo spedisca al client del visitatore e da questo al suo hard disk un pacchetto di dati contenenti alcune informazioni quali l'indicazione del server mittente, una scadenza ed altri dati che interessano lo stesso server mittente.

In occasione delle visite successive, il server del sito Web chiede al client del visitatore di inviargli, sulla base delle istruzioni precedentemente impartite, dei piccoli file di testo, chiamati "cookies".

Questi, dal punto di vista tecnico, hanno la funzione di velocizzare il caricamento delle pagine web, facilitando il riconoscimento dell'utente.

Gli stessi cookies consentono tuttavia al server che li richiede di raccogliere dati sui siti e sulle pagine web precedentemente visitati dall'utente, potendo così ricostruire le abitudini e le preferenze di questo.

In sostanza, si tratta di una vera e propria "schedatura" all'insaputa dell'interessato, che molte volte ignora addirittura l'esistenza stessa di tali file,

diretta generalmente ad incrementare il "direct marketing", ma che contrasta pienamente con la tutela della privacy.

In conclusione, su Internet esistono numerose occasioni in cui, tramite appositi programmi, è possibile individuare i siti visitati da un utente della Rete, le sue scelte ed i suoi gusti, in una parola, penetrare con la massima facilità nella sua privacy.

Un settore nel quale, più d'ogni altro, si combatte la battaglia della tutela della privacy è quello del commercio elettronico.

Questo è stato definito dalla commissione UE nella Comunicazione "Un'iniziativa europea in materia di commercio elettronico" [COM (97)157] come "lo svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica; la distribuzione on-line di contenuti digitali; l'effettuazione per via elettronica di operazioni finanziarie e di borsa; gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo delle Pubbliche Amministrazioni".

La definizione è molto ampia, comprendendo non soltanto gli scambi realizzati tra computer collegati in una rete telematica, quale Internet, ma tutte le fattispecie che implicano l'utilizzazione di strumentazioni elettroniche, indipendentemente dalle modalità e dalle procedure seguite.

Il commercio elettronico non si limita al contatto tra fornitore e compratore, ma s'estende alle fasi della trattativa e della negoziazione, della stipulazione del contratto e del pagamento dei prodotti o servizi acquistati e, nel caso di vendita di beni immateriali (quali software, informazioni ed altri servizi), anche della loro consegna.

Disciplinare il commercio elettronico con leggi nazionali è praticamente impossibile, poiché il traffico segue percorsi diversi, in relazione ai contratti stipulati dai venditori con i vari provider e da questi con altri provider.

In genere, gli utenti non si rendono neppure conto se il server al quale si connettono si trovi in Italia oppure all'estero, atteso che una pagina web può essere costituita da frammenti provenienti da server sparsi in tutto il mondo.

Peraltro, ove si voglia applicare una normativa nazionale a tutela dei dati personali, questa può essere facilmente elusa dal venditore, collocando il proprio server in un Paese con una legislazione più permissiva, e quindi più adatta alle proprie necessità.

Secondo una recente ricerca condotta un anno fa dall'IBM, negli Stati Uniti la preoccupazione maggiore della quasi totalità degli acquirenti di beni e servizi tramite il commercio elettronico è rappresentata proprio dall'insufficiente tutela della privacy.

E proprio tale timore ha determinato in tale Paese una diminuzione degli acquisti pro capite tramite la Rete.

Tutelare la privacy in maniera adeguata diventa così un'esigenza che, nata a livello individuale e sociale, viene ad avere rilevanti implicazioni anche in campo economico.

La necessità di un intervento efficace e tempestivo, che possa ridare fiducia, è ormai avvertita da tutti, anche perché la criminalità non sta certo a guardare.

Una recentissima fonte giornalistica ha evidenziato l'esistenza di un fenomeno molto inquietante, quello degli "ID theves" o ladri di identità.

Si tratta di criminali che riescono a procurarsi tutti i dati personali di un individuo (numeri di conto corrente, carta di credito e ogni elemento che possa identificare una persona), per assumerne l'identità nei confronti di banche, assicurazioni, negozi e chiedere prestiti o mutui, contrarre debiti, fare acquisti impunemente (negli USA circa 30.000 casi nell'ultimo anno).

Pare che su Internet esisterebbero addirittura dei siti che per 100 dollari renderebbero un buon numero di elementi capaci di caratterizzare un individuo.

La necessità di tutelare i dati personali su Internet quale condizione indispensabile per il commercio elettronico è stata riconosciuta dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali con un documento che risale al 23 febbraio 1999.

CAPITOLO IV

WEB REPUTATION E IDENTITA' DIGITALE

4.1 E' possibile rinunciare ad essere digitali?

In un articolo pubblicato sulla rivista "Informatica e diritto" già nel 2008 Miranda Brugi, professore a contratto di Sistemi informativi per la pubblica amministrazione presso la Facoltà di ingegneria dell'Università degli Studi di Padova si interrogava su una questione essenziale per il futuro del nostro essere digitali: se un cittadino, oggi, e indipendentemente dal suo utilizzo di Internet, volesse rinunciare al suo "essere digitale" gli sarebbe possibile? Quanta effettiva competenza ha un soggetto qualsiasi per decidere fino in fondo quando uscire da una rete digitale nella quale può entrare suo malgrado? La domanda nella sua banalità, apre di fatto scenari diversi e suscita molteplici riflessioni da parte degli addetti ai lavori. Le risposte, a loro volta, sono molte, spesso ancora abbozzate e rivelatrici della poca dimestichezza che si ha nel considerare il problema dell'identità digitale oltre la sua rappresentazione in termini di tecnologie usate per la gestione. È degli ultimi anni la consapevolezza che il tema è dei più delicati e necessita di un'analisi approfondita e multidisciplinare, tale da produrre risultati che possano essere condivisi e conosciuti dai proprietari delle informazioni che partecipano alla costruzione in rete di una loro identità per presentarsi ad altre identità con le quali intendono relazionarsi. Riflettere compiutamente sulle differenti implicazioni sottostanti ai molti punti di vista è una necessità se si vuole rispondere ad un bisogno ormai avvertito di trovare categorie idonee alla interpretazione dei cosiddetti diritti di cittadinanza digitale all'interno dei quali il diritto alla privacy è uno dei più rammentati.

Fare chiarezza su alcuni concetti che possono fin dall'inizio originare confusione all'interno di uno schema di riferimento in cui si intende muoverci è auspicabile. Asserire che il problema della identificazione in rete non si pone solo per Internet aiuta a decifrare l'ambito di applicazione delle regole tecnico giuridiche che man mano vanno delineandosi, dovendo essere comunque gestite attraverso la rete un numero sempre più elevato di relazioni tra cittadini e cittadini, tra cittadini ed imprese, tra cittadini, imprese e pubblica amministrazione.

Parlare di identificazione significa, nella prassi giuridica, riferirsi specificamente a persona fisica ed alle caratteristiche indispensabili e immutabili alle quali si riconduce una entità per differenziarla dalle altre che compongono l'insieme; ma significa anche assumere che un soggetto terzo ne effettui l'associazione in un documento che "a vista" dimostri ciò che dagli atti, in archivi appositamente costruiti e predisposti per rispondere a domande specifiche, risulta si debba dimostrare di essere in quel preciso momento. Tale documento indipendentemente dal supporto fisico che lo contiene diventa il pass, la chiave idonea ad aprire le porte fisiche o virtuali attraverso le quali si raggiungono i luoghi che, previa identificazione da parte del tenentario e certificatore dei dati, si è autorizzati a visitare. Il luogo in questo caso è da considerarsi come la metafora di ciò di cui abbiamo bisogno, informazioni, servizi e quant'altro possa rappresentare una risposta. L'identificazione rappresenta quindi la prima tappa di un procedimento che sfocia nell'autorizzare chi ne ha titolo – e solo lui – a fare o non fare ciò per cui lo stesso soggetto è stato prima identificato e successivamente autorizzato.

Come si può ben comprendere, la confusione interpretativa dei due momenti o addirittura la loro assimilazione rende difficile una corretta valutazione delle problematiche connesse alla gestione, in primo luogo, della identità personale, indipendentemente dalle regole di registrazione dei dati che la rappresentano, e secondariamente della identità digitale. Quest'ultima non è, per sua intrinseca natura, la versione digitale di quella fisica, anche se l'algoritmo che può rappresentarla permette l'accesso ai servizi offerti dalla rete, quando

richiesto, così come il documento di identità permette, sempre che l'identificazione ne sia condizione indispensabile, l'ammissione alla presentazione della domanda per ricevere un servizio ad un front-office fisico.

Un individuo può assumere in rete tutte le identità che la sua fantasia gli permette o può scegliere quella corrispondente alla sua reale posizione anagrafica attribuendosi ogniqualvolta i connotati che più lo soddisfano. Lo stesso individuo può altresì essere costretto a identificarsi o meglio autenticarsi con le regole tecniche e gli attributi personali stabiliti da leggi dello stato quando deve interfacciarsi con la PA. Comunque sia chi usa una o più password sa che al momento della richiesta di digitare lettere e numeri o di introdurre una carta elettronica lascia parte di sé o di quello che in quel momento e per quel servizio ha deciso di essere ed è ammesso che sia. Nella numerosità degli algoritmi usati, quando le regole gli appartengono, sta la convinzione di chi crede di poter salvare il proprio intero patrimonio informativo esponendo, di volta in volta, solo la quota di informazioni utili al soddisfacimento di uno specifico bisogno di cui la rete trasporta le soluzioni desiderate. In sostanza nel momento in cui attraverso un sistema si eseguono delle operazioni di autenticazione si condivide con il sistema un procedimento che pone alternative alla risposta ed è indifferente agli attributi di cui ci si vuole ornare a meno che la visibilità in termini di identificazione del richiedente espressa con connotati personali unici non sia prevista dalla normativa.

Il cittadino portato nella rete suo malgrado, in quanto cittadino di uno Stato, inteso nella accezione di tutta la PA, che sceglie di sostituire, approfittando di quanto oggi è possibile ottenere dalle ICT, i suoi sistemi informativi con sistemi interamente digitali, all'interno però di un sistema di governance del processo innovativo che prevede una trasformazione graduale anche del suo sistema ordinamentale in modo da codificare ciò che è ammesso e ciò che è negato. In questo caso la manifestazione di volontà del cittadino di essere o non essere soggetto digitale è espressa nei vari passaggi previsti dalla norma che accompagna il procedimento digitale cui è comunque obbligato a rispondere per essere o non essere qualcosa. In questo contesto non esiste alternativa e

quindi potremmo dire che si diventa digitali nel momento in cui si diventa cittadini di una tale realtà statale. Fino a che esisterà invece la possibilità di rivolgersi ad un front-office fisico, la scelta potrà essere fra il pensare di tutelarsi dando o chiedendo a voce certe informazioni ad uno specifico addetto, o il credere che i contatti on-line con la PA non sono meno sicuri, visto che – comunque esso sia acquisito – il dato è ormai gestito digitalmente e quindi soggetto alla velocità di trasferimento e trattamento in ogni dove a cui prima è stato accennato.

La tecnologia è oggi il motore per una rapidissima evoluzione verso soluzioni sempre più spinte nella ricerca di dematerializzare i procedimenti burocratici sottostanti ai rapporti tra cittadino e PA, per la qual cosa il cittadino è uno spettatore utente più o meno interessato e accondiscendente al cambiamento che gli viene proposto. Quando il passaggio alla versione completamente digitale di tali procedimenti sarà avvenuto, e meglio sarebbe se tale passaggio fosse accompagnato da consenso e accrescimento culturale, la possibilità per il cittadino di sottrarsi del tutto al cambiamento verrà meno, giacché lo stato di necessità lo obbligherà a certe operazioni derivanti dal suo stato di cittadinanza.

A questo livello il problema dell'identità in rete deve, come di fatto sta lentamente avvenendo, essere gestita con regole e tecnologie definite e ascrivibili a strumenti certi che riferiscono a sistemi pubblici appositamente normati. La persona fisica a cui viene associata una sua versione digitale sarà tanto più tranquilla quanto più avrà fiducia nella PA alla quale digitalmente si relaziona. La fiducia verso chi tiene i dati è però un presupposto della tranquillità anche prima di arrivare al momento della autenticazione in rete, e precisamente già quando gli archivi digitali vengono organizzati per i successivi trattamenti. Il fatto che possano sussistere dubbi sulla corretta tenuta delle banche dati o che il dato possa essere usato impropriamente, non può essere ritenuto problematico solo nel contesto digitale. Leggere le eventuali difficoltà dell'utenza nell'uso di sistemi digitali di identificazione pensando solo a ciò potrebbe infatti risultare fuorviante e riduttivo.

Seguendo questo ragionamento si può affermare che in ambito pubblico il cittadino deve poter stare nel digitale con la convinzione di essere protetto nella sua persona e quindi con le sicurezze che egli si aspetta vengano attivate a salvaguardia dei suoi diritti fondamentali, digitali e non. Ai fini del ragionamento sin qui svolto appare utile considerare inoltre che il tema della fiducia si riferisce alla PA in tutte le sue articolazioni e a chi la stessa PA delega le sue attività gestionali oltre che a tutti quei fornitori di servizi digitali pubblici e privati ai quali l'uomo di oggi ormai quotidianamente si interfaccia.

La seconda fattispecie in cui può riconoscersi l'umanità del duemila è rappresentata da colui che con manifestazioni di volontà afferenti alla propria sfera privata sceglie di utilizzare servizi presenti in rete nelle più diverse e sofisticate tecnologie, aderendo a regole tecniche che altri soggetti privati, pur condizionati da norme di valore generale, gestiscono per il funzionamento della rete stessa. In questo caso il tema della volontarietà ad acquisire caratteristiche o meglio essenze digitali assume altri significati per le conseguenze che possono scaturire dall'accettazione a stare in rete a quelle condizioni. La decisione di essere o non essere digitale in certi contesti è completamente a capo del soggetto che compie la scelta. Conoscere le regole è un suo dovere per poter poi decidere i modi con cui stare ed usare le potenzialità della rete nonché quelle per relazionare con gli altri soggetti della comunità. A tale proposito potrebbe dirsi che la tutela dei diritti deriva dalla norma generale, ma la controparte con la quale potrebbe verificarsi il contenzioso non ha sempre, per motivi oggettivi o per scelta, quella riconoscibilità alla quale il soggetto pubblico, PA o chi in quel momento la rappresenta, è obbligato a dare consistenza nel momento che gli viene richiesto. Se in rete e con riferimento alla comunità di appartenenza si ha più fiducia di affidare le credenziali ad un soggetto pubblico o privato dipende, molto probabilmente dalla percezione che il cittadino ha del livello di maturità democratica espresso da chi quella comunità rappresenta e di quanto il senso democratico è presente nel vissuto quotidiano dei suoi interlocutori reali.

Importante appare, in entrambi i casi sommariamente descritti, la possibilità di poter disporre da parte dell'uomo del terzo millennio delle conoscenze necessarie alla decodifica, in un linguaggio naturale, dei passaggi che gli vengono imposti dal sistema nella costruzione del procedimento digitale, qualunque esso sia, e della comprensione del valore, in termini di bene personale, che assumono in rete le informazioni che gli permettono la navigazione e i diversi livelli di accesso.

Certo è che la complessità dei sistemi poco garantisce chi non è esperto e, a maggior ragione, la sensazione di trovarsi impotenti di fronte ad un uso improprio di quanto scorre in rete può spingere a resistere al nuovo modo di essere. La scarsa conoscenza delle potenzialità dello strumento può produrre effetti quali la rinuncia all'uso e all'apprendimento dello stesso da una parte o, alternativamente, la richiesta di servizi formativi dall'altra. Il secondo comportamento è proprio di chi vuole possedere, come consumatore di nuovi beni, quanto serve in termini di patrimonio informativo per poter consapevolmente e in assoluta libertà gestire il proprio essere digitale, avendo conoscenza di quelli che sono i veri rischi che corre in rete rispetto alla propria privacy e rivendicando altresì il principio che la libertà all'accesso non possa essere limitata dalla convinzione di non poter esercitare con certezza il diritto ad uscire con cancellazione certa delle sue credenziali quando lo desidera. Sentirsi completamente nelle mani di altri per una cancellazione, o addirittura comprendere che con quello che di noi resta in rete si possa costruire, al bisogno, un altro soggetto che ci assomiglia e che può sostituirci nelle responsabilità che derivano dalle relazioni, fa aumentare la richiesta di sicurezza, esprimibile con ulteriori difficoltà tecnologiche da frapporre fra l'utilizzatore e gli altri cui intende nascondersi.

Il "consumatore evoluto" di Internet, frequentatore di siti e portali che effettua transazioni on-line con o senza pagamenti, cosciente di quali possano essere i punti deboli di tutto il sistema, sa che le fasi da attraversare vanno, a seconda del servizio che si chiede, dall'identificazione all'autenticazione e all'autorizzazione, come più volte sin qui evidenziato, ed ha la capacità di

decidere come stare nella comunità telematica. Conosce il rischio e ne accetta le conseguenze. Per un consumatore meno o per niente esperto la percezione di dipendere completamente dai corretti comportamenti di altri soggetti non agevola l'uso, se degli altri non si ha totale e piena fiducia.

4.2 LA REGOLAMENTAZIONE DELL'IDENTITÀ DIGITALE

Con la legge n. 98 del 9 Agosto 2013 il Governo Italiano ha introdotto all'art. 17-ter il Servizio Pubblico di Identità Digitale (SPID). Il tema dell'Identità Digitale è stato più volte identificato, a ragion veduta, come uno dei pilastri dell'Agenda Digitale. L'uso di Identità Digitali sicure permetterà di aumentare la fiducia dei cittadini nei servizi Internet, ivi inclusi i sistemi di pagamento online, facilitando l'accesso ai servizi e abilitando una serie di nuove funzionalità utili sia per i portali della Pubblica Amministrazione, sia per i servizi offerti dai privati, come l'e-commerce. L'uso di un sistema pubblico di Identità Digitale consentirà inoltre di contrastare in maniera molto efficace i fenomeni criminali e in particolare il Furto d'Identità e l'impersonificazione", tipologie di frode informatica in rapida crescita. L'Identità Digitale come concepita in SPID consentirà un aumento della tutela della Privacy, visto che verranno notevolmente ridotti gli archivi contenenti dati personali.

L'Identità Digitale è l'insieme delle informazioni che ci permette di accedere a servizi digitali di qualsiasi natura. Ci permette di essere riconosciuti, di proteggere il nostro accesso e i nostri dati. Lo standard ISO 24760 parte 1 la definisce come un insieme di attributi relativi ad una entità (persona fisica, persona giuridica, sistema, oggetto, ecc.). Questi attributi possono essere informazioni personali (Nome, Cognome, data di nascita), informazioni relative al nostro profilo (indirizzo di email, consenso privacy, abilitazioni a servizi, ecc.). Tra gli attributi, ve ne sono alcuni speciali denominati credenziali: sono utilizzati per poter accedere in modo sicuro ai servizi. La forma più semplice e conosciuta di credenziale è la "Password", ma negli ultimi anni si sono diffusi sistemi molto più affidabili e sicuri, dalle "One Time Password" alle Smart Card (Carta Nazionale dei Servizi), dalle App di sicurezza ai sistemi biometrici.

Normalmente ogni servizio o sistema informativo ha il suo sistema di Identità. E' per questo motivo che ogni qual volta accediamo ad un nuovo servizio, ci viene richiesto di registrarci e di fornire una credenziale (Password) per proteggere il nostro profilo. Con questo sistema negli ultimi anni abbiamo assistito ad una esplosione di profili. Se in linea teorica ogni servizio dovrebbe essere protetto con una password diversa, la quasi totalità degli utenti sceglie sempre la stessa password, che spesso coincide con la password utilizzata per l'accesso all'Email. Questo fa sì che l'email sia diventata di fatto un sistema di identità digitale, una sorta di Portachiavi digitale, facilissimo da violare, come è dimostrato dalla crescita esponenziale dei furti di identità.

A dimostrazione della gravità della situazione, il rapporto Verizon su Cyber Security del 2012 mostra che tra le sei prime tipologie di attacco, cinque riguardano il furto o la violazione di identità digitale.

E' su queste premesse che è stato creato SPID. Nato da una proposta di legge predisposta dagli on. Stefano Quintarelli, on. Paolo Coppola, e on. Antonio Palmieri, SPID è diventato un progetto della Presidenza del Consiglio, con il supporto di un ottimo gruppo di esperti e appassionati del tema. Il lavoro ha portato alla creazione di un modello innovativo, per certi versi unico.

Partendo dall'analisi dei progetti portati avanti da altri paesi come gli Stati Uniti (con il framework NSTIC), l'Inghilterra, l'Estonia, la Svezia e l'Azerbaijan, si è arrivati a creare un sistema innovativo che rispettasse le regole non scritte del Digitale e le aspettative degli utenti, che prediligono servizi semplici e diretti. Il risultato è un Decreto che, a differenza del passato, non entra nei dettagli tecnici, ma definisce uno schema generale che servirà di supporto alla creazione dell'ecosistema delle identità Digitali.

In questo ecosistema ci saranno diversi attori. L'attore più importante, al centro di tutto, è il cittadino, il quale potrà ottenere una o più identità digitali. L'identità Digitale è di fatto l'equivalente di un Passaporto Digitale, che conterrà alcune informazioni identificative obbligatorie, come il codice fiscale, il nome, il cognome, il luogo di nascita, la data di nascita e il sesso. Oltre a queste informazioni, l'Identità conterrà altre informazioni come un indirizzo di

email e un numero di telefono, utili per poter comunicare con il soggetto titolare dell'Identità. Oltre a queste informazioni, l'Identità conterrà una o più credenziali, utilizzate per poter accedere ai servizi in modo sicuro. Il secondo attore è il Gestore delle Identità. Il Gestore è un soggetto pubblico o privato che, previo accreditamento presso l'Agenzia per l'Italia Digitale, si occuperà di creare e gestire le Identità Digitali.

Oltre ai Gestori di Identità, sono previsti i Gestori di Attributi qualificati, ovvero soggetti che per legge sono titolati a certificare alcuni attributi, come un titolo di studio, una abilitazione professionale, ecc.

Il Cittadino potrà utilizzare l'Identità Digitale sui "Gestori di Servizi". I Gestori di Servizi saranno tutte le pubbliche amministrazioni, ovvero tutti quei soggetti privati che decideranno di aderire a SPID in maniera volontaria. Il Cittadino che desidera ottenere una Identità Digitale, si dovrà rivolgere ad uno dei Gestori di Identità Digitale accreditati. Il Gestore per poter fornire una Identità Digitale dovrà procedere con un riconoscimento forte del cittadino, attraverso una verifica de-visu. La verifica da parte del Gestore prevederà anche il controllo in tempo reale della coerenza degli attributi sull'ANPR, l'Anagrafe Nazionale della Popolazione Residente. Questo permetterà di rendere praticamente impossibili tentativi di creazione di Identità con attributi non corretti.

Nel caso in cui il cittadino disponga già di una Identità Digital SPID, oppure già in possesso di una Carta d'Identità Elettronica attiva o di una Carta Nazionale dei Servizi o di una Tessera Sanitaria con Carta Nazionale dei Servizi, potrà richiedere un'Identità SPID direttamente on-line, poiché il Gestore dei Servizi potrà usufruire della verifica de-visu e degli attributi già effettuata. Al momento della creazione dell'Identità Digitale, il cittadino verrà fornito di una o più credenziali di sicurezza. Queste credenziali dipenderanno dal sistema di autenticazione offerto dal Gestore di Identità Digitale. La grande innovazione è che SPID non prevede a priori uno specifico sistema di autenticazione, bensì consente al Gestore di Identità Digitale di fornire vari sistemi sulla base delle ultime evoluzioni tecnologiche. Il Decreto identifica tre differenti livelli di sistemi di autenticazione, sulla base dello Standard ISO/IEC 29115 :2013. Il

primo livello di SPID corrisponde al livello II dello Standard e prevede sistemi di autenticazione a un fattore, come ad esempio la password. Nel secondo livello, corrispondente al Livello III dello standard ISO/IEC 29115:2013, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, come ad esempio le One Time Password o sistemi di autenticazione basati su App.

Nel terzo livello, corrispondente al Livello IV dello standard ISO/IEC 29115:2013, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, come ad esempio le Smart Card e le SecureSIM.

Questo schema permette un grande livello di flessibilità, sia perché i Gestori di Identità Digitale potranno optare per lo stesso livello di sistemi di Autenticazione di tipo diverso, sia perché vi sarà la possibilità di far evolvere nel tempo i sistemi di Autenticazione sulla base delle nuove tecnologie messe a disposizione dal mercato.

Sebbene l'Identità Digitale contenga una serie di informazioni sul cittadino, SPID risponde al principio di condivisione minima degli attributi. Il Gestore dell'Identità Digitale fornire le informazioni sul Cittadino solamente previo consenso esplicito dello stesso. Un Gestore di Servizi potrebbe richiedere la conoscenza del nome, del cognome e la data di nascita del Titolare per poter accedere al proprio servizio: i dati verranno passati dal Gestore dell'Identità Digitale solamente se vi sarà l'esplicito consenso del Cittadino. Nel caso contrario nessuna informazione sarà fornita. SPID potrà essere utilizzato anche solo per la verifica delle credenziali, fornendo quindi anche un servizio di "Pseudonymity". In ogni caso, i Gestori dell'Identità Digitale saranno tenuti a trattare le informazioni dei cittadini secondo elevati criteri di sicurezza,

secondo il regolamento tecnico che sarà emesso dall’Agenzia per l’Italia Digitale.

Il Decreto è stato pubblicato in Gazzetta Ufficiale Serie Generale n.285 del 9-12-2014. A seguito di questo, è stato avviato un progetto Pilota aperto a tutte quelle società che vi vorranno partecipare sia in qualità di Gestori di Identità, sia di Gestori di Servizi. Il Pilota, della durata di sei mesi, sarà particolarmente importante per la finalizzazione delle Regole Tecniche, che dovranno essere emesse entro tre mesi dalla fine del Pilota.

Tutti i siti della Pubblica Amministrazione dovranno adeguarsi ai sistemi di Identificazione Elettronica previsti dall’art. 64 del Codice dell’Amministrazione Digitale. Tutti quei siti che oggi non permettono l’accesso tramite Carta d’Identità Elettronica o Carta Nazionale dei Servizi, potranno consentire l’accesso tramite SPID. Poiché SPID è neutro rispetto ai sistemi di autenticazione, le CIE e le CNS potranno essere utilizzate, fornendo così all’amministrazione un unico sistema di accesso che copre sia i sistemi già implementati, che quelli futuri.

4.3 LA VIA EUROPEA E LA VIA STATUNITENSE

Una volta appurato che Internet è una realtà composita l’applicazione pura e semplice nei confronti degli utenti delle Rete delle norme sui dati personali e sulle telecomunicazioni elaborate dalle singole nazioni e dall’ UE, pone notevoli problemi.

Infatti fino a quando il traffico Internet si svolge esclusivamente all’interno di uno Stato, è ovvio che si applicano le norme nazionali concernenti la protezione dati di quello Stato.

Tale situazione è tuttavia del tutto eccezionale dal momento che, nella quasi totalità dei casi, la trasmissione dei dati avviene, anche inconsapevolmente, utilizzando dei nodi collocati addirittura in altre zone del Pianeta.

Tutto questo mette in crisi alcuni concetti enunciati dalla normativa internazionale e nazionale, relativi alla protezione dati, come quelli di responsabile del trattamento, di trasferimento dei dati all'estero, del soggetto cui inviare l'informativa circa l'elaborazione dei dati e così via.

Mentre le utilizzazioni di Internet sono aperte a tutti e sono facilitate da procedure semplici, mancano degli efficaci sistemi di controllo.

Com'è stato evidenziato dal Consiglio di Stato francese in un'analisi svolta il 2 luglio 1998, "Internet e le reti numeriche sono soprattutto un nuovo spazio di espressione umana, uno spazio internazionale che trascende le frontiere, uno spazio decentralizzato che nessun operatore né alcuno Stato padroneggia interamente".

Da una parte la regolamentazione di origine statale deve ormai combinarsi con l'autoregolamentazione dei protagonisti, degli attori, dei servizi comunicativi; d'altra parte, tenuto conto dei limiti inerenti ad ogni iniziativa puramente nazionale, spetta alla cooperazione internazionale tra gli Stati far rispettare gli interessi pubblici in uno spazio largamente dominato dall'iniziativa privata.

Per una efficace regolamentazione della "Rete delle Reti" è necessario quindi fare ricorso ad una nuova "cyberlaw".

In tale ambito la prevalenza dev'essere data indubbiamente alla cooperazione internazionale che, tramite lo strumento giuridico dei Trattati, consente di costruire sistemi di controllo efficaci per evitare e reprimere ogni abuso e di individuare con maggiore successo la normativa di tutela di volta in volta applicabile.

Su questa strada si è mossa l'Unione Europea, che con le proprie direttive ha inteso operare sia nel campo delle fonti sovranazionali, sia nell'ambito dei singoli diritti nazionali.

In tutti questi casi abbiamo avuto una semplice regolamentazione di principio, che si limita a porre poche regole fondamentali, quali:

- stabilire la legge da applicare per individuare il luogo dove è stato commesso il fatto, determinando di conseguenza la giurisdizione, e quindi la competenza di questo o quel giudice nazionale, con riferimento quindi anche al tempo dell'azione;
- stabilire delle regole procedurali minime sulla rilevanza e sul carattere delle prove;
- individuare alcune azioni da considerare comunque dannose o vietate, anche a prescindere da quanto previsto dalle legislazioni nazionali;
- stabilire i riferimenti giuridici per poter eseguire un eventuale condanna nei confronti di un soggetto straniero

A tale fonte, con funzione integrativa, deve affiancarsi l'elaborazione di codici di autodisciplina, informali e per questo stesso in grado di essere aggiornati immediatamente (come le netiquettes statunitensi), per fronteggiare in maniera adeguata i problemi sempre nuovi proposti dall'uso delle tecnologie avanzate.

E' questa la soluzione preferita dagli USA, che sui codici di autoregolamentazione hanno costruito il loro sistema di tutela della privacy informatica, ancorché in maniera talvolta lacunosa, e quindi non del tutto soddisfacente.

Insomma, secondo i più accreditati studiosi di diritto internazionale, solo da tale sinergia dei trattati internazionali e dei codici di autodisciplina può venire la necessaria regolamentazione, per rendere Internet un luogo sicuro.

Quale che sia la soluzione preferita, un intervento che porti ordine nella circolazione delle informazioni all'interno della Rete è ormai necessario e non più rinviabile.

A livello ufficiale, la questione è stata posta già all'inizio dell'era di internet, con uno "studio ad interim" della Omega Foundation di Manchester, denominato "Una valutazione delle tecnologie di controllo politico" (PE 166.499), presentato allo STOA - Scientific and Technological Options

Assessment in data 18 dicembre 1997 ed alla Commissione sulle libertà civili e gli affari interni in data 27 gennaio 1998.

Nel predetto documento, sottoposto al Parlamento europeo in sessione ristretta nel settembre 1998 sotto forma di Sommario esecutivo aggiornato, vengono toccati vari argomenti.

Viene in particolare evidenziato lo sviluppo di nuove tecnologie, dalle lenti a visione notturna ai microfoni parabolici in grado di captare conversazioni a voce ad oltre un chilometro di distanza, dalle reti di sorveglianza televisiva a circuito chiuso ai sistemi automatici di riconoscimento dei veicoli tramite il numero di targa, dai computer mobili in grado di intercettare le conversazioni trasmesse da telefoni mobili in un certo settore alla camera stroboscopica danese Jai, in grado di scattare centinaia di foto in pochi secondi, per fotografare individualmente tutti i partecipanti ad una manifestazione o ad una marcia.

Si chiarisce che tali tecnologie, nate originariamente per i settori della Difesa e dell'Intelligence, si sono rapidamente diffuse nei servizi di mantenimento dell'ordine pubblico ed anche nel settore privato.

Sempre nello stesso documento si afferma l'esistenza di due sistemi mondiali d'intercettazione, di cui il primo chiamato "ECHELON" (comprendente attività di strutture d'intelligence USA, quali la NSA e la CIA, ed inglesi, quali GCHQ ed M16) ed il secondo chiamato EU - FBI (comprendente varie agenzie di ordine pubblico, quali FBI e Polizie di Stato dell'UE).

Secondo il rapporto, ECHELON dispone di apparecchiature di ascolto e sorveglianza diffuse in tutto il mondo, che costituiscono un sistema puntato su tutti satelliti chiave Intelsat, utilizzati come infrastrutture di trasmissione satellitare per comunicazioni telefoniche, Internet, posta elettronica, fax e telex.

I siti di questo sistema sono situati negli USA, in Nuova Zelanda, in Australia, ad Hong Kong e nel Regno Unito.

Dalla massa indiscriminata delle informazioni raccolte vengono estratti gli elementi interessanti mediante l'utilizzo di sistemi di intelligenza artificiale come Memex, mediante l'utilizzo di parole chiave.

Sempre secondo il rapporto, le informazioni raccolte concernono non soltanto le eventuali attività terroristiche, ma anche le attività di carattere economico.

Secondo alcune informazioni giornalistiche, alcune società USA sarebbero state avvantaggiate per talune forniture all'estero mediante l'utilizzazione di notizie riservate raccolte tramite ECHELON.

Quanto al sistema EU – FBI, questo è stato creato in segreto nel dicembre 1996 dall'Unione Europea e dagli Usa, su sollecitazione di quest'ultimo Paese, per integrare il sistema ECHELON.

Si tratterebbe di una rete internazionale di posti d'ascolto telefonici nel quadro del "terzo pilastro" degli accordi di Maastricht, concernente la cooperazione nel campo giuridico e dell'ordine pubblico.

Di tale nuovo sistema, oltre i paesi dell'UE e gli Usa, farebbero parte anche l'Australia, il Canada, la Norvegia e la Nuova Zelanda.

A seguito della presentazione di tale documento, il Parlamento Europeo in data 16 settembre 1998 ha adottato una Risoluzione sulle relazioni transatlantiche e sul sistema ECHELON, con la quale, dopo aver riconosciuto l'importanza delle relazioni USA - UE a livello economico, politico e della sicurezza mondiale, ha affermato testualmente nei punti salienti che:

- Riconosce il ruolo vitale della cooperazione internazionale per quanto riguarda la vigilanza elettronica nel bloccare e prevenire le attività dei terroristi, dei trafficanti di droga e della criminalità organizzata;
- Riconosce inoltre, tuttavia, l'importanza vitale di disporre di sistemi di controllo democraticamente responsabili per quanto riguarda l'uso di queste tecnologie e le informazioni ottenute;

- Chiede che tali tecnologie di sorveglianza vengano discusse apertamente tanto a livello nazionale quanto a livello UE e che nei loro confronti vengano adottate procedure che assicurino il controllo democratico;
- Chiede l'adozione di un codice di condotta per assicurare la possibilità di ottenere risarcimenti in caso di utilizzazione illecita o abusiva di tali tecnologie;
- Ritiene che la crescente importanza di Internet e delle telecomunicazioni mondiali in generale, e del sistema Echelon in particolare, nonché i rischi connessi al loro abuso richiedano misure precauzionali per quanto concerne le informazioni economiche così come un efficace criptaggio.

4.4 LE DUE ANIME DELLA PRIVACY

Insomma la privacy, nata come "right to be let alone" (privacy-property), è divenuta ai giorni nostri il "diritto di controllare l'uso che altri facciano delle informazioni che mi riguardano" (informational privacy). In base a ciò si può attuare una utilizzazione persecutoria dei dati stessi, una distorsione dell'identità sociale del soggetto, tale da comprometterne le relazioni con i soggetti frequentati quotidianamente o ancora la divulgazione indiscriminata di notizie, che impediscano al soggetto stesso di operare delle scelte in maniera autonoma.

La sua efficiente tutela può essere garantita soltanto se si riconosce l'esistenza di un vero e proprio diritto alla privacy, che affonda le proprie radici nei Trattati internazionali (Dichiarazione universale dei diritti dell'uomo, Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali) ed al tempo stesso se si intensificano gli interventi normativi (sia di tipo istituzionale, sia di tipo spontaneo, quali i codici di autoregolamentazione) in materia di tutela del trattamento dei dati personali, in quanto i nuovi strumenti tecnologici sono in grado di creare sempre più penetranti forme di intrusione, senza che gli individui se ne rendano conto e senza che i singoli Stati siano in grado di tenere il passo con tale incessante evoluzione.

Siamo in presenza di due aspetti tra loro complementari ed imprescindibili, perché non ha senso parlare di protezione dei dati personali se non si considera il valore giuridico fondamentale da tutelare, ossia la privacy.

Allo stesso modo la privacy non può essere intesa in maniera corretta ed adeguata, in tutte le sue necessarie implicazioni con riferimento alla società contemporanea, se non ci si rende conto della necessità di proteggere i dati personali.

4.5 DALLA PRIVACY ALLA WEB REPUTATION

In molti cercano su Google o sui social network il nome della persona appena conosciuta al telefono o in riunione per reperire il massimo numero di informazioni. Vengono presi in considerazione età, formazione, ruolo, luogo di lavoro o semplicemente per dargli un volto. Il web offre oggi tutte queste "curiosità" su un piatto d'argento e in molti casi reperirle è facile come un click.

Ma cosa succede se i risultati che appaiono nelle prime pagine del motore di ricerca non risultano legati alle proprie esperienze lavorative o formative, ma al contrario a situazioni - come foto o video - non propriamente "professionali" e che rischiano di mettere in imbarazzo? Quanto questo tipo di informazioni possono influire nella ricerca di un lavoro?

In questo contesto entra in gioco il personal branding che consiste nella promozione di se stessi, delle proprie capacità, professionalità e reputazione proprio come se la persona fosse un marchio. La rete rappresenta oggi il primo mezzo di personal branding e gli strumenti messi a disposizione dal mondo online contribuiscono a creare la propria identità digitale, la cosiddetta digital reputation. Scopo del personal branding è quello di renderci visibili, riconoscibili e ben reputati agli occhi di chi cerca il nostro nome sul web.

In effetti l'immagine online è il nostro primo biglietto da visita; per sapere qualcosa di una persona appena conosciuta la prima cosa che facciamo è digitare il suo nome su Google. Ciò che appare sulla prima pagina di risultati orienta immediatamente la nostra opinione. Se poi i contenuti dovessero avere una valenza negativa o addirittura lesiva, la prima impressione si

trasformerebbe in un giudizio. Questo vale naturalmente anche per i contenuti positivi. Un terzo caso è quello in cui nella prima pagina si trovino cose che non c'entrano nulla con noi, in questo modo è come se non esistessimo online. E anche questo potrebbe deporre a nostro sfavore, specie se la ragione del contatto è professionale. Per questo è di fondamentale importanza lavorare innanzitutto su quel primo spazio di incontro, i primi risultati associati al nostro nome sul motore di ricerca. Posizionare il contenuto desiderato proprio lì è un obiettivo non semplice che richiede lavoro e perseveranza e, nei casi più difficili, l'intervento di un professionista.

Innanzitutto quando si è alla ricerca di un lavoro. È di fondamentale importanza verificare, prima di proporsi per un colloquio, che la propria identità digitale risulti adeguata, quindi innanzitutto che non sia compromessa da contenuti sconvenienti. Particolare attenzione va dedicata alle foto e ai video, che sono i primi contenuti ad attirare l'attenzione e anche i primi proposti dal motore di ricerca. La situazione ideale è quella in cui i primi risultati raccontano già qualcosa di noi, di ciò che sappiamo fare e della nostra reputazione in un determinato settore. Per questo è molto importante anche la cura del proprio profilo nei portali specialistici e social network professionali, dove abbiamo la possibilità di pubblicare il nostro curriculum, intervenire in dibattiti pubblici nel nostro settore, stringere relazioni significative e dunque mostrare che abbiamo competenza. Se a questo si aggiunge anche un proprio sito personale, completo e aggiornato nelle informazioni, i punti guadagnati aumentano.

Come vengono reperite le informazioni sui candidati da ipotetici datori di lavoro?

Secondo i risultati dell'indagine Adecco 2013 su "Social Recruiting e Digital Reputation" il 77% dei responsabili HR ha cercato il nome di un candidato attraverso un motore di ricerca e l'88% utilizza almeno un canale online nel proprio lavoro di selezione, i primi tre sono: Facebook, LinkedIn e Twitter. Il primo motivo è verificare il CV, il secondo allargare il bacino dei candidati e il terzo è trovare candidati mirati. Infine il 34% dichiara di aver assunto

qualcuno utilizzando i social network. Sono numeri significativi e in crescita, che dimostrano quanto la reputazione digitale sia un elemento cruciale per conquistare opportunità di lavoro.

Esistono delle regole di massima che può essere utile tenere a mente per non incorrere in errori che potrebbero compromettere la propria reputazione online:

1. Prima di pubblicare su YouTube video di situazioni imbarazzanti (scherzi in spiaggia, battute da osteria, atteggiamenti o situazioni particolari, ecc.) è bene ragionare sul fatto che diventeranno di pubblico dominio. È importante inoltre non firmarli con nome e cognome.
2. Datori di lavoro, selezionatori del personale così come colleghi, docenti e compagni di scuola monitorano sempre i social network. È meglio usare immagini del proprio profilo non troppo ardite.
3. Verificare le impostazioni relative alla privacy dei propri account sui social network? Quando si postano foto o commenti personali è necessario prima pensare a chi è listato tra i propri contatti (solo amici, o anche colleghi, capo ufficio, professori, ecc.). E se le cartelle sono private o pubbliche.
4. Attenzione a inviare proprie foto a persone appena conosciute tramite chat, sms, e-mail: non si sai mai a chi potrebbero essere inviate.
5. Attenzione ai TAG! Esseri taggati rende pubbliche ad altri le foto che magari non avresti mai voluto girassero sul web.
6. Prima di farsi fotografare in locali pubblici in situazioni "imbarazzanti" è bene sapere che probabilmente le foto saranno pubblicate sul sito e sulle pagine social del locale e condivise innumerevoli volte.
7. Attenzione alla geolocalizzazione (tag luoghi, check in, ecc.) quando si postano foto o messaggi. Soprattutto se non si vuol far sapere dove ci si trova.
8. Il contatto Facebook è il nuovo numero di telefono, è meglio distribuirlo con parsimonia.

9. Non postare mai le date di partenza e rientro: anche i ladri monitorano il web

10. Attenzione a postare sui social network le immagini di minori

4.6 IL CONCETTO DI REPUTAZIONE

Per capire meglio i contorni giuridici ed economici della web reputation è opportuno partire dall'analisi del concetto di reputazione. Di reputazione si parla attivamente dagli anni '50, quando si cominciano a valutare l'importanza e le implicazioni dei concetti legati all'immagine aziendale. Molti studiosi hanno riaffermato più volte la valenza strategica per un'azienda della sua reputazione e come questa sia una risorsa importante in grado di determinare i risultati economici e di mercato e di quanta influenza possa avere per la soddisfazione di clienti. Una buona reputazione è un segnale forte per il mercato e la concorrenza in grado di comunicare la qualità dei servizi e dei prodotti offerti e può consentire maggiore flessibilità nelle dinamiche di formazione dei prezzi. Inoltre è stata sottolineata in varie occasioni la relazione fra reputazione e la possibilità di attrarre risorse umane di maggiore qualità o di migliorare l'accesso al mercato dei capitali e meglio attrarre investitori.

Anche se non esiste un significato univoco per il termine, che dipende dal contesto nel quale esso è utilizzato, in generale possiamo pensare alla reputazione come a un concetto legato all'immagine ma soprattutto a giudizi di valore dati dal pubblico riguardo alle qualità di fiducia e affidabilità di un'organizzazione formatesi in un periodo di tempo abbastanza lungo.

L'avvento e la grande diffusione di Internet e delle attività commerciali che si svolgono attraverso le applicazioni disponibili in Rete hanno ulteriormente aumentato l'importanza della reputazione di chi offre prodotti e servizi online e del clima di fiducia che questi operatori riescono a creare. Infatti, le attività di vendita online si svolgono di solito fra parti che non si conoscono o difficilmente hanno avuto altri rapporti e in un ambiente nel quale il consumatore, spesso, non ha un'informazione completa su quanto sta

acquistando e perfeziona la transazione prima di poter ricevere e controllare le merci o i servizi. Quindi il consumatore deve avere un certo livello di fiducia nel venditore e, come ben osservato fin dagli inizi della storia recente di Internet la mancanza di questo clima di fiducia o del riconoscimento di una buona reputazione nei confronti del venditore riduce di molto o elimina del tutto la propensione all'acquisto.

Una buona reputazione è quindi un elemento fondamentale per una qualunque organizzazione e molte attività di marketing e di promozione vengono tradizionalmente svolte con questo obiettivo.

Internet ha acuito il problema, e ancor di più quello strano coacervo di tecnologie e comportamenti noto oggi col nome di Web 2.0, che ha dato al termine significati e valenze nuove. L'importanza è grande come testimoniano ricerche molto recenti che dimostrano come piattaforme quali Facebook o Twitter abbiano un'influenza diretta sul traffico e sulle visite ai siti web degli operatori economici.

4.7 LE RECENSIONI ONLINE

Nel contesto di Internet 2.0 un aspetto che indubbiamente contribuisce alla reputazione e all'immagine di un'organizzazione è la discussione che si attiva sulle diverse piattaforme online sulle diverse caratteristiche di un'azienda e sui suoi prodotti e servizi. Come noto il fenomeno delle recensioni e dei commenti degli utenti è in crescita esplosiva e viene da molti seguito, studiato e anche temuto. A volte in maniera poco razionale si cerca di combattere questa espansione senza, spesso, comprenderne bene gli effetti e le reali possibilità di presa sul pubblico. Non bisogna dimenticare che guide, commenti e critiche sono da sempre state pubblicate e discusse su tutti i mezzi di informazione. Oggi il fenomeno ha assunto un gran peso per l'utilizzo capillarmente diffuso di Internet e del Web.

La qualità e numero delle recensioni hanno certamente un impatto sugli affari delle strutture interessate, ma le scelte del consumatore sono influenzate in

maniera diversa a seconda del suo livello di coinvolgimento: il numero di recensioni influenza i meno coinvolti, la qualità i più consapevoli.

Le recensioni si polarizzano, in genere valutazioni medie sembrano non valere il tempo e le risorse necessarie a scriverle. I commenti negativi, se ben gestiti, possono essere rovesciati nei loro effetti, ma se ignorati o snobbati possono avere conseguenze abbastanza pesanti. In ogni caso, positive o negative che siano, le recensioni online sono indicatori molto affidabili e utili per una migliore conoscenza del mercato e della concorrenza. Inoltre, cosa non secondaria, possono essere fonte essenziale per azioni di miglioramento dell'offerta. Infatti, come dimostra un recente lavoro (Cunningham et al., 2010), la valutazione espressa nelle recensioni pubblicate su TripAdvisor migliora nel corso del tempo, segno che gli hotel interessati traggono beneficio dai commenti dei visitatori e si impegnano nel miglioramento della qualità del servizio.

L'idea che molte recensioni, soprattutto quelle negative, siano infondate o in mala fede è falsa, in ogni caso cominciano a esistere metodi e tecniche per isolarle, anche se, per ora almeno, di non facile applicazione. In ogni caso il lettore è molto più sensibile di quanto non si creda ed è in grado, attraverso la consultazione di fonti diverse, di farsi un quadro abbastanza neutrale.

Eccessi di positività, come di negatività, nei commenti vengono (intuitivamente) identificati come poco affidabili e scartate nella formazione del giudizio.

Ovviamente queste sono indicazioni non sempre facilmente generalizzabili, anche se costruite su metodologie solide, collaudate e verificate e inevitabilmente si tratta di risultati medi e casi estremi non sono del tutto improbabili. In definitiva, il quadro che sembra emergere è quello di strumenti che se ben utilizzati possono rivelarsi estremamente utili ed efficaci per il miglioramento e la crescita del settore.

4.8 I MECCANISMI CHE STANNO ALLA BASE DI UNA BUONA REPUTAZIONE

E' a questo punto interessante comprendere i meccanismi principali che stanno alla base della diffusione di una buona reputazione. In altre parole, cerchiamo di rispondere alla domanda: una volta raggiunta una buona reputazione, come si fa a far sì che il più gran numero di persone lo sappiano? Quali sono i fattori che influenzano questa diffusione e come si possono (se si possono) controllare? Per fare ciò, tre sono gli elementi da considerare: la diffusione della reputazione, l'influenza che in questa diffusione hanno gli elementi più autorevoli della Rete e le risorse necessarie per innescare e favorire questa diffusione.

Possiamo considerare la reputazione come un qualcosa (un'idea, un messaggio, un concetto, un pettegolezzo, una moda) che viene comunicato attraverso la rete sociale. Lo scopo è quello di far sì che il maggior numero possibile di elementi della rete ne vengano a conoscenza (e accettino l'idea) nel più breve tempo possibile. In questo il meccanismo di diffusione è del tutto simile a quello della diffusione di un virus o di una malattia. Medici ed epidemiologi conoscono molto bene questo meccanismo e lo hanno studiato a fondo. Le prime idee risalgono addirittura a Ippocrate (IV secolo a.C.) e nel 1766 un famoso articolo del matematico svizzero Daniel Bernoulli è uno dei primi tentativi di descrivere con un modello matematico-statistico l'evoluzione di un'infezione.

Per quanto riguarda la diffusione di idee o di messaggi, esiste un certo numero di individui pronti ad accettare un'idea. A un certo punto un individuo si infetta, ha un'idea, e comincia a comunicarla a qualche altro membro del gruppo sociale cui appartiene. Esiste una certa probabilità che un altro individuo accolga quest'idea e quindi si ammali a sua volta. Passato un certo tempo, però, questo individuo può trovarsi nella situazione di dimenticare quanto gli era stato trasmesso e quindi torna nello stato di individuo suscettibile.

Dopo un certo periodo di tempo avremo una certa frazione della popolazione che stiamo studiando che ha accolto l'idea iniziale.

Va inoltre considerato che la diffusione della rete è stata accompagnata dalla crescita e dalla diffusione di un pubblico rinnovato, non più formato unicamente da consumatori passivi, ma da utenti consapevoli che diventano produttori di contenuti e di senso, detti anche prosumer. Il Social web o web 2.0, ha contribuito a generare nuove dinamiche socio-economiche e dinamiche partecipative che hanno profondamente inciso sul ruolo e dunque sul comportamento delle singole imprese tanto da rendere urgente il ripensamento delle classiche teorie di marketing e lo svecchiamento dei messaggi pubblicitari.

Il processo di circolazione delle informazioni avviene sempre più in un ecosistema che coinvolge professionisti, amatori, semplici consumatori che divengono produttori, e nuove forme comunitarie o di network sociali. Nel web le persone utilizzano i mezzi di comunicazione ogni giorno per costruire le proprie competenze, per ottenere informazioni, per discutere con altri utenti relativamente alle proprie passioni e ai propri interessi, per recensire e commentare prodotti o servizi.

Nello spazio creato da queste nuove forme tecnologiche, si creano comunità e mondi sociali in cui gli attori, per diversi motivi e interessi, entrano in contatto reciproco e si scambiano informazioni riguardo alle proprie conoscenze ed esperienze.

La reputazione si crea, si sviluppa e si distrugge in una complessa trama di relazioni e conversazioni che avvengono all'interno del "web sociale". Sempre di più le persone scrivono e leggono i blog, consultano i forum, guardano video, lasciano recensioni e influenzano così altri utilizzatori della rete su un determinato prodotto, su un marchio, ma anche su territori-destinazioni. La comunicazione e soprattutto l'influenziazione dei potenziali clienti, non avviene grazie ad una conversazione "one to many" o "one to one", ma è una conversazione essenzialmente "many to many", sociale, in cui chiunque può partecipare e dire la propria, commentare, segnalare, recensire, esaltare un prodotto, sia esso un paio di scarpe o una vacanza.

Per le imprese si aprono scenari del tutto inediti: obiettivo del marketing e della comunicazione non è più quella di convincere il cliente della bontà di un prodotto-servizio, ma è quella di mettersi in ascolto e dialogare con i propri utenti/clienti, senza fare affidamento alle sole relazioni pubbliche di tipo tradizionale e monodirezionale.

CAPITOLO V

Aspetti legislativi della web reputation

5.1 La novità di internet 2.0 nella vita di relazione

Preliminari ad ogni analisi sulla web reputation devono essere sia la consapevolezza dell'importanza dell'argomento trattato sulla vita quotidiana di ogni individuo, e sia della delicatezza che esso inevitabilmente porta con sé, anche in considerazione del possibile conflitto tra diritti fondamentali che spesso viene ad ingenerarsi, e quindi dal necessario bilanciamento che tra gli stessi deve essere operato.

Il problema infatti può porsi ogni qualvolta in internet vengano immesse notizie e informazioni relative ad una persona (fisica o giuridica) che portino ad una lesione dei diritti della personalità – immagine, nome, reputazione – della stessa, da bilanciarsi con i diritti di libertà di espressione, di critica o di cronaca del soggetto che tale informazioni ha diffuso o tali opinioni ha espresso.

Va però tenuto presente che la diffusione di internet quale mezzo di informazione e comunicazione fondamentale nella vita quotidiana è molto aumentata, ma ne sono cambiate negli anni anche e soprattutto le modalità di fruizione, in quanto ad oggi si è davanti ad una navigazione che permette un alto grado di interazione tra il sito e l'utente dove - basti pensare ai blog, ai forum o ai social network - sono gli utenti a creare i contenuti del sito mentre i gestori degli spazi si limitano a regolare e vigilare sul rispetto delle regole all'interno delle piattaforme.

Tali nuove e diverse modalità di fruizione non possono che influire anche sulla qualità delle informazioni che circolano in rete, dove ogni utente e "frequentatore" dei diversi siti, blog, forum e social network, scrive, commenta e diffonde qualunque tipo di informazione, con il rischio, quindi, di far circolare, notizie eventualmente false o comunque prive di una verifica sulla loro veridicità.

Sembra che, con il favore dell'anonimato, profittando di una normativa né chiara né uniforme, chiunque abbia la possibilità di screditare il prossimo, confidando nell'impunità e, molto spesso, anche nell'impossibilità del soggetto leso di ottenere qualsivoglia tutela.

L'Avvocato Generale Pedro Cruz Villalón, nelle conclusioni presentate nelle cause riunite C-509/09 e C-161/10, eDate Advertising GmbH/X, Olivier Martinez, RobertMartinez/MGN Limited, presentate in data 29 marzo 2011, ha infatti affermato: "...le eventuali vittime di pubblicazioni lesive dei diritti della personalità si trovano in una posizione particolarmente vulnerabile quando il loro supporto è fornito da Internet. La portata universale delle informazioni contribuisce a rendere la lesione potenzialmente più incisiva di quella subita, ad esempio, attraverso un mezzo convenzionale. La gravità della lesione si scontra con la molteplicità di regimi applicabili, dato che la dispersione territoriale fa sì che coesistano diversi sistemi nazionali e con questi, altrettanti sistemi giurisdizionali nazionali competenti a conoscere in merito. Il titolare del diritto della personalità lesa può quindi subire un danno potenzialmente maggiore, e al contempo vedere affievolita la tutela giuridica di tale diritto, a seguito della frammentazione e della incertezza giuridica della stessa."

Ad un primo impatto, quindi, sembra che, nella "giungla di internet" possano essere bypassate le cautele e le linee guida che dottrina e giurisprudenza nel corso degli anni hanno, in tema di tutela dei diritti della personalità, in conflitto con il diritto alla libertà di espressione (nelle varie forme della libertà di stampa nonché nel diritto di critica e di cronaca) approntato al fine di contribuire al bilanciamento dei diritti inviolabili della persona che vengono in rilievo, con la complicità di ordinamenti non sempre "al passo coi tempi".

5.2 I Profili penali

Cominciamo con l'analisi dei profili penali che potrebbero venire in rilievo attraverso l'utilizzo di internet in modo tale da essere lesivo per la reputazione di altro soggetto, a causa della diffusione di notizie o informazioni false, non veritiere o comunque disonoranti.

Chiunque diffonde siffatte informazioni, e qualora tale diffusione sia idonea ad offendere l'altrui reputazione, potrebbe incorrere nella commissione del reato di diffamazione commesso con la stampa o altri mezzi, previsto e punito dall'art. 595 terzo comma del codice penale.

Il diritto all'onore ed alla reputazione, rientrando tra i diritti inviolabili dell'uomo sanciti nella Convenzione e richiamati dall'art. 2 della Costituzione della Repubblica Italiana, deve essere bilanciato con il rispondente diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione, anch'esso tutelato dalla Convenzione e costituzionalmente garantito nell'art. 21 e – diritto che ricomprende a sua volta diritti di cronaca e di critica – e che ovviamente non può essere ritenuto un diritto riservato a chi fa informazione professionalmente, ma che fa riferimento ad ogni individuo.

Pertanto, chiunque, nell'esercizio dei propri diritti di cronaca, di critica e di libera manifestazione del proprio pensiero, si trovi nella possibilità di riferire fatti e di manifestare opinioni e, anche qualora con tale azione dovesse trovarsi a ledere la reputazione altrui, potrebbe essere esente da responsabilità penale, poiché, appunto, avrebbe agito "nell'esercizio di un diritto" e quindi nella previsione della scriminante contenuta nell'art. 51 c.p.; tuttavia, come precisa una consolidata giurisprudenza della Corte di Cassazione, purché questo avvenga entro limiti segnati.

È stato infatti chiarito, con sentenze conformi negli anni, che l'applicazione della scriminante non può essere "automatica" e che, pertanto, i diritti cronaca e di critica devono necessariamente essere sottoposti ad alcuni limiti, che sono:

- la rilevanza sociale dell'argomento trattato,
- la verità obiettiva dei fatti riferiti (nei limiti in cui ciò sia accertabile),
- il rispetto della continenza nelle espressioni utilizzate (ovvero riguardo all'utilizzo di una decenza espressiva), precisando che tali valutazioni sono da effettuarsi caso per caso dal giudice di merito, il cui vaglio rimane insindacabile in sede di legittimità, se adeguatamente motivato.

Tali considerazioni, sono state ribadite dalla Suprema Corte, la quale ha applicato i medesimi limiti che usualmente venivano riferiti alla diffamazione a mezzo stampa anche avuto riguardo il reato di diffamazione compiuto con ladiffusione di notizie e opinioni tramite un sito web (31392/2008).

Qualora il comportamento dovesse travalicare tali limiti giurisprudenzialmente segnati e non fosse quindi possibile per il soggetto agente ottenere l'applicabilità della scriminate di cui all'art. 51 c.p., il soggetto resosi responsabile della immissione in internet delle notizie false, o comunque di carattere diffamatorio, verrebbe quindi chiamato a risponderne penalmente.

Considerato che in casi di lesione alla web reputation, l'interesse primario per il soggetto leso, sia, più che "La Giustizia" in astratto considerata, l'immediata rimozione delle notizie o delle informazioni ritenute dal giudice di natura diffamatoria e, fino a quel momento, cristallizzate in rete.

Pertanto si intende qui valutare se e come una tutela cautelare in sede penale rivolta ad ottenere il parziale "oscuramento" del sito contenente l'informazione a carattere diffamatorio possa essere una via percorribile al fine di ottenere tutela e di arginare le conseguenze della condotta diffamatoria.

La giurisprudenza, sia di merito sia di legittimità, si è trovata infatti più volte apronunciarsi sulla possibilità, nonché sulla legittimità del sequestro preventivo dei siti internet, ovvero del loro parziale oscuramento, limitatamente agli scritti aventi carattere diffamatorio per il soggetto querelante.

Sul punto si registrano orientamenti spesso discordanti.

La Cassazione, infatti, con la pronuncia 7155/2011, confermando le decisioni assunte dal Tribunale di Milano in funzione di Giudice del Riesame, ha dichiarato la legittimità del sequestro preventivo di un articolo pubblicato su di un sito internet, in quanto ritenuto, in alcune affermazioni, lesivo della reputazione e dell'onore.

La Cassazione sottolinea che nei casi simili a quello sottoposto al Tribunale di Milano, la misura cautelare del sequestro preventivo possa essere concessa, sempre adottando le dovute attenzioni, poiché la pubblicazione e la diffusione di un articolo giornalistico a mezzo internet costituisce una manifestazione del proprio pensiero, e potendo quindi la stessa essere limitata solamente dalla necessità di effettuare una corrispondente tutela di diritti di pari dignità costituzionale.

Infatti la Corte ha specificato che "...Il sequestro preventivo, a sua volta, allorché cada su di un qualsiasi supporto destinato a comunicare fatti di cronaca ovvero espressioni di critica o ancora denunce su aspetti della vita civile di pubblico interesse non incide solamente sul diritto di proprietà del supporto o del mezzo di comunicazione, ma su di un diritto di libertà che ha dignità pari a quello della libertà individuale.

Occorre, quindi, che la sua imposizione sia giustificata da effettiva necessità e da adeguate ragioni, il che si traduce, in concreto, in una valutazione della possibile riconducibilità del fatto all'area del penalmente rilevante e delle esigenze impeditive tanto serie quanto è vasta l'area della tolleranza costituzionalmente imposta per la libertà di parola...".

In un'altra sentenza, invece, la Corte di Cassazione (Cass. 56054/2011) legittimava la misura del sequestro preventivo del sito internet, non accogliendo il motivo addotto dal ricorrente, ovvero che, con il sequestro del sito, stante la natura dello stesso di mezzo di comunicazione con più persone, lo si sarebbe reso indisponibile da parte di chiunque, associati, collaboratori ed utenti.

I giudici, infatti, affermavano, per contro, che il Tribunale del Riesame di Torino ben aveva fatto a confermare la misura, poiché ciò che veniva sottoposto a cautela reale era lo strumento tramite il quale il reato era stato consumato, non potendo avere rilievo la natura del bene che ne è stato oggetto, non potendo ritenersi che la sua naturale destinazione alla comunicazione con più persone potesse impedirne il sequestro preventivo, sottolineando altresì che l'adozione della misura viene giustificata quando essa è l'unica a apparire idonea ad assicurare che la condotta illecita non si ripeterà.

I giudici in tale pronuncia, ebbero l'occasione di trattare brevemente anche il tema del contrasto tra la misura cautelare e il mezzo oggetto del sequestro quale strumento idoneo a manifestare il proprio pensiero, e quindi un diritto tutelato dalla Carta Costituzionale così affermando: "il ricorso sul punto pare adombrare un conflitto di tutele tra il diritto alla libera manifestazione del pensiero, garantito dall'art. 21 Cost. e le norme che consentono il sequestro preventivo degli strumenti che costituiscono il veicolo tramite il quale il pensiero viene manifestato.

Valga in contrario osservare che la manifestazione del pensiero, a prescindere dal mezzo utilizzato, non può essere garantita anche per consumare reati come, nel caso di specie, la diffamazione".

Tuttavia, sebbene le sentenze sopra richiamate sembrano concordi nella possibilità di ammettere la misura del sequestro preventivo, i contrasti interpretativi sul punto sono comunque presenti.

Infatti, non va dimenticata la vigenza nel nostro ordinamento di due normative: Innanzitutto la c.d. "legge sull'editoria", ovvero la Legge n. 62/2001 che all'art. 1 comma 1 afferma : "Per «prodotto editoriale», ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con

esclusione dei prodotti discografici o cinematografici”, equiparando così i giornali on-line alle testate giornalistiche cartacee.

Tale norma, è stata interpretata in modo da estendere sicuramente le garanzie tipiche della stampa su supporto cartaceo anche ai giornali on-line. Proseguendo l’analisi della giurisprudenza in materia di sequestro preventivo, quindi, si intende analizzare come tale estensione abbia influito; la prima garanzia che va considerata è quella costituzionalmente prevista dall’art. 21 comma 3 Cost, ove prevede il sequestro degli stampati solo previo atto motivato dell’autorità giudiziaria nel caso di delitti per i quali la legge ordinaria lo prevede.

Tale legge ordinaria, nel nostro ordinamento è vigente, ed è il regio decreto legislativo 31 maggio 1946 n. 561: infatti tale norma all’art. 1 prevede l’insequestrabilità di edizione dei giornali o di qualsiasi altra pubblicazione o stampato (e per i siti web – cui la garanzia di non sequestrabilità se non nei limiti della legge è estesa ex art 1 comma 1 Legge 62/2001 - si intenderebbe l’oscuramento di una o più pagine) se non in virtù di una sentenza irrevocabile dell’autorità giudiziaria, salva la possibilità di concedere il sequestro di non oltre tre esemplari dei giornali o delle pubblicazioni o stampati che importino una violazione della legge penale. Tale ultima disposizione, contenuta nel secondo comma dell’art. 1 della normativa citata, viene tendenzialmente riferita dalla giurisprudenza alla possibilità di disporre un sequestro probatorio, anche perché il sequestro di solo tre copie non può certamente essere ritenuto conforme alle finalità tipiche del sequestro preventivo.

Orbene, per quanto di interesse, e quindi in materia di diffamazione a mezzo internet, vi sono delle pronunce di merito che, scostandosi dall’interpretazione riferita più sopra, hanno affermato che, qualora un blog abbia un contenuto squisitamente politico-informativo, esso non possa essere ritenuto differente da una qualsiasi rivista di opinione, ove vengono quindi espresse idee e giudizi i quali costituiscono espressione della libertà di critica politica e pertanto, “anche qualora il contenuto delle pubblicazioni ivi contenute integrasse gli estremi del delitto di diffamazione a mezzo stampa, il sequestro del sito web

sarebbe comunque precluso dall'art. 1 del d.l. 31 maggio 1946 n. 561, che vieta il sequestro della "edizione di giornali o di qualsiasi altra pubblicazione o stampato", con ciò riferendosi al sequestro inteso come "chiusura" del giornale (o "oscuramento" del sito web), incidente, cioè, sull'attività di "edizione" in sé e non su singoli e ben determinati supporti cartacei o di altro tipo".

L'ufficio indagini preliminari di Nocera Inferiore nel 2010, rigettando la richiesta di sequestro di sito web, ha accolto la tesi contenuta in alcune sentenze di legittimità che (Cass. Pen, sez. IV, 4 dicembre 2003) ed ha affermato come il regio decreto legislativo D.Lgs n. 561 del 1946 nell'art. 1 comma secondo non operi alcuna distinzione tra i tipi di sequestro (probatorio o preventivo) che possono essere ordinati dall'autorità giudiziaria, e che quindi, il limite della sequestrabilità di non più di tre esemplari deve essere osservato anche quando trattasi di sequestro con finalità preventive, disposto ai sensi dell'art. 321 c.p.p., salvo che ricorra l'ipotesi di cui all'art. 2 del citato R.D.L, riguardante le pubblicazioni da ritenersi oscene od offensive della pubblica decenza (come affermato da Cass. Pen., sez. V, 4 giugno 2004).

Il Tribunale di Nocera Inferiore, quindi, pur dando atto nella motivazione di un orientamento favorevole alla concessione del sequestro preventivo del sito web e contenuto in diverse pronunce della Cassazione, ha ritenuto preferibile aderire alla tesi da ultimo illustrata, sia perché ritenuta più conforme al dettato della legge e sia poiché maggiormente rispettosa del dettato costituzionale.

Ultima pronuncia in tema di sequestro preventivo da analizzare è quella contenuta nella sentenza 11 dicembre 2008 n. 10535 della Suprema Corte. In tale frangente la Cassazione si è pronunciata sulla legittimità di un sequestro non di un sito internet, ma di un "forum" ovvero di una "bacheca virtuale" ove gli utenti, a volte solo registrati altre volte viceversa senza un previo obbligo dell'inserimento dei propri dati, esprimono opinioni e scambiano informazioni su diversi argomenti.

In tale occasione il Tribunale di Catania dispose il sequestro di alcune pagine del forum, mentre, in sede di riesame venne disposto il dissequestro, previa rimozione dei "post" dai contenuti offensivi.

In sede di legittimità il Supremo Collegio precisò come fosse necessario operare una distinzione sul "luogo virtuale" in cui si ritiene commesso il reato. Infatti, qualora trattasi di "giornale on-line", ad esso devono applicarsi le garanzie estese ai sensi dell'art. 1 L. n. 62 del 2001. Tuttavia, per quanto attiene i nuovi mezzi di espressione del libero pensiero - quali "newsletter", "blog", "newsgroup", "mailing list", "chat", messaggi istantanei, etc.- la Corte afferma che essi non possano essere inclusi in blocco nella nozione di "stampa", ma che sia compito dell'interprete valutare caso per caso la loro eventuale qualifica di prodotto editoriale. Per il forum l'equiparazione - e la conseguente tutela - al prodotto stampato viene esclusa, non ritenendolo dissimile dalla bacheca classicamente intesa; ovvero un luogo dove ognuno può manifestare il proprio pensiero o comunicare delle informazioni, ma che deve restare privo di quelle garanzie che lo assimilano ad una testata giornalistica on-line ed alla quale sono applicabili tutte le normative sulla stampa.

Non va dimenticato che in ambito di reati commessi con il mezzo della stampa, è prevista anche la responsabilità penale non solo del soggetto che materialmente ha commesso il reato ma anche di altri soggetti individuati da specifiche norme penali. Trattasi, specificatamente del direttore o del vice-direttore responsabile (art. 57 c.p. per la stampa periodica) se omettono di esercitare il controllo sul periodico per colpa, o all'editore (per la stampa non periodica ex art. 57 bis c.p) qualora l'autore sia ignoto o non imputabile o a colui che ha provveduto alla stampa, qualora l'editore rimanga ignoto o non imputabile.

L'applicazione di tali articoli ai siti web, permetterebbe di estendere la responsabilità penale per il reato di diffamazione al direttore del giornale on-line, come al gestore del forum o del blog, fin'anche ai provider (ovvero i fornitori dei servizi internet).

Vale la pena di ricordare che la Cassazione (Sentenza 16 luglio 2010 n. 35511/2010) ha stabilito che tali normative non possono essere ritenute applicabili al direttore del giornale on-line sia perché la lettera della norma fa espresso riferimento alla stampa, sia perché, considerata l'assenza dell'esplicita estensione della responsabilità ex art. 57 c.p. al direttore del giornale on-line ad opera della L n. 62 del 2001, si incorrerebbe in un'analogia in malam partem, vietata dalla legge penale. Viene fatta salva ovviamente, l'eventuale ipotesi di concorso nel reato commesso da parte del gestore del sito, che rispondere non ex art. 57 ma ex art. 110 e 595 comma terzo.

La sentenza, esplicitamente esclude la responsabilità penale ex. Art. 57 c.p. per i reati commessi in rete, sia per "gli access provider, i service provider e gli hosting provider a meno che non fossero al corrente del contenuto criminoso del messaggio diramato (ma, in tal caso, come è ovvio, essi devono rispondere a titolo di concorso nel reato doloso e non certo ex art. 57 c.p.)." sia anche per i coordinatori dei blog e dei forum.

Il tema da ultimo citato dalla sentenza introduce quindi un ulteriore tema da trattare. Considerato che, fermo il bilanciamento degli interessi costituzionalmente garantiti, la tutela penale immediata, nella forma del sequestro preventivo, non è sempre considerata legittimamente applicabile ai siti internet e comunque sottoposta a moltissimi vincoli – e quindi la web reputation del soggetto continuerebbe a rimanere cristallizzata su internet e nella totale fruibilità di un numero indeterminato di utenti, liberi a loro volta di "condividere" su altre pagine o siti la notizia o l'informazione lesiva, moltiplicando gli effetti della lesione – ci si chiede se vi sia la possibilità di ottenere una pronuncia in sede civile che riesca a tutelare il soggetto leso.

5.3 La tutela in sede civile

Lo strumento giuridico per ottenere tutela d'urgenza in sede civile è già previsto nel nostro ordinamento, ed è il ricorso cautelare d'urgenza disciplinato dall'art. 700 c.p.c., che consente di ottenere, seppur in via cautelare, una

tutela immediata. I presupposti dell'azione sono, come per ogni controversia a carattere cautelare, il "fumus boni iuris" (e cioè la verosimiglianza che il comportamento denunciato offende un bene tutelato dall'ordinamento) e il pericolo grave ed irreparabile che ne deriverebbe in caso di mancata tutela.

Quanto al giudice competente, per le controversie insorte all'interno dello Spazio Giudiziario Europeo trova applicazione il regolamento 44/2001 sulla competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, ove all'art. 5 punto 3 afferma che la competenza stabilita in via generale del "foro del convenuto" è derogata in materia di illeciti civili dolosi o colposi, poiché il soggetto reso responsabile degli stessi può essere convenuto nel foro del suo domicilio, bensì davanti al giudice del luogo in cui l'evento dannoso è avvenuto o può avvenire;

L'applicazione di tale norma in relazione alla diffusione su internet di notizie o comunque di affermazioni dal contenuto diffamatorio, è stata recentemente affermata dalla Corte di Giustizia, Grande Sezione con la sentenza del 25 ottobre 2011 resa nei procedimenti riuniti C-509/09 e C-161/10 eDate Advertising GmbH contro X e Olivier Martinez, Robert Martinez contro MGN Limited.

Nella causa C-509/09 i fatti di causa trattavano della pubblicazione su di un sito internet, in gestione alla eDate Advertising GmbH, stabilita in Austria, di una notizia risalente al 1999 relativa al Sig. X (domiciliato in Germania) – condannato all'ergastolo in Germania nel 1993 per omicidio e dal 2008 ammesso alla libertà condizionale - e che riportava l'intenzione di presentare un ricorso, avverso la condanna penale subita, alla Corte Costituzionale federale, nonché l'affermazione – tramite l'avvocato – inerente la volontà di provare come, nel corso del processo, molti dei principali testimoni dell'accusa non avrebbero dichiarato il vero.

Nonostante il sig. X ingiungesse all'eDate Advertising di smettere di riportare una simile notizia - e di assumersi un obbligo di non fare mediante un'apposita dichiarazione - la società gestore del sito non ha fornito risposta, ma, in data

18 giugno 2007, essa ha eliminato dal proprio sito Internet l'informazione contestata. Il Sig. X, pertanto, decise di adire il giudice tedesco per chiedere all'eDate Advertising di non riportare più notizie che lo concernono, indicando il suo nome per esteso in relazione all'atto commesso. Nonostante l'eDate Advertising contestasse la competenza dei giudici tedeschi in favore di quelli austriaci, X otteneva tutela nei primi due gradi di giudizio.

L'eDate Advertising ripresentava quindi le questioni di competenza alla Corte di Giustizia Federale di Germania, si chiedeva se

1) i giudici dei gradi inferiori avessero, a giusto titolo, riconosciuto la propria competenza internazionale per dirimere la controversia conformemente all'art.5, punto3, del regolamento 44/2001

2) qualora dovesse essere accertata la competenza internazionale dei giudici tedeschi, fosse applicabile il diritto tedesco o il diritto austriaco, e ciò in dipendenza dell'interpretazione dell'art.3, nn.1 e 2, della direttiva 2000/31 CE (che per comodità di lettura qui si riportano art. n. 1 "Ogni Stato membro provvede affinché i servizi della società dell'informazione, forniti da un prestatore stabilito nel suo territorio, rispettino le disposizioni nazionali vigenti in detto Stato membro nell'ambito regolamentato"; Art. 3 n. 2 "Gli Stati membri non possono, per motivi che rientrano nell'ambito regolamentato, limitare la libera circolazione dei servizi società dell'informazione provenienti da un altro Stato membro").

Pertanto, ferme queste considerazioni, sospendeva la causa e rimetteva alla Corte di Giustizia con rinvio pregiudiziale al fine di ottenere risposta sulle seguenti questioni. "Se per la (minacciata) violazione di diritti della personalità attraverso contenuti di un sito Internet l'interpretazione corretta dell'art. 5 n. 3 del regolamento 44/2001 sia da intendersi nel senso che l'interessato possa rivolgersi, al fine di esercitare azioni inibitorie nei confronti del gestore del sito, a qualsiasi giudice dei Paesi in cui il sito risulta essere consultabile, indipendentemente dal luogo di stabilimento del gestore o se la "mera accessibilità al sito non sia sufficiente, essendo necessario specifico

collegamento, o dei contenuti controversi o del sito Internet, con lo Stato del foro adito”.

Inoltre veniva richiesto se agli artt.3, nn.1 e 2, della direttiva 2000/31 dovesse essere attribuito carattere di norme di conflitto, nel senso che esse, anche nell’ambito del diritto civile, prescrivono la sola applicazione del diritto vigente nel paese d’origine, con esclusione delle norme di conflitto nazionali.

I fatti della causa C-161/10 riguardano la vicenda riguardante dell’attore francese Olivier Martinez e del di lui padre Robert Martinez, i quali venivano nominati in una notizia di “gossip” pubblicata sul sito internet di un giornale inglese, nella sua edizione on-line. In base alla normativa francese veniva intrapresa un’azione legale a tutela dell’immagine e della reputazione nanti i giudici francesi contro la società di diritto inglese MGN, editrice del sito del quotidiano britannico. Tale società eccepiva l’incompetenza del tribunale francese per mancanza di un sufficiente collegamento tra la pubblicazione on-line controversa e il presunto danno sul territorio avvenuto in territorio francese, e proprio su tale punto il giudice francese innanzitutto rilevava che: “un evento dannoso, il cui supporto è costituito dalla rete Internet, può essere considerato come prodottosi sul territorio di uno Stato membro soltanto qualora sussista un nesso sufficiente, sostanziale o significativo, che lo colleghi con detto territorio” e pertanto effettua rinvio pregiudiziale alla Corte di Giustizia sulla questione di competenza territoriale per la violazione dei diritti della personalità commessi sulla rete internet, a partire da un sito edito da persona domiciliata in altro Stato membro, “...ed essenzialmente destinato al pubblico di quest’altro Stato...”, poiché tale competenza “...non emerge chiaramente dal tenore letterale degli artt. 2 e 5, punto 3, del regolamento.”

Riunite le cause, la Corte ha stabilito che il principio contenuto nell’art. 5.3 del Regolamento 44/2001, in deroga al principio del foro del domicilio del convenuto, si fonda sull’esistenza di un collegamento particolarmente stretto tra una data controversia e i giudici del luogo in cui l’evento dannoso è avvenuto, e che, per giurisprudenza della medesima Corte per “luogo in cui

l'evento dannoso è avvenuto" deve intendersi sia il luogo del fatto generatore del danno sia il luogo in cui il danno si è concretato.

Pertanto qualora ci si trovi davanti al risarcimento di un danno immateriale asseritamente causato da una pubblicazione diffamatoria, la Corte ha considerato il danno causato da una stampa cartacea diffusa in diversi Stati membri (stampa a diffusione internazionale) dove è stato stabilito che la vittima della lesione derivante da tale pubblicazione può adire sia i giudici del luogo ove è stabilito l'editore della pubblicazione diffamatoria – i quali saranno competenti a conoscere l'integrità del danno causato, oppure qualsiasi giudice ove la stampa è stata diffusa, e tale giudice sarà competente a conoscere i danni cagionati unicamente nello stato del giudice da ultimo adito (giurisprudenza Shevill) e, come anche osservato dall'Avvocato Generale, tali considerazioni sono applicabili anche agli altri mezzi di diffusione delle notizie, quale internet, certamente, è.

Tuttavia, la Corte osserva che la fruibilità dei contenuti in rete non è circoscritta come la pubblicazione della stampa cartacea, ma risulta essere universalmente accessibile da chiunque, e pertanto ritengono i Giudici che i criteri della giurisprudenza Shevill debbano essere adattati alla peculiarità del mezzo, ritenendo innanzitutto che il giudice che maggiormente sia in grado di valutare l'impatto di un'informazione messa in rete, sui diritti della personalità di un soggetto, sia quello in cui la presunta vittima possiede il proprio centro di interessi, inteso come la residenza abituale di tale soggetto leso (viene altresì precisato che non necessariamente il foro dovrà essere quello della residenza, ben potendo una persona avere il proprio centro di interessi anche in uno Stato membro diverso da quello in cui risiede abitualmente, ove altri indizi, quali l'esercizio di un'attività professionale, possano dimostrare l'esistenza di un collegamento particolarmente stretto con tale Stato, ed allora potrà instaurare la controversia nanti tale giudice.)

Precisa la Corte che il soggetto leso ben potrà ottenere ristoro per la totalità del danno subito anche davanti i giudici dello Stato membro del luogo di stabilimento del soggetto che ha emesso tali contenuti.

Concludono i Giudici della Corte di Giustizia che in luogo di un'azione di risarcimento per la totalità del danno cagionato, il soggetto leso può altresì esperire un'azione dinanzi ai giudici di ogni Stato membro sul cui territorio un'informazione messa in rete sia accessibile oppure lo sia stata. Questi ultimi, tuttavia, saranno competenti a conoscere unicamente del solo danno cagionato sul territorio dello Stato membro del giudice adito.

Sull'altro quesito oggetto di rinvio pregiudiziale, ovvero la presenza all'interno della direttiva 2000/31 di norme di conflitto, la Corte precisa che: "l'art. 3 della direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico»), deve essere interpretato nel senso che esso non impone un recepimento in forma di norma specifica di conflitto. Nondimeno, per quanto attiene all'ambito regolamentato, gli Stati membri devono assicurare che, fatte salve le deroghe autorizzate alle condizioni previste dall'art. 3, n. 4, della direttiva 2000/31, il prestatore di un servizio del commercio elettronico non sia assoggettato a prescrizioni più rigorose di quelle previste dal diritto sostanziale applicabile nello Stato membro di stabilimento di tale prestatore."

Le basi giuridiche per un'effettiva tutela tuttavia, sono offerte dal diritto dell'Unione europea e dal diritto internazionale e dai principi contenuti nella Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, ove la dignità umana trova la sua naturale collocazione e una reale garanzia ogni qualvolta essa venga lesa. Inoltre lo stesso diritto interno, in via ricettiva del diritto internazionale elabora proprie valutazioni.

4) La Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali quale base giuridica per una tutela effettiva (i) I Paesi membri del Consiglio d'Europa, firmando a Roma in data 04 novembre 1950 la Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, intendevano riaffermare i principi contenuti Dichiarazione Universale dei Diritti dell'Uomo (adottata dall'Assemblea Generale delle Nazioni

Unite a Parigi, 10 Dicembre 1948) e, per il tramite della Convenzione stessa, ottenere una coesione più stretta tra gli Stati stessi attraverso lo sviluppo e la salvaguardia dei diritti fondamentali, attivandosi pertanto al fine di attuare in modo coordinato ed efficiente le misure necessarie alla loro garanzia collettiva.

La Convenzione è per l'Italia, primariamente, un obbligo derivante da trattato internazionale e secondo l'impostazione tradizionale, non poteva avere una forza superiore alla legge nazionale che lo recepiva nel nostro ordinamento. Tuttavia, a seguito della riforma dell'art. 117 Cost. (dove è affermato che "La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali") e dell'interpretazione data dalla Corte Costituzionale, ai trattati internazionali è stato un valore di rango superiore rispetto alle fonti legislative nazionali, anzi, viene dato agli stessi la stessa forza vincolativa per il legislatore pari a quella prevista per la Costituzione e per i trattati europei.

Tuttavia, solo limitatamente alla Convenzione, la Corte Costituzionale, con le sentenze 348 e 349 del 2007 ha innovato il rapporto tra ordinamento interno e Convenzione, dotando quest'ultima di una forza particolare. Infatti, tale giurisprudenza afferma che la Convenzione non solo è limite per il legislatore, al pari della Costituzione e dei Trattati europei, ma è anche parametro interposto di costituzionalità e pertanto i giudici nazionali, ogni volta che rilevino un contrasto tra le norme, (e quindi una violazione da parte dell'ordinamento italiano di uno o più diritti fondamentali) sono in primis tenuti cercare di risolvere il contrasto per via interpretativa, a mezzo di interpretazione conforme alla Convenzione.

Qualora tale composizione del conflitto non dovesse portare ad una risoluzione dell'antinomia, sono tenuti a rimettere la questione alla Corte Costituzionale, poiché l'eventuale incompatibilità tra norme interne e Convenzione si presenta come una questione di legittimità costituzionale, per eventuale violazione del 117, I comma; la Corte, valutata la costituzionalità della norma della Convenzione (c.d. "teoria dei controlimiti") effettuerà una valutazione sulla

conformità della norma interna all'art. 117 Cost, utilizzando la Convenzione quale parametro interposto, e, in caso di conflitto, potrà non applicare la normativa interna.

Con la firma del Trattato di Lisbona del 13 dicembre 2007 (entrato in vigore nel 01 dicembre 2009) si sono introdotte notevoli modifiche all'ordinamento europeo e, per quanto riguarda la tutela dei diritti fondamentali, le novità introdotte sono principalmente due.

L'art. 6 primo paragrafo TUE contiene il riconoscimento alla Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza del 07 dicembre 2000 e adattata il 12 dicembre 2007 a Strasburgo), da parte dell'Unione, del medesimo valore giuridico dei Trattati (senza estendere tuttavia le competenze dell'Unione come definite nei trattati) e, in tal modo, essa viene resa a tutti gli effetti diritto dell'Unione, con tutte le conseguenze in termini di prevalenza sugli ordinamenti nazionali; pertanto, a seguito del Trattato di Lisbona, qualora una legge interna dovesse contrastare con una norma della Carta di Nizza, la prima potrà essere disapplicata dal giudice nazionale.

La seconda novità in materia di diritti fondamentali è contenuta nell'art. 6 paragrafi secondo e terzo del TUE e riguarda la Convenzione. In tali paragrafi viene consentita l'adesione alla stessa da parte dell'Unione Europea (subordinata alle procedure contenute nel protocollo n. 8) e viene inoltre previsto il riconoscimento dei contenuti della Convenzione quali "principi generali" dell'Unione – senza modificare le competenze dell'Unione europea definite nei trattati.

Venendo ai contenuti nella Convenzione, e nei suoi protocolli, si può scorgere un filo conduttore, un "minimo comune denominatore" consistente nella tutela della dignità umana che è, e non può non essere, presente in ogni articolo della stessa e deve essere tenuto sempre a mente da qualsiasi operatore del diritto che intenda approcciarsi alla materia dei diritti fondamentali, che nella Convenzione trova come si è detto un riferimento fondamentale.

Ne deriva quindi che, tutti i principi generali – e il principio di tutela della dignità umana che domina tutta la Convenzione – devono in ogni caso essere rispettati e garantiti anche all'interno dei singoli Stati e, ovviamente, anche nel caso in cui venga lesa la riservatezza dei singoli attraverso la violazione dei diritti fondamentali, come attraverso il mancato rispetto della propria vita privata e familiare (artt. 8 della Convenzione europea dei Diritti dell'Uomo nonché dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea) ne venga posta in essere sul web. Essi hanno quindi applicazione diretta e sono sufficienti ad integrare e fornire una base giuridica adeguata per la tutela nel caso di violazioni poste in essere all'interno di uno Stato.

Non va da ultimo scordato come la Convenzione stessa si occupi di tutela della riservatezza, e ciò nell'art. 10, dedicato alla tutela del diritto di espressione. Viene affermato infatti in tale articolo, paragrafo 2 che tale diritto può essere sottoposto a "...formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge..." per garantire, tra l'altro "...la protezione della reputazione o dei diritti altrui..."

5.4 La tutela tradizionale

Precisato ciò si cercherà di analizzare quali siano le domande da rivolgere al giudice al fine di ottenere tutela non solo immediata ma anche effettiva, in sede civile, come ad esempio, ottenere la rimozione dei contenuti lesivi dal sito internet. Non è possibile rinvenire nel nostro ordinamento una norma che esplicitamente tuteli la web reputation, tuttavia, è possibile provare a compiere un'interpretazione delle norme vigenti che attualmente tutelano il nome e l'immagine di una persona, e per essa quindi la sua la reputazione, l'onore e il decoro – e verificarne l'efficacia nel tema della web reputation.

Una tutela sotto questi aspetti è fornita dagli artt. da 7 a 10 del codice civile, preposti a garanzia del nome, dello pseudonimo e dell'immagine, nonché gli artt. 96 e 97 della legge 22 aprile 1941 n. 633 (diritto al ritratto e limiti all'utilizzo dello stesso) attraverso i quali è possibile ricostruire il sistema di

garanzie negli anni approntato per tutelare le lesioni ingiustamente subite alla reputazione.

Tali normative attraverso l'accertamento in sede civile della lesione ai beni tutelati, permettono al giudice di inibire la riproduzione dell'immagine, e di ottenere il ristoro dei danni eventualmente subiti.

Ovviamente, lo si ribadisce, ai fini della tutela effettiva della propria web reputation, ciò che conta è la cessazione dell'abuso, ovvero che la notizia non veritiera, contenente il proprio nome, o la propria immagine non sia più fruibile in rete.

Tuttavia, risulta evidente come, nelle norme citate, la tutela del nome o dell'immagine così intesa, sia ancora eccessivamente legata all'utilizzo e alla pubblicazione illegittima sui giornali, o alla diffusione della notizia in televisione: il codice civile, infatti, prevede quale rimedio la pubblicazione della eventuale sentenza di condanna su uno o più giornali (chiaro è che non potrebbe essere certamente disposta la rimozione della foto o della notizia, essendo questa già andata in stampa oppure essendo già stata trasmessa in televisione) e tale rimedio non sembra essere adeguato ad un'immagine o ad un nome utilizzati in modo improprio e cristallizzati su una o più pagine internet, sempre accessibili e liberamente condivisibili da ogni utente della rete.

Pertanto, per il danneggiato, non solo la pubblicazione della sentenza sulla pagina internet e l'inibizione all'utilizzo di informazioni, dati e immagini, ma solo un'effettiva rimozione dei contenuti offensivi o falsi sarebbe la soluzione auspicata in tema di lesione (e danneggiamento) della web reputation.

Sul punto la giurisprudenza offre alcune pronunce interessanti.

Il tribunale di Teramo, in data 11 dicembre 1997 (www.dejure.it, Foro it. 1998, I, 594) ha affermato che "...va accolta la richiesta di tutela cautelare urgente avanzata da una banca che lamenta la lesione del diritto all'onore, decoro e reputazione derivante dalla presenza, in un "sito" Internet, di notizie

incomplete sull'accertamento giudiziario di una truffa posta in essere dalla banca medesima".

Un'altra pronuncia che si intende riportare è stata resa dal Tribunale di Napoli in data 05 ottobre 2009. Il signor X proponeva atto di citazione per vedere dal Tribunale convalidata l'ordinanza pronunciata in sede di reclamo ove veniva ordinata al Ministero dell'Interno (convenuto) la cancellazione del nominativo dell'X dal sito internet che, riportando l'analisi delle attività svolte dalla DIA, inseriva tale nominativo in un elenco contenente nomi di soggetti pregiudicati.

Oltre alla cancellazione del proprio nome, X richiedeva inoltre il riconoscere l'illiceità di tale inserimento, il riconoscimento del danno alla reputazione, all'immagine e all'onore che da tale inserimento era derivato, dichiarare la lesione causa di ingenti danni patrimoniali (da accertarsi in separato giudizio) e non patrimoniali, e pertanto dichiarare il Ministero responsabile al risarcimento del danno nonché alla pubblicazione della sentenza sul sito internet.

In punto risarcimento del danno il Tribunale ha applicato i criteri normalmente utilizzati dalla giurisprudenza la quale "...per pervenire alla concreta quantificazione del danno utilizzando i criteri comunemente accettati, considera significative la potenziale diffusione del mezzo usato (dato che Internet, per sua natura, è destinato ad essere normalmente visitato da un numero indeterminato di soggetti), e la provenienza qualificata della notizia, nonché la gravità dell'offesa, consistente nell'attribuzione di fatti penalmente rilevanti".

Si osserva, per completezza della trattazione, che X chiedeva altresì l'applicazione della disposizione prevista dall'art. 12 legge 47/1948 - disposizioni sulla stampa - il quale prevede: "Nel caso di diffamazione commessa col mezzo della stampa, la persona offesa può chiedere, oltre il risarcimento dei danni ai sensi dell'art. 185 del Codice penale, una somma a titolo di riparazione. La somma è determinata in relazione alla gravità dell'offesa ed alla diffusione dello stampato".

Tale somma non veniva concessa dal Tribunale di Napoli sia perché diffamazione non avvenuta con il mezzo della stampa (ma avvenuta a mezzo

internet) e poi perché tale sanzione secondo il giudice sarebbe applicabile solo al diretto responsabile dell'illecito e non al Ministero in quanto soggetto amministratore del sito o soggetto responsabile per l'operato dei suoi dipendenti.

Non si può prescindere dall'analizzare il D.lgs. 196/2003, c.d. "Codice della privacy", il quale protegge i dati personali (dei quali la definizione fornita dal codice, all'art. 4, lettera b) è: "qualunque informazione relativa a persona fisica, [persona giuridica, ente od associazione,] identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale") di ogni individuo da parte dei soggetti preposti al loro trattamento, nonché alla loro conservazione, dalla diffusione o comunicazione all'esterno, senza che sia stato preventivamente espresso un valido consenso.

Ciò che può rilevare ai fini della presente trattazione è l'utilizzo (indebito) da parte di altri soggetti di dati personali i quali, una volta immessi nel mare di internet, contribuiscano a creare una web reputation ingiustamente negativa o comunque falsa.

Innanzitutto va considerato che il Codice della privacy all'art. 1 afferma che "Chiunque ha diritto alla protezione dei dati personali che lo riguardano" e che all'art. 2 comma 1 prevede che: "Il presente testo unico, di seguito denominato codice, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali", nonché all'art. 11, ove garantisce il diritto ad un trattamento lecito e secondo correttezza, e che tali dati siano esatti ed aggiornati, stabilendo all'art. 15 che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c." e 31 (in materia di sicurezza dei dati trattati e conservati).

Qualora si riscontri una violazione nell'utilizzo dei dati personali e possibile, in alternativa alla tutela giurisdizionale, rivolgersi all'Autorità preposta alla tutela degli stessi, il Garante per la protezione dei dati personali, tramite la proposizione di reclamo, segnalazione o ricorso.

A seguito della proposizione del ricorso, l'Autorità può pronunciarsi in via espressa, oppure, qualora non dovesse pronunciarsi, tale mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, deve considerarsi provvedimento di rigetto. Contro tali provvedimenti, sia espressi che taciti, è proponibile opposizione, ai sensi dell'art. 151 del codice della privacy, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito, ovvero entro sessanta giorni se il ricorrente risiede all'estero, davanti il tribunale del luogo in cui ha la residenza il titolare dei dati trattati (procedimento che sarà regolato dal rito del lavoro, secondo quando disciplinato dal d.lgs 150/2011).

Recentemente la Corte di Cassazione (Cass Civ. Sez III, 05 aprile 2012, 5525/2012) ha giudicato su di un'opposizione ad un reclamo presentato al Garante per la protezione dei dati personali. In tale occasione sia il Garante che il Tribunale rigettavano la richiesta di blocco dell'utilizzo dei dati personali avanzata dal ricorrente circa l'inserimento della notizia dell'arresto che riguardava il ricorrente stesso, avvenuta in precedenza, pubblicata sul giornale, e solo recentemente ripubblicata nell'archivio storico on-line e quindi, accessibile sul sito X e fruibile attraverso i motori di ricerca.

Il ricorrente lamentava non la falsità della notizia, osservando che la stessa ai tempi in cui era stata pubblicata era certamente vera, ma il fatto che non fosse possibile rinvenire traccia nell'articolo, nella pagina o in nessun altro modo, di cenni o rinvii alle notizie successive - pubblicate successivamente - e che trattavano del suo proscioglimento dalle accuse che a quell'arresto avevano portato, richiamando tra gli altri, l'art. 7 del d.lgs 196/2003 che afferma il diritto del titolare dei dati al loro aggiornamento rettifica o integrazione.

Tale sentenza affronta così il tema del "diritto all'oblio" ovvero del diritto a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati, sempre considerando il bilanciamento dei contrapposti interessi del diritto alla riservatezza e del diritto all'informazione.

In tale specifica occasione i giudici della Suprema Corte, affermando che: "atteso che il trattamento dei dati personali può avere ad oggetto anche dati pubblici o pubblicati (v.Cass., 25/6/2004, n. 11864), il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità. Il soggetto cui l'informazione oggetto di trattamento si riferisce ha in particolare diritto al rispetto della propria identità personale o morale, a non vedere cioè "travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale" (v. Cass., 22/6/1985, n. 7769), e pertanto alla verità della propria immagine nel momento storico attuale. Rispetto all'interesse del soggetto a non vedere ulteriormente divulgate notizie di cronaca che lo riguardano si pone peraltro l'ipotesi che sussista o subentri l'interesse pubblico alla relativa conoscenza o divulgazione per particolari esigenze di carattere storico, didattico, culturale o più in generale deponenti per il persistente interesse sociale riguardo ad esse."

Operati tali ragionamenti, la Corte osserva come una notizia ben possa essere conservata negli archivi, considerato il suo "valore storico". Osserva anche come un archivio tradizionalmente inteso abbia un metodo di consultazione e intercorrelazione tra le notizie appositamente creato per agevolare la consultazione, ed evidenzia come internet non sia uno strumento creato per archiviare le notizie (inteso come sopra) ma semplicemente per "memorizzarle", anzi, osserva come molte volte le notizie in internet "...non

sono in realtà organizzate e strutturate, ma risultano isolate, poste tutte al medesimo livello ("appiattite"), senza una valutazione del relativo peso, e prive di contestualizzazione, prive di collegamento con altre informazioni pubblicate" venendo in rilievo, quindi, per la Cassazione l'esigenza di garantire correttezza e affidabilità dell'informazione.

La Corte conclude affermando che gli archivi sono quelli immessi in internet dagli utenti, nei loro siti, mentre i gestori degli stessi (i provider) rivestono il ruolo di prestatori intermediari di servizi (ai sensi del d.lgs 70/2003, di cui si dirà meglio nel prosieguo) e così anche i motori di ricerca, che offrono "ospitalità sui propri server a siti internet gestiti dai relativi titolari in piena autonomia, i quali negli stessi immettono e memorizzano le informazioni oggetto di trattamento", e che quindi questi ultimi non svolgono un ruolo attivo nella gestione o nella scelta delle immagini memorizzate.

Osserva la Corte che il problema che può prospettarsi non è la pubblicazione di notizie non più attuali, quanto la permanenza nel web di notizie non aggiornate, e pertanto il bilanciamento che in tale situazione deve essere effettuata tra i diritti all'informazione e di cronaca, in bilanciamento con il codice della privacy che vuole che le informazioni contenenti dati personali vengano aggiornate.

Pertanto, proseguono i giudici del Supremo Collegio, non essendo applicabile la misura della rimozione o della rettifica in quanto non integrabile il reato di diffamazione, appare necessario individuare una misura che consenta un'adeguata fruizione della notizia aggiornata - discostandosi dalle conclusioni cui è pervenuto il Garante per il quale era sufficiente che notizie "aggiornate" risultassero comunque reperibili nel "mare di internet" - individuandola nella "... predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia" in modo da consentirne il rapido accesso e un adeguato approfondimento.

In ultimo, si segnala come il codice della privacy preveda, all'art. 167, anche alcune norme di carattere penale nelle quali viene prevista l'applicazione di una

sanzione di carattere penale in caso di illecito trattamento di dati personali, qualora il soggetto responsabile del trattamento tenga determinati comportamenti in violazione di determinate norme del codice, al fine di trarne profitto per sé o per altri o con lo scopo di recare altrui danno.

Un esempio molto noto nella giurisprudenza è la sentenza del tribunale di Milano Sez IV del 12 aprile 2010, n.1972 che ha applicato le sanzioni previste nell'art. 167 del d.lgs 196/2003 ai gestori del sito sul quale gli utenti caricavano contenuti multimediali (nella specie si trattava di materiale audiovisivo), affermando che in capo ai gestori sorge l'obbligo giuridico di fornire agli utenti medesimi tutte le necessarie avvertenze in ordine al rispetto della disciplina del trattamento dei dati personali, comprese quelle che concernono la necessità di procurarsi l'obbligatorio consenso in ordine alla diffusione di dati personali sensibili.

Pertanto concludono i giudici del Tribunale di Milano, se non è possibile ravvisare una responsabilità per diffamazione ex art. 595 comma terzo in capo ai gestori del sito per la diffusione dei contenuti, tale comportamento integra comunque la violazione delle norme del codice della privacy, e quindi la conseguente irrogazione delle sanzioni previste ivi previste con l'art. 167 codice privacy; si precisa che i PM chiedevano anche la condanna per il reato di concorso nel reato di diffamazione per non aver provveduto i gestori del sito a rimuovere il video dai contenuti illeciti e individuando l'esistenza di una posizione di garanzia a carico del sito web in parola, posizione derivante da un obbligo giuridico contenuto nella legge sulla privacy, anche in considerazione che il video è rimasto in rete per molti mesi nonostante le proteste degli utenti. Il Tribunale non condivideva la ricostruzione sul punto effettuata dai magistrati, osservando come non sia possibile ravvisare un obbligo di legge codificato che imponga agli ISP – Internet Service Provider – un controllo preventivo sui contenuti immessi in rete dagli utenti, e che, nemmeno sia possibile ricostruire l'esistenza in capo agli stessi di una posizione di garanzia rinvenibile negli obblighi contenuti nel d.lgs 196/2003. Infatti, concludono i giudici "...la presenza di una posizione di garanzia da cui derivi un obbligo di

attivazione in mancanza del quale ricorre la previsione del cpv. dell'art. 40 CP, non può essere frutto di una seppur ingegnosa costruzione giurisprudenziale, ma, come insegna la S.C., deve derivare da "da un lato, da una fonte normativa di diritto privato o pubblico, anche non scritta, o da una situazione di fatto per precedente condotta illegittima, che costituisca il dovere di intervento, dall'altro lato, dall'esistenza di un potere giuridico, ma anche di fatto, attraverso il corretto uso del quale il soggetto garante sia in grado, attivandosi, di impedire l'evento".

5.5 Il codice delle comunicazioni elettroniche

Altra normativa da analizzare è il d.lgs 259/2003 il quale, abrogando parte del D.P.R. 156/1973 (c.d. Codice delle poste) ha disciplinato i servizi di comunicazione elettronica ad uso pubblico ed ad uso privato, recependo nell'ordinamento italiano le direttive comunitarie sul punto.

Ai fini dell'analisi che si sta effettuando occorre sottolineare come tale norma recepisce, nei principi generali riferibili a tutta la materia disciplinata, chiarisca come debbano essere garantiti i diritti inderogabili di libertà delle persone, l'accesso e l'uso dei mezzi e dei servizi di comunicazione elettronica, nonché il diritto di iniziativa economica ed il suo esercizio in regime di concorrenza nel settore delle comunicazioni elettroniche.

Viene inoltre precisato che i provvedimenti riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, debbano rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto dell'Unione europea, e tali provvedimenti - riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica - che dovessero ostacolare l'esercizio di tali libertà fondamentali, possono essere adottati soltanto se appropriati, proporzionati e necessari nel contesto di una

società democratica, acquisiti nel rispetto della presunzione di innocenza e nel rispetto di un'efficace tutela giurisdizionale e di un giusto processo.

Nel D.lgs 259/2003 viene indicato nell'art. 13 - Obiettivi e principi dell'attività di regolamentazione- comma sesto come l'Autorità per le Garanzie nelle Comunicazioni (AGCOM), debba promuovere, in collaborazione con il Ministero e ognuno nell'ambito delle rispettive competenze, gli interessi dei cittadini, e quali determinati fini tale Autorità debba pertanto perseguire, tra cui contribuire "...a garantire un livello elevato di protezione dei dati personali e della vita privata" e promuovere "...la capacità degli utenti finali di accedere ad informazioni e distribuirle o eseguire applicazioni e servizi di loro scelta".

Sembra pertanto che i principi generali e le funzioni dell'Autorità, come anche delineate nella legge 349/1997 che della stessa è istitutiva, (che include tra le funzioni della predetta Autorità il potere di intervento "...nelle controversie tra l'ente gestore del servizio di telecomunicazioni e gli utenti privati") lascino pensare a legittimi spazi di intervento in tale ambito per l'AGCOM.

In ogni caso, come ex lege (art. 11 legge 248/2000 che ha inserito l'art. 182 bis nella legge 633/1941) sono stati attribuiti all'AGCOM i poteri di prevenire e accertare le violazioni in materia di protezione del diritto d'autore, non si può escludere un eventuale ampliamento di funzione e competenze dell'Autorità anche sulle controversie sorte per le violazioni dei diritti tutelati dalla Convenzione europea la salvaguardia dei diritti dell'uomo e delle libertà fondamentali commesse, dai gestori delle reti e dai fornitori dei servizi.

5.6 La responsabilità del provider

La direttiva 2000/31/CE disciplina taluni aspetti giuridici dei servizi della società dell'informazione - ed in particolare il commercio elettronico - nel mercato interno (c.d "direttiva sul commercio elettronico") ed ha avuto il merito di regolare anche la materia della responsabilità dei fornitori di servizi nel "mare di internet".

Infatti, riconoscendo l'importanza, la rapida diffusione, le prospettive di crescita – anche in ambito occupazionale - del commercio elettronico, l'Unione europea ha inteso regolare i rapporti tra il prestatore di tali servizi e gli utenti, sottolineando alcuni fondamentali aspetti nei considerando 9 e 10 della direttiva medesima.

Si legge infatti nel considerando 9 che l'esercizio della libera prestazione di tale attività è possibile che rifletta specificamente nel diritto comunitario un principio più generale, e cioè la libertà di espressione prevista all'articolo 10, paragrafo 1, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali che è stata ratificata da gli Stati membri. Pertanto deve essere assicurato che tale attività possa essere svolta liberamente alla luce di tale articolo, sottoposta soltanto alle restrizioni di cui al paragrafo 2 di tale articolo, ovvero che la libertà di espressione può essere limitata da legislazioni nazionali solo quando, tra l'altro, sia allo scopo di tutelare la reputazione altrui.

Ma non si può non dare rilievo alla portata del considerando successivo, il quale afferma che "In conformità con il principio di proporzionalità, le misure previste dalla presente direttiva si limitano al minimo necessario per raggiungere l'obiettivo del buon funzionamento del mercato interno. La presente direttiva, nei casi in cui si deve intervenire a livello comunitario per far sì che lo spazio interno sia veramente libero da frontiere per il commercio elettronico, deve garantire un alto livello di tutela degli obiettivi di interesse generale, come la protezione dei minori e della dignità umana, la tutela del consumatore e della sanità pubblica...".

La tutela della dignità umana, quale valore fondamentale della Convenzione e quale principio generale dell'Unione Europea, è quindi in questo contesto garantita e tutelata direttamente dalla normativa europea di carattere derivato.

La direttiva in esame, quindi, disciplina una tutela effettiva per il soggetto che, leso nella sua reputazione da comportamenti illeciti, intenda rimuovere dalla

rete i contenuti lesivi rivolgendosi non verso chi o coloro che hanno immesso il contenuto lesivo ma contro coloro che tali contenuti "memorizzano" in rete.

Infatti, tale normativa individua tre tipologie di "prestatori intermediari" ovvero coloro che forniscono i servizi delle società dell'informazione, che nello specifico consistono a volte nel trasmettere, o a volte nel memorizzare dati che vengono forniti dal destinatario del servizio fornito, viene specificato che essi non rispondono degli illeciti commessi da tali soggetti (cioè dai destinatari dei servizi), tranne nei casi in cui sia la direttiva stessa a prevedere il sorgere di tale specifica responsabilità.

Nel dettaglio, si possono delineare tre categorie di operatori e vengono altresì indicati in quali casi – seppur in modo negativo – i prestatori intermediari dovranno rispondere degli illeciti civili commessi dai destinatari dei servizi forniti:

a) colui che si occupa del "mero trasporto" (art. 12 della direttiva) dell'informazione in rete (colui che fornisce l'accesso alla rete o trasmette le informazioni fornite dal destinatario del servizio), non è responsabile per le informazioni che trasmette a condizione che

- non dia origine alla trasmissione
- non selezioni il destinatario della trasmissione
- non selezioni o modifichi le informazioni trasmesse.

b) il prestatore dei servizi di caching (art. 13 della direttiva), ovvero l'esercente attività di memorizzazione temporanea dei dati, per il quale è prevista l'assenza di responsabilità per il gestore dei servizi solo qualora egli:

- non modifichi le informazioni;
- si conformi alle condizioni di accesso e alle norme di aggiornamento delle informazioni;
- non interferisca con l'uso lecito della tecnologia utilizzata nel settore per ottenere dati sull'utilizzo delle informazioni;

- agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.

c) l'hosting provider (art. 14 della direttiva), ovvero il soggetto che svolge attività di memorizzazione di informazioni fornite dal destinatario del servizio, il quale non risponderà civilmente per le immagini memorizzate dal destinatario del servizio allorquando:

- non sia effettivamente al corrente del fatto che l'attività o l'informazione memorizzata sia illecita e - per quanto attiene ad azioni risarcitorie - non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione;

- non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Tutti e tre gli articoli sopra richiamati della direttiva 2000/31 contengono una disposizione comune, che lascia impregiudicata la possibilità - secondo gli ordinamenti degli Stati membri - per l'organo giurisdizionale o un'autorità amministrativa di esigere che il prestatore impedisca o ponga fine ad una violazione, prevedendo così un dovere di collaborazione con le autorità interne, per tutti i prestatori di servizi indicati.

Va tenuto tuttavia presente che sia la direttiva 2000/31 all'art. 15 che il D.lgs di attuazione della direttiva all'art. 17 espressamente non prevedono un obbligo generale di sorveglianza, al fine di evitare il crearsi di una forma di responsabilità oggettiva non prevista dalla legge.

Pertanto, benché secondo il dettato normativo, i prestatori di servizi intermediati indicati dalla direttiva non sono assoggettati ad un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino

la presenza di attività illecite, viene comunque precisato che, fatte salve le disposizioni di cui agli articoli 14, 15 e 16 del d.lgs 70/2003 (e degli artt.12, 13 e 14 della direttiva) essi sono comunque tenuti:

1) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione;

2) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Nell'ultimo comma dell'articolo 17 del D.lgs 70/2003 attuativo della direttiva è infine stabilito che "Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente".

All'interno del nostro ordinamento, quindi, il soggetto che svolge un'attività di commercio elettronico e che vedrà contenuti falsi od offensivi ad esso riferibili su di un sito internet, al fine di ottenere la rimozione di tali contenuti, dovrà informare il fornitore dei servizi dell'illiceità del contenuto (affinché vi sia così la certezza dell'avvenuta conoscenza da parte del provider dell'illiceità del contenuto - requisito previsto dall'art. 14 lettera a) della direttiva) e, qualora questi non dovesse decidere di provvedere autonomamente alla rimozione, sarà tenuto ad adire il giudice al fine di ottenere una pronuncia contenente l'ordine di rimozione dei contenuti illeciti.

Solo a questo punto il provider, il quale, nonostante fosse stato messo a conoscenza del contenuto illecito e nonostante fosse stata ordinata la rimozione dall'autorità competente, - giudiziaria o amministrativa - non ha

comunque provveduto alla rimozione dei contenuti illeciti, sarà considerato civilmente responsabile – a titolo di colpa specifica per violazione di legge – per l’illecito commesso dai terzi destinatari dei servizi.

La giurisprudenza italiana di merito ha offerto un esempio di quanto fino ad ora affermato. Il Tribunale di Milano è stato investito di un ricorso ex. art. 700 c.p.c. – successivamente reclamato - presentato da un soggetto, esercente attività imprenditoriale prevalentemente on-line che lamentava l’associazione, tramite lo strumento “suggest-search” di un noto motore di ricerca, del suo nome ai termini “truffa” e “truffatore”.

Richiedeva quindi in via d’urgenza al Tribunale di ordinare al provider di rimuovere tale associazione in quanto lesiva della sua reputazione sia personale che lavorativa, allegando la lettera raccomandata inviata in precedenza, con cui informava la società dell’esistenza dell’illecito.

Concesso il provvedimento cautelare, fondato sulla natura lesiva in quanto diffamatoria dell’associazione effettuata dallo strumento “suggets-search” del motore di ricerca, che disincentivava l’approfondimento, anche in termini professionali delle conoscenze sul ricorrente, la società proponeva reclamo al collegio (ex art. 669 terdecies c.p.c.) il quale, lo rigettava argomentando come segue.

Il motore di ricerca deve essere qualificato come “host provider”, ovvero un soggetto che si limita a memorizzare le informazioni prese da altri, e non un “content provider”, ovvero il fornitore diretto dei contenuti. Pertanto la responsabilità del motore di ricerca nel caso in esame sorge non per il contenuto in sé, ma per la funzione di agevolazione della ricerca - basata su di un algoritmo che calcola le parole chiave più ricercate dagli utenti – che, abbinando il nome del soggetto ricorrente alle parole “truffa” e “truffatore” ledeva la reputazione altrui. Pertanto la società non è stata ritenuta responsabile per il contenuto illecito del terzo non rimosso, ma per non aver rimosso il contenuto ritenuto lesivo che essa stessa aveva “creato” tramite il servizio di “suggest-search” utilizzato, causando quindi una lesione del diritto

alla reputazione del ricorrente (senza che il giudice ritenesse sussistenti nella fattispecie altri diritti di pari rango meritevoli di tutela che avrebbero potuto essere compresi dalla riduzione del servizio di ricerca, attraverso la non combinazione delle parole "truffa" e "truffatore" in abbinamento al nome del ricorrente).

Si riporta infine un'ultima pronuncia (la quale, sebbene resa in materia di marchi e brevetti assume rilevanza anche per la materia qui trattata) del Tribunale di Firenze del 25 maggio 2012, ove il giudice si è pronunciato su un ricorso avanzato da un soggetto che lamentava l'illiceità della condotta del "webmaster" rimasto tuttavia ignoto, il quale aveva sia utilizzato indebitamente il marchio ad uso esclusivo del ricorrente, e sia aveva compiuto campagne diffamatorie relativamente a tale marchio.

Il giudice in primis premette l'interpretazione che la Corte di Giustizia ha effettuato dell'art. 14 della direttiva 2000/31 - ovvero che sia applicabile al prestatore di un servizio di posizionamento su internet solo quando egli non abbia svolto un ruolo attivo sui contenuti, atto a conferirgli la conoscenza o comunque il controllo su di essi - e successivamente precisa che l'attività svolta dal motore di ricerca debba essere ricondotta a quella tipica del caching provider, (in quanto esso "procede alla indicizzazione dei siti ed alla formazione di copie cache dei loro contenuti, con memorizzazione temporanea delle informazioni").

Nella motivazione di rigetto, poi, in relazione al contenuto diffamatorio delle informazioni immesse sul sito web - non rilevando in questa sede le valutazioni in merito al deposito dei marchi e dei brevetti - argomentava il giudice, in primo luogo circa il concetto di "conoscenza della pretesa illiceità" dei contenuti del sito, la quale non era desumibile dal decreto di archiviazione del GIP (reso contro ignoti e privo di alcun accertamento in relazione alla sussistenza del reato stesso, che non può essere dato per presupposto). Inoltre, ritiene il Giudice di non poter desumere la pretesa illiceità nemmeno dalle diffide presentate dal ricorrente stesso, in quanto di provenienza unilaterale, e che, pertanto, nessuna responsabilità potesse essere ravvisabile in capo al motore

di ricerca, poiché "al fine di valutare se un ISP abbia effettiva conoscenza, è necessario che un "organo competente abbia dichiarato che i dati sono illeciti, oppure abbia ordinato la rimozione o la disabilitazione dell'accesso agli stessi, ovvero che sia stata dichiarata l'esistenza di un danno" e che l'ISP stesso sia a conoscenza di una tale decisione dell'autorità competente".

In secondo luogo, il Giudice osserva che sul sito erano stati pubblicati atti giudiziari, della cui veridicità non si può dubitare, e che in ogni caso potevano considerarsi espressione del diritto di critica.

Va precisato, in chiusura dell'analisi della disciplina del D.lgs 70/2003 che sono esclusi espressamente dall'ambito di applicazione tutti i profili di responsabilità – e le conseguenti controversie – nascenti dall'illecito o improprio trattamento dei dati personali, che pertanto andranno disciplinate secondo le norme contenute nel codice della privacy.

Compiuta un'analisi della normativa vigente nel nostro ordinamento, osservato come le innovazioni e le soluzioni fino ad oggi proposte derivino da interventi di matrice comunitaria, pare doveroso concludere con due osservazioni

Le norme che possono essere poste a tutela della web reputation – sia in materia civile che penale – sono già presenti nell'ordinamento italiano; sia nei confronti del soggetto direttamente reso responsabile della lesione, sia nei confronti del provider – anche se con tutte le limitazioni di responsabilità in sede civile, e l'esclusione di responsabilità in sede penale per il reato di diffamazione ex art. 57 c.p. - tuttavia, anche considerata la delicatezza degli interessi trattati e la molteplicità delle fattispecie concrete con cui le lesioni vengono poste in essere, le norme non possono coprire le molteplici situazioni in cui la lesione della reputazione viene posta in essere.

L'inevitabile conseguenza è una giurisprudenza non uniforme che, pertanto, non riesce a segnare precedenti che fungano da "faro" per chi, nel mare di internet cerchi un approdo a tutela della sua web reputation.

CAPITOLO VI

DALLA TEORIA ALLA PRATICA: MONITORARE LA WEB REPUTATION

6.1 La capacità di ascoltare la rete

L'attività di social media monitoring si esplica nell'attivazione, attraverso metodologie e strumenti, di un ascolto della rete e riabilitazione delle informazioni ricavate allo scopo di pianificare e ottimizzare le proprie scelte di business.

Le analisi possono riguardare nello specifico o i dati provenienti dai propri presidi online (pagine Facebook, account Twitter...) chiamata anche social media analysis o media owned, oppure le informazioni tracciabili al di fuori di essi. Il primo tipo di analisi ha lo scopo di conoscere le performance del brand sui propri canali e capire come sta cambiando la propria community di riferimento.

La seconda ha lo scopo di capire come il proprio brand o prodotti siano percepiti dagli utenti in rete.

Brand reputation.

La reputazione di un brand dipende principalmente da due fattori strettamente collegati tra loro: ciò che viene comunicato dall'azienda e ciò che viene percepito dall'audience. Monitorare il passaparola online che riguarda il brand e verificare quindi se la percezione coincide con il messaggio e l'identità che vuole comunicare è fondamentale per poter curare la propria reputazione e il rapporto con l'utente. A tal fine è necessario conoscere le dinamiche proprie della rete e i processi che sono alla base del funzionamento del processo formativo della reputazione online. Alcuni punti importanti, riportati da Gianluca Diegoli nel libro "Social Media Marketing" sono:

Persistenza: qualsiasi frase scritta è reperibile e ne resta traccia in rete anche dopo molto tempo se si attiva una giusta ricerca.

Virulenza: ogni traccia presente in rete può essere diffusa con il semplice copia e incolla, la potenza virale del web è al tempo stesso arma a doppia taglio.

Incancellabilità: gli algoritmi che regolano la diffusione delle notizie online permettono una rintracciabilità delle informazioni anche dopo esser state cancellate: gli screenshot permettono di fotografare e fissare immediatamente un'informazione scomoda che potrebbe essere cancellata immediatamente dopo.

Verificabilità: la reputazione online è molto più pubblica di quanto non lo fosse quella offline ed esiste indipendentemente dal fatto che l'azienda decida di monitorarla o meno.

Ponderabilità: la reputazione in rete è basata su opinioni che a loro volta dispongono di altre reputazioni: la novità consiste nel fatto che esistono e tendono a moltiplicarsi in rete 44 influencer che hanno a loro volta conquistato una reputazione consistente in gruppi di follower.

Multimedialità: l'espansione nell'uso dei video in rete ha creato un nuovo potente e diretto modo di vivere in prima persona e quindi di diffusione dell'esperienza relativa al brand. Con i nuovi smartphone tutti si possono scoprire reporter e raccontare in diretta e in real time l'esperienza vissuta. Questa crescita per tale tipologia di contenuti è confermata dall'avvento di Vine: una nuova applicazione per iPhone e per iPad che offre la possibilità ai propri utenti di realizzare video dalla durata di 6 secondi da condividere attraverso Twitter e Facebook.

La particolarità dei suoi video è quella di poter interrompere e riprendere il video potendo così creare effetti simili a quelli che si possono trovare nei video realizzati tramite la tecnica del slow-motion.

Frammentarietà degli interlocutori e dei messi di comunicazione: l'icona della comunicazione muta da "uomo con il megafono" a quella di "uomo con il microscopio". Si rende fondamentale la conoscenza dei canali in cui gli utenti si trovano a condividere le proprie opinioni e delle meccaniche che li governano.

Incontrollabilità: tutti i precedenti punti sottolineano come la reputazione online sia data sempre più dalla somma delle opinioni espresse da persone terze e sempre meno da ciò che viene comunicato su sé stessi, dunque l'unica possibilità di influenza deriva dal dialogo e ancora prima dall'ascolto delle conversazioni.

La reputazione di un brand si costruisce con i propri stakeholder e secondo Gianluca Diegoli "le 4 P" che delineano il rapporto tra azienda e propria community o potenziale sono: Prodotto: bene, servizio o più in generale l'oggetto di discussione degli utenti in riferimento alla specifica azienda.

Personalità: il brand che comunica e decide di essere presente in rete per i suoi consumatori deve essere "umano", non deve preconfezionare e riciclare risposte standard, ma deve rivelarsi essere un ascoltatore e parte coinvolta nella discussione (che la riguarda tra le altre cose).

Pazienza: le relazioni che si costituiscono in rete non seguono i tempi delle campagne commerciali o pubblicitarie, solitamente una cura della propria community o della potenziale community richiede tempo e per misurare il ROI è necessario aspettare diversi mesi, osservarne il trend e le variazioni, studiarne le evoluzioni e ottimizzare le strategie.

Passione: oltre all'umanità gli utenti sempre più esigenti si aspettano di dialogare con un'azienda che mostri una passione e una predisposizione alla comprensione almeno pari a quella che spinge l'utente a riferirsi direttamente ad essa per l'acquisto di un bene.

Essere all'altezza delle aspettative dell'utente online non è semplice, né immediato, richiede un notevole dispendio di energie e risorse da parte dell'azienda che deve essere pronta ad affrontare un dialogo basato sulla trasparenza, sulla non autoreferenzialità, sul testing e l'ammissione di un eventuale insuccesso.

L'attività di social monitoring o ascolto della rete circa la reputazione web di un brand si fonda sull'analisi del passaparola in rete o buzz online in modo

sistematico e pianificato su tutti i principali spazi web (forum, siti di news, blog e social network).

Il social media monitoring si differenzia dalle tradizionali ricerche di mercato perché:

- mentre i sondaggi ricavano delle risposte a domande prestabilite, che confermano o smentiscono dubbi o ipotesi già formulate, l'ascolto delle opinion spontaneamente pubblicate in rete porta a scoprire aspetti ancora non tenuti in considerazione (nuovi competitor, nuove funzionalità dei prodotti, temi che più appassionano o preoccupano gli utenti).
- A differenza dei focus group e delle interviste da cui si ricavano dati necessariamente influenzati dalla consapevolezza dei rispondenti di essere osservati, valutati, misurati, il monitoraggio raccoglie le conversazioni spontanee degli utenti. Le parole, la sintassi e la grammatica sono quelle degli utenti, dei lettori, dei consumatori, dei cittadini.
- Diversamente dai dati ricavati attraverso le tradizionali ricerche di mercato, le opinioni espresso online sono pubbliche e per questo in grado di influenzare gli altri. Uno degli scopi dell'attivazione di un'attività di ascolto della rete è proprio per acquisire tutte le informazioni sopra accennate e in particolar modo l'obiettivo è:
 - acquisire feedback dai consumatori e dagli addetti ai lavori;
 - conoscere la percezione online dei topics considerati;
 - verificare l'efficacia delle proprie attività;
 - conoscere i principali temi di discussione degli utenti online intorno alle keyword settate;
 - tutelare la propria immagine rilevando criticità in modo tempestivo;
 - individuare influencer/partner per i propri mercati, settori ed iniziative.

L'attività di monitoraggio ad opera del social media analyst si avvale di un mix tra strumenti tecnologici e lavoro manuale.

Gli strumenti tecnologici sono delle piattaforme di monitoraggio che permettono la raccolta ed elaborazione dei dati, anche attraverso l'automatizzazione di alcune fasi come il tracciamento dei risultati per determinate keyword e la realizzazione dei grafici

6.2 Fasi di un'attività di monitoraggio della reputazione in rete.

La prima fase, dopo aver messo a fuoco l'obiettivo dell'analisi, è il set up del progetto che consiste nell'elaborazione di una serie di parole chiave inerenti l'oggetto di studio che permette di ottenere risultati inerenti e focalizzati che permetteranno un utile ed efficace analisi.

L'ottimizzazione delle keyword è un processo continuo e dinamico perché prevede la modifica ed implementazione delle stesse anche durante l'attività: può capitare infatti che durante l'ascolto della rete si rilevino altre parole chiave utili e si renda perciò necessaria l'aggiunta delle stesse. Il monitoraggio, oltre ad avere un'impostazione strutturata deve anche seguire lo spontaneo "movimento" dei trend dettati dalle conversazioni in rete: l'analyst deve sapere dove cercare determinate informazioni e al tempo stesso deve lasciarsi trasportare da quello che è l'andamento delle conversazioni per capirne in tempo utile i mutamenti (gli utenti spesso, in riferimento ad un accaduto, vanno da affrontare altri temi, più o meno correlati a quello di partenza, spostando quindi il focus delle loro conversazioni).

Più articolato e complesso possibile sarà il panel di keyword settato e maggior probabilità si avrà di analizzare il focus giusto, senza tralasciare informazioni importanti.

Una volta raccolti i risultati contenenti le keyword settate, si opera una prima scrematura dei risultati al fine di rilevare eventuali incongruenze e operare una depurazione dei risultati non inerenti: questo si ottiene solitamente attraverso l'esclusione di keyword correlate a quello che viene considerato semplice "rumors".

Una volta ottenuto un database di informazioni inerenti si procede alla lettura e classificazione dei risultati mediante dei tag, ovvero delle etichette che distinguano e classifichino le occorrenze rilevate. Questi tag possono essere riferiti sia al sentiment, ovvero alla percezione e giudizio espresso dall'utente (solitamente viene inquadrato in positivo negativo e neutro), sia ai temi di discussione del risultato analizzato. La quantità di tag e quindi il dettaglio dell'analisi è a volte vincolato anche dalle stesse feature della piattaforma in uso, alcune di esse infatti hanno delle limitazioni nel numero di tag implementabili, mentre più spesso vengono scelte soluzioni che permettono una gestione in totale libertà dei tag. Per arginare questo limite molto spesso si procede all'estrazione del database in format excel che viene successivamente rielaborato ed integrato. Dopo aver classificato, si procede all'analisi e rielaborazione dei dati per trasformarli in informazioni fruibili ed utili che andranno a costituire un output quali-quantitativo con diverse delivery a seconda delle necessità: da aggiornamenti quotidiani, a settimanali, mensili, semestrali.

6.3 Tipologie di monitoraggio

L'attività di monitoraggio della rete può assumere forme diverse in relazione agli obiettivi che sono posti, alla tipologia di attori e ai dipartimenti aziendali coinvolti. Alcune forme possono essere:

- **Alert.** Consiste nella segnalazione tempestiva di criticità potenzialmente pericolose per la reputazione del brand. Per agevolare la comunicazione essa avviene, nella maggior parte dei casi, tramite mail diretta al comparto coinvolto e si esaurisce in un testo breve, chiaro ed esaustivo della criticità rilevata e correlata possibile modalità di gestione e risposta. Possono appartenere a questa categoria risultati dai toni polemicici, negative o critici: in questo caso è fondamentale contestualizzare la rilevazione e capire se la fonte è autorevole o virale (in questo caso può rappresentare una minaccia per il brand). Fondamentale distinguere l'alert da un messaggio dai toni

semplicemente negativi: possono infatti essere rilevati dei messaggi negativi ma non pericolosi per la reputazione del brand.

- Rassegna. Rispetto all'alert il servizio di rassegna è più completo perché fornisce una lista completa di messaggi contenenti le keyword di interesse e viene inviata con periodicità prefissata. Questo output può consistere in un semplice invio di elenco link dei risultati inerenti, oppure essere integrata da altre informazioni utili di tipo quali quantitativo come fonte di provenienza, autore, ranking e sentiment/temi.
- Report periodico. Un'analisi più dettagliata e completa è quella che solitamente viene fornita attraverso una reportistica approfondita di analisi quantitativa e qualitativa.

Questi report possono essere redatti:

o prima dell'inizio di un'attività di digital communication per fare una fotografia dell'attuale situazione in rete al fine di studiarne poi le evoluzioni (Brand assessment); o durante l'attività di monitoraggio con diverse periodicità a seconda delle esigenze; o post evento o iniziativa di comunicazione, campagna per avere un quadro della performance ottenuta. L'analisi che ne deriva è di tipo sia quantitativo che qualitativo. L'analisi quantitativa mira a fornire un quadro sui volumi di risultati rilevati in rete riferiti all'oggetto di analisi, per determinate keyword. Le occorrenze vengono suddivise per provenienza della fonte, per lingua o country (se si tratta di un monitoraggio internazionale) e successivamente classificati per sentiment e temi/micro temi.

L'analisi qualitativa oltre che vertere sulle tematiche di discussione e il sentiment delle stesse è volta ad individuare anche i possibili detractor e brand lover, al fine di mappare la community di riferimento rintracciando quelli che possono essere considerati influencer.

Strumenti e piattaforme tecnologiche per il monitoraggio della digital reputation. La digital reputation analysis si può avvalere dell'utilizzo di tool di monitoraggio, oltre che del metodo di ricerca manuale direttamente sulle principali fonti web. Gli strumenti tecnologici permettono una maggior

automatizzazione di alcuni processi quali la raccolta dei risultati attraverso il set up delle keyword e la creazione dei grafici, quello che non può fare al momento è un'affidabile ed esaustiva classificazione automatica del sentiment e dei temi di discussione. Nel mercato ci sono, infatti, strumenti che producono una classificazione del sentiment automatico, soprattutto per la lingua inglese, ma da test effettuati sui risultati classificati si registra una bassissima affidabilità del tagging: una macchina non riesce, infatti, a distinguere un risultato negativo da uno sarcastico, non riesce a cogliere le sfumature di un'espressione, spesso border line e difficilmente comprensibile anche da mente umana. Per quel che riguarda le analisi semantiche, ormai quasi tutti i tool di monitoraggio producono una tag cloud dei termini più ricorrenti che compaiono nei risultati raccolti dal tool, in alcuni casi si trovano tag cloud sui concetti espressi (come Blogmeter), ma questo è ben lontano dall'individuazione dei temi effettivi di discussione degli utenti.

Ci sono però degli strumenti statisticamente interessanti, come la piattaforma SAS che sta sviluppando un modulo sulla social media analisi, che dopo una prima fase di campionatura e tagging manuale dei risultati, attraverso lo sviluppo di regole basate sull'analisi fatta a campione applica un tagging automatico del sentiment con risultati di affidabilità alti.

Le piattaforme più conosciute sul mercato sono Blogmeter, Salesforce-Radian6, Alterian, Buzzmetric, Sysomos, Visibile, Brandwatch, The Fool, Synthesio e moltissime altre, più una serie copiosissima di tool gratuiti che presentano chiaramente delle limitazioni e vincoli più forti, ma che possono costituire una buona base per integrare l'uso di altri strumenti come Socialmention, Rocket, Topsy e molti altri.

6.4 Gestire una crisi

Il monitoraggio della propria reputazione online ha anche lo scopo di individuare tempestivamente focolai pericolosi che possono comportare reali criticità per la reputation del brand sfociando in crisi. Una crisi è un evento non

pianificato (ma non necessariamente imprevedibile) che richiede decisioni strategiche di alto livello in tempo reale, in circostanze in cui prendere decisioni errate, o non rispondere con sufficiente velocità e proattività, potrebbe danneggiare seriamente l'organizzazione.

La reputazione ha un ruolo chiave nell'influenzare l'atteggiamento, e quindi il comportamento, di tutti gli stakeholder; e dal momento che una crisi è l'espressione più acuta del rischio reputazionale, essa può danneggiare significativamente:

– il prezzo dei prodotti, il valore del brand, le vendite, i ricavi, il tasso di fedeltà della clientela, l'attrattiva sui collaboratori potenziali, la qualità delle relazioni con i fornitori, delle alleanze strategiche e delle partnership (in termini di stabilità, economicità delle condizioni contrattuali...), l'equilibrio nelle relazioni con istituzioni, autorità. Questi effetti possono essere temporanei oppure durare a lungo. Ma quando si genera una crisi? Un commento negativo può rappresentare un caso isolato, o dar vita ad un flusso di discussioni più o meno animato oppure scatenare una vera e propria crisi per il brand. I fattori importanti da tenere in considerazione al momento dell'individuazione di un possibile caso di crisi sono:

- entità del commento. È fondamentale distinguere un risultato dal sentiment negativo da un risultato effettivamente pericoloso e dannoso: non tutti i commenti dal sentiment negativo infatti rappresentano dei pericoli per la reputazione online, scontento e polemiche fanno parte delle diverse percezioni.
- Autorevolezza della fonte di provenienza. Il valore di un commento proveniente da un utente con un limitato seguito e uno proveniente da una personalità considerata influente sortiscono ovviamente risultati differenti sia in termini di diffusione della notizia che in termini di consenso che può riscuotere.
- Amplificazione: spesso una negatività parte da una fonte e difficilmente resta confinata a quello specifico luogo, molto più frequentemente invece trova diffusione e amplificazione anche su altri canali, acquistando il carattere della multicanalità.

- Velocità di diffusione: aspetto fondamentale perchè individua il grado di viralità che può ottenere un risultato.

Il crisis management, soprattutto in ambiente digitale, non segue un processo rettilineo con un inizio e una fine, ma presenta piuttosto delle dinamiche circolari, una delle caratteristiche principali del web è infatti l'essere "liquido", non contenibile in ristretti e precisi ambiti predittivi.

Si possono comunque individuare quattro principali fasi di un processo di crisi:

- l'analisi e la pianificazione;
- la decisione e l'azione;
- la verifica;
- l'aggiustamento e la nuova azione.

Questo schema richiama il ciclo di Deming o ciclo di PDCA (plan-do-check-act): un modello studiato per il miglioramento continuo della qualità sul lungo periodo. Esso parte dall'assunto che per il raggiungimento del massimo della qualità sia necessaria la costante interazione tra ricerca, progettazione, test, produzione e vendita e seppur originariamente pensato in ottica industrial/produttiva, ben si presta per rendere il processo di crisis management. Le sue fasi sono:

- P - Plan. Pianificazione.
- D - Do. Esecuzione del programma.
- C - Check. Test e controllo, studio e raccolta dei risultati e dei riscontri.
- A - Act. Azione per rendere definitivo e/o migliorare il processo.

L'organizzazione e definizione di un processo interno che sia in grado di affrontare le eventuali crisi reputazionali minimizzandone le conseguenze rappresenta, insieme alla loro prevenzione, un obiettivo prioritario per le aziende, è infatti necessario che ci siano dei flussi virtuosi di comunicazione

veloce tra i diversi comparti aziendali affinché si possa gestire l'emergenza in modo agile, incisivo ed ottimale.

6.5 IL WEB REPUTATION MANAGER

Il web offre la possibilità di verificare rapidamente la credibilità di una persona (la sua reputazione), attraverso: i commenti postati sui blog/forum, le menzioni ricevute da altri soggetti, le immagini postate sui social networks, ecc. Questa possibilità può diventare un rischio per chi pubblica incautamente informazioni che lo riguardano, perchè spesso esistono scostamenti tra l'identità personale e l'identità digitale della stessa persona, dovuti al modo in cui la personalità dell'individuo viene 'costruita' in rete.

Tale problema ha dato luogo alla creazione di una nuova figura professionale: quella dell'"online reputation manager". Naturalmente ciò riguarda soprattutto le persone che hanno una immagine pubblica da difendere, ma ciò diventerà una necessità anche per le persone comuni. Quando la credibilità online di una persona viene danneggiata (dai suoi comportamenti reali o da quelli di altri) esiste la possibilità che essa si rivolga a un servizio di ricostruzione della propria reputazione digitale. Un suggerimento utile a controllare bene cosa si posta online lo suggerisce Google, più di una volta sulla graticola per la gestione delle informazioni personali dei suoi utenti. Nella sezione gestione della reputazione online Google spiega come "Oggi circola sul Web una quantità sempre maggiore di informazioni personali. Ad esempio, qualche tuo amico potrebbe menzionare il tuo nome su un social network o taggarti in alcune foto online, oppure il tuo nome potrebbe comparire in un post su qualche blog o in un articolo". Pochi sanno che se c'è un contenuto che ci riguarda, visibile nei risultati di ricerca di Google, si può chiedere di rimuoverlo attraverso l'esclusione delle informazioni personali da Google o attraverso la rimozione di una pagina o un sito dai risultati di ricerca di Google.

CONCLUSIONI

Abbiamo visto che la **Web Reputation** (reputazione sul web) è un'attività di raccolta e monitoraggio di tutto quanto viene detto on line riguardo a un determinato prodotto, servizio, progetto o evento. Si tratta di un'attività che sta diventando sempre più strategica fondamentale per le aziende e le organizzazioni, perché consente di capire qual è in generale l'opinione diffusa on line riguardo alla tematica a cui si è interessati.

E' passato un ventennio dal primo tentativo di fornire una definizione completa del concetto di identità digitale messo a punto da Hal Abelson e Lawrence Lessing del MIT (Massachusetts Institute of Technology) che la riassumevano ne "l'insieme delle caratteristiche essenziali e uniche di un soggetto sono ciò che è in grado di identificarlo".

Dall'identità digitale si è poi passati alla costruzione del più complesso concetto di web reputation.

Il monitoraggio della web reputation può essere un'attività *in continuum*, qualora si stia svolgendo una determinata attività di comunicazione on line e se ne vogliono misurare gli effetti nel tempo, o un'attività istantanea volta a fare una sorta di fotografia della situazione del momento: ad esempio, perché si vuole conoscere l'opinione degli utenti prima di entrare in un determinato mercato.

Nel corso dei capitoli precedenti si è altresì evidenziato che le attività di web reputation consentono l'analisi di due riferimenti differenti: il primo è rappresentato da opinion leader e stampa, il secondo dagli utenti direttamente interessati. Infatti, attraverso il monitoraggio, le aziende e le organizzazioni interessate possono conoscere in tempo reale eventuali *minus* e *plus* dei propri prodotti, servizi, progetti o eventi, in quanto gli utenti hanno ormai l'abitudine di recensire on line e di condividere con altri utenti le proprie opinioni sulle cose che stanno più a cuore.

Tuttavia la verifica della propria reputazione on line non riguarda solo aziende e organizzazioni. Sono i personaggi pubblici, infatti, i primi ad utilizzare questo

servizio, seguiti dalle aziende che vendono i propri prodotti o servizi on line e quelle vendono tecnologie, divertimento, alimentazione e benessere. Come per le Digital PR, da qualche anno anche le aziende farmaceutiche e quelle legate al mondo della salute, hanno cominciato a servirsi di questo tipo di analisi per verificare l'opinione degli utenti riguardo ai proprio farmaci e dispositivi medici.

Il tutto lascia presagire un fortissimo sviluppo delle figure professionali legate a queste attività di monitoraggio e soprattutto evidenzia un forte bisogno formativo che necessita continui aggiornamenti, necessari per tenere il passo con le continue novità presentateci dal web 2.0 e dalla nuova economia della reputazione.

Se poi volessimo analizzare da un punto di vista sociologico il concetto di web reputation è facile notare come il timore di essere espropriato di qualcosa che riconduce solo a lui medesimo accompagna la storia dell'uomo dal momento in cui, per l'evidente motivo di essere riconosciuto e accettato quale soggetto stanziale in un determinato territorio, ha dovuto concedere informazioni uniche a chi a sua volta avrebbe dovuto registrare il suo passaggio come facente parte di quella comunità nella quale lo stesso uomo avrebbe accettato i doveri ed ottenuto i benefici collegati alla residenza.

Con la gestione digitale delle informazioni sono pertanto cambiate la velocità con cui ciò che ci appartiene può essere diffuso e impropriamente utilizzato e la pervasività della rete che trasporta ovunque i dati rendendo possibile la loro esposizione ed utilizzazione a prescindere dalla volontà di chi ne è titolare.

Tanti pezzi di una identità ricostruibili attraverso il web e la possibilità di ricomporli in profili identificativi specifici, delicati nei contenuti e per i quali l'appropriazione indebita rappresenta un vero e proprio reato, danno vita a timori che molti avvertono quando, volontariamente o obbligati dal fornitore di un determinato servizio online, devono digitare una password o introdurre una carta che la contiene.

La storia ci insegna che le tracce del nostro essere stati qualcosa rimangono e servono a ricomporre la storia degli uomini singoli e delle comunità alle quali, a titolo diverso, sono appartenuti e attraverso le quali hanno transitato.

Attualmente invece nessuno può immaginare un mondo in cui un soggetto fisico può essere cittadino digitale, con tutte le caratteristiche che gli permettono di formulare la propria identità come sintesi di quello che è nelle varie e innumerevoli attribuzioni che lo riguardano e quindi con elementi di riconoscimento oltre ai propri dati anagrafici, nonché rappresentabile, se lo vuole, da una identità biografica vera e propria ed essere contemporaneamente anonimo quando quello che chiede alla rete è riferibile a se stesso. Abbiamo anche visto che tutti ritengono indispensabile che si possano rendere invisibili ad altri i legami fra il portatore di una istanza e l'erogatore di un servizio quando la richiesta comporta il trattamento di informazioni e dati sensibili. Nell'era predigitale, fino alla fine del Novecento, era il soprannome a qualificare la reputazione di una persona. C'era "Tiradritto" per il boss della 'ndrangheta Giuseppe Morabito, che con il mitra non sbagliava un colpo; "il Picconatore" per il presidente della Repubblica Francesco Cossiga.

Nell'era veloce di internet, Google è il moderno oracolo da interrogare prima di agire, e la reputazione è diventata la nuova moneta globale. Prima di un colloquio di lavoro; prima di scegliere un prodotto, un albergo, un ristorante; prima di investire in azioni di questa o quella società; per valutare un candidato politico, un avvocato, un commercialista, tutti noi, ne "googliamo" il nome. Avere una buona reputazione online è moneta sonante. Al contrario, averne una pessima, o semplicemente avere un omonimo sbagliato, può renderci la vita un inferno.

Il nostro passato, quello che abbiamo immesso in rete, le nostre tracce digitali, ma anche quello che gli altri dicono di noi, rimarrà scritto per sempre. Pronto a essere tirato fuori al momento giusto. O, più spesso, al momento sbagliato. Già, perché siccome l'intelligenza è artificiale, Google valuta con criterio squisitamente matematico cosa mostrare nella prima fondamentale riga della prima pagina di ricerca, che è il biglietto da visita più letto. Quello fatale.

Per persone, governi, aziende e istituzioni, l'algoritmo favorisce le voci più visitate. Così, nella ricerca sulla secolare "Guardia reale di Buckingham Palace", domina il racconto di quell'unica volta in cui dopo anni di onorata carriera l'integerrimo soldato in giacca rossa e colbacco scivolò davanti a centinaia di turisti e cadde a terra durante la cerimonia del cambio della guardia.

Che dire poi di quel bravo poliziotto, uno dei migliori capi della Mobile d'Italia il cui nome, dopo vent'anni di onorata carriera e centinaia di casi risolti, verrà d'ora in poi identificato solo con l'unico errore giudiziario.

Tutto il glorioso passato e l'edificante futuro prima e dopo questi episodi buffi, gonfiati, o anche gravi, insomma "cliccati" verrà dimenticato; sepolto in quinta o sesta pagina di Google. Quelle che nessuno arriva mai a leggere.

I danni possono essere gravissimi, irrecuperabili, come nel caso dell'ex ministro francese Dominique Strauss-Khan, che vede comparire solo dopo pagina 25 le prime voci che ricordano la sua abilità professionale da direttore generale del Fondo monetario internazionale, o solo terribilmente fastidiosi.

Con una cattiva reputazione online un uomo non potrà diventare autista di Uber, aprire un'attività di ristorazione in casa, trovare amici o soci in una nuova città.

Lo sa bene la Corte europea che con una singolare sentenza ha di fatto abdicato in favore del motore di ricerca, ammettendo implicitamente di non controllare più le politiche nazionali, o sovranazionali, nella controversa questione del diritto all'oblio e forzando Google a entrare in una decisione quasi giuridica. Ora c'è dunque la possibilità di cancellare dai risultati di ricerca link a contenuti lesivi della reputazione; ma a determinate, ferree condizioni. Sia chiaro, il link rimarrà nel web, ma non nei motori di ricerca europei.

Una potente azienda italiana, quando i motori di ricerca muovevano i primi passi, immaginò che pagando, o comprando azioni di Google, si potessero “persuadere” i suoi dirigenti a far eliminare per sempre i link ai contenuti poco edificanti riguardanti il suo amministratore delegato. Fu grande lo stupore quando si capì che l’algoritmo non scende a compromessi, e non fa sconti.

Nel mondo anglosassone il problema viene aggirato tramite la cosiddetta “ingegneria reputazionale”: nell’Università di Oxford, ad esempio, è nato un dipartimento in cui si studia come creare, sostenere, ricostruire una reputazione. “Ogni azienda ha una reputazione multipla. Ognuna di queste reputazioni è riferita a un ambito e recepita da un target circoscritto. Possono essere scisse, isolate e valutate economicamente una per una”, spiega Rupert Younger, direttore del centro di Corporate Reputation. Come si agisce? “Nel caso di gravi danni reputazionali, invece di tentare di rispondere a tutti gli attacchi nei socialnetwork si produce ad hoc una massiccia dose di contenuti positivi”. Talmente tanti e condivisi, da arrivare nel tempo a spingere quelli negativi più in basso e nelle pagine meno lette di Google.

Anche a Mountain View, sede di Google in Silicon Valley, se ne sono resi conto e hanno adottato un software “antibufala”, che penalizzerà i contenuti inattendibili spingendo in basso i risultati di siti web che più spesso di altri si sono rivelati menzogneri.

Virtuale e reale ormai sono vasi comunicanti. Anzi, un unico vaso. Un ambiente connesso che il filosofo Luciano Floridi, direttore dell’Internet Institute di Oxford, ha battezzato “infosfera”, in cui le azioni compiute nel reale hanno immediate conseguenze nel virtuale e viceversa. I più scaltri, consapevoli di essere uomini “onlife”, cominciano a pensare e valutare bene le conseguenze reputazionali prima di agire. Si comportano non più come sarebbe nella loro natura, ma nel modo in cui vogliono essere considerati, orientando l’identità verso il proprio ideale. Un fortissimo condizionamento autoimposto che secondo gli anglosassoni, può portare a migliorare se stessi.

Come Pollicino i più disciplinati lasciano continuamente tracce digitali nel solco prescelto che poi ripercorreranno. Aiutati dagli algoritmi – che propongono spontaneamente contenuti nuovi basandosi sulle orme delle ricerche del passato – otterranno così un doppio risultato, nella reputazione e nella formazione.

La questione reputazionale investe anche l’Aldilà. Se Cecilia Metella, nobildonna romana, nel suo mausoleo funebre fece incidere la storia (rivisitata) sua e della sua famiglia, privilegiando gli aspetti che intendeva tramandare ai posteri, Facebook sta pensando alla gestione delle bacheche dei defunti, che tra pochi decenni saranno più numerose di quelle dei vivi. Passeranno da “pagine del diario” a “pagine del ricordo”. L’“interramento digitale” prevede la cancellazione di dati sensibili e poco edificanti, per le visite dei posteri.

Tuttavia può essere più semplice accogliere l’idea che la rivoluzione che stiamo vivendo impone una rielaborazione dei valori e la riconsiderazione del concetto di perdono. L’onta da lavare, l’onore leso per sempre, la disperata vergogna sono tali infatti solo se riferiti a valori legati a un’era in cui si era portati a vivere una sola vita, un solo matrimonio, un solo mestiere e l’identità si cristallizzava nel tempo e nello spazio. Nell’iperstoria è superato. I nativi digitali sono naturalmente allenati ad accettare, inglobare e ricomporre ricordi belli e brutti all’interno di repentini cambiamenti di vita e identità. Addirittura valorizzano gli errori commessi. Gli abitanti della Silicon Valley hanno scoperto che “chi sbaglia impara” e, pensa un po’, ci fanno intere lezioni a Stanford.

Anche Pizia – la sacerdotessa dell’antica Roma che pronunciava oracoli in nome di Apollo nel santuario di Delfi – in cambio delle sue visioni sul passato e sul futuro, riceveva offerte dai pastori. Ora che Google sta per cambiare il proprio metodo di interrogazione, gli esperti del marketing hanno recuperato il termine “Oracle” per definire il nuovo sistema di gestione. Knowledge Vault è l’evoluzione dell’algoritmo che Google definisce “oracolo

digitale". Abbandona le interrogazioni basate su parole chiave e compone i dati in vere e proprie porzioni di conoscenza, interpretando le "entità", cioè le relazioni e i collegamenti, temporali o di causa-effetto tra oggetti e concetti del sapere umano. Promette inedite interpretazioni di eventi e personaggi della storia alla luce delle connessioni tra i documenti e i dati a disposizione in un database valutato come corretto e affidabile al 90 per cento. In pratica indaga, valorizza e potenzia i sistemi relazionali, più vicini a quelli umani, fornendo informazioni automatiche. Potrebbe essere dunque in questo nuovo algoritmo la soluzione per una reputazione più conforme a quello che realmente siamo e che dovremmo forse accettare di vedere riconosciuto. Cioè persone con una vita e una personalità non sempre coerente e spesso anche contraddittoria; riprendendoci il diritto di avere più sfaccettature. Ma di questo tratteremo, forse, in un prossimo manuale per chi è interessato a capire la complessità della "web reputation"...

Bibliografia

Aaker D.A., Keller K.L. (1990), Consumer Evaluations of Brand Extensions, "Journal of Marketing", vol. 54, n. 1, pp. 27-41.

Ainsworth M., *Attachment: Retrospect and prospect*, London, 1982.

Alexander N., Colgate M. (2005), Customer's Responses to Retail Brand Extension, "Journal of Marketing Management", pp. 393-419

Anderson Chris, *La coda lunga*, Codice Edizioni, Torino, 2007.

Armstrong A., Hagel J. III (1996), The Real Value of Online Communities, "Harvard Business Review", May-June, pp. 134-41.

Baron R. M., Kenny D. A. (1986), The Moderator-mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations, "Journal of Personality and Social Psychology", vol. 51, pp. 1173-1182.

Bottomly P.A., Holden S. (2001), The Formation of Attitudes towards Brand Extensions: Empirical Generalizations Based on Secondary Analysis of Eight Studies, "Journal of Marketing Research", vol. 38, november, pp. 484- 500.

Boush D. Loken B. (1991), A Process Tracing Study of Brand Extension Evaluation, in "Journal of Marketing Research", vol. 28, n. 2, pp. 16-28.

Bowlby J., *Attaccamento e perdita: La separazione dalla madre* (1973), vol 2, Trad. it. Boringhieri, Torino, 1975.

Bridges S., Keller K.L., Sood S. (2000), Explanatory Links and the Perceived Fit of Brand Extensions: the Role of Dominant Parent Brand Associations and Communications Strategies, "Journal of Advertising", vol. 29, n. 4, pp. 1-11.

Broniarczyk S.M., Alba J.W. (1994), The Importance of Brand in Brand Extension, in "Journal of Marketing Research", vol. 31, may, pp. 214-28.

Brufi Miranda, *Dall'identità digitale all'identità personale*, Informatica e diritto, Vol. XVII, 2008, n.12, pp. 167-193

Busacca B., Bertoli G., Levato F. (2006), Brand extension & Brand loyalty, in Proceedings of the 5th International Congress on Marketing Trends Venezia, Ca' Foscari, 20-21 gennaio 2006.

Castaldo S, Botti S. (1999), La dimensione emozionale dello shopping: una ricerca esplorativa sul ruolo del punto di vendita, "Economia & Management", n. 1, pp. 17-37.

Castells Manuel, *L'età dell'informazione: economia, società, cultura*, Egea, Milano, 2009.

Centeraro, Sorchiotti (2013). *Personal Branding. Promuovere se stessi on line e creare nuove opportunità*.

Cooley C. H., *Human nature and social order*, Child Development, New York, 1902.

Coopersmith S., *The antecedent of self-esteem*, Freeman, San Francisco, 1967.

Cosenza Vincenzo, *Social Media ROI*, Apogeo, Milano, 2012.

Crabtree A., *Animal Magnetism, Early Hypnotism and Psychiatry*, White Plains, New York, 1988.

Dacin P., Smith D.C. (1994), The Effect of Brand Portfolio Characteristics in Consumer Evaluations of Brand Extensions, in "Journal of Marketing Research", vol. 31, may, pp. 229-42.

Dawar N. (1996), Extensions of Broad Brands: the Role of Retrieval in Evaluations of Fit, in "Journal of Consumer Psychology", vol. 5, n. 2, pp. 189-207.

De Baggis Mafe, *World Wide We*, Apogeo, Milano, 2010.

de Ruyter K. e Wetzels M. (2000), The Role of Corporate Image and Extension Similarity in Service Brand Extension, "Journal of Economic Psychology", vol. 21, pp. 639-59.

DeGraba P., Sullivan M.W. (1995), Spillover Effects, Cost Savings, R&D and the Use of Brand Extensions, "International Journal of Industrial Organization", vol. 13.

Descartes R, *Discorso sul metodo*, Laterza, Roma-Bari, 1974.

Dholakia U., Bagozzi R.P. (2001), "Consumer Behaviour in Digital Environments", in J.Wind, V. Mahajan (eds.), *Digital Marketing*, John Wiley & Sons, New York, pp. 163-200.

Diegoli Gianlica, *Social media marketing, Manuale di comunicazione aziendale 2.0*, Hoepli, 2015

Dossena (2013). *Le nuove Reputazione, apprendimento e innovazione nelle imprese. Il ruolo delle online community*, Efficiency, "Journal of Marketing Research", august, pp. 296-313.

Erikson E., *Infanzia e Società*.(1950), Armando Editore, Roma, 1968, p. 35.

Evans P., Wurster T.S. (1999), *Blown to Bits. How the New Economics of Information Transforms Strategy*, Harvard Business School Press (trad. It. Bing bang, Milano, Il Sole 24Ore, 2000).

Farquhar P.H., Herr P.M. (1993), *The Dual Structure of Brand Associations*, in D.A. Aaker, A.L. Biel (a cura di), *Brand Equity and Advertising: Advertising Role in Building Strong Brands*, Hillsdale, Lawrence Erlbaum.

Floridi Luciano, *Infosfera, Etica e filosofia nell'età dell'informazione*, Giappicchelli, 2009

Fournier S. (1998), *Consumer and their Brands: Developin Relationship Theory in Consumer Research*, "Journal of Consumer Research", vol. 24, n. 4, pp. 343-73.

Fraia Guido, A cura di. *Social Media Marketing*. Hoepli, Milano, 2011.

Fridman J. A., *Le origini del Sé e dell'identità*, Astrolabio, Roma, 2001, pp.44-51.

Ghislandi Roberto, *Email Marketing. Guida pratica per fare business con l'email*. Agostini, De Nardis (2013). *La tua reputazione su Google e Social Network*.

Gronhaug K., Hem L., Lines R. (2002), *Exploring the Impact of Product Category Risk and Consumer Knowledge in Brand Extensions*, "Journal of Brand Management", vol. 9, n. 6, pp. 463- 76.

Gunderson J., et al, *The phenomenological and conceptual interface between borderline personality disorder*, *American Journal of Psychiatry*, 1993, n. 150, pp. 19-27.

Hem L.E., de Chernatony, Iversen N.M. (2003), *Transfer to Brand Equity in Brand Extensions: the Importance of Brand Loyalty*, in "Advances in Consumer Research", vol. 30, pp. 72-77.

Herr P.M., Farquhar P.H., Fazio R.H. (1996), *Impact of Dominance and Relatedness on Brand Extensions*, in "Journal of Consumer Psychology", vol. 5, n. 2, pp. 135-59.

Hilgard E., *The hidden observer and multiple personality*, *International Journal of Clinical and Experimental Hypnosis*, 1984, n. 32, pp. 248-253. American Psychiatric Association, DSM-4, 1994, p. 525.

Hume D., *Opere filosofiche*, Laterza, Roma- Bari, 1992, vol. 2.

Hutchinson J.W. (1983), *Expertise and the Structure of Free Recall*, in R.P. Bagozzi, A.M. Tybout (a cura di), *Advances in Consumer Research*, vol. 10, Ann Arbor, Association of Consumer Research.

Invernizzi G., *Manuale di Psichiatria e Psicologia Clinica*, McGraw-Hill, Milano, 2000.

Keller K.L. (1993), *Conceptualizing, Measuring, and Managing Customer-Based Brand Equity*, "Journal of Marketing", vol. 57 (1), pp. 1-22. 19

Keller K.L., Aaker D.A. (1992), *The Effects of Sequential Introduction of Brand Extensions*, in "Journal of Marketing Research", vol. 29, february, pp. 35-50.

Kernberg F., *Relazioni d'amore. Normalità e Patologia*, Raffaello Cortina

Lane V.R. (2000), *The Impact of Ad Repetition and Ad Content on Consumer Perceptions of Incongruent Extensions*, in "Journal of Marketing", vol. 64, april, pp. 80-91.

Licklider J.C.R & W. Clark, «On-Line Man Computer Communication», August 1962

MacInnis D.J., Nakamoto K (1990), *Cognitive Associations and Product Category Comparison: the Role of Knowledge Structure and Context*, working paper, University of Arizona.

Martinez E., de Chernatony L. (2004), *The Effect of Brand Extension Strategies upon Brand Images*, "Journal of Consumer Marketing", vol. 21 (1), pp. 39-50.

Massarotto Marco, *Internet P.R. il dialogo in Rete tra aziende e consumatori*. Apogeo, Milano, 2008.

Massarotto Marco, *Social Network. Costruire e comunicare identità in Rete*. Apogeo, Milano, 2011.

Micelli S. (1997), *Comunità virtuali di consumatori*, "Economia & Management", n.2, pp. 97-107.

Muthukrishnan A.V., Weitz B.A. (1990), *Role of Product Knowledge in Brand Extensions*, in R.H. Holman, M.R. Solomon (a cura di), *Advances in Consumer Research*, vol. 18, Provo, Association form Consumer Research.

Myers-Levy J., Tybout A.M. (1989), *Schema Congruity as a Basis for Product Evaluation*, "Journal of Consumer Research", vol. 16, june.

Nunnally J.C. (1978), *Psychometric Theory*, New York, McGraw Hill, 2nd ed.

Park C.W., Jaworski B., MacInnis D.J. (1986), *Strategic Brand Concept-image Management*, "Journal of Marketing", vol. 50, october, pp. 135-45.

Park C.W., Kim K. (2001), *Role of Consumer Relationship with a Brand in Brand Extensions: Some Exploratory Findings*, "Advances in Consumer Research", vol. 28, pp. 179-85.

Park C.W., Milberg S., Lawson R. (1991), Evaluation of Brand Extension: the Role of Product Level Similarity and Brand Concept Consistency, in "Journal of Consumer Research", vol. 18, september, pp. 185-93.

Peretti Paola, Marketing digitale. Scenari, strategie, strumenti. Apogeo, Milano, 2011.

Peters Tom, The brand called you, Fast Company, 1997

Rangaswamy A., Burke R.R., Oliva T.A. (1993), Brand Equity and the Extendibility of Brand Names, "International Journal of Research in Marketing", vol. 10, pp. 61-75.

Santoro (2013). *WEB 2.0 e social media in medicina* Pensiero Scientifico Editore

Sheinin D.A. (2000), The Effects of Experience with Brand Extensions on Parent Brand Knowledge, "Journal of Business Research", vol. 49, pp. 47-55.

Smith D.C., Park C.W. (1992), The Effects of brand Extension on Market share and Advertising

Stradtman, Cennamo (2014). *Gestire la reputazione on line for Dummies*.

Sullivan M.W. (1992), Brand Extensions: When to Use Them, "Management Science", vol. 38, n. 6, june, pp. 793-806.

Van Riel A.C.R., Lemmink J., Ouersloot H. (2001), Consumer Evaluation of Service Brand Extensions, "Journal of Service Research", vol. 3, February, pp. 2002-31.