Appunti di viaggio 158

La privacy

13 gennaio 2012

I social network offrono nuovi servizi. Ma niente è gratis

Giuseppe Romano, 2012

L'allegra svendita della privacy sulla bancarella di Internet

Due atteggiamenti si ripetono con frequenza tra molti iscritti a Facebook & c.: l'ignoranza e la pigrizia. Ignoranza rispetto a ciò che altri possono fare con i dati che ognuno mette online, pigrizia rispetto allo sforzo per informarsi. Col passar degli anni e per l'altrui insistenza, Facebook ha effettivamente concesso ai suoi iscritti maggior protezione e libertà di scelta nella gestione dei dati personali. A patto che ci si informi: quanti sanno che è possibile selezionare una ***modalità sicura*** per accedere a Fb difendendo la privacy? Quanti sono informati del fatto che in questi giorni a tutti gli utenti arriva notifica dell'attivazione (obbligatoria) della modalità ***Diario***, che metterà in ordine cronologico, pubblicamente, tutti gli elementi del proprio profilo? Altra inquietante novità Fb è l'annunciata ***condivisione senza attrito*** (*frictionless sharing*), opzione in virtù della quale il social network potrà annotare e divulgare automaticamente agli ***amici*** qualsiasi scelta da noi compiuta su Internet (articoli letti, canzoni ascoltate, film scaricati...).

Bullismo senza privacy (Beppe Grillo, 2006)

Un **bambino autistico** viene seviziato in un istituto tecnico di **Torino** da alcuni compagni, il resto della classe non interviene e osserva con indifferenza come se fosse un fatto abituale. Il pestaggio viene filmato e messo su **YouTube**. È visto 5.500 volte e poi rimosso in seguito a una segnalazione. per tale motivo tre dirigenti di Google sono stati condannati a sei mesi per non aver impedito la pubblicazione del video. La condanna è avvenuta nonostante fosse stata ritirata la querela dai legali del ragazzo. Internet consente la pubblicazione di contenuti su diverse piattaforme. La responsabilità del contenuto è di chi pubblica, non del gestore della piattaforma. Se ogni contenuto dovesse essere controllato dal punto di vista legale prima di essere messo on line, Internet dovrebbe chiudere i battenti.

Se viene scritto **su un muro** un insulto diffamatorio, non si può condannare il proprietario dello stabile per averlo permesso o non averlo cancellato immediatamente. Se si usa **il telefono** per diffondere notizie che dovrebbero essere protette dalla privacy non si denuncia la compagnia telefonica. Senza il video il bambino sarebbe ancora vittima dei suoi seviziatori, lo scandalo è scoppiato solo grazie alla visibilità data da YouTube. **I colpevoli** sono nell'ordine: gli insegnanti e il preside che non hanno vigilato, i compagni che lo picchiavano abitualmente, i compagni che assistevano senza muovere un di-

to, coloro che sapevano e non hanno sporto denuncia. YouTube ha reso pubblico un reato. Qualcuno è stato punito per quel reato? Si è punito chi ha rivelato uno spaccato delle scuole italiane e del **bullismo da quattro soldi** con genitori assenti o complici del comportamento dei loro figli. I dirigenti di **Google** non solo sono innocenti, ma dovrebbero ricevere una medaglia. La sentenza è **un monito**: i disabili nelle scuole italiane si possono pestare, ma **in incognito**. È, come chiunque può capire, un problema di privacy.

I social network offrono nuovi servizi. Ma niente è gratis

Giuseppe Romano, 4 gennaio 2012, Avvenire

I social network consentono di intrattenere rapporti e di ripescare vecchie conoscenze. Com'è noto, ne deriva in genere un chiacchiericcio superficiale che ha poco da vedere con ***l'amicizia*** compiutamente intesa, anche perché quasi tutti si compiacciono di esprimersi e pochi di ascoltare. In certi casi è divertente dibattere su questioni grandi e piccine, ma queste schermaglie verbali scompaiono rapidamente sul fondo della pagina. Quello che resta, invece, sotto il pelo dell'acqua è la memoria totale di tutte le nostre tracce nella Rete, nonché di ogni connessione anche occasionale che ci siamo concessi. La piega che molti social network stanno prendendo non va affatto verso quel contesto che tra gli esseri umani si definisce ***sociale***, ovvero una civiltà rispettosa dei diritti e scrupolosa nel difenderli. Se entri in un social network, sai – o dovresti sapere – che in cambio ti verranno espropriate informazioni da destinare a usi che non governerai: commerciali, per lo più. La maggior parte delle volte queste informazioni vengono ***incrociate*** e sfruttate in modo anonimo, è vero, ma nulla impedisce che i dati personali servano a qualcuno per compilare accurati profili di gusti, preferenze, fobie, consuetudini. Un'indagine recente svolta dal californiano *Center for the Digital Future* sostiene che la maggior parte degli utenti del Web non accorda particolare fiducia alla qualità e alla veridicità delle informazioni. Va nei social network per condividere parole, foto, video, e pazienza per la spazzatura. Condivisibile, entro certi limiti, la tolleranza degli internauti: il bicchiere è pur sempre mezzo pieno, e dentro ci sono straordinarie opportunità di informarsi, nonché di allacciare rapporti sinceri. Un po' di prudenza basterebbe però a schivare molta parte dei rischi connessi a una frequentazione in stile Vispa Teresa. Per dirne una, adesso che nei social network sono letteralmente esplosi i ***giochi sociali*** si dovrebbe fare attenzione a quale sia il prezzo da pagare per ***giocare gratis***.

Un gioco italiano recente e popolare su Fb detta, per l'accesso ***gratuito***, condizioni d'ingresso onerose: a chi s'iscrive viene richiesta l'autorizzazione per «accedere alle tue informazioni di base (nome, foto, sesso, Id identificativo del pc e qualsiasi informazione pubblica)», per «pubblicare su Facebook a tuo nome», compresi messaggi, note, foto e video, per «accedere ai post nella tua sezione notizie e accedere ai tuoi dati in qualsiasi momento», anche quando non si sta usando l'applicazione, e per attingere «alle tue notifiche e contrassegnarle come lette». Un'autentica invasione occulta. Sono condizioni che si possono liberamente sottoscrivere, certo, ma non alla

cieca, se vogliamo che il mondo della Rete globale ospiti cittadini consapevoli piuttosto che greggi di faciloni manipolabili.

La privacy non è uguale per tutti

Franco Bernabè, 24 settembre 2011, il sole24ore

La possibilità offerta dalle nuove tecnologie di raccogliere e archiviare informazioni che riguardano la nostra vita privata e pubblica è un tema di stretta attualità che merita un'attenta riflessione. Qualche numero: ogni giorno in Italia vengono effettuate ben oltre 100 milioni di telefonate in mobilità; più di 4 milioni di transazioni attraverso forme di pagamento elettronico; nelle aree metropolitane oltre un milione di telecamere registrano il passaggio di milioni di individui e veicoli. A queste informazioni vanno aggiunte dichiarazioni dei redditi, presenze scolastiche, ricoveri in ospedale, presenza nelle strutture alberghiere e tantissime altre. Tutte le informazioni raccolte tramite questi canali sono sottoposte a un severo regime di tutela della riservatezza. Ci sono poi le informazioni raccolte da parte dei soggetti fornitori di servizi attraverso la rete Internet e attraverso i prodotti di elettronica di consumo in grado di rilevare e registrare gli spostamenti. Queste informazioni non sono sottoposte agli stessi vincoli.

Come sappiamo alcune pratiche di raccolta d'informazioni da parte di aziende, sono addirittura sconfinate in attività illegittime e sono state pertanto sanzionate e sospese. Si pensi alla raccolta, dichiarata accidentale, di dati dalle reti WiFi domestiche da parte delle vetture incaricate di realizzare le immagini per il servizio Street View di Google. Oppure alla funzione denominata "Beacon" introdotta nel 2007 con la quale Facebook rendeva disponibili informazioni sugli acquisti effettuati dai propri utenti su siti partner, poi ritirata a fine 2009 a seguito di una class action. L'elenco potrebbe continuare, però anche solo da questa breve carrellata si ha la netta impressione che il sistema di sanzioni che dovrebbe fungere da deterrente per questo tipo di comportamenti non sia efficace.

Tali pratiche, in realtà, rappresentano solo la punta dell'iceberg di un'azione di raccolta dati sistematica e continuativa compiuta ormai da qualche anno da parte dei principali attori di Internet. Per farsi un'idea delle dimensioni del fenomeno basti pensare che quotidianamente i 600 milioni di utenti di Facebook si scambiano 1,5 miliardi d'informazioni sotto forma di commenti, messaggi, fotografie e quant'altro. Negli ultimi anni il rischio di una minor tutela della privacy non deriva peraltro unicamente da una crescita del fenomeno in termini di numero di utenti, ma anche e soprattutto da un progressivo ammorbidimento della tutela delle privacy.

Ma veniamo dunque al punto che per noi operatori di TLC è fondamentale: l'asimmetria normativa che penalizza la capacità competitiva degli operatori di TLC europei nei confronti delle aziende che offrono servizi online, principalmente statunitensi. Oggi, infatti, le imprese Usa e gli operatori di TLC europei, anche quando si rivolgono entrambi ai cittadini europei, sono sottoposti a due regimi in materia di privacy sostanzialmente differenti, soggiacendo le prime a un sistema di regole significativamente più lasco rispetto a quello europeo a cui sono soggetti gli operatori del Vecchio conti-

nente.

Questa asimmetria è ascrivibile, per le imprese europee, a una prescrizione contenuta nella Direttiva comunitaria, nella parte in cui si sancisce il cosiddetto "principio di stabilimento", ovvero il principio secondo il quale la disciplina della privacy comunitaria si applica solo alle imprese la cui sede o i cui apparati sono ubicati sul territorio degli Stati membri. La direttiva è oggi in corso di revisione e il settore delle tlc ha chiesto a gran voce che si ponga fine a questa asimmetria. L'obiettivo potrebbe essere raggiunto anche attraverso un reciproco avvicinamento delle due normative, statunitense ed europea, verso posizioni intermedie rispetto a quelle oggi vigenti.

Partendo dalla considerazione che non è pensabile arrivare a bloccare l'accesso ai siti che non rispettano la normativa europea, perché questo non sarebbe accettato dai cittadini europei, esistono fondamentalmente tre vie per portare gli Usa su posizioni più simili a quelle europee: una via politico-giuridica; una via tecnica; una via che potremmo definire di mercato. La prima è probabilmente la più complessa. È necessario arrivare alla definizione di accordi internazionali giuridicamente vincolanti che consentano alle imprese europee di operare sulla base del principio di reciprocità. È bene intervenire anche dal punto di vista tecnico, individuando e promuovendo adeguate soluzioni. A questo proposito vale la pena citare l'iniziativa dei ricercatori della Stanford University, che prevede l'introduzione di uno specifico suffisso da apporre alla fine della dicitura http, che identificherebbe i siti che non raccolgono alcun tipo d'informazione. Da segnalare l'iniziativa del Parlamento europeo per la creazione di un regime di certificazione Ue per i siti web che rispettano la normativa in materia di protezione dei dati. Vi è infine la possibilità d'intervenire con soluzioni di mercato, che mettano l'utente nelle condizioni di autotutelarsi.

Cos'è la privacy?

La privacy o diritto alla riservatezza delle informazioni personali, della propria vita privata e al controllo sui propri dati personali, ***ossia il diritto di essere lasciati in pace***, secondo la formulazione del giurista statunitense di origini ebraiche Louis Brandeis che nel 1890 fu probabilmente il primo al mondo a formulare una legge in materia. Ma ora le nuove tecnologie hanno contribuito ad abbassare la barriera, come ad esempio con la tracciabilità dei cellulari o gli indirizzi di posta elettronica.

Già la Convenzione europea dei diritti dell'uomo, all'art. 8, stabiliva che non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge, salvo se necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine, per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui. Inoltre la Carta dei diritti fondamentali dell'Unione europea, prevede che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano, che devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai

dati raccolti che lo riguardano e di ottenerne la rettifica.

Nella legislazione italiana la riservatezza nei diritti inviolabili dell'uomo è garantita dalla costituzione negli art. 2, 14, 15 e 21, riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero. Ma se uno ha scelto la notorietà, si presume una sua rinuncia a parte della riservatezza se direttamente correlata alla sua dimensione pubblica.

Il rapporto fra diritto di cronaca e privacy è regolato da un'apposita carta di autoregolamentazione dei giornalisti che si propone di tutelare la libertà di informazione nel rispetto dei diritti della persona, col dovere di rettifica, la presunzione di innocenza e le incompatibilità professionali. Vieta qualsiasi tipo di discriminazione per razza, religione, sesso ecc., la pubblicazione di notizie sulla vita privata, e prevede la tutela dei minori e dei soggetti deboli con l'obbligo del loro anonimato.

Vieta inoltre di rendere identificabili o presenti in trasmissioni televisive, quando possano esserci pericoli: minori, vittime di violenze sessuali, membri delle forze di pubblica sicurezza e dell'autorità giudiziaria e congiunti di persone coinvolte in fatti di cronaca. Vieta trattare dati sullo stato di salute e sulla vita sessuale, senza consenso, dell'interessato o dei genitori, se minore.

Importante è la protezione dei dati sensibili archiviati digitalmente sia di privati cittadini, sia d'imprese. I reati connessi alla violazione della riservatezza riguardano: la violazione, sottrazione, soppressione e rivelazione di corrispondenza informatica, l'intercettazione di comunicazioni informatiche, le installazioni abusive di apparecchiature per le intercettazioni, la falsificazione, alterazione e sottrazione di comunicazioni informatiche, la rilevazione del contenuto di documenti segreti, l'accesso non autorizzato a siti, lo spionaggio informatico, l'intervento con qualsiasi modalità non autorizzata su dati, informazioni o programmi, contenuti in un sistema informatico che produca ingiusto profitto con altrui danno.

Inoltre per la pubblicazione delle foto in cui si riconosce una persona non famosa, bisogna avere la sua autorizzazione, salvo nei casi giornalistici che non risultino dannosi per l'individuo con l'esclusione di foto di minori se riconoscibili.

Con i cellulari si possono scattare foto solo se le immagini catturate sono per uso personale, tranne per le persone pubbliche e note. In ogni caso è vietata l'esposizione e la messa in commercio di immagini se recano pregiudizio all'onore, alla reputazione o al decoro della persona ritratta.

Inoltre le aziende possono effettuare chiamate telefoniche di tipo commerciale sino a quando l'interessato non esprima parere contrario che può venire espresso in qualunque chiamata. Per tale motivi le aziende per approvvigionarsi in modo legale di contatti di potenziali clienti, hanno intrapreso campagne mediante concorsi a premi o raccolte punti.