SOCIAL NEWS

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

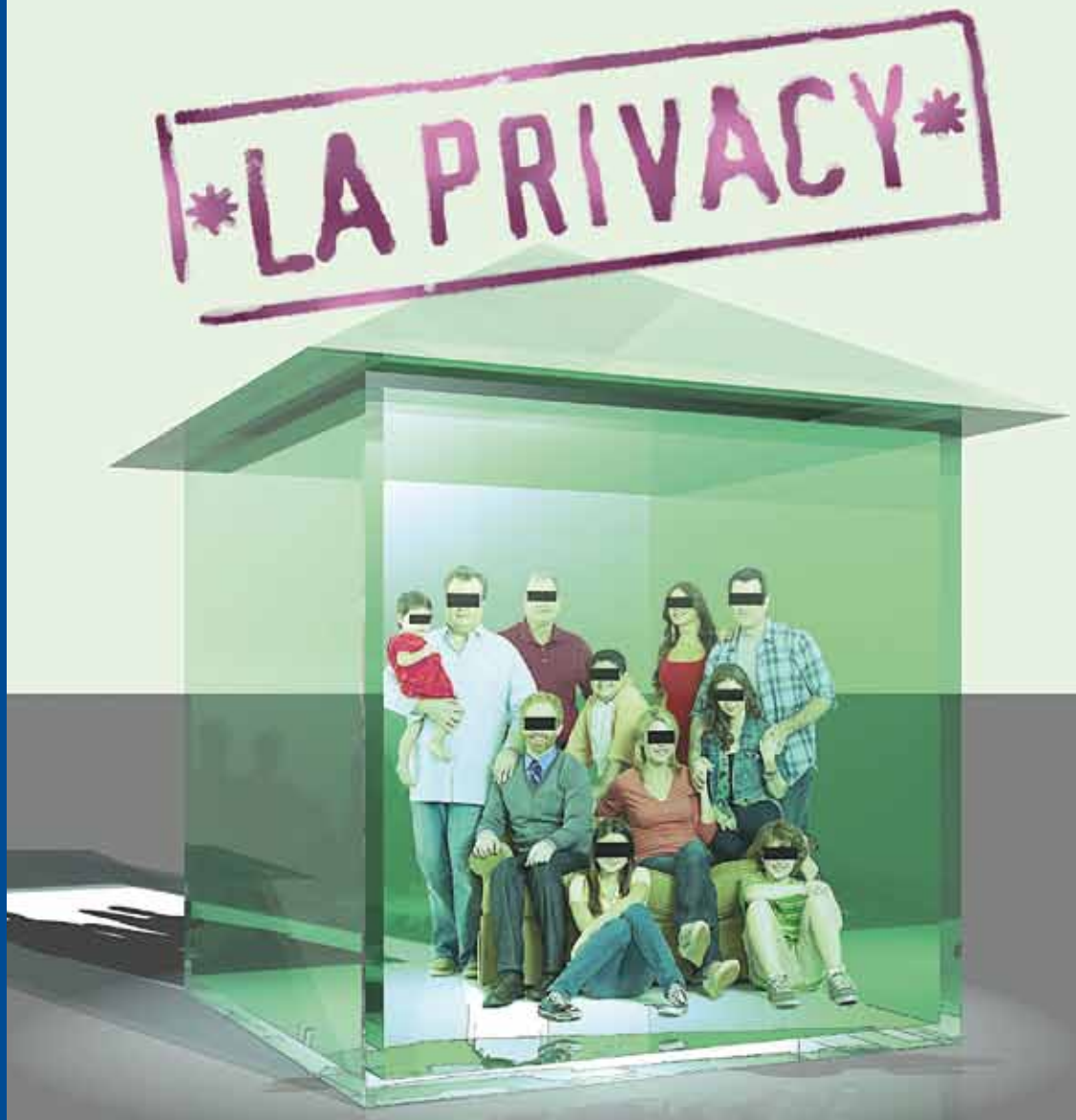
CULTURE A CONFRONTO - MENSILE DI PROMOZIONE SOCIALE

PREMIATO EUROMEDITERRANEO2008

www.socialnews.it

Anno 9 - Numero 6
Luglio - Agosto 2012

Con il contributo satirico di Vauro Senesi



Quanto ci tutela veramente? Come dobbiamo usarla?

realizzazione e distribuzione gratuita

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

INDICE

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

I SocialNews precedenti. **Anno 2005**: Tsunami, Darfur, I genitori, Fecondazione artificiale, Pedopornografia, Bambini abbandonati, Devianza minorile, Sviluppo psicologico, Aborto. **Anno 2006**: Mediazione, Malattie croniche, Infanzia femminile, La famiglia, Lavoro minorile, Droga, Immigrazione, Adozioni internazionali, Giustizia minorile, Tratta e schiavitù. **Anno 2007**: Bullismo, Disturbi alimentari, Videogiochi, Farmaci e infanzia, Acqua, Bambini scomparsi, Doping, Disagio scolastico, Sicurezza stradale, Affidi. **Anno 2008**: Sicurezza e criminalità, Sicurezza sul lavoro, Rifiuti, I nuovi media, Sport e disabili, Energia, Salute mentale, Meritocrazia, Riforma Scolastica, Crisi finanziaria. **Anno 2009**: Eutanasia, Bambini in guerra, Violenza sulle donne, Terremoti, Malattie rare, Omosessualità, Internet, Cellule staminali, Carcere. **Anno 2010:** L'ambiente, Arte e Cultura, Povertà, Il Terzo Settore, Terapia Genica, La Lettura, Il degrado della politica, Aids e infanzia, Disabilità a scuola, Pena di morte. **Anno 2011:** Cristianesimo e altre Religioni, Wiki...Leaks... pedia, Musica, Rivoluzione in Nord Africa, Energie rinnovabili, Telethon, 150 anni dell'Unità d'Italia, Mercificazione della donna, Disabilità e salute mentale, Le risorse del volontariato. **Anno 2012:** Inquinamento bellico e traffico d'armi, Emergenza giustizia, Il denaro e l'economia, Gioco d'azzardo, Medicina riproduttiva.

Direttore responsabile:
Massimiliano Fanni Canelles

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

Collaboratori di Redazione:
Roberto Casella
Rossana Carta
Giulia Cella
Angela Deni
Eva Donelli
Gemma d'Urso
Marta Ghelli
Susanna Grego
Bianca La Rocca
Ilaria Liprandi
Elisa Mattaloni
Christian Mattaloni
Cinzia Migani
Maria Rita Ostuni
Patrizia Pagnutti
Russo Grazia
Enrico Sbriglia
Cristina Sirch
Claudio Tommasini
Elena Turchetto
Valeria Vilardo

Con il contributo di:
Gemma d'Urso
Elisa Mattaloni
Cinzia TH Torrini
Gianfranco Turano

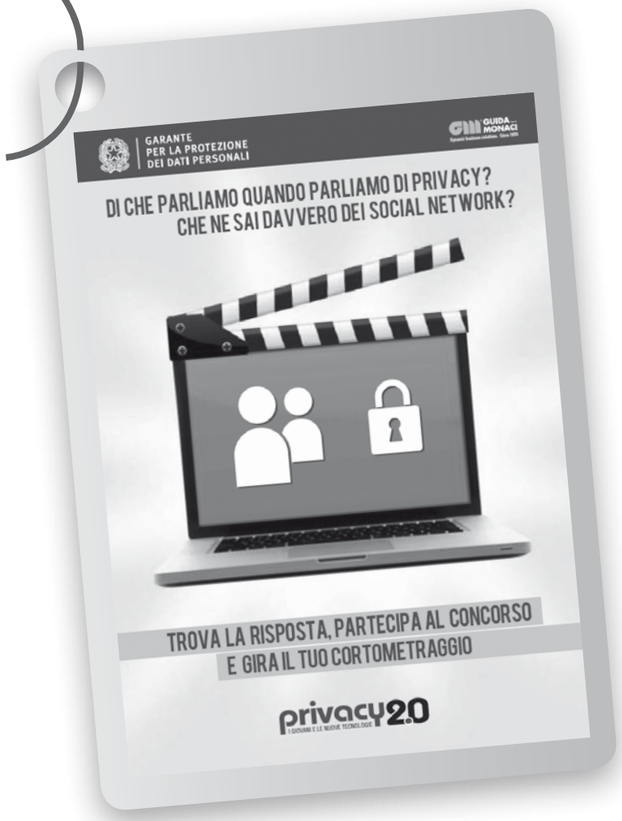
Vignette a cura di:
Paolo Buonsante
Vauro Senesi

Periodico Associato

Si ringrazia per la collaborazione e i contributi la professoressa Antonietta Gatti, associato all'Istituto ISTEC CNR di Faenza e Visiting Professor of the Institute for Advanced Sciences Convergence (Department of State, USA)

QR CODE

Tutte le informazioni, gli articoli, i numeri arretrati in formato PDF li trovate sul nostro sito:
www.socialnews.it Per qualsiasi suggerimento, informazioni, richiesta di copie cartacee o abbonamenti, potete contattarci a: **redazione@socialnews.it**
Ufficio stampa: **ufficio.stampa@socialnews.it**
Registr. presso il Trib. di Trieste n. 1089 del 27 luglio 2004 - ROC Aut. Ministero Garanzie Comunicazioni n° 13449. Proprietario della testata: Associazione di Volontariato @uxilia onlus www.auxilia.fvg.it - e-mail: info@auxilia.fvg.it
Stampa: **AREAGRAFICA - Meduno PN - www.areagrafica.eu**



Un "corto" sulla privacy

Il Garante privacy e il concorso per gli studenti delle scuole superiori

Di che parliamo quando parliamo di privacy? Quale idea ne hanno i giovani che usano in maniera disinvolta cellulari di nuova generazione e Internet? Quanto sanno davvero che cos'è un social network?

A queste e ad altre questioni sono stati invitati a dare risposta gli studenti delle scuole superiori italiane che il Garante per la privacy ha voluto coinvolgere con il concorso "Privacy 2.0 - I giovani e le nuove tecnologie", organizzato in collaborazione con Guida Monaci.

Il concorso prevedeva che gli studenti delle terze e quarte classi delle scuole sorteggiate per ogni provincia italiana girassero un video originale di tre minuti scegliendo un tema, un aspetto, un fenomeno legati alla protezione dei dati in rapporto alle nuove tecnologie. Gli studenti potevano realizzare il "corto" da soli o in gruppo, assistiti o meno da un insegnante.

Il concorso ha avuto termine a novembre 2011 e la premiazione dei vincitori è avvenuta il 28 gennaio 2012, in occasione della Giornata Europea della protezione dei dati.

"Proteggi il tuo mondo!" è il titolo del "corto" del Liceo "Galileo Ferraris" di Taranto che ha vinto i 5.000 euro del concorso "Privacy 2.0 - I giovani e le nuove tecnologie".

Al secondo posto si è classificato il video "Pubblica intimità" realizzato dagli studenti del Liceo "Amaldi" di Novi Ligure, mentre al terzo posto è giunto "Vite inscatolate" dell'Istituto Magistrale "Renier" di Belluno.

La Pubblica Amministrazione nell'era digitale

di Massimiliano Fanni Canelles

La necessità di ridurre i costi della Pubblica Amministrazione conduce ad un progressivo ammodernamento tecnologico ed informatico. Una maggiore valorizzazione delle nuove tecnologie, grazie a progetti ad elevata innovazione e sostenibilità, permette di conciliare la riduzione del budget con una maggiore qualità dei servizi offerti. Purtroppo, l'ICT (Information and Communication Technology) delle amministrazioni pubbliche italiane non è finora decollato, anche se, per alcuni aspetti, qualche "sperimentazione" in tal senso è stata compiuta, come la fatturazione elettronica ed i certificati medici on-line.

La strada timidamente intrapresa potrebbe essere ulteriormente valorizzata con le sempre più perfezionate innovazioni che la tecnologia digitale rende oggi disponibili. Determinante risulterebbe la centralizzazione delle banche dati e l'interconnessione tra le varie amministrazioni, possibilmente con l'utilizzo di un unico software in grado di ridurre i costi di gestione e manutenzione. Lo sviluppo delle tecnologie di riconoscimento vocale basate sulla logica semantica permetterebbe l'integrazione dei servizi di sportello e la digitalizzazione degli stessi. La tecnologia Nfc (Near field communication) trasformerebbe i nostri cellulari in strumenti adatti ad effettuare acquisti e validare le operazioni dei servizi pubblici.

Il ruolo chiave dell'ICT nella riduzione della spesa della Pubblica Amministrazione è evidenziato dai risultati presentati dall'Osservatorio ICT&Management del Politecnico di Milano: il risparmio stimato potrebbe toccare i 43 miliardi di euro l'anno. In particolare, la digitalizzazione di alcuni processi burocratici condurrebbe ad un risparmio di circa 23 miliardi l'anno ed una più snella gestione dei pagamenti equivarrebbe ad un taglio della spesa di circa 1 miliardo l'anno. Secondo lo studio dell'avvocato Walter Paolicelli, le nuove tecnologie permetterebbero, con estrema facilità, la creazione di centraline virtuali ed un'infinità di linee telefoniche caratterizzate da spese ridottissime grazie all'utilizzo della banda larga. Con la piattaforma Skype è, infatti, possibile videochiamare in tutto il mondo ed il costo del servizio corrisponde al solo abbonamento alla rete internet. Non ultima è da considerare l'ipotesi della migrazione verso i software open source, i quali permetterebbero alle pubbliche amministrazioni un risparmio considerevole soprattutto riguardo all'acquisto delle licenze.

Scenari affascinanti ed attraenti, che però necessitano di attenzione nella sostituzione delle tradizionali forme di erogazione dei servizi: non devono, infatti, essere trascurate le difficoltà di interazione con le nuove tecnologie da parte degli amministratori e degli utenti e non va sottovalutato l'investimento sulla protezione dei dati sensibili. Nella società tecnologica, il concetto di privacy ha vissuto continue evoluzioni, passando, in pochi anni, da materia riservata agli addetti ai lavori ad argomento quotidiano che si concretizza nel pericolo di dispersione di informazioni personali e del loro utilizzo per scopi illeciti o non autorizzati.

Ogni giorno migliaia di informazioni sensibili lasciano traccia all'interno di telecamere, supporti di memoria digitale, pc domestici, aziendali, in rete e nei server. Dati contenuti in file che costituiscono l'elemento base di una tecnologia evolutasi velocemente, la quale può agevolare le indagini di polizia, ma non sempre garantisce la necessaria riservatezza ed in alcuni casi diventa veicolo per nuove forme di reato. Il progresso informatico ci coglie tutti impreparati, compresi il legislatore, il magistrato che esercita il potere giudiziario, l'amministratore della cosa pubblica e le forze dell'ordine. Forse, per questo motivo, professionisti, politici, persone comuni ed organi di stampa si interrogano quotidianamente sulle contraddizioni di una società sempre più simile ad un Truman Show.

Rosario Imperiali
Presidente Comitato Scientifico Istituto Italiano per la Privacy

Un problema di privacy

«Non ha più senso parlare di riservatezza on-line, le norme sociali sono cambiate. Ormai gli utenti condividono senza problemi le informazioni personali on-line. E così è finita l'era della privacy», Mark Zuckenberg.

Privacy & Social

L'essere umano ragiona da sempre tramite semplificazioni e connessioni concettuali. Il tormentone di Celentano sull'alternativa tra "rock e liscio" si basava su entrambi questi profili, ma anche l'esperienza di successo di Fazio e Saviano, con la suddivisione della realtà circostante tra "vado via o resto qui", prendeva spunto dalla tendenza dell'uomo a classificare semplificando. Anche in questa circostanza si potrebbe continuare l'esercizio, dividendo la nostra quotidianità tra "privacy e social": "social" è "rock" e "privacy" è "lento"? O "vado via" perché la privacy è morta e "resto qui" perché...
Beh, perché il giochino questa volta non vale, in quanto "privacy" non è termine antagonista a "social" e, soprattutto, perché ciò che intendiamo per "privacy" non è "privacy".
Confusi? No problem!

Il significato dubbio di "privacy"

Forse mai come in questa circostanza l'uomo dei nostri tempi ha trattato di un aspetto che tanto lo riguarda senza averne compreso davvero il significato. Le espressioni "a tutela della mia privacy", "è vietato dalla privacy", "firmi qui per la privacy" sono entrate nel lessico quotidiano, ma raramente denotano un comportamento conseguente e responsabile, cioè di chi, a parole, è in grado di esprimere il senso di ciò che realmente intende. È l'inesorabile sorte dei termini in voga, come, recentemente, "la cifra", "outing", "ossimoro" e, più indietro nel tempo, "implementazione" o "problematiche".

La privacy è morta?

È cascato nel tranello anche il fondatore di Facebook, Mark Zuckenberg - non si sa quanto per errore e quanto per provocazione – quando, un paio d'anni fa, rilasciò una famosa dichiarazione secondo cui «non ha più senso parlare di riservatezza on-line, le norme sociali sono cambiate. Ormai gli utenti condividono senza problemi le informazioni personali on-line. E così è finita l'era della privacy».

La disciplina nella UE

Ha ragione Zuckenberg o l'Unione Europea la quale, al tema della cd Privacy, ha dedicato tante energie approvando una direttiva sin dal 1995, frutto di un complesso iter preparatorio che ancora oggi costituisce un record imbattuto: ben cinque anni di discussione preliminare. Ed ora, Consiglio e Parlamento dell'Unione sono chiamati ad approvarne una riforma radicale, promossa dalla Commissione con lo strumento del Regolamento comunitario. Ad approvazione avvenuta, disporremo di un articolato programma di conformità per le aziende che utilizzano dati personali.

"Privacy" come "riserbo"

Cos'è, quindi, la privacy di cui ci interessiamo? Di certo non è – o forse non è più – il diritto a sottrarsi allo sguardo o alla conoscenza di terzi, il potere di chiamarsi fuori, scegliendo di non fare parte di un certo contesto. Originariamente, infatti, ci si riferiva al diritto ad "essere lasciati soli": quasi una rivendicazione conclamata dell'inviolabile libertà di adesione. Sia "privacy", sia l'omologo italiano "riservatezza" contengono il significato etimologico di "sottrazione" o di "riserbo". La "privacy" protegge un'informazione o un oggetto sottraendolo alla presa di conoscenza di chicchessia e circoscrivendone la circolazione entro una ristretta cerchia di soggetti. Questo tipo di privacy, riconducibile all'intimità della persona ed al senso naturale del pudore, è altro rispetto a quanto oggi ci interessa e, ci sembra, non sia questo il motivo per cui il termine "privacy" sia divenuto d'uso popolare nella nostra società dell'apparire.

Il vero significato di "privacy"

La "privacy" odierna è, in un certo senso, il manuale d'uso delle informazioni personali, le buone regole – ancorché imposte per legge e presidiate da gravi sanzioni – per una corretta gestione delle informazioni che consentono di risalire all'individuo, per questo dette "dati personali". Non si questiona, quindi, della riservatezza che ne può rappresentare un profilo indiretto, ma delle regole d'uso delle informazioni e del loro rispetto. A prescindere che si sia "social" o "private". Un esempio può chiarire.

I "dati personali" non sono sempre oggetto di "riserbo"

Non tutte le informazioni personali interferiscono col senso etimologico di "privacy" (cioè di pudore o riserbo), mentre tutti i dati personali mettono in gioco la disciplina che qui interessa. L'uso del mio nome e cognome, ad esempio, non può certamente essere considerato un'informazione oggetto di riserbo, secondo il significato storico di "privacy". Eppure, nome e cognome sono "dati personali" e, in quanto tali, vanno utilizzati nel rispetto della disciplina che li tutela.

"Privacy" e "social" non sono termini antagonisti

Ed allora, se all'attuale espressione "privacy" si attribuisce il significato di "corretta gestione delle informazioni personali", si comprende chiaramente come "privacy" e "social" non siano necessariamente termini antagonisti. Piuttosto, essi sono complementari. Ben si può essere "social" o partecipare attivamente ad un social network, semmai rilasciando informazioni personali alla propria cerchia di amici e, contemporaneamente, voler preservare i propri diritti per un corretto utilizzo delle medesime informazioni vietandone l'uso a terzi che non facciano parte del gruppo, oppure nutrendo la legittima aspettativa che le stesse non vengano utilizzate impropriamente dal gestore. Un'aspettativa legittima che va presidiata, specie se si considera che più di un quarto dei ragazzi di età inferiore ai 13 anni possiede un profilo pubblico (fonte EuKids Online), mentre il codice di autoregolamentazione "Media e minori" tarda a divenire operativo dal 2007.

L'importanza dello scopo d'uso

Si deve proprio alla disciplina posta a tutela dei dati personali il merito di aver dato rilevanza allo scopo per il quale si

utilizzano queste informazioni. In gergo, ciò si indica col termine "finalità". Nella società attuale, l'uso dell'informazione non può essere regolamentato in via astratta, occorre tener conto dello scopo che con esso si intende concretamente perseguire. Significa cosa si vuol fare o ottenere con quella informazione. Ad esempio, riprendendo l'esempio di prima, l'utilizzo di un'anagrafica a fini di corrispondenza epistolare ad uso personale assume una rilevanza ed un impatto diversi se paragonato allo stesso utilizzo condotto con l'obiettivo di promuovere commercialmente la vendita diretta di un prodotto oppure per creare un profilo soggettivo dell'interessato, magari classificandolo in classi sociali predeterminate.

Finalità e disponibilità dell'informazione

L'importanza della finalità è tale da incidere sul concetto stesso di "utilizzabilità" dell'informazione: non è, infatti, detto che l'informazione personale sia liberamente utilizzabile per il solo fatto di essere "pubblicamente disponibile". Questo, ad esempio, è il principio basilare da rispettare quando si è in Internet. Sul web è disponibile un'incredibile quantità di informazioni personali, semmai rilasciate per partecipare a gruppi di discussione o a social network o per richiedere informazioni su prodotti o servizi on-line o anche solo per soddisfare il principio di trasparenza sulla riferibilità di un sito web al relativo responsabile. La raccolta sistematica di tali informazioni, ad esempio per creare un profilo informativo della persona, talvolta molto dettagliato, non può ritenersi lecito sul mero presupposto che le informazioni sono "liberamente disponibili" in Internet. L'ipotetica raccolta violerebbe il principio di finalità e, quindi, risulterebbe in contrasto con le regole comunitarie sull'uso dei dati personali. In questi casi, infatti, la raccolta e l'uso di dati personali perseguono finalità ben diverse da quelle originarie per le quali gli stessi dati erano stati rilasciati sul web.

Trasparenza

L'esempio dello scandaglio del web alla ricerca di dati personali di terzi da aggregare per la creazione di profili personali è criticabile anche sotto altro profilo. Questa operazione avviene normalmente all'insaputa dei soggetti ai quali gli stessi dati si riferiscono, violando così un altro dei capisaldi della "civiltà informativa": la trasparenza. "Trasparenza" significa che la raccolta e l'uso delle informazioni personali devono essere portate a conoscenza del diretto interessato. Liceità e correttezza impongono che tali operazioni siano realizzate in modo trasparente, senza sotterfugi.

Controllo dell'interessato

Mettere a conoscenza l'interessato delle operazioni di raccolta o dell'uso di informazioni che lo riguardano costituisce il presupposto essenziale affinché quest'ultimo possa controllare che tali operazioni si svolgano in modo compatibile con i propri interessi e diritti. Solo se si è consapevoli di quanto sta accadendo rispetto all'uso dei propri dati da parte di terzi si può effettivamente decidere se si sia d'accordo o meno. Per questo si parla, tecnicamente, di "consenso informato", in quanto la propria valutazione o autodeterminazione risulta libera solo se l'interessato gode di un effettivo diritto di scelta. A sua volta, questa scelta dipende dalla conoscenza completa della situazione di riferimento.

Banalizzazione della privacy

Trasparenza e diritto di scelta svolgono in concreto la missione loro assegnata dal disegno legale di tutela solo nel caso in cui essi siano attuati in modo efficiente ed efficace. Trasparenza significa "presa di coscienza" e questa non la si ottiene certo mediante la trasmissione di lunghe e complesse nozioni tecniche rivolte al destinatario dell'informativa. Oramai, anche a livello internazionale vi è un consolidato set di regole volte a spostare l'attenzione della comunicazione "legale" dal momento trasmissivo a quello ricettivo: non importa tanto il contenuto tecnico trasmesso, bensì quanto il destinatario possa ragionevolmente comprendere. La frase tristemente nota del "firmi qui per la privacy" è il segno emblematico di questa rovinosa banalizzazione.

Equo bilanciamento

Se, da un lato, il potere di controllo dell'interessato è parte dell'impianto delle tutele assicurato dalla legge, dall'altro, la necessità di assicurare la circolazione delle informazioni a fondamento dello sviluppo della personalità individuale e della crescita sociale impone spesso la ricerca di un giusto equilibrio tra interessi o diritti apparentemente contrapposti. La tutela dei dati personali, diritto incluso tra quelli della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza), è un diritto trasversale che interseca spesso altri diritti costituzionalmente garantiti, in un apparente conflitto di valori. Queste situazioni vanno risolte facendo ricorso a taluni principi di base, come quello di proporzionalità ed essenzialità. Secondo il principio di proporzionalità, il diritto alla tutela dei dati personali arretra entro limiti giustificati dal corretto esercizio dell'altro diritto apparentemente antagonista. Secondo il criterio di essenzialità, invece, l'indietreggiamento della privacy è giustificato solo quando esso risulti essenziale per il godimento dell'altro diritto. Si tratta di un'operazione che si avvale di "pesi e contrappesi" e che non risulta sempre agevole, tanto da contribuire a determinare quel senso di incertezza in ambito privacy a cui si faceva riferimento all'inizio.

Casi di allarme

A fronte di questi conflitti, assistiamo a numerose prese di posizione, anche di segno opposto. I fotografi "di strada" lanciano l'allarme perché ritengono minacciate le testimonianze fotografiche dei fenomeni sociali e dei comportamenti collettivi a causa delle "pecette" d'ordinanza poste a tutela della privacy. Il fenomeno della "tv del dolore", nella quale i protagonisti di casi di cronaca nera in Italia sono divenuti personaggi di veri reality televisivi laddove – secondo dati dell'Osservatorio di Pavia – lo spazio dedicato alla "nera" dai tg italiani di prima serata è il doppio di quello della BBC e più di dieci volte maggiore di quello della tedesca ARD. Sen-

Un po' di storia

La privacy degli ultimi 50 anni

Mentre cambiano le nostre abitudini – solo pochi anni fa ci saremmo affidati ad un'enciclopedia o, più semplicemente, al nostro medico di famiglia per controllare e curare i sintomi influenzali - l'era dell'informazione ha lasciato il posto all'era del big data.

Mentre scrivo questo articolo, impazza la notizia della multa che l'americana Federal Trade Commission (FTC) ha imposto a Google: un accordo monetario da 22,5 milioni di dollari.

L'accusa è che Google avrebbe aggirato le configurazioni di protezione della privacy del web server Safari per poter "inseguire" i suoi utenti durante la navigazione on-line, tracciandone i movimenti. Questo ha permesso al motore di ricerca di offrire suggerimenti pubblicitari personalizzati in base ai gusti del singolo utente. In pratica: visiti siti dedicati alla pesca? Il giorno dopo, mentre leggi on-line il tuo quotidiano preferito, ecco che, nello spazio pubblicitario, compare un'offerta per l'acquisto di una canna da pesca o per l'abbonamento ad una rivista specializzata.

Questo modo di servire messaggi pubblicitari non è illegale in sé e per sé: si chiama "behavioural advertising", pubblicità basata sul comportamento.

Con vari gradi di consapevolezza, da qualche anno a questa parte seminiamo cospicuamente i nostri dati personali, on-line e off-line. Pensiamo al modo in cui condividiamo le nostre vite sui social network o a come ci affidiamo ad internet per acquistare prodotti e cercare informazioni o lavoro. Non solo. Pensiamo a tutte le volte in cui veniamo ripresi dalle telecamere di videosorveglianza o quelle in cui ci serviamo di un tesserino RFID per accedere al nostro ufficio, alla metropolitana, alla palestra.

Se aggiungiamo a questa lista la quantità di dati accumulati dai Governi, dalla ricerca scientifica, dalle attività finanziarie e commerciali, non sarà difficile capire perché, negli ultimi mesi, la parola sulla bocca di tutti sia diventata "big data". Si tratta di un concetto riferito, appunto, al flusso continuo e cospicuo di dati ormai impossibili da gestire con un normale database, ma che – se analizzati ed aggregati appropriatamente – possono assumere un alto valore.

Da un punto di vista commerciale, ciò è evidente. Le informazioni su dove viviamo, dove lavoriamo, quali siano i nostri gusti, i nostri interessi, cosa facciamo e dove andiamo nel nostro tempo libero possono essere aggregate in veri e propri profili che permettono alle compagnie di marketing di offrirci prodotti e servizi pensati apposta per noi. Ma c'è dell'altro. Un esempio su tutti è Google Flu Trends. In uno studio pubblicato sul giornale scientifico Nature, Google ha scoperto che, tramite l'aggregazione dei dati relativi alle ricerche dei propri utenti, è possibile calcolare, con una certa precisione ed in tempo reale, quali zone del mondo siano colpite da un'epidemia influenzale.

Mentre cambiano le nostre abitudini – solo pochi anni fa ci saremmo affidati ad un'enciclopedia o, più semplicemente, al nostro medico di famiglia per controllare e curare i sintomi influenzali - l'era dell'informazione ha lasciato il posto all'era del big data.

Questa evoluzione è riflessa nell'emergere, negli anni, di una serie di leggi che regolano il trattamento dei dati personali – leggi che, mentre scrivo, sono in discussione al Parlamento Europeo – e nella nascita di una nuova professione.

In Europa, la protezione dei dati personali è un diritto fondamentale, sancito all'articolo 8 della Convenzione Europea dei diritti dell'uomo. Firmata nel 1950, la Convenzione protegge dalla possibile "ingerenza di un'autorità pubblica nell'esercizio di tale diritto". A pochi anni dalla fine della guerra, con il ricordo delle dittature ben vivo nella mente dei relatori della Convenzione, il diritto alla privacy nasce con l'intenzione di proteggere i cittadini europei dall'intrusione dei Governi nelle loro vite.

Nel 1981, il Consiglio d'Europa apre alla firma la Convenzione sulla protezione delle persone con riferimento al trattamento automatizzato di dati a carattere personale. La Convenzione vieta il trattamento dei dati personali relativi all'origine razziale, alle opinioni politiche, alla salute, all'orientamento religioso e sessuale ed alle condanne penali in assenza di specifiche garanzie previste dal diritto interno degli Stati firmatari. La Convenzione introduce, inoltre, il diritto dei soggetti a conoscere le informazioni catalogate su di essi e ad esigere, se necessario, delle rettifiche.

Nel 1995, infine, l'Unione Europea vara la Direttiva relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

La Direttiva del 1995 è ancora in vigore, ma la Commissione Europea ha svelato, all'inizio di quest'anno, una proposta di riforma della legislazione europea sulla privacy, attualmente al vaglio del Parlamento Europeo.

Oltre ad una serie di leggi che regolano la protezione dei dati personali in Europa e nel Nord America, gli anni '90, quelli del boom del dot-com, hanno dato alla luce una nuova generazione di professionisti: "chief privacy officers" in Nord America, "data protection officers (DPOs)" in Europa o, più semplicemente, responsabili del trattamento dei dati personali.

Negli ultimi dodici anni, da quando IBM ha nominato il primo chief privacy officer, nel 2000, il ruolo di questi professionisti di livello dirigenziale – che si guadagnano da vivere fornendo alle compagnie per cui lavorano gli strumenti necessari per agire nel rispetto delle leggi che regolano la protezione dei dati personali - non ha fatto che rafforzarsi. Al punto che, nella sua proposta di riforma della legislazione europea sulla privacy, la Commissione Europea ha inserito l'obbligo per le aziende con più di 250 dipendenti di nominare un data protection officer.

Cosa aspettarsi nei prossimi dieci anni? In un mondo sempre più interconnesso, conoscere e saper interpretare le leggi nazionali, ed anche quelle europee, non è più sufficiente. Sempre più spesso, i professionisti della privacy devono rispondere a sfide di carattere internazionale. Aspettiamoci, dunque, di continuare a sentir parlare di privacy ancora a lungo.

Rita Di Antonio
Managing Director IAPP Europe, la divisione europea della International Association of Privacy Professionals (IAPP)

za tener conto dell'inesauribile filone dell'"infotainement nero". Su altro versante, la minaccia della "legge bavaglio", riguardante la proposta contenuta nel disegno di legge sulle intercettazioni, poi cancellata, che prevedeva l'obbligo di rettifica di ogni contenuto pubblicato da parte di qualsiasi sito internet sulla base di una semplice richiesta da parte di soggetti ritenutisi lesi, con sanzioni per i gestori del sito che si fossero rifiutati. Oppure, l'analogo tentativo contenuto originariamente nella legge comunitaria per cui qualunque soggetto interessato avrebbe visto riconosciuto il diritto di ottenere dal provider la rimozione su Internet di informazioni da lui considerate illecite o la disabilitazione all'accesso alle stesse. Infine, l'attacco al principio della segretezza delle fonti giornalistiche – lamentato dalla stampa – a seguito di sequestri probatori invasivi ordinati dalla magistratura per l'accertamento dei reati, in assenza del vaglio del bilanciamento dei valori. Questi sono tutti esempi emblematici della difficoltà intrinseca di una corretta sintonizzazione di quel "giusto equilibrio".

Apparenti conflitti

Il bisticcio, quindi, non è confinato tra "privacy" e "social", ma, in un certo senso, è registrato nel medesimo codice genetico del diritto alla tutela dei dati personali. Già nella sua genesi, infatti, questo diritto nasce dal compromesso tra esigenze di tutela e libera circolazione dei dati e tale equilibrio si riproduce in una molteplicità di situazioni, assumendo connotati diversi. Il caso delle intercettazioni – nella composizione del bilanciamento tra la necessità di ricercare le prove degli illeciti e la tutela della riservatezza dei cittadini – è di drammatica attualità. Ma di non minore importanza sono i casi delle esigenze di trasparenza della macchina amministrativa rispetto alla "privacy" del cittadino (con il recente fenomeno di web-tv nella p.a.), l'interconnessione di banche dati per l'ottimizzazione delle attività amministrative rispetto alla sindrome da "grande fratello", oppure l'interesse collettivo alla sanità pubblica (si vedano i progetti di sanità elettronica) verso il rispetto della dignità del paziente, il miglioramento dell'amministrazione della giustizia (v. il processo telematico) e la "privacy" dei litiganti, il diritto all'informazione e di cronaca ed il rischio di "sbattere il mostro in prima pagina" (anche alla luce del recente connubio tra carta stampata, televisioni locali e web). La lista potrebbe continuare a lungo, traendo esempi dalla cronaca quotidiana, come quando, dai tragici fatti terroristici del settembre 2001, abbiamo imparato che occorreva rinunciare a sostanziali fette del nostro privato, da immolare sull'altare del prevalente interesse della sicurezza pubblica.

Equilibrio e civiltà

Eppure, il livello di civiltà si misura proprio sulla capacità di determinare l'equilibrio tra valori, nonostante la sua tipica variabilità. La sovraesposizione personale, di natura mediatica o "social", non può essere interpretata come automatica rinuncia del valore del riserbo né, tanto meno, del diritto al corretto utilizzo delle proprie informazioni personali. Allo stesso modo come, usando una metafora, sarebbe illogico desumere la conseguente rinuncia alla propria sicurezza fisica dalla mera decisione di transitare in autostrada a velocità sostenuta. Chi sceglie l'autostrada intende accorciare i tempi di percorrenza muovendosi ad una velocità legittimamente superiore a qualsiasi altro contesto, ma senza che ciò interferisca in alcun modo col proprio diritto fondamentale alla salute ed alla vita. Allo stesso modo, essere "social" non significa, di per sé, fare a meno della propria "privacy". Anzi, proprio al fine di abbattere le barriere inibitorie al "social", occorre garantire efficace tutela alla "privacy".

Antonio Palmieri
Deputato e responsabile nazionale della comunicazione elettorale e Internet del Popolo delle Libertà

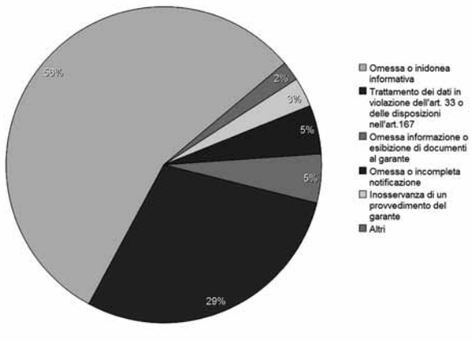
Una questione di educazione

Un processo di educazione efficace dev'essere trasversale e in questo caso dovrebbe poter coinvolgere il Garante, le scuole e i media stessi, dai giornali cartacei alla televisione, con lo scopo non di porre vincoli, ma condizioni in cui una persona possa muoversi con coscienza.

La privacy rappresenta, senza ombra di dubbio, uno dei temi più delicati tra quelli che possono assurgere ad oggetto di dibattito politico e sociale. Gli stimoli sono molteplici e provengono da ambiti diversi come, per esempio, l'avanzamento delle nuove tecnologie e dei new media ed eventi di attualità.
La normativa vigente è quella racchiusa nel Decreto Legislativo 30 giugno 2003, n. 196, intitolato "Codice in materia di protezione dei dati personali" e comunemente noto come "Testo Unico sulla privacy". Nonostante questo provvedimento legislativo abbia ormai quasi dieci anni, non è attualmente in corso un dibattito in Parlamento su un'eventuale modifica del testo. L'attenzione è posta, piuttosto, sull'implementazione della normativa vigente e sulla figura da essa confermata del Garante per la protezione dei dati personali.
L'aspetto più problematico, proprio perché sviluppatosi successivamente all'entrata in vigore del TU, è quello che riguarda il rapporto tra la protezione della privacy e l'utilizzo dei nuovi mezzi di comunicazione, internet ed i social network in particolare. L'assunto fondamentale posto alla base di quella che dovrebbe essere l'azione in questo ambito è la ricerca della consapevolezza nel cittadino. I media digitali non sono un semplice prolungamento del proprio spazio casalingo, ma un luogo di incontro esterno in cui tutto ciò che viene pubblicato è, a tutti gli effetti, esposto on-line. Gli utenti vi si approcciano ancora adesso con leggerezza, non valutando con la dovuta attenzione quali possano essere le conseguenze della pubblicazione di dati o fotografie e dimostrando, così, una certa imprudenza. L'esposizione al rischio di violazioni o abusi è, quindi, praticamente quotidiana.
Questa consapevolezza ancora assente deve costituire l'obiettivo finale di diverse tipologie di azioni. Un processo di educazione efficace dev'essere trasversale e in questo caso dovrebbe poter coinvolgere il Garante, le scuole e i media stessi, dai giornali cartacei alla televisione, con lo scopo non di porre vincoli, ma condizioni in cui una persona possa muoversi con coscienza. Come ogni luogo, anche il web ha bisogno di utenti che tengano un comportamento consono alla situazione.
A mio avviso, lo Stato, in questo processo, può assumere un ruolo successivamente e tutto l'ambiente politico può esercitare una funzione primariamente esortativa. Chi si occupa di politica, a tutti i livelli, può utilizzare la sua visibilità per porre il problema; può utilizzare i mezzi di comunicazione in tutte le forme possibili per vivacizzare il dibattito in modo che raggiunga sempre più persone; può stimolare il governo dei media affinché essi non trascurino l'aspetto educativo; può, infine, incentivare ed incoraggiare l'azione del Garante che dispone dei mezzi normativi per garantire una tutela effettiva ed efficace dei diritti dei cittadini in questo settore.
Inoltre, è proprio riguardo alla figura del Garante che è possibile compiere un ulteriore passo in avanti. Potrebbe essere interessante, infatti, implementare una funzione preventiva atta alla diffusione di questa forma di consapevolezza del ruolo e del posto di ciascuno all'interno del web. Ciò potrebbe condurre ad una riduzione del rischio di incorrere in violazioni ed abusi permettendo, di conseguenza, una più efficace tutela della privacy di ogni cittadino.

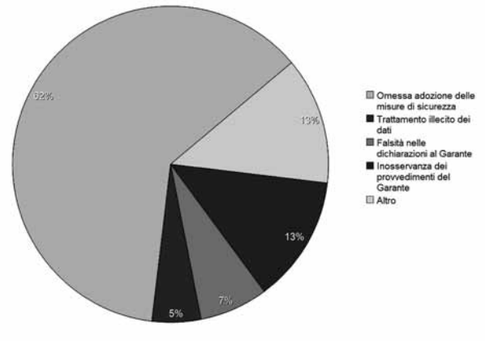
Dichiarazioni raccolte da Angela Caporale

La natura delle sanzioni



Fonte: www.schmidtconsulting.it

Privacy, violazioni penali



Fonte: www.schmidtconsulting.it

Anna Rossomando
Avvocato - Onorevole alla Camera dei Deputati
Commissione Giustizia - Giunta per le Autorizzazioni

Esigenze investigative

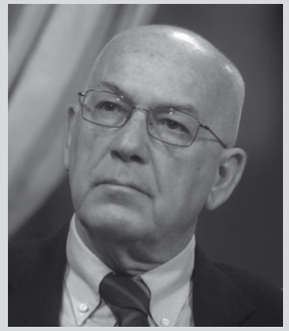
Nonostante alcuni importanti risultati ottenuti a seguito del lavoro svolto allora quale opposizione nelle Commissioni parlamentari ed in Aula nel testo che, di volta in volta, si "minaccia" di riesumare, permangono una serie di gravi criticità.

In tempi di gravi difficoltà economiche e sociali per il nostro Paese, intervenire sulla disciplina delle intercettazioni telefoniche non costituisce davvero una priorità. E non appare superfluo sottolineare, ancora una volta, quanto l'efficienza del servizio Giustizia incida sui costi del sistema Paese, sulle sue capacità di competere e, in definitiva, sullo sviluppo e la modernità dello stesso. Altri sono, pertanto, i provvedimenti urgenti in tema di Giustizia e tra questi non possiamo certo tacere sul sovraffollamento delle carceri, assurto a drammatica emergenza. Questo non significa che non si possa discutere in assoluto di intercettazioni, con una premessa, però, non superabile: il terreno del confronto non può essere rappresentato dal testo oggi giacente (non a caso) sul cosiddetto "binario morto". Tale provvedimento è giunto a conclusione di una dura battaglia parlamentare, la quale ha prodotto un testo che non presenta soluzioni coerenti con la discussione apertasi nelle passate legislature. Il punto era come garantire l'effettivo contemperamento delle esigenze investigative, e quindi il diritto dovere dello Stato di reprimere ed accertare i reati, con il più volte citato diritto alla riservatezza e, correlativamente, con il diritto dei cittadini ad essere informati su fatti rilevanti e di interesse pubblico. Questo costituiva e costituisce il tema al centro del confronto sull'attuale regime delle intercettazioni, ovvero sulla pubblicabilità del loro contenuto. Del tutto inadeguato è stato l'approccio che la passata maggioranza del Governo Berlusconi ha avuto con le diverse susseguenti proposte di modifica dell'attuale regime. In tutti i testi ed in tutte le versioni succedutesi a partire dal 2008, infatti, l'obiettivo perseguito, così come emergeva dai testi proposti, era una limitazione dello strumento investigativo, più che un reale sforzo per disciplinare la pubblicazione delle conversazioni cosiddette irrilevanti in quanto estranee all'oggetto dell'indagine.
Tutti gli interventi susseguitisi erano diretti a depotenziare lo strumento di indagine e di ricerca della prova più che ad affrontare davvero la questione della pubblicabilità di ciò che viene considerato irrilevante ed estraneo alle indagini e come evitare fughe di notizie.
Paradossalmente, questo avveniva mentre si approvavano roboanti "pacchetti sicurezza". Nonostante alcuni importanti risultati ottenuti a seguito del lavoro svolto allora quale opposizione nelle Commissioni parlamentari ed in Aula nel testo che, di volta in volta, si "minaccia" di riesumare, permangono una serie di gravi criticità.
Ne cito alcune tra le più rilevanti:
1) *La previsione della competenza del tribunale del distretto in composizione collegiale quale giudice che deve autorizzare le intercettazioni è assolutamente irragionevole ed avrà un impatto organizzativo disastroso sul sistema Giustizia.* Significa che, per ogni intercettazione telefonica, ogni utenza, ogni proroga, ogni captazione ambientale, ogni convalida di atto urgente adottato dal Pm, sarà necessario riunire un collegio di tre persone nella sede del distretto di Corte d'Appello. Se si considera che un solo giudice ha per legge il potere di disporre non solo custodie cautelari in carcere e altre limitazioni della libertà personale, ma anche di irrogare pene detentive, compreso l'ergastolo, nella sede del giudizio abbreviato, si comprende l'assurdità della proposta. Sul piano organizzativo, inoltre, si pone il problema della disponibilità di risorse umane (giacché saranno necessari più magistrati); le operazioni risulteranno maggiormente complicate, visto che la competenza ricadrà sul tribunale nella sede della Corte d'Appello, verosimilmente lontano dalla sede delle indagini; senza parlare della possibilità di incorrere in incompatibilità.
2) E' stata abrogato l'articolo 13 della "legge Falcone" (l. n. 203 del 1991). Questa abrogazione modifica la *possibilità di effettuare operazioni di intercettazione per reati gravi di criminalità organizzata*. Infatti, i requisiti meno severi (sufficienti anziché gravi) che questa legge richiede oggi per intercettare le reti del crimine organizzato saranno previsti domani solo per delitti commessi con finalità di terrorismo, delitti di associazione mafiosa e talune ipotesi di associazione per delinquere. *Resta fuori da questo elenco, rispetto alla "legge Falcone", il reato di costituzione di organizzazioni criminose stabili (articolo 416 cp) volte a perpetrare gravi reati comuni tra cui usura, bancarotta, truffa, aggravata e non, corruzione, concussione, peculato, abuso d'ufficio, sfruttamento della prostituzione e della manodopera agricola e, in genere, tutti i reati commessi dalla criminalità organizzata*.
Sarà più difficile per magistrati e forze dell'ordine perseguire questi reati. Proprio grazie a questa legge, anche di recente, nelle inchieste sulle cosiddette "cricche degli appalti", sono stati ottenuti risultati investigativi importanti.
3) Le intercettazioni ambientali. Il testo – pur lievemente migliorato – resta confuso e gravemente limitativo dei poteri investigativi. Si prevede, infatti, che per disporle occorre che nel luogo sottoposto a controllo debba essere in corso l'attività criminosa. S*i richiede, in sostanza, la flagranza del reato, la quale da sola consentirebbe l'arresto.* È pur vero che è stata introdotta la possibilità di svolgere le intercettazioni ambientali anche in carenza di flagranza, ma solo se dalle indagini già esperite emerga che la captazione potrebbe consentire l'acquisizione di elementi fondamentali per l'accertamento del reato. Tale possibilità vale, però, solo per gli ambienti diversi dalla privata dimora, per la quale resta valida la regola della flagranza. Si tratta, nel complesso, di un ostacolo irragionevole e talora determinante sul risultato delle indagini. Conseguentemente, l'intercettazione ambientale non potrà costituire il primo mezzo di ricerca della prova, ma dovrà scalare ad elemento di conferma.
4) I *tabulati telefonici vengono irragionevolmente accomunati alle intercettazioni.* Si tratta di un grave errore logico e giuridico. *Il tabulato è solo l'elenco dei contatti telefonici stabiliti tra due utenze.* Rivela una frequenza di contatti, ma non il contenuto delle conversazioni. È dunque meno di un'agenda, spesso usato dagli inquirenti per svolgere le prime verifiche e scartare le piste più improbabili.
Sottoporre questo strumento agli stessi requisiti gravosi delle intercettazioni significa lasciare brancolare nel buio gli investigatori.
Con il testo approvato nell'ottobre del 2011, risulterà possibile utilizzarli quando lo stato delle indagini è già in fase avviata. *Ad esempio, per il reato di truffa, non sarà possibile estrarre il tabulato dell'indagato per dimostrare il legame con la vittima.* Dal punto di vista giuridico, poi, sottoporre i tabulati allo stesso regime delle intercettazioni potrebbe addirittura far venire la tentazione di mutuarne il medesimo valore probatorio. Ciò sarebbe assurdo, in quanto il tabulato restituisce meno informazioni dell'intercettazione.
5) Relativamente agli *strumenti investigativi diversi dalle intercettazioni*, in particolare ispezioni, perquisizioni e sequestri – i tipici mezzi a sorpresa di ricerca della prova – è stato, infine, introdotto un ulteriore, incredibile limite alle indagini.
Viene, infatti, previsto che, *per l'atto di ispezione o perquisizione o sequestro, disposto in seguito a notizie apprese da intercettazioni, che possono essere anche in corso, il pm deve provvedere al deposito delle intercettazioni rilevanti nella cancelleria del giudice collegiale nella sede del distretto, con contestuale trascrizione e informazione alla parte*.
In pratica, *se da un'intercettazione emerge che la persona sequestrata è tenuta presso un certo luogo, il pm dovrà prima depositare le intercettazioni e poi andare a svolgere la perquisizione per liberare il sequestrato, mettendo in guardia i rapitori*. È ovvio che una simile procedura può adattarsi alle inchieste semplici, nelle quali il decreto di perquisizione o sequestro è emesso ed eseguito alla fine dell'indagine; ma appare veramente contro ogni ragionevolezza e mette a serio rischio l'efficacia dell'investigazione nelle indagini complesse, nelle quali la perquisizione o l'ispezione vengono svolte in costanza di intercettazioni telefoniche che proseguono, e devono proseguire, nella segretezza, a meno di non comprometterne il risultato.
In sostanza, le proposte contenute nel testo licenziato dalla passata maggioranza porterebbero ad una limitazione delle indagini, burocratizzando inutilmente le autorizzazioni ed aumentando in concreto la fuga di notizie.
Quindi, mentre rimane insoddisfacente la risposta all'esigenza di maggiore tutela della riservatezza laddove vi siano contenuti penalmente irrilevanti ed estranei alle indagini, si pongono seriamente a rischio importanti strumenti investigativi e la trasparenza ed il controllo democratico garantiti dalla funzione dell'informazione. Sotto quest'ultimo aspetto, infatti, l'approccio "punitivo" nei confronti della stampa non può essere accettato, nonostante sia stato introdotto qualche temperamento rispetto al testo iniziale. Personalmente, ritengo positivo l'accoglimento di una delle nostre proposte, ovvero l'individuazione della cosiddetta udienza filtro come spartiacque per la pubblicabilità del contenuto delle intercettazioni ritenute rilevanti dal giudice in tale udienza. Così come ritengo che si potrebbe ragionare su una maggiore vincolabilità e specificità di motivazione del provvedimento autorizzativo dell'intercettazione da parte del giudice. Per ottenere ciò e riaprire la discussione deve cambiare completamente l'impostazione del provvedimento, che non può essere di tipo "punitivo" nei confronti delle indagini o dell'informazione e, tanto meno, essere di volta in volta brandito sul tavolo di una "trattativa" politica sul tema del controllo di legalità; trattativa che non può in alcun modo essere accettata e non sarà mai aperta. Il controllo di legalità non è "trattabile". Si può discutere, quindi, di intercettazioni? Certo, ma occorre riportare il dibattito sulla rotta giusta, partendo da un nuovo testo; questo proprio per porre al centro l'esigenza di tutela della riservatezza, dei diritti personali del cittadino che godono di copertura costituzionale e, per ultimo, ma non meno importante, una più puntuale disciplina sulla fuga di notizie.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI — *Servizio relazioni con i mezzi di informazione*

La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare

Obbligo del consenso per video e foto sui social network. Scrutini e voti pubblici. Sì alle foto di recite e gite scolastiche. No alla pubblicazione on line dei nomi e cognomi degli studenti non in regola coi pagamenti della retta. Su cellulari e tablet in classe l'ultima parola spetta alle scuole.



Antonello Soro

Mancano pochi giorni all'apertura delle scuole e il Garante per la t dei dati personali ritiene utile fornire a professori, genitori e studenti, sulla base dei provvedimenti adottati e dei pareri resi, alcune indicazioni generali in materia di tutela della privacy.

Temi in classe
Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale. Sta invece nella sensibilità dell'insegnante, nel momento in cui gli elaborati vengono letti in classe, trovare l'equilibrio tra esigenze didattiche e tutela della riservatezza, specialmente se si tratta di argomenti delicati.

Cellulari e tablet
L'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati.
Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.

Recite e gite scolastiche
Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

Retta e servizio mensa
È illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa. Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio mensa in quanto appartenenti a famiglie con reddito minimo o a fasce deboli. Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale. A salvaguardia della trasparenza sulla gestione delle risorse scolastiche, restano ferme le regole sull'accesso ai documenti amministrativi da parte delle persone interessate.

Telecamere
Si possono in generale installare telecamere all'interno degli istituti scolastici, ma devono funzionare solo negli orari di chiusura degli istituti e la loro presenza deve essere segnalata con cartelli. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. Le immagini registrare devono essere cancellate in generale dopo 24 ore.

Inserimento professionale
Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale le scuole, su richiesta degli studenti, possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali dei ragazzi.

Questionari per attività di ricerca
L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori sono stati prima informati sugli scopi delle ricerca, le modalità del trattamento e le misure di sicurezza adottate. Gli studenti e i genitori devono essere lasciati liberi di non aderire all'iniziativa.

Iscrizione e registri on line, pagella elettronica
In attesa di poter esprimere il previsto parere sui provvedimenti attuativi del Ministero dell'Istruzione riguardo all'iscrizione on line degli studenti, all'adozione dei registri on line e alla consultazione della pagella via web, il Garante auspica l'adozione di adeguate misure di sicurezza a protezione dei dati.

Voti, scrutini, esami di Stato
I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'Istruzione. È necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l'istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

Trattamento dei dati personali
Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. Spesso le scuole utilizzano nella loro attività quotidiana dati delicati - come quelli riguardanti le origini etniche, le convinzioni religiose, lo stato di salute - anche per fornire semplici servizi, come ad esempio la mensa. È bene ricordare che nel trattare queste categorie di informazioni gli istituti scolastici devono porre estrema cautela, in conformità al regolamento sui dati sensibili adottato dal Ministero dell'Istruzione. Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

Roma, 6 settembre 2012

Roberta Bruzzone
Psicologa Forense e Criminologa, Evidence Collector Specialist
Presidente Accademia Internazionale delle Scienze Forensi (AISF) – www.robertabruzzone.com

Siamo davvero tutti spiati?

Nell'epoca in cui la tecnologia è parte integrante delle nostre vite, il prezzo da pagare è molto alto: è dalla tecnologia che arrivano gli strumenti utilizzati per monitorare ogni nostro spostamento, ogni nostro gusto o ogni nostro pensiero.

Siamo davvero tutti spiati? Stando agli ultimi dati noti, la risposta è SI. Spyfiles, un recente studio di Wikileaks svolto in collaborazione con il Bureau of Investigative Journalism e Privacy International, ha reso noti alcuni aspetti significativi di questo fenomeno. Sono state individuate ben 130 aziende in 25 Stati diversi: una vera e propria industria internazionale in grado di fornire a chi paga i mezzi per sorvegliare le popolazioni. Si parla di un giro d'affari di 5 miliardi di dollari. Un semplice telefono cellulare o un computer, ad esempio, sono in grado di fornire miriadi di informazioni all'insaputa della persona che li utilizza. In che modo? Sono stati creati dei virus Trojans i quali, oltre a localizzare il luogo in cui l'apparecchio viene utilizzato, diventano una specie di microspia in grado di registrare le immagini e le conversazioni che avvengono nel luogo in cui l'ignaro utente si trova. Non solo. Questi virus sono in grado, a loro volta, di inviare mail, sms e files dagli apparecchi infetti. Si tratta, ovviamente, di azioni illegali. Ma l'estrema difficoltà nello scoprirle ne garantisce l'impunità. Per assurdo, esistono anche fiere ed eventi dedicati allo sviluppo di questi sistemi. La gente comune e gli organi di stampa non possono, però, parteciparvi. Anche in Italia è stata individuata una di queste società di sorveglianza: si chiama Hacking Team, ha sede a Milano ed è stata fondata nel 2003 da David Vincenzetti e Valeriano Bedeschi. Nel sito internet dell'azienda è possibile visionare alcuni video che spiegano il funzionamento dei Remote Control System, sistemi, per l'appunto, in grado di spiare un individuo che si trova dall'altra parte del mondo. Si tratta di strumenti efficacissimi per combattere il crimine. Ma se finiscono nelle mani sbagliate, possono provocare danni catastrofici.

SPIATI DALLA TECNOLOGIA

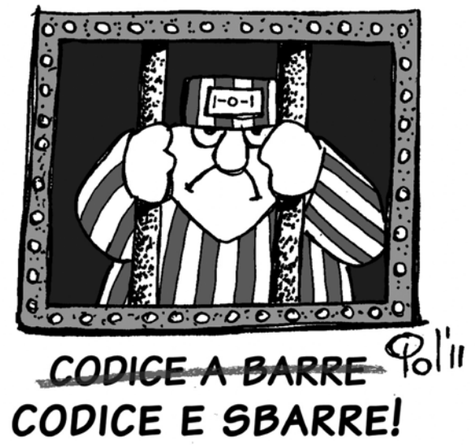
Nell'epoca in cui la tecnologia è parte integrante delle nostre vite, il prezzo da pagare è molto alto: è proprio dalla tecnologia, infatti, che arrivano gli strumenti utilizzati per monitorare ogni nostro spostamento, ogni nostro gusto o ogni nostro pensiero. Attualmente, sono 3 i principali progetti utilizzati dagli Stati Uniti a questo scopo. Il primo è il TIA, il Terrorism Information Awareness, uno strumento messo a punto dopo l'11 settembre. Il TIA permette di interconnettere i dati sensibili provenienti da diverse fonti, come passaporti, carte di credito, biglietti aerei ed acquisti di prodotti, al fine di localizzare possibili terroristi e cercare di anticipare le loro mosse. Il 12 agosto scorso, il Senato Americano ha negato la concessione di ulteriori finanziamenti a questo progetto.
Un altro sistema, entrato anch'esso in funzione dopo l'attentato alle Torri Gemelle, è il Carnivore, detto anche Digital Collection System. Si tratta di un dispositivo hardware e software gestito direttamente dall'FBI, in grado di filtrare i pacchetti di dati che transitano tra l'utente ed il provider e di ricostruire i messaggi scambiati: mail, pagine internet visitate, chat, telefonate, invio e ricezione di file.
Infine, c'è il CAPPS II, il Computer Assisted Passenger Prescreening System II, che si occupa del controllo dei passeggeri di aeromobili. Tutte le persone che salgono a bordo vengono schedate; in base alle informazioni a disposizione, vengono assegnati loro 3 colori: rosso, se si tratta di individui pericolosi, giallo, nel caso di sospetti e verde per gli inoffensivi.
Come si evince, tutti questi strumenti di controllo vengono adoperati dai governi con l'obiettivo della sicurezza del cittadino, il più nobile degli intenti. Ma cosa succederebbe se, ad esempio, salisse al potere un governo dittatoriale? Che uso potrebbe fare di tutti questi strumenti di indiscusso controllo sociale?

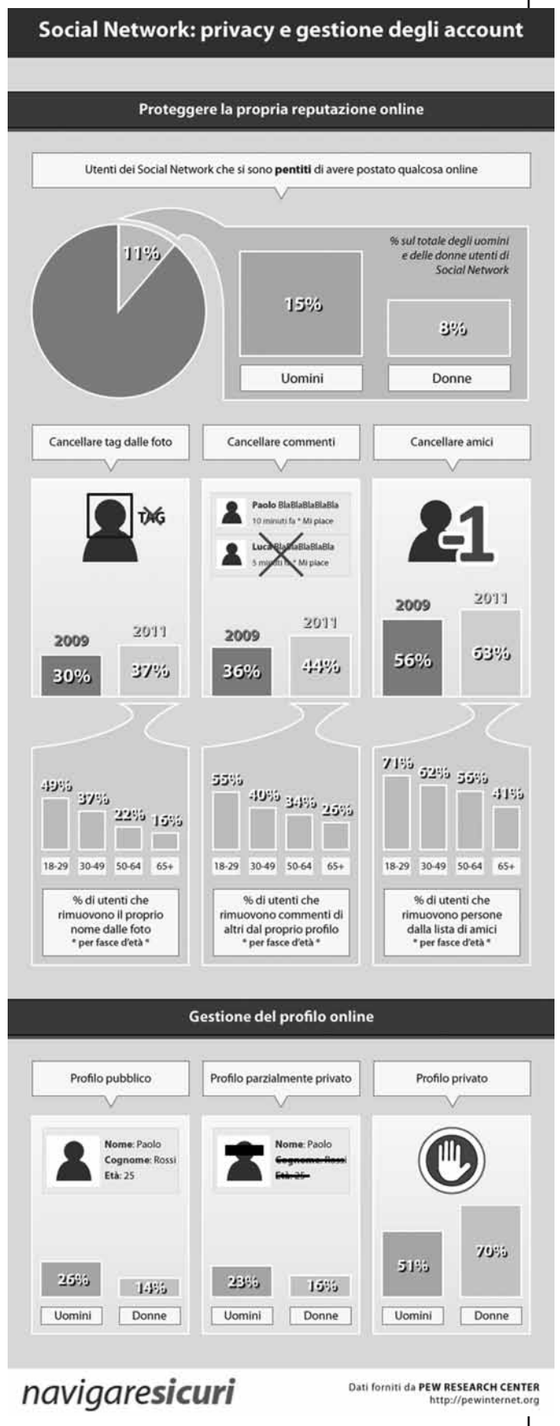
SPIATI E SPIONI

Non più solo 007 o spie stile "Mata Hari": nell'epoca in cui la tecnologia compie passi da gigante e diviene accessibile ad un numero sempre maggiore di persone, anche lo spionaggio diventa un fenomeno "fai da te". Con una semplice ricerca, è facile imbattersi in svariati siti internet che vendono prodotti in grado di favorire il controllo: microspie e telecamere nascoste negli oggetti più impensabili come penne, occhiali, cravatte, zainetti, portachiavi, orologi. Ancora: gps, microregistratori, cellulari criptati... Davvero una miriade di oggetti che va ad aggiungersi ai più classici strumenti di investigazione, per un giro d'affari, evidentemente, proficuo. I costi di questi prodotti variano di molto, ma mediamente sono abbastanza elevati: una penna con videocamera incorporata oscilla da un minimo di 50 euro ad un massimo di 1.000. Accanto agli strumenti "per spiare", poi, ci sono anche tutti quelli per il controspionaggio, ossia per scoprire se qualcuno ci sta spiando.
Ma chi sono i potenziali acquirenti? Sicuramente le forze dell'ordine, gli investigatori privati e le aziende. Il fenomeno più dilagante è, però, quello dei privati cittadini: partner che sospettano un'infedeltà o genitori che desiderano controllare i figli. Quando le più consuete tecniche di controllo, come leggere di nascosto gli sms o pedinare il presunto traditore, non bastano più, ecco la tentazione di ricorrere a metodi più sofisticati. Esistono, addirittura, dei "kit dell'infedeltà": presentano un costo abbordabile e servono per identificare eventuali tracce di sperma lasciate negli abiti o nella biancheria intima del partner fedifrago.
Le cronache ci stanno ormai abituando a questo nuovo fenomeno. Nel 2007, l'inchiesta "Spy phones" ha coinvolto oltre 420 persone, le quali hanno dovuto rispondere a vario titolo di creazione, installazione, vendita ed utilizzo del software "Polifemo": inserito in un cellulare, questo permetteva di monitorarne chiamate ed sms e fungeva anche da cimice ambientale. Nell'ambito dell'inchiesta, è emersa la storia di due coppie residenti in un condominio di Napoli: i coniugi delle due coppie avevano intrecciato tra loro delle relazioni all'insaputa dei rispettivi partner. Tutti e quattro erano però dotati di telefoni spia, così la tresca incrociata è stata scoperta. I quattro si sono quindi trovati nella duplice veste di indagati e parti offese.
Teniamo ben presente, infatti, che, se gli strumenti di spionaggio di per sé non hanno nulla di illegale, chi li utilizza per propri fini personali rischia, invece, di essere denunciato: violazione della privacy, stalking, interferenza illecita della vita privata. Le intercettazioni telefoniche, ad esempio, sono vietate per legge non solo tra privati, ma anche tra coniugi. Le sole intercettazioni consentite sono quelle stabilite dall'autorità giudiziaria.
I "detective improvvisati" devono quindi stare attenti perché rischiano di pagare a caro prezzo il loro vizietto. Meglio, forse, provare a fidarsi un po' di più di chi ci sta accanto o, nei casi più gravi, affidarsi a persone esperte e qualificate.

COME PROTEGGERSI DAGLI SPIONI

Siamo tutti potenziali concorrenti di un Grande Fratello globale. Tanto più uno utilizza cellulare, computer, fa acquisti on-line e naviga su internet, tanto più rischia di essere monitorato in ogni sua attività. Come difendersi da tutto ciò? Certo, un buon metodo sarebbe quello di compiere un balzo indietro di vent'anni, rinunciare a tutte le tecnologie e tornare, ad esempio, a scrivere le lettere a mano... In questo senso, forse, alcuni dei nostri nonni sono le persone meno a rischio di essere spiate. Ma, al giorno d'oggi, rinunciare agli agi della tecnologia è tutt'altro che semplice e rischia di crearci handicap sul piano personale e professionale. Meglio, allora, conoscere il problema, adottare dei comportamenti corretti e, nei casi più sospetti, agire di conseguenza. Spesso, gli stessi siti internet che promuovono i sistemi di spionaggio forniscono anche i sistemi per difendersi: rivelatori di microspie e di telecamere, sistemi di bonifica ambientale ed apparecchi criptati in certe situazioni possono rivelarsi di grande aiuto. L'importante è non farsi prendere dal panico o dall'ossessione di essere spiati e ricorrere a queste misure solo se effettivamente necessario.





Social News 06_2012

Paolo Di Marzio
Magistrato Tribunale di Napoli

Interessi superiori alla riservatezza

La tutela della privacy diventa un problema quando questa confligge con altri interessi costituzionalmente rilevanti. Gli organi di informazione devono svolgere il loro compito di informare il pubblico, ma non sembra che, a tal fine, possano utilizzare fonti rivelatesi inidonee a perseguire il diverso fine che ha giustificato l'acquisizione dei dati personali.

Il diritto alla privacy è, secondo la definizione più diffusa, "il diritto di essere lasciato in pace" (*the right to be let alone*, L. Brandeis).
Facile riscontrare che, oggi, questo "diritto" è a rischio di essere pregiudicato più che in ogni altra epoca. Tutti siamo infastiditi dalle decine di telefonate di piazzisti da noi ricevute e dal riempimento delle nostre cassette postali con materiale pubblicitario non richiesto.
Ma la definizione citata pecca, forse, per genericità. Probabilmente, è possibile circoscrivere la nozione ed affermare che la tutela della privacy è il diritto alla riservatezza dei dati personali, con particolare riferimento ai c.d. dati sensibili.
Il problema, sempre esistito, sta divenendo sempre più grave a seguito della diffusione degli strumenti di comunicazione di massa in forma elettronica. È oggi possibile far conoscere indiscrezioni ad un numero anche molto elevato di utenti della rete in tempo reale. Non solo. La diffusione della possibilità di concludere transazioni commerciali mediante internet sta moltiplicando i problemi di tutela dei dati di ogni persona, perché riuscire ad appropriarsi di questi dati, commettendo un c.d. furto d'identità, permette ai criminali informatici di concludere, in nome del derubato, quasi ogni tipo di contratto, e la vittima non ha sempre un compito semplice per dimostrare di essere estranea alla vicenda.
Le istituzioni, anche in Italia, cercano di fare la loro parte. Nel 2003 è stato promulgato il D.Lgs. n. 196, che detta un'articolata normativa a tutela della privacy, sostituendo, dopo solo sette anni, la precedente legge sulla riservatezza. Nel nostro Paese opera anche il Garante per la protezione dei dati personali, ed è stato costituito un nucleo speciale della Guardia di Finanza per la tutela della privacy. Si tratta di iniziative condivisibili e lodevoli. Ciononostante, la tutela della riservatezza oggi garantita non appare rassicurante. Questo dipende anche da alcune opinioni consolidate le quali, forse, meriterebbero qualche ripensamento.
Sembra possa considerarsi un dato acquisito che esista un interesse pubblico alla conoscenza della realtà. Ad esempio, è espressione propria dei regimi autoritari (impegnarsi a) controllare l'informazione, specie per ostacolare la conoscenza del dissenso e pure della condotta della classe dominante. Pare corretto, allora, che le informazioni sulla vita dei protagonisti della scena pubblica debbano poter essere diffuse, anche limitando il diritto alla riservatezza delle persone coinvolte. In altre realtà, penso agli Stati Uniti, ad esempio, la condotta privata riprovevole di un uomo politico nuoce in misura determinante alla sua carriera. Tanto, peraltro, non impedisce che alcuni esponenti rimangano coinvolti in scandali di vario genere.
Da noi, in Italia, siamo evidentemente più permissivi, ed i comportamenti sconvenienti che coinvolgono uomini politici di tutte le appartenenze sono socialmente sanzionati in misura assai più lieve. Tuttavia, mi sembra giusto che il cittadino, nel momento in cui si trova ad esprimere un voto, debba avere la possibilità di eleggere una persona moralmente non censurabile, anche se questo non è sempre possibile con la legge elettorale vigente. Se ne sono resi conto subito anche coloro che l'hanno proposta e votata.
Quello che sembra già dubbio, però, è che, per il solo fatto di essere un personaggio pubblico, si debba rimanere esposti alla diffusione di qualsiasi informazione sulla propria vita privata, anche mediante la pubblicazione di immagini. Anni fa, perse il giudizio una nota attrice che contestava la pubblicazione non autorizzata di sue fotografie in cui appariva svestita. Tenuto conto che si trattava di foto relative ad un film in cui tutti avevano potuto vederla senza veli, la decisione, allo stato della legislazione e dell'orientamento giurisprudenziale vigente, poteva apparire corretta. Il corpo è un elemento essenziale per chi recita e, se si tratta di un'attrice famosa, può ammettersi che esista un interesse pubblico a conoscerlo. Mi sembra, però, che questo discorso non valga nella stessa misura quando il personaggio è sì pubblico, ma non ha nulla a che fare con la recitazione. Anche settimanali ad ampia diffusione pubblicarono, anni fa, le fotografie in cui l'Avvocato di Torino appariva senza nulla indosso e senza, naturalmente, che avesse autorizzato la pubblicazione delle sue immagini. Non si trattava di un attore, ma di un imprenditore. Quale interesse pubblico esisteva a conoscerne la nudità? Siamo in presenza di un conflitto tra diritti, ed occorre operare un bilanciamento, in questo caso tra il diritto alla riservatezza ed il diritto di cronaca.
A maggior ragione, poi, sembra debba assicurasi la miglior tutela della riservatezza di chi un personaggio pubblico non è, e questo discorso coinvolge una pluralità di tematiche.
La Cassazione, sez. III, sent. 30.01.2009, n. 2468, ha condannato una struttura sanitaria per la diffusione dei dati relativi all'accertata infezione da HIV di cui era risultato affetto un suo paziente dal quale non era stato acquisito il consenso all'effettuazione delle indagini. La struttura sanitaria ed il medico che le aveva disposte si sono difesi sostenendo che le analisi erano state svolte nell'interesse del paziente, ma la Suprema Corte ha ritenuto che il consenso dovesse comunque essere acquisito. La Cassazione ha anche precisato che l'effettuazione di analisi senza consenso può ritenersi lecita quando occorra tutelare interessi superiori alla riservatezza stessa, come la salute degli altri pazienti e del personale medico e paramedico. Anche in simili casi occorre, quindi, operare un bilanciamento tra gli interessi in gioco. Peraltro, quello che è stato giudicato comunque colpevole dalla Suprema Corte è che un dato sicuramente sensibile non sia stato custodito con adeguata attenzione presso la struttura sanitaria, in modo da evitarne la diffusione.
Merita, in proposito, di essere specificato che, ai sensi della legislazione sulla privacy (D.Lgs. n. 196/2003, art. 4), sono considerati dati personali sensibili, e pertanto oggetto della massima tutela, quelli idonei a rivelare: l'origine razziale ed etnica; le convinzioni religiose, filosofiche o di altro genere; le opinioni politiche; l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale; lo stato di salute e la vita sessuale. Altri dati di indubbio rilievo, come il reddito percepito, non sono inclusi nell'elenco e ricevono, pertanto, una tutela ridotta. Questa scelta ha suscitato perplessità. Non c'è dubbio che i dati sul reddito possano e debbano essere accertati dagli organi competenti ai fini dell'imposizione fiscale. Tali organi, in conseguenza, avranno la disponibilità dei dati. Più dubbio è che questi dati non ricevano la massima tutela avverso la loro diffusione, specie quando riguardino singole persone e non intere categorie.
Peraltro, il settore in cui il conflitto tra l'interesse alla conoscenza del dato e la tutela della riservatezza risulta più evidente è forse proprio il mondo giuridico. Ne è espressione la polemica in atto in materia di intercettazioni. Sembra corretto partire dalla premessa che l'attività giudiziaria, per sua natura, sia quando risulti promossa dalle parti private come avviene di regola per la giustizia civile, sia quando trovi impulso nell'iniziativa degli organi dello Stato a tutela della collettività, come avviene di regola nel settore penale, comporta l'acquisizione di dati riservati. Negli ultimi anni, in riferimento al più delicato settore penale, la giustizia in Italia ha potuto contrastare più efficacemente la diffusione della criminalità organizzata, un triste primato del nostro Paese, grazie all'apporto assicurato dai collaboratori di giustizia. Oggi, pure gran parte dei processi di questo tipo utilizza ampiamente lo strumento delle intercettazioni, telefoniche ed ambientali. Non credo se ne possa fare a meno, ne dipende la sicurezza di noi tutti e, comunque, la possibilità di assicurare la migliore tutela della legalità. Il problema sembra essere questo: o l'intercettazione è utilizzata nel processo cui è finalizzata, e quando diviene pubblica secondo la legge potrà essere anche diffusa dagli organi di informazione; oppure, se pubblicata, si risolve in un'intromissione nella vita privata delle persone che pare ingiustificata. Sembra possa dubitarsi che le intercettazioni non utilizzabili in un giudizio debbano essere regolamentate nella loro diffusione, si tratta invero di atti lesivi della privacy e non pare priva di fondamento l'opinione che, semplicemente, non debbano essere pubblicate. Gli organi di informazione devono svolgere il loro compito di informare il pubblico, ma non sembra che, a tal fine, possano utilizzare fonti rivelatesi inidonee a perseguire il diverso fine che ha giustificato l'acquisizione dei dati personali.
La tutela della sicurezza suggerisce anche altre riflessioni in materia di protezione dei dati personali. In un processo celebrato con rito direttissimo, pochi mesi fa, ho avuto la sorpresa di costatare che la prova regina della responsabilità del malvivente per aver commesso una grave rapina dipendeva dal fatto di essere rimasto immortalato mentre fuggiva "da una delle telecamere poste lungo le vie della città", come scriveva l'informativa della Polizia Giudiziaria. Pur vivendoci, non mi ero reso conto che la città di Napoli disponesse di un efficace sistema di videosorveglianza. Ora, una registrazione di immagini a ciclo continuo può probabilmente giustificarsi a tutela della sicurezza dei cittadini, ma qual è la sorte delle riprese? Quando vengono distrutte? È possibile che, se sono sorpreso dalle telecamere, ad esempio mentre conduco la mia autovettura ed ho ha bordo tre studentesse, possa derivarmene nocumento?
Un problema complesso, quello della tutela della privacy, quando questa confligga con altri interessi costituzionalmente rilevanti. Impegnerà anche le generazioni future perché le normative in materia, non solo primarie, avranno bisogno di continui aggiornamenti, anche in conseguenza degli sviluppi delle tecnologie, che un giorno consentiranno di monitorare gli spostamenti e, semmai, anche i dialoghi di ciascuno di noi, servendosi, che so, di un satellite. Un problema su cui la società civile deve interrogarsi e ricercare soluzioni equilibrate, e la politica deve essere in grado, a seguito di un confronto leale, di recepirle.

Valentina Frediani
Avvocato, fondatore del sito www.consulentelegaleinformatico.it

Le nuove leggi

Il Codice della Privacy: dalle semplificazioni del legislatore italiano alle valorizzazioni del Regolamento Europeo. Cos'è cambiato e cosa sta cambiando per le aziende italiane.

Privacy. Una parola ormai utilizzata nella quotidianità, spesso violata, altre volte sottovalutata, certamente non approfondita in ambito aziendale, dove assume sovente un ruolo di "ulteriore gabella" da accettare. Ma è davvero e solo questo ciò che ruota attorno ad una normativa posta a tutela della riservatezza ed in vigore, in Italia, ormai dal 1996?

In realtà, dal 1996 la normativa sulla privacy ha subito modifiche non solo normative. Si è assistito ad un succedersi diverso sotto il profilo psicologico, variabile negli anni. Quando, nel 2004, è uscito il nuovo Codice della Privacy (Decreto Legislativo 196/2003) le aziende hanno mal sopportato l'obbligo di adottare le misure minime di sicurezza a tutela dei dati personali gestiti dai propri sistemi informatici. Oggi, invece, l'adeguamento normativo è spesso utilizzato dalla Direzione e dal Responsabile dei sistemi ICT come "perno" per razionalizzare l'accesso ai dati e l'utilizzo della strumentazione informatica.

Negli ultimi mesi sono state molte le modifiche normative subite dal testo originario del 2003. Ad aprile è stato abolito l'obbligo di redazione del documento programmatico di sicurezza e, non di meno, il concetto di interessato (ovvero soggetto i cui dati sono tutelati dal Codice) è stato riformulato, non andando più a comprendere anche persone giuridiche, associazioni ed enti, ma solo ed esclusivamente le persone fisiche. Due modifiche "forti" rispetto a quanto voluto dal legislatore originariamente e protetto dall'Autorità Garante negli anni.

L'abolizione del DPS è stata oggetto di critiche, condivisibili considerando che era l'unico documento riassuntivo dello status di applicazione della normativa alla struttura di riferimento. Tanto che, ad oggi, benché il DPS sia venuto meno formalmente, moltissime aziende non intendono assolutamente abbandonarlo. In caso di controllo dell'Autorità Garante, della Guardia di Finanza o della Polizia Postale, poter esibire un documento condiviso dai vari responsabili e dai vertici aziendali dal quale emerga in modo sintetico e diretto com'è stato recepito il dictat normativo in azienda o nell'ente ne fa indubbiamente uno strumento non solo di tutela verso l'esterno, ma anche di tutela dei singoli responsabili internamente alla struttura: una volta condiviso, non è possibile "scaricare" responsabilità in merito alle scelte operate. Diviene, quindi, documento di trasparenza per tutti i ruoli coinvolti nell'applicazione della legge.

Ben diverse le valutazioni sull'opportunità di modificare il concetto di dato personale. Originariamente, con dato personale si indicava qualsiasi dato che facesse riferimento, in modo diretto o indiretto, ad una persona fisica o giuridica, ad un'associazione o ad un ente. Ciò tutelava i dati anche delle persone giuridiche, in particolare in merito agli aspetti di natura promozionale. D'altra parte, però, diveniva proibitivo in ambito commerciale, dovendo raccogliere il consenso preventivo anche per contattare una persona giuridica alla quale proporre beni o servizi. Così, aderendo formalmente al concetto di interessato come concepito a livello europeo, il nostro legislatore ha prodotto un ridimensionamento del dato personale, restringendolo alla sola persona fisica. Ciò rappresenta una scelta razionale e certamente condivisibile, se non fosse che ha portato con sé un decadimento degli obblighi di protezione dei dati in formato elettronico. Difatti, l'obbligo di adozione delle misure minime ed idonee di sicurezza, rappresentato nel Codice privacy e nell'Allegato B del medesimo, è attuabile solo nei confronti dei dati soggetti a tutela della normativa stessa. Fino alla riformulazione del concetto di dato personale e di interessato, adottare credenziali di autenticazione, proteggere le reti, disporre di antivirus e procedure di back-up erano tutte misure obbligatorie su dati facenti riferimento a persone sia fisiche, sia giuridiche. Queste ultime, a seguito della riformulazione, non saranno più soggette ad obblighi di tutela in materia di riservatezza.

Questo aspetto fa regredire con un battito di ciglia gli sforzi prodotti negli ultimi dieci anni per far progredire le aziende ed insegnare loro a tutelare il proprio patrimonio aziendale passando da un obbligo normativo.

La privacy aveva finalmente assunto un ruolo nelle aziende fungendo da parametro principale per verificare lo stato di sicurezza dei dati ed era richiamata nelle verifiche ISO 9001, dalla 231 in materia di prevenzione dei reati connessi ai dati personali e nei rapporti contrattuali con trasmissione dei dati funzionalmente agli accordi intrapresi.

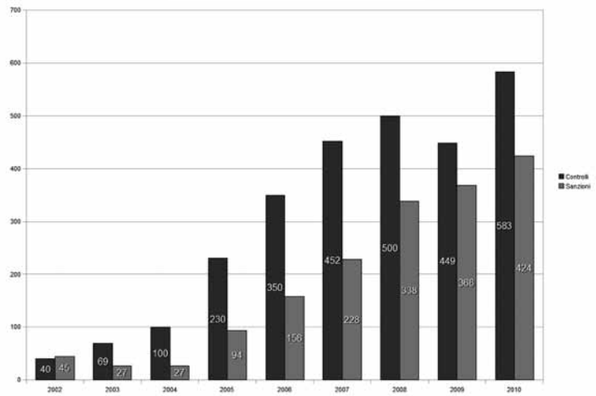
Cambierà davvero questo scenario? La prospettiva non è così definitiva. A fronte, infatti, di un taglio ingente effettuato dal legislatore italiano, abbiamo alle porte un 2013 non poco impegnativo, mittente Europa: è attualmente al vaglio il Regolamento europeo in materia di privacy e, all'orizzonte, le incombenze per le aziende non sono così snelle! Al contrario.

Occorre premettere che il Regolamento si applicherà – a differenza delle Direttive – immediatamente, in ogni Paese, all'atto dell'emanazione. Secondariamente, andrà a disciplinare specificatamente grandi realtà aziendali (a prescindere dalla titolarità di dati di persone fisiche o giuridiche) ed attività che abbiano ad oggetto comunque masse di dati facenti riferimento alle persone fisiche. Gli obblighi saranno più sostanziali che formali e, a fronte di scarse incombenze documentali, il Regolamento si concentrerà sull'effettiva protezione dei dati aziendali sotto il profilo informatico, logico e procedurale. La questione, insomma, prenderà ben altra piega. Molto più organizzativa, passando da un concetto di mera applicazione di una norma ad una modalità di concepimento di tutela del dato aziendale in quanto bene aziendale. Tanto che dovrà essere adottata la figura del cosiddetto Privacy Officier, una figura dedicata, con capacità e conoscenze più ampie del semplice Responsabile. Una figura che dovrà coniugare conoscenze giuridiche e tecnologiche. Già si parla di un'esternalizzazione di questa figura in molte realtà aziendali, proprio perché le specificità di applicazione spesso non saranno gestibili internamente. Maggiore professionalità, insomma, per maggiore sicurezza ed organizzazione dei dati. Le violazioni del Regolamento potranno comportare sanzioni pari al 2% del volume di affari, sino ad arrivare anche a revoche di licenze per talune attività che impattino particolarmente sulla gestione dei dati.

In sostanza, possiamo affermare che la tutela della privacy non stia affatto scemando, ma, al contrario, si stia rafforzando con maggiore attenzione verso quelle realtà che, per massa o tipologia dei dati, debbano rispondere a parametri di protezione ben più garantisti.

Il 2013 sarà un anno molto intenso ed il valore aggiunto sotto il profilo privacy per le aziende che dovranno adempiere correttamente ai nuovi obblighi sarà quello di capire che il dato non va protetto per obbligo di legge, ma perché costituisce la base degli affari. E dati non protetti, o non corretti, non consentono di ottimizzare le prospettive di business.

Privacy, controlli e sanzioni



Fonte: www.schmidtconsulting.it

Nicola Bernardi
Presidente Federprivacy - Federazione Italiana della Privacy

Il futuro dei dati personali

Con il Regolamento Europeo arriveranno nuove tutele e nuovi diritti per gli interessati al passo con i tempi. Ad esempio, sarà introdotto esplicitamente il diritto all'oblio: per motivi legittimi, ogni persona potrà, finalmente, richiedere la cancellazione dei propri dati in possesso di terzi.

Nella società tecnologica e ossessivamente "on-line" in cui viviamo, il concetto di privacy ha vissuto continue evoluzioni, passando, in pochi anni, da materia intricata, riservata agli addetti ai lavori, ad argomento quotidiano, penetrando sottilmente non solo negli uffici, ma anche nel privato delle nostre abitazioni, non di rado dibattuto in famiglia davanti ad un tg della sera o a seguito di una telefonata promozionale.
In effetti, sembrano trascorsi secoli da quando cominciammo a sentirci chiedere una firma in più per ogni banale contratto che dovevamo sottoscrivere: "é per la legge sulla privacy" ci veniva spiegato. Per diversi anni, nel pensare comune, quei moduli sono stati considerati solo "carta buttata via, la solita noiosa burocrazia". Si trattava della legge 675 del 1996, introdotta dal Governo del nostro Paese per recepire la direttiva comunitaria 95/46/EC. Se, all'epoca, firmavamo tutti passivamente quelle informative, quando oggi ci viene chiesto di fornire i nostri dati ed esprimere un consenso con una firma, siamo quantomeno assaliti da qualche dubbio del tipo: "come saranno utilizzate le informazioni che mi riguardano?" Già, perché praticamente tutti abbiamo sperimentato, almeno un volta, cosa significhi vedere invasa in una certa misura la propria sfera privata. Una telefonata all'ora di cena che ci propone un'offerta commerciale, una serie di telecamere che osservano ogni nostro movimento mentre facciamo shopping, avvisi pubblicitari mentre navighiamo in internet così corrispondenti ai nostri gusti personali da sembrare studiati apposta per noi. Con tutta probabilità, e a nostra insaputa, lo sono davvero.
In questi ultimi anni, le insidie alla nostra privacy hanno assunto sfaccettature ancora più complesse, addirittura non completamente conosciute dalla maggioranza, forse quasi inimmaginabili allo stesso legislatore quando sfornò la prima normativa sulla protezione dei dati personali nel 1996.
Ad esempio, è ultimamente in aumento, anche attraverso certi social network, l'utilizzo di sistemi di geolocalizzazione che, più o meno consapevolmente, consentono a terzi di conoscere ogni nostro piccolo spostamento, mentre portiamo tranquillamente in tasca la spia, che altro non é che il nostro cellulare.
Ma, anche con la rapida diffusione del "cloud-computing", mentre ci affanniamo a capire come saranno utilizzati i nostri dati personali, dovremmo cominciare a domandarci anche dove vanno a finire.
Tutte le trappole finalizzate al furto d'identità, come il phishing, utilizzate da hacker senza scrupoli per spillare soldi dai nostri conti, ci fanno sentire, inoltre, sempre più vulnerabili e ci fanno avvertire quanto i ladri del terzo millennio si avvalgano sempre meno di passamontagna e pistola, mirando direttamente ad impossessarsi delle nostre informazioni personali per i loro scopi criminali. È mai capitato a qualcuno che conoscete, o direttamente a voi, di essere derubati, anche solo di una piccola somma, dal vostro conto o dalla vostra carta di credito da parte di sconosciuti? Se la risposta è no, probabilmente è perché non utilizzate alcuna carta di credito e tenete i vostri soldi sotto il materasso o, più semplicemente, siete stati fortunati.
Anche se è vero che il cittadino può godere di una certa tutela (l'ultima volta in cui il legislatore ha messo mano all'impianto della normativa privacy in Italia risale al D. Lgs. 196/2003, tutto sommato, di recente), è pure dato di fatto che la data-protection costituisca un campo in cui, a motivo dell'inarrestabile progresso tecnologico, le regole devono essere scritte mentre si gioca la partita, poiché ogni pur ottimo impianto normativo messo a punto, dopo poco tempo risulta già non completamente adeguato a causa del mutamento degli scenari. Ecco, quindi, che la tecnologia corre più veloce della legislazione, e quest'ultima si trova a dover rincorrere gli eventi.
Poiché ogni intervento normativo pare puntualmente risultare solo un tentativo più o meno efficace di garantire un assetto stabile alla materia, la sfida della data-protection del futuro si gioca nella dinamicità di un impianto che contenga quanti più principi immutevoli nel tempo, non poggiando su regole rigide che possano divenire in breve tempo di ardua applicazione a causa di nuovi strumenti o nuove tecniche poco prima neanche esistenti.

A distanza di 17 anni, l'Europa raccoglie di nuovo questa sfida e lo fa in maniera anche più ambiziosa ed imponente rispetto al passato. Se, all'epoca, emanò la cosiddetta Direttiva Madre 46/1995, la quale doveva essere recepita entro 18 mesi da ogni singolo Stato membro con una legge nazionale ad hoc, il 25 gennaio del 2012 la Commissione Europea ha invece presentato l'impianto di un nuovo Regolamento Europeo che, terminato il suo iter legislativo, sarà direttamente applicabile nei 27 Stati membri, senza necessità alcuna di legiferare da parte dei singoli Governi. Questi dovranno occuparsi solamente di far rispettare le nuove regole.
Se dovessimo assegnare un voto a questa scelta dell'Europa, quella di proporre un'unica normativa all'intera Comunità Europea, per coraggio meriterebbe, fin d'ora e senza alcun dubbio, un bel 10, per la corretta valutazione dell'importanza e della delicatezza del problema e per la decisione di "prendere il toro per le corna".
Sotto questo aspetto, ci attende una legge sulla privacy immodificabile autonomamente, sulla quale nessuno Stato membro UE potrà decidere da solo di apportare interventi per semplificare o inasprire la materia, a seconda degli orientamenti politici dei Governi che, negli anni, si succederanno.
Con il Regolamento Europeo arriveranno, inoltre, nuove tutele e nuovi diritti per gli interessati al passo con i tempi. Ad esempio, sarà introdotto esplicitamente il diritto all'oblio: per motivi legittimi, ogni persona potrà, finalmente, richiedere la cancellazione dei propri dati in possesso di terzi. Questo accadrà, per esempio, *on-line*, quando un utente farà eliminare i propri dati detenuti da un *social network* o altro servizio *web.* Non è poco, dato che, di fatto, la prassi oggi è che questi operatori continuino a conservare i dati dei loro utenti vita natural durante.
Più in generale, gli interessati avranno diritto alla massima trasparenza e ad essere compiutamente informati su ogni trattamento dei loro dati personali, anche quando associato a complesse ed articolate filiere di sub-appalto (si pensi, appunto, al caso del *cloud computing*).
Inoltre, si provvederà espressamente a proteggere i dati dei minori: almeno in questo, la UE sembra avere imparato qualcosa dalla *privacy* d'oltreoceano.
Per le imprese ed i loro preposti, saranno introdotte nuove responsabilità, come il principio di "*accountability" che* comporterà l'onere di dimostrare l'adozione di tutte le misure e le cautele sulla privacy in capo a chi tratta i dati, senza troppi formalismi, com'è stato finora, ma badando, piuttosto, alla sostanza.
Altra grande novità per le aziende con più di 250 dipendenti, e per tutti gli enti pubblici, sarà l'obbligo di nominare un "privacy *officer*", interno oppure anche esterno, una figura di stampo manageriale, indipendente, competente e in diretta relazione con i vertici aziendali. A questo proposito, nei tempi di crisi occupazionale che il mercato del lavoro sta attraversando, è se non altro rincuorante evidenziare che, stando alle statistiche attuali, solo in Italia la nomina obbligatoria del privacy officer offrirà nuove opportunità professionali a circa 24.000 persone.
Nel caso in cui si verifichi una violazione di dati personali (ad esempio, un hacker che ruba i nostri dati dal sito web della nostra banca), avremo la garanzia aggiuntiva di dover essere avvisati tempestivamente (l'obbligo di notifica dovrà essere eseguito sia a noi come diretti interessati, sia alle autorità).
Anche in tema di multe, con l'Europa non si scherzerà: le imprese che non rispetteranno le suddette regole e tutte le altre contenute nel Regolamento Europeo rischieranno sanzioni salatissime, che potranno arrivare fino al 2% del volume d'affari annuale.
Probabilmente ci vorrà ancora un altro anno prima che il Regolamento Europeo sulla privacy venga definitivamente approvato, ma possiamo già osservare come il lavoro fin qui svolto segni davvero una svolta storica rispetto alle precedenti normative. Finalmente, sotto la direzione europea, la legge si occuperà in modo concreto dei pericoli più evoluti che minacciano la nostra privacy, specialmente quelli che incontriamo on-line. Probabilmente questo non segnerà una vittoria (siamo piuttosto noi che dobbiamo imparare a difendere la nostra privacy con i denti), ma possiamo comunque affermare che l'Europa ha raccolto la sfida della privacy nel migliore dei modi. In qualità di cittadini, potremo beneficiarne più di quanto possiamo immaginare al presente.

Pasquale Troncone
Professore aggregato di Diritto Penale dell'Economia – Facoltà di Giurisprudenza, Università degli Studi Federico II di Napoli

Un nuovo diritto di libertà

Nella sua configurazione giuridica, la privacy segna, e con decisione, un nuovo diritto di libertà della persona umana, un nuovo modo, moderno e deciso, di declinare il più ampio e tradizionale diritto alla libertà individuale.

Affrontare oggi il tema della privacy significa toccare uno dei nodi problematici più attuali, più controversi e, forse, più condizionanti della vita di relazione nella comunità umana moderna. Una comunità di uomini che ha la possibilità di vivere i rapporti interpersonali in due diversi ambiti relazionali, i concreti e reali contatti individuali e la vita immateriale della Rete la quale, in assenza di contatti fisici, è organizzata con connessioni e mezzi tecnologici. Va opportunamente premesso che il diritto alla libertà, su cui sono fondate tutte le Carte costituzionali contemporanee e che contribuisce a radicare il principio di Democrazia nella politica e di partecipazione dei cittadini alla vita comunitaria, trova progressivamente nuove forme di espressione che spostano sempre più in avanti le frontiere mobili dei diritti fondamentali della persona umana. Uno dei nuovi profili del diritto di libertà è proprio il diritto alla privacy il quale, pur non trovando un riconoscimento pieno e coerente nella legislazione moderna - quantomeno in Italia - si propone come nuovo terreno di ricerca e di tutela, spinto dalle rapidissime evoluzioni della ricerca tecnologica e delle sue sorprendenti applicazioni, ormai divenute onnipervasive per la vita di ciascuno di noi. Se è vero che il diritto di cittadinanza di ciascun membro della collettività si impone nella vita concreta della società umana organizzata, è tuttavia vero che un nuovo diritto di cittadinanza si affaccia all'attenzione dell'uomo e poi del giurista: è quello che, di fatto, ha trovato un suo specifico radicamento in una comunità umana virtuale, quale quella della Rete, nella quale la caratteristica di fondo è di non possedere regole e vivere le relazioni ed i contatti personali in maniera del tutto anarchica, senza alcuna possibilità di regolazione con la legislazione attuale. Occorre, dunque, interrogarsi se e fino a che punto il giurista e le sue regole siano compatibili con un mondo insofferente alla riservatezza personale e caratterizzato dalla veicolazione rapida e massiva di informazioni anche sensibili. Basta, per questo, pensare all'uso delle informazioni personali carpite dalle "piazze virtuali" o dai "social network", improvvidamente diffuse e riutilizzate senza alcun consenso dell'interessato. Nella sua configurazione giuridica, la privacy segna, e con decisione, un nuovo diritto di libertà della persona umana, un nuovo modo, moderno e deciso, di declinare il più ampio e tradizionale diritto alla libertà individuale. Tuttavia, l'attuale legislazione in materia di privacy si presenta priva di una coerenza concettuale e le stesse norme, ormai inserite in diversi ed eterogenei settori normativi del nostro ordinamento giuridico, non soddisfano sempre il criterio di chiarezza e precisione. Privacy è un vocabolo che si presta a molteplici significati, dal tradizionale concetto di riservatezza della vita privata alla tutela dei dati identificativi della persona, fino alla tutela dei mezzi attraverso i quali passano le informazioni personali, come la corrispondenza o le comunicazioni telefoniche. Certamente, la Rete assume un ruolo centrale tra i mezzi di comunicazione quale modo per vivere relazioni personali oppure organizzare il mercato ed i commerci, ma nel cui ambito si insinuano sempre più frequentemente soggetti, anonimi, che la utilizzano come strumento per commettere reati, modalità di illecito profitto che sfuggono alle regole tassative definite dalla legislazione penale. Il furto d'identità, che ormai costituisce una delle maggiori preoccupazioni dei navigatori della Rete, non è oggetto di norme di tipo repressivo, allo stesso modo in cui il trattamento dei dati personali in Rete non è sottoposto alle regole di abilitazione stabilite dal D.Lgs. n. 196/2003 che regola il corretto trattamento dei dati personali (si pensi al consenso). Si tratta, in parte, di norme inadeguate e non al passo con i tempi, per altro verso di norme che sfuggono a qualsiasi tentativo di fare sistema e, di conseguenza, alla possibilità di esprimere una tutela giuridica completa, coerente ed efficace. Ecco perché la sfida che in futuro ci attende non sarà quella di condizionare la Rete, ma mettere in campo regole di protezione che riescano a far convivere la libera ed anarchica vita virtuale con la necessità di garantire a tutti il diritto di libertà e, con esso, il diritto alla privatezza personale.

Concetta Giunta
Ricercatrice di Istituzioni di Diritto Pubblico - Università degli Studi di Roma 'Tor Vergata'

A tutela del cittadino

Anche la dottrina, in maniera concorde, individua il fondamento costituzionale del diritto alla privacy nell'art. 2 Cost., nel quale "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità".

"Tutti si interessano ai fatti miei come fossero miei parenti", scriveva Manzoni all'amico Fauriel. La tentazione, diffusa in ogni tempo, di varcare la soglia della sfera privata altrui è ancor più temibile in contesti sociali nei quali proliferano strumenti in grado di rendere sbiadito il confine tra ciò che si desidera condividere con terzi e ciò che si intende mantenere nella propria sfera privata.

Cercare, nella Costituzione italiana, un argine a tali ingerenze può apparire esercizio sterile sin dalle premesse, dal momento che, come è noto, nessuna disposizione costituzionale tutela in maniera diretta ed immediata il diritto alla privacy.

Ciononostante, i contrasti che quotidianamente oppongono l'esigenza di riservatezza ad interessi diversi possono trovare, nel testo costituzionale, una composizione meno partigiana - e giuridicamente più convincente - rispetto allo schierarsi aprioristicamente dalla parte del Grande Fratello di orwelliana memoria o degli ipergarantisti intransigenti.

Una lettura sistematica delle norme fondamentali mostra, infatti, come, nonostante l'assenza di una specifica disciplina, la Costituzione riconosca "un particolare pregio all'intangibilità della sfera privata negli aspetti più significativi e più legati alla vita intima della persona umana" (Corte cost., sent. n. 366/1991).

Il fondamento di tale pregio è stato rinvenuto, nella prima sentenza del Giudice costituzionale che ha affrontato la questione, negli artt. 2, 3, secondo comma, e 13, primo comma i quali, riconoscendo e garantendo i diritti inviolabili dell'uomo, tutelerebbero, indirettamente "quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione, sanciti espressamente negli artt. 8 e 10 della Convenzione europea sui diritti dell'uomo" (Corte cost., sent. n. 38/1973).

Anche la dottrina, in maniera concorde (seppur attraverso percorsi argomentativi diversi), individua il fondamento costituzionale del diritto alla privacy nell'art. 2 Cost., a norma del quale "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità".

Secondo la lettura che sembra più convincente, l'art. 2 fonda il diritto alla riservatezza nella misura in cui accoglie il primato della persona (principio personalistico) ed estende la tutela dei suoi diritti anche contro i rischi e le ingerenze che dalle formazioni sociali di cui si è parte possono derivare. In altri termini, la Costituzione riconosce e garantisce che la personalità si formi, si nutra e si svolga nella società, ma anche al riparo da essa.

Analogamente, l'art. 3, primo comma, Cost., riconoscendo la pari dignità sociale e, fondando così il diritto all'onore, non è indifferente rispetto alle violazioni dello stesso che possono derivare da un'indebita invasione dell'intimità dei cittadini (si pensi, ad esempio, alla diffusione tendenziosa dei dati che il "Codice in materia di protezione dei dati personali" definisce "sensibili").

Una più penetrante protezione della sfera privata emerge, poi, proseguendo nella lettura della Costituzione, dalla disciplina delle tre libertà che la Costituzione definisce in maniera espressa "inviolabili": libertà personale, inviolabilità del domicilio, libertà e segretezza delle comunicazioni. Gli articoli 13, 14 e 15 Cost., dedicati a tali diritti, confermano la centralità che assume nella Costituzione italiana la persona, tanto nel suo essere fisico, quanto nella sua proiezione spaziale e nel suo comunicare con altri. L'intromissione in tali ambiti materiali è, in via generale, preclusa ad ogni altro soggetto, pubblico o privato.

A ciò si aggiunga che l'art. 21 Cost., nel disciplinare la libertà di manifestazione del pensiero, fornisce pari tutela alla forma di godimento negativa della stessa: il c.d. diritto al silenzio, ovvero la facoltà di non diffondere fatti o pensieri giuridicamente qualificabili come "propri" dal titolare del diritto medesimo.

La considerazione sinottica dei diritti appena citati concorre a delineare quello che, significativamente, la dottrina nordamericana ha definito "right to be let alone". Anzi, rispetto al diritto alla riservatezza - definito dalla Corte costituzionale come il potere del soggetto "di controllare le informazioni che lo riguardano e le modalità con cui viene effettuato il loro trattamento" (sent. n. 271/2005) - si rinviene nella Costituzione, in determinati casi, un più penetrante divieto di acquisizione di dati e notizie ricadenti nella sfera intima della persona.

In tale ultima prospettiva si considerino, ad esempio, i citati artt. 14 e 15 Cost., i quali configura-

no diritti ad escludere terzi (iura ecxcludendi alios) dall'accesso, rispettivamente, nella dimensione spaziale privata (inviolabilità del domicilio) e dalla cognizione di comunicazioni interpersonali (segretezza delle comunicazioni). Non si tratta, dunque, di un mero obbligo di riservatezza nel trattamento di dati acquisiti, quanto, piuttosto, del divieto di acquisirli. Attenta dottrina ha distinto, in tal senso, il diritto alla segretezza dal più generico diritto alla riservatezza. In altre parole, da una parte la Costituzione garantisce che l'ambito privato non venga turbato da intromissioni esterne e, per altro verso, quando ciò è consentito, l'ordinamento si allerta affinché l'utilizzo di tali informazioni sia esclusivamente rivolto al perseguimento delle finalità che consentono tali deroghe, onde evitarne l'ulteriore ed incontrollata diffusione.

Cosa accade, però, quando la menzionata, multiforme, protezione della sfera privata risulti incompatibile con la tutela di altri interessi costituzionalmente disciplinati?

Per rispondere a tale domanda, occorre premettere che limitazioni ai diritti riconosciuti ad esclusivo vantaggio del singolo (c.d. diritti individualistici, quali senz'altro sono i citati "diritti di esclusione") sono legittimi soltanto per la protezione di interessi protetti dall'ordinamento con la medesima forza (costituzionale). Quelli che più spesso collidono con la tutela della privacy sono: il diritto alla salute, il diritto di cronaca, l'interesse alla prevenzione e repressione dei reati, il buon andamento dell'amministrazione (dal quale consegue il principio della trasparenza dell'azione amministrativa).

Vi è, nella Costituzione, almeno una pista per appianare tali contrasti?

Non potendo in questa sede affrontare ognuno di essi, si consideri il caso paradigmatico delle intercettazioni telefoniche. La cognizione di comunicazioni riservate è consentita, entro i limiti previsti dal codice di procedura penale (come è noto, da anni oggetto di tentativi di modifica) esclusivamente nell'interesse - costituzionalmente fondato – dell'amministrazione della giustizia.

Dal che si può concludere che esse, pur costituendo un vulnus alla segretezza delle comunicazioni, sono costituzionalmente legittime, nella forma meno invasiva possibile, allorquando siano indispensabili per la prevenzione o la repressione dei reati.

Il tema delle intercettazioni telefoniche mostra, però, con sempre maggiore evidenza, ulteriori ed attualissimi profili critici qualora il mezzo di ricerca della prova varchi i confini del procedimento penale e venga utilizzato come fonte di informazioni per la divulgazione di notizie.

Gli interessi costituzionalmente protetti coinvolti in fattispecie di questo tipo sono: il segreto investigativo (riconducibile alla prevenzione e repressione dei reati); il diritto di cronaca (tutelato dall'art. 21 Cost. nell'ambito della libertà di manifestazione del pensiero); la segretezza delle comunicazioni, protetta dall'art. 15 Cost.; la dignità sociale dei cittadini (art. 3 Cost.).

Il trattamento di notizie acquisite in deroga alla disciplina costituzionale della segretezza delle comunicazioni è riservato all'autorità giudiziaria, la cui "intrusione" è consentita al solo fine di amministrare la giustizia. Dunque, le comunicazioni intercettate non dovrebbero essere utilizzate fuori dal processo.

E il diritto ad essere informati? A dispetto di letture sbrigative quanto à la page, non può prevalere rispetto ai configgenti, richiamati interessi, in quanto, secondo le ricostruzioni più rigorose e "garantiste", non è tutelato con pari forza (costituzionale) dall'ordinamento.

Lo stesso diritto di cronaca, garantito dall'art. 21 Cost. (soltanto quando le notizie diffuse siano acquisite lecitamente), deve cedere il passo davanti alla tutela della segretezza delle comunicazioni ed al rispetto della dignità sociale dei soggetti coinvolti. Gli artt. 3 e 15 Cost. costituiscono, infatti, in via generale, limiti alla libertà di manifestazione del pensiero.

Una precisazione è però indispensabile, onde evitare di trarre da quanto sin qui detto conseguenze inaccettabili. Se un Ministro si accorda telefonicamente con un Capo di Stato Maggiore per organizzare un colpo di Stato, i cittadini non hanno il diritto di sapere?

Come in altra occasione ipotizzato, nell'ambito della generalità dei cittadini si potrebbe enucleare una categoria più ristretta con riferimento a quelli che ricoprono cariche pubbliche, giacché non sembra incongruo ritenere che, per essi, la protezione della dignità sociale e del diritto alla segretezza possano essere modulati in senso restrittivo, in quanto l'interesse pubblico all'informazione, in quel caso, troverebbe fondamento nella responsabilità politica diffusa per coloro che rivestono cariche politiche elettive e nelle norme costituzionali che tutelano l'autorità, l'unità ed il prestigio dello Stato per i pubblici funzionari.

Lia Valetti
Università di Padova - Facoltà di Scienze Politiche, Relazioni Internazionali e Diritti Umani

È una vera tutela?

Non si può nascondere che dietro alle finalità nobili delle leggi poste a tutela della privacy - il rispetto della dignità umana, la non discriminazione, il mantenimento della sicurezza e molte altre - se ne nascondano di meno nobili.

La tutela della privacy è un argomento che compare e scompare dalla lista dei cosiddetti hot terms del dibattito politico e culturale. Come spesso succede in questi casi, attorno al tema si è creata una nuvola di svariate informazioni che rende più difficoltosa la comprensione del nocciolo della questione.
Per "privacy" si intende il diritto alla riservatezza della propria vita privata. In altre parole, un diritto all'intimità. Si potrebbe, metaforicamente, pensare all'insieme delle leggi sulla tutela della privacy come ad una linea sottile che divide la vita sociale dalla vita del singolo. Non a caso, la normativa americana trova nella privacy "the right to be let alone". Per estensione, il termine ha iniziato a fare riferimento ad un diritto individuale a che le informazioni riguardanti la propria persona (i propri dati) siano utilizzati solo in caso di necessità e solo dopo l'espresso consenso della persona interessata, la quale deve essere informata e garantita della custodia e del trattamento di tali dati. Questa seconda accezione riflette meglio la formula utilizzata nei Paesi di common law, nei quali si parla di habeas data.
Sarebbe legittimo chiedersi perché mai le persone dovrebbero preoccuparsi di allontanare dagli occhi altrui la propria vita e nascondere informazioni su se stesse. Hanno forse qualcosa da nascondere? In realtà, il discorso non è così semplicistico e rimanda a riflessioni storiche e filosofiche: in primo luogo, l'evoluzione della classe borghese e, di conseguenza, l'individualismo.
Una volta conquistata la solidità economica, la borghesia iniziò a desiderare un posto nella società accanto a clero e nobiltà, chiedendo l'abolizione dei privilegi e dei diritti feudali di questi ultimi e rivendicando il potere politico. La storia della borghesia non avrebbe potuto avere luogo senza la logica individualista, che vede nell'individuo un valore superiore ed antecedente ai suoi rapporti interpersonali. Rodotà nota che "la possibilità di godere pienamente della propria intimità è un connotato differenziale della borghesia rispetto alle altre classi e la forte componente individualistica fa sì che quella operazione si traduca, poi, anche in uno strumento di isolamento del borghese all'interno della sua stessa classe" [1]. La borghesia si isola, quindi, dalla società per potersi affermare come classe sociale e il bourgeois si isola dalla borghesia stessa per poter affermare la propria personalità individuale. In questo senso, la tutela della privacy risponde all'esigenza di crearsi uno spazio individuale, personale, sicuro e protetto, in contrapposizione con la piazza e la strada, costantemente pervase da minacce quotidiane. Con il tempo, questo aspetto ha trovato il suo fondamento nel rispetto della dignità umana: la società costringe l'uomo al rispetto di regole le quali, per quanto giuste siano, sono necessariamente sentite come dei limiti esterni. Se, quindi, un individuo non si sente libero di poter esprimere sé stesso nemmeno nel suo spazio, la sua dignità ne risulterà lesa.
Un'altra motivazione che ha portato alla nascita di norme a tutela della privacy è molto lontana dal voler evitare la conoscenza pubblica di informazioni personali, ma risiede nell'intenzione di impedire la discriminazione e la stigmatizzazione per l'appartenenza ad un'organizzazione o un'associazione o per religione, orientamento sessuale, professione. Si può ora ben capire come la tutela della privacy sia formata da varie facce che costituiscono ognuna uno specifico diritto più ampio: il diritto alla dignità umana inviolabile, il diritto alla non discriminazione, il diritto alla libertà personale, l'inviolabilità del domicilio, la segretezza della corrispondenza, la libertà d'opinione. Tali diritti trovano ognuno il proprio posto all'interno della Costituzione, ma anche in altri strumenti. Testimonianza di questo è l'articolo 8 dello Statuto dei Lavoratori, che impedisce al datore di lavoro di svolgere indagini sulle opinioni religiose, politiche e sindacali del lavoratore.
Allargando un po' il focus giuridico, la normativa italiana di riferimento per quanto riguarda la tutela della privacy è il Decreto Legislativo 30 giugno 2003 n. 196 (o Testo Unico sulla Privacy) il cui articolo 1 recita che "chiunque ha diritto alla protezione dei dati personali che lo riguardano". Ben più interessante l'articolo 2, c.1, che riconosce come finalità principale della legge la garanzia 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." Bisogna, però, porre attenzione a non farsi ingannare: insieme alle leggi che l'hanno integrata e modificata, questa è la legge generale, ma spesso si accettano condizioni al trattamento dei propri dati personali che non hanno affatto intenzione di tutelarli. Quanti leggono, ogni volta in cui divulgano i propri dati per svariati motivi su qualche foglio burocratico, o su Internet, quella cinquantina di righe a pié di pagina in cui si spiegano le modalità con cui verranno trattati il proprio nome, la propria età, la via in cui si abita?
I dati personali si distinguono in: identificativi (atti ad individuare l'identità di una persona fisica o giuridica), sensibili (riguardanti orientamento religioso, politico, sessuale...) e giudiziari (in materia di casellario giudiziario) e possono trovarsi in una molteplicità di luoghi differenti: anagrafi, archivi ospedalieri, scolastici, giudiziari, bancari, catasti, ma, soprattutto, in Internet. Proprio su quest'ultimo strumento è necessario soffermarsi maggiormente: forum, blog e social network sono, infatti, dei contenitori illimitati di dati personali, il cui trattamento non appare sempre così trasparente. Un articolo del Wall Street Journal denunciava, ad esempio, come Facebook avesse

1 S. Rodotà, La vita e le regole, pag.102, Feltrinelli

trasmesso ad aziende pubblicitarie l'identità degli utenti senza che questi ne fossero consapevoli, dato che avevano accettato la normativa sulla privacy proposta dallo stesso social network in cui veniva annoverata anche tale operazione. [2]

Qui inizia ad essere ravvisabile una delle tante contraddizioni che il tema "tutela della privacy" nasconde: da una parte, il bisogno di sentirsi tutelati nei propri dati personali, dall'altra, quello di non rimanere soli, di farsi conoscere, di vivere il proprio "quarto d'ora di popolarità". Ecco, in questo modo, spiegato il grande successo di programmi come "Il Grande Fratello", di cui si può dire che conceda di tutto ai suoi partecipanti, ma non di godere della propria privacy. A volte si ha l'impressione che il nucleo su cui fanno perno tali programmi sia una vera e propria ossessione per il comportamento di persone che potrebbero essere vicini di casa, con cui si è perfettamente identificabili. A questo punto, la domanda è: perché? L'ossessione per la vita dei personaggi famosi è scontata: gli attori di successo, le star suscitano invidia, ammirazione. Sapere, quindi, ciò che fanno nella vita privata è il primo passo per cercare di emularli nelle loro imprese, per sentirsi più vicini a loro. Ma dove nasce l'ossessione per ciò che fanno dei ragazzi che dovrebbero aver raggiunto l'età adulta, che svolgono professioni ordinarie o sono studenti, di media cultura, di ambizioni quasi esclusivamente legate alla notorietà televisiva? Probabilmente, proprio il fatto che si tratti di ragazzi come tante migliaia di altri suscita una curiosità morbosa per il loro modo di comportarsi. Si tratta di un modo per confrontare i propri modi di fare e, magari, trovarne una conferma. Fatto sta che nessuno sembra sentire il bisogno di sostenere che anche questi ragazzi avrebbero diritto alla loro privacy, per lo meno alla toilette.

La tecnologia ha sicuramente cambiato il modo di affrontare il tema della privacy ed i nuovi sistemi di comunicazione appaiono in netto conflitto con la tutela dei dati personali: ad esempio, i cellulari permettono di rintracciare una persona anche senza chiamarla. Non solo. La tecnologia ha inciso soprattutto per quanto riguarda i nuovi sistemi per garantire la sicurezza pubblica: quasi tutti i negozi sono dotati di telecamere di sorveglianza a circuito chiuso, sulla maggior parte degli angoli di tutte le città, dai piccoli comuni alle grandi metropoli, sono installate telecamere più o meno nascoste o camuffate da lampioni. La sicurezza è diventata, soprattutto dopo l'11 settembre, la principale preoccupazione per l'incolumità dei propri cittadini. Di conseguenza, la riduzione delle garanzie di riservatezza si è resa necessaria per motivi di trasparenza. D'altra parte, è risaputo che le dichiarazioni dei diritti sono seguite dalla limitazione agli stessi per motivi di ordine pubblico o sicurezza e nemmeno la Dichiarazione Universale dei diritti umani ne è immune: all'art.29, c.2 si legge che "nell'esercizio dei suoi diritti e delle sue libertà, ognuno deve essere sottoposto soltanto a quelle limitazioni che sono stabilite dalla legge per assicurare il rispetto dei diritti e delle libertà degli altri e per soddisfare le giuste esigenze della morale, dell'ordine pubblico e del benessere generale (...)". Il diritto alla privacy, quindi, sussiste, ma può essere derogato per il bene di tutti. Inoltre, il Garante per la protezione della privacy, autorità indipendente istituita dal D. Lgs. n. 196 che assicura il corretto trattamento dei dati ed il rispetto dei diritti fondamentali delle persone in tutti i settori, pubblici e privati, ha adottato due provvedimenti (29 novembre 2000 e 29 aprile 2004) in seguito ai quali la legittimità della videosorveglianza è sottoposta ai criteri di liceità, necessità, proporzionalità e finalità. La videosorveglianza deve essere manifesta grazie ad appositi cartelli informativi, ma è consentita anche senza necessità del consenso, qualora sia effettuata per tutelare persone o beni.

Non si può nascondere che dietro alle finalità nobili delle leggi poste a tutela della privacy - il rispetto della dignità umana, la non discriminazione, il mantenimento della sicurezza e molte altre come, ad esempio, lo sforzo di mantenere un legame con tutte le informazioni su sé stessi contenute in rete o in archivi informatici, il cosiddetto corpo elettronico - se ne nascondano di meno nobili. Spesso, chi ha più necessità di tenere sotto ossessivo controllo i dati che lo riguardano è anche chi beneficia del fatto che questi siano segreti. Chi sa di essere in regola con la finanza, perché dovrebbe lamentarsi del fatto che le dichiarazioni dei redditi siano pubbliche? Si potrebbe rispondere che una delle motivazioni sia il rispetto della dignità umana: i più ricchi direbbero di non voler mettere in imbarazzo i più poveri e i più poveri di non volersi sentire umiliati nei confronti dei più ricchi. In realtà, già nella vita di tutti i giorni ognuno si mette la propria dichiarazione dei redditi addosso, nel modo di vestire, di mangiare, di muoversi. La dichiarazione dei redditi non dovrebbe essere altro che uno strumento idoneo a far sì che tutti paghino proporzionalmente a ciò che guadagnano. Se qualcuno è a ciò contrario, si trova in contrasto con l'idea politica di proporzionalità e non si trova a favore di un'idea sociale di tutela della privacy, nata, come già detto, per tutelare la proprietà privata in modo da poter affermare la propria personalità in uno spazio riservato e non subire discriminazioni. Così anche per quanto riguarda le intercettazioni: la cattiva informazione, talvolta, ha portato a pensare che la riservatezza di chiunque possa essere violata. In realtà, l'intercettazione è consentita dal codice di procedura penale solo nel caso in cui sussistano gravi indizi per determinati tipi di reato e sia ritenuta necessaria per la scoperta di nuove prove. Chi sa di non aver commesso alcun reato può già sentirsi tutelato dagli articoli della Costituzione che sanciscono l'inviolabilità del domicilio (art.14), la segretezza delle comunicazioni (art.15), il diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione (art.21).

Bisogna, dunque, considerare la tutela della privacy come un argomento poliedrico, che dietro a lati positivi e facilmente interpretabili può celarne anche di meno chiari, a vantaggio non di chi si impegna a far sì che la propria sfera personale non venga lesa o sfruttata a piacimento per interessi altrui, ma anche di chi possiede buoni motivi perché la pubblica autorità o chi di competenza non venga a conoscenza di dati che lo riguardano. La normativa italiana sul tema è vasta, ma con i mezzi moderni è anche facilmente individuabile. È risaputo, però, che quasi sempre la legge è suscettibile di deroga. Occorre, quindi, fare attenzione prima di barrare la casellina "accetto la normativa sulla privacy" ed averla letta almeno nelle parti più significative. Una buona idea sarebbe quella di rendere più leggibile l'informativa con dei piccoli correttivi, per lo meno visivi: un elenco puntato e qualche parola in grassetto potrebbero aiutare ad essere più consapevoli dei propri diritti e meno diffidenti nei confronti di chi vuole avere a che fare con i nostri dati.

2 Laura Turini, Il Sole 24 ore, 19 ottobre 2010

Monica Gobbato
Avvocato, Consulente Privacy dell'Ordine dei Consulenti del Lavoro di Milano.

Diritto di cronaca

La disciplina sulla privacy ha, di fatto, trasformato il mondo dell'informazione. Il diritto di cronaca ha costituito per anni l'alibi per la realizzazione di violazioni imperdonabili.

Premessa.

La disciplina Privacy nasce in Europa con la direttiva n. 46/1995, divenuta legge italiana nel 1996, con la n. 675, poi innovata, tanto da divenire Testo unico sulla Privacy grazie alla legge n. 196 del 2003 (il Codice). Successivamente, ci sono state diverse modifiche, tecnologiche e sociali, che hanno portato all'approvazione della bozza del Regolamento Europeo sulla Privacy del 25 Gennaio 2012, il quale dovrà essere pubblicato entro l'anno sulla Gazzetta della Comunità Europea per divenire immediatamente obbligatorio. Occorre notare che ai tempi della direttiva non esistevano i social network e neanche i blog e i siti internet erano, di fatto, poco più di un manifesto espositivo. L'interazione tra i soggetti, i rapporti tra gli utenti, non erano - ai tempi - degni di attenzione del legislatore, né europeo, né italiano. Oggi, grazie soprattutto anche alle impreviste evoluzione e diffusione dei dispositivi mobili intelligenti, si è assistito ad un utilizzo smodato ed imprevedibile dell'internet sociale, il quale mira non solo alla condivisione dei contenuti, ma anche alla partecipazione delle persone a diverse tipologie di organizzazioni sociali. Molte nuove applicazioni, inoltre, rendono il flusso transfrontaliero dei dati non più l'eccezione, ma la regola.

Di ciò si sono resi ben conto i Garanti europei, i quali si riuniscono periodicamente ai sensi dell'art. 29 della Direttiva 46 ed hanno pubblicato diversi pareri sui fenomeni dei social network, dei motori di ricerca e del diritto all'oblio.

Un esempio concreto di evoluzione della privacy concerne l'informazione. Fino a qualche anno fa, si credeva che, in nome del diritto di cronaca, si potesse pubblicare qualsiasi informazione, anche quelle non essenziali. Oggi, sempre più spesso, il diritto di cronaca deve bilanciare gli interessi con il diritto alla privacy.

Negli ultimi anni – che a parer mio coincidono con la Presidenza Pizzetti – si è osservata, in Italia, un'emanazione costante e sistematica di provvedimenti contenenti linee guida nelle materie più delicate, quali quelle riferite a:

1) alcuni singoli settori commerciali;
2) area del personale;
3) sanità;
4) marketing e carte di fidelizzazione;
5) motori di ricerca e social network;
6) giornalismo e diritto di cronaca.

Nella trattazione di questo articolo evidenzierò le più importanti modifiche intervenute in alcune delle aree sopra menzionate, verificandone i provvedimenti relativi, amministrativi o di giustizia ordinaria.

1. Diritto di cronaca

La disciplina sulla privacy ha, di fatto, trasformato il mondo dell'informazione. Il diritto di cronaca ha costituito per anni l'alibi per la realizzazione di violazioni imperdonabili. Si analizzeranno alcuni casi già studiati dal Garante o dal giudice ordinario.

Nel 2010, il Garante ha dovuto esaminare numerosi casi. Sono, infatti, pervenute diverse segnalazioni concernenti la pubblicazione di dati ed immagini relativi alle vittime di reato, nelle quali l'Autorità ha chiarito che il limite dell'"essenzialità dell'informazione" va valutato con particolare rigore quando il trattamento riguardi dati personali concernenti le vittime di episodi criminosi. Tale rigore si giustifica anche alla luce della considerazione degli ulteriori rischi cui la diffusione di tali dati può esporre l'interessato, considerato il contesto sociale o familiare in cui egli è già inserito.

L'Autorità ha chiarito che la pubblicazione dei dati relativi a procedimenti penali è ammessa anche senza il consenso dell'interessato, ma nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico da valutarsi in concreto, caso per caso, nel rispetto delle disposizioni che tutelano il segreto delle indagini e degli atti processuali.

Estremamente interessante sul fronte giudiziario è la sentenza della V Sezione penale della Cassazione n. 45051/2009, la quale ha invitato ad un "maggior rigore" da parte dei talk show che rivisitano processi in tv.

I giudici criticano quel "singolare fenomeno mediatico che tende ad offrire una realtà immaginifica o virtuale, capace, per forza di persuasione, di sovrapporsi, ove acriticamente recepita dagli utenti, a quella sostanziale o, quanto meno, a collocarsi in un ambito in cui i confini tra immaginario e reale diventano sempre più labili e non facilmente distinguibili. Secondo un fatto di costume oggi invalso e comunemente accettato, è consentito pure rivisitare nei talk show televisivi gravi fatti delittuosi oggetto di indagini e persino di processo, nella ricerca di una verità mediatica in parallelo a quella sostanziale o a quella processuale".

2. Diffamazione e Trattamento Illecito di dati personali

Sempre nell'ambito del diritto di cronaca, occorre rilevare che, al fianco del reato di diffamazione, si è spesso invocato anche il trattamento illecito dei dati. Considerato che il primo si verifica ogniqualvolta l'agente, "comunicando con più persone, offende l'altrui reputazione", ciò può avvenire "anche" comunicando dati personali in modo illecito. Ma i due reati non solo non coincidono, sono estremamente diversi.

Un caso di presunta o reale coesistenza dei due reati riguarda un ragazzo down di Torino il quale, nel 2006, era stato vessato ed umiliato da un gruppo di bulli coetanei, che avevano poi caricato i filmati sulla sezione video di un noto motore di ricerca. Le accuse nei confronti dei vertici pro-tempore della società sono di diffamazione aggravata e trattamento illecito di dati personali a fini di profitto.

Il processo su tale vicenda è giunto a sentenza nel febbraio del 2010. Il Tribunale di Milano ha condannato a sei mesi di reclusione tre fra dirigenti ed ex dirigenti di Google ritenuti colpevoli di violazione delle norme sulla privacy per non aver impedito la pubblicazione del video. Nelle motivazioni si legge: "Google Italy trattava i dati contenuti nei video caricati sulla piattaforma e ne era responsabile quindi per lo meno ai fini della legge sulla privacy. L'informativa era del tutto carente e comunque talmente nascosta nelle condizioni generali del contratto da risultare assolutamente inefficace per i fini previsti dalla legge".

Buona parte della dottrina ritiene che il Giudice abbia condannato Google soprattutto per violazione della disciplina sulla privacy, in quanto non avrebbe

avvertito in maniera sufficientemente chiara della necessità di prestare attenzione al rispetto della stessa. Sostanzialmente, il motivo della decisione sarebbe un'incompleta ed inidonea informativa. La conseguenza disarmante sarebbe che le motivazioni di una "così grave" condanna risiedano tutte in una inidonea informativa ed ancor più "disarmante" sarebbe che lo stesso Giudice, poche pagine più avanti, avrebbe poi rigettato la tesi accusatoria (secondo cui Google Italy sarebbe responsabile anche di concorso in diffamazione) scrivendo testualmente "pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla privacy che costituisca l'obbligo giuridico fondante la posizione di garanzia, non vi è chi non veda che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto 'impedire l'evento' diffamatorio".
In altre parole, il Giudice si sarebbe contraddetto perché, nonostante l'esistenza e conseguente colpevolezza di Google derivante dall'inidonea informativa che avrebbe prodotto il caricamento illecito del video, avrebbe poi dichiarato il contrario e cioè che, anche se l'informativa sulla privacy fosse stata fornita in modo chiaro e comprensibile, non si sarebbe potuto escludere che l'utente medesimo avrebbe caricato il file video incriminato commettendo il reato di diffamazione.
Io non sono affatto d'accordo con la dottrina dominante. Innanzitutto, il ragionamento del Giudice va considerato alla luce di una più ampia visione della disciplina di protezione dei dati personali che vede l'informativa non come mero adempimento burocratico, ma come vero e concreto elemento di base per un trattamento corretto. Per il giudice, infatti, l'inidonea informativa è indice di una totale e più ampia disattenzione nei confronti di tutta la disciplina. Disattenzione resa ancora più lampante dalla ricostruzione dell'insediamento in Italia di Google, che mai si era preoccupata di utilizzare i propri legali italiani anche ai fini della privacy, sostenendo che di tali adempimenti si dovesse occupare Google Inc., senza peraltro indicare a quest'ultima alla legge di quale Paese (visto che opera in 160 Paesi) si facesse effettivamente riferimento.
Sulla presunta contraddizione intendo far notare che il giudice ha evidenziato che non è conforme alla disciplina sulla privacy nascondere l'informativa nell'ambito delle condizioni generali, concretizzando tale comportamento una precisa volontà di minimizzare la disciplina ed anche una mancanza di correttezza nella comunicazione con gli utenti.
Non si vede, poi, alcuna contraddizione nelle affermazioni del giudice che, quando parla di inidonea ed inefficace informativa, intende propria significare che quest'ultima non avrebbe mai costretto l'utente a caricare i video con l'attenzione dovuta. Occorre rilevare che qui il Giudice analizza il concretizzarsi del reato di diffamazione e non di trattamento illecito già analizzato. In pratica, il reato di trattamento illecito di dati personali poteva realizzarsi anche qualora il video non fosse stato caricato, essendo lo stesso un reato di pericolo. La disciplina privacy è comportamentale: la sua violazione può realizzarsi semplicemente evitando o sapientemente aggirando le sue prescrizioni, indipendentemente dal verificarsi dell'evento dannoso. Infatti, la violazione di una misura minima di sicurezza comporta la conseguenza penale indipendentemente dal verificarsi dell'evento dannoso. Ai fini della diffamazione, invece, occorre il concretizzarsi del comportamento delittuoso che, nel caso di Google, sarebbe necessariamente derivato dal caricamento del video.
La conclusione, a mio modesto avviso, è che il giudice italiano abbia deciso correttamente.

3. Diritto all'oblio

Il diritto all'oblio è comunemente definito una particolare forma di garanzia che prevede la non diffondibilità di precedenti pregiudizievoli, con tali intendendosi propriamente i precedenti giudiziari di una persona. In base a questo principio, non è legittimo diffondere dati circa condanne ricevute o comunque altri dati sensibili di analogo argomento, salvo si tratti di casi particolari ricollegabili a fatti di cronaca.
Secondo il mio parere, invece, il diritto all'oblio si estende al diritto dell'interessato a non vedere riproposti all'infinito fatti, situazioni, immagini, a sé pregiudizievoli, anche non gravi e quindi non necessariamente a contenuto giudiziario, ma semplicemente non onorabili o comunque lesivi del proprio diritto alla riservatezza.
In tema di diritto all'oblio, si è assistito ad un illuminante provvedimento ad hoc del Garante: il diritto di cronaca è stato riconosciuto, ma con la consapevolezza che il motore di ricerca non ha nessun obbligo di informazione, non essendo la sua attività istituzionale, mentre l'utente non deve avere alcun diritto di aspettativa nei confronti del motore. In pratica, con questo provvedimento si inibisce una ricerca "facilitata" (dal motore) della notizia, ma non si inibisce la presenza della stessa nell'archivio storico del giornale.

RELAZIONE 2010

Nella Relazione 2010, presentata nel luglio del 2011, il Garante ha osservato che anche l'esame delle vicende concernenti il trattamento di dati personali in ambito giornalistico mette in luce gli effetti che su una fattispecie di tipo tradizionale produce l'attuale pervasivo dispiegarsi delle nuove tecnologie.
È infatti facile notare come, ormai, gran parte delle vicende giornalistiche portate all'attenzione del Garante concernono, più che i profili strettamente connessi alla verità ed alla correttezza delle informazioni, le modalità con le quali le stesse sono rese disponibili sulla rete Internet attraverso i siti delle testate giornalistiche con i quali molti dati vengono "captati" e fatti oggetto di cronaca.
Il catalogo degli esempi è molto vasto: dalle più recenti frontiere del giornalismo d'inchiesta che utilizza spesso microtelecamere nascoste per documentare fatti altrimenti difficilmente proponibili all'attenzione della pubblica opinione alla presenza dilagante di dati trattati dai social network, all'acquisizione ed al "rilancio" in chiave di cronaca di scambi di opinione all'interno di forum e blog, alla divulgazione del contenuto di sms fino alle ben note problematiche legate all'uso di materiali d'indagine depositati agli atti di procedimenti penali, fra cui le spesso copiose intercettazioni telefoniche messe sempre più frequentemente a disposizione anche nel formato audio.
Dimostrazione emblematica di questa realtà (relativa, cioè, alla potenza dei nuovi mezzi tecnologici che sfugge alla capacità di governo dei vari attori) è la problematica connessa alla messa a disposizione on-line, libera e gratuita, degli archivi storici dei quotidiani. La disponibilità sulla rete di questa enorme massa di informazioni (unita alla capacità di collegamento e di "aggregazione informatica" dei cd. "motori di ricerca") ha portato ad emersione i problemi connessi all'associazione di notizie ormai datate, in tanti casi contenenti riferimenti "negativi" a persone comuni che vedono ora "rilanciati" in rete episodi legati a fasi ormai lontane della propria esperienza di vita. Risulta evidente, sempre secondo il Garante, con il quale sono perfettamente d'accordo, che non è affatto facile equilibrare le iniziali finalità giornalistiche con le attuali finalità documentaristiche che legittimano l'ulteriore conservazione per fini storici e le esigenze di tutela di persone che possono legittimamente invocare l'oblio su vicende ormai non più attuali e lontane (anzi, spesso confliggenti) con il proprio attuale percorso di vita.
Nel 2010 l'orientamento del Garante non è cambiato ed il punto di equilibrio fra le contrapposte esigenze è stato trovato nel ricorso ai protocolli informatici che permettono di interdire l'indicizzazione automatica da parte dei motori di ricerca (quando le pubblicazioni on-line vengono riproposte nonostante il lungo tempo trascorso, la natura non pubblica del soggetto interessato, la lesività che l'informazione può comportare, la mancanza di interesse attuale alla diffusione giornalistica del dato, ecc.).
Ciò, ferma restando la conservazione integrale dei medesimi "pezzi" giornalistici sul sito Internet "sorgente", in modo da permettere comunque uno sguardo integrale su pubblicazioni storicamente avvenute e quindi non sottraibili alle esigenze della conservazione e dell'utilizzo a fini di ricerca storica e scientifica.

SENTENZA CORTE DI CASSAZIONE 5525 DEL 2012

Con la sentenza n. 5525/2012 la Corte di Cassazione afferma importanti novità sul riconoscimento del diritto all'oblio.
Il caso esaminato riguarda un esponente politico di un piccolo Comune lombardo, appartenente al Partito Socialista, arrestato per corruzione nel 1993, il quale, alla fine del procedimento giudiziario, viene prosciolto. Ciononostante, il politico lamentava che, successivamente, e per molti anni, attraverso una normale ricerca in rete, la notizia appariva on-line e, precisamente, nell'archivio web del "Corriere della Sera", con esclusivo riferimento all'arresto e senza nessun invece necessario riferimento all'epilogo favorevole della vicenda giudiziaria. La Suprema Corte ritiene il ricorso fondato e motiva la propria decisione con una complessa ed articolata disamina che illustra l'evoluzione del concetto di privacy in un'ottica non statica, ma dinamica e fa riferimento alle nuove implicazioni in rapporto alla cronaca giudiziaria.
In particolare, secondo la Corte, l'interessato ha diritto a che l'informazione oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale. In questo senso, gli è attribuito il diritto di conoscere in ogni momento chi possieda i suoi dati personali e come li utilizzi, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione ai sensi dell'art. 7 del Codice.
Sempre secondo la Corte, "se l'interesse pubblico sotteso al diritto all'informazione costituisce un limite al diritto fondamentale alla riservatezza, al soggetto cui i dati appartengono è correlativamente attribuito il diritto all'oblio e cioè a che non vengano ulteriormente divulgate notizie che, per il trascorrere del tempo, risultano ormai dimenticate o ignote alla generalità dei consociati". Solo se un fatto di cronaca assume rilevanza quale fatto storico ciò può giustificare la permanenza del dato, ma mediante la conservazione in archivi diversi (es. archivio storico) da quello in cui esso è stato originariamente collocato.
Allo scopo di tutelare l'identità sociale del soggetto cui si riferisce la notizia, bisogna garantire l'aggiornamento della stessa e cioè il collegamento ad altre informazioni successivamente pubblicate, concernenti l'evoluzione della vicenda, che possano completare o, addirittura, mutare il quadro sorto a seguito della notizia originaria. Secondo la Corte, detti principi vanno applicati anche ad Internet. È, infatti, pacifico che sul web le notizie non siano organizzate come in un archivio, ma presenti in maniera fondamentalmente caotica, senza alcuna modalità predeterminata. Il motore di ricerca è, nei fatti, un mero intermediario telematico che offre un sistema automatico di reperimento di dati ed informazioni attraverso parole chiave, senza alcuna pretesa di veridicità, né cronologica, né sostanziale.
Nel caso di specie, se l'interesse pubblico alla persistente conoscenza di un fatto avvenuto in epoca di molto anteriore trova giustificazione nell'attività politica svolta dall'interessato dei dati, e tale vicenda ha registrato una successiva evoluzione, non si può prescindere da quest'ultima, altrimenti la notizia diviene non aggiornata e, pertanto, sostanzialmente non vera. Questo compito di aggiornamento spetta al titolare del sito e non al motore di ricerca.
In caso di disaccordo tra le parti, spetta al giudice di merito individuare ed indicare le modalità da adottarsi in concreto per il conseguimento delle indicate finalità da parte del titolare dell'archivio.
È indubbio che questa sentenza susciti un certo scalpore, obbligando il titolare del sito fornitore delle notizie ad un costante aggiornamento delle stesse, al fine di evitare la violazione dei principi di cui all'art. 11 Codice Privacy (completezza, esattezza, aggiornamento, pertinenza, ecc.).

Proposta di Regolamento Europeo sulla Privacy

Sempre in tema di diritto all'oblio, si evidenzia che l'Unione Europea, nell'ambito di un più ampio progetto di riforma della privacy contenuta all'interno della proposta di regolamento del Parlamento Europeo e del Consiglio "concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati", presentata dalla Commissione lo scorso 25 gennaio (unitamente alla proposta di direttiva sulla "tutela delle persone fisiche con riguardo al trattamento dei dati personali") ha sancito che i cittadini europei hanno diritto al pieno controllo sui propri dati.
In particolare, la nuova proposta di Regolamento introduce due importanti articoli, il 16 ed il 17, i quali riguardano, rispettivamente, il Diritto di rettifica ed il Diritto all'oblio.
In base all'art. 16 (Diritto di rettifica) "L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica di dati personali inesatti. L'interessato ha il diritto di ottenere l'integrazione di dati personali incompleti, anche mediante una dichiarazione rettificativa". In base all'Articolo 17 (Diritto all'oblio) "L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia ad un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore, se sussiste uno dei motivi seguenti: a) i dati non sono più necessari rispetto alle finalità

per le quali sono stati raccolti o trattati; b) l'interessato revoca il consenso su cui si fonda il trattamento, oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattarli; c) l'interessato si oppone al trattamento di dati personali (salvo che il Titolare del trattamento dimostri l'esistenza di motivi preminenti e legittimi per procedere al trattamento); d) il trattamento dei dati non è conforme al presente regolamento salvo che il Titolare del trattamento dimostri l'esistenza di motivi preminenti e legittimi per procedere al trattamento (omissis).
Le nuove previsioni sembrano accogliere la tesi che sempre di più occorre tutelare l'interessato il quale, anche in seguito all'uso smodato di dispositivi mobili intelligenti, è costretto a vivere in uno stato virtuale permanente in cui sempre più spesso il suo privato diventa pubblico, non sempre con la dovuta consapevolezza. Ritengo, inoltre, corretto che, anche quando ciò sia potuto avvenire consapevolmente, ogni interessato abbia il diritto di poter intervenire allo scopo di riportare ciò che è divenuto pubblico nel proprio privato.

4. Social Network

Facebook, Youtube, MySpace, Netlog, Linkedin, Viadeo, Twitter sono i nomi di soltanto alcune delle più note piattaforme di social network, un fenomeno sociale e tecnologico di grande successo, sempre in crescita. Un servizio di social network consiste nella creazione e nella gestione di reti sociali on-line destinate a comunità di soggetti che condividono determinati interessi ed attività. Numerose sono le modalità di interazione fra gli utenti.
In tali siti abbondano informazioni fornite volontariamente. Naturalmente, i Garanti per la protezione dei dati personali si sono interessati al fenomeno.
Ad oggi, i documenti fondamentali che si occupano di questi strumenti sono il Memorandum di Roma del marzo del 2009, la Risoluzione di Strasburgo dell'ottobre del 2009 ed il parere sui Social Network del Gruppo ex art. 29.
Nel Memorandum di Roma si legge "Mentre le norme "tradizionali" in materia di privacy vertono sulla definizione di regole che tutelino i cittadini dal trattamento sleale o sproporzionato dei loro dati personali, vi sono pochissime norme che disciplinino la pubblicazione di dati personali su iniziativa dei singoli". Il Memorandum spiega "siamo dinanzi ad una nuova generazione di utenti. Si tratta della prima generazione cresciuta con Internet. Questi indigeni digitali hanno sviluppato approcci peculiari rispetto all'utilizzo dei servizi Internet ed al concetto di privato ovvero pubblico". Inoltre, essendo in buona parte adolescenti, sono probabilmente più disposti a mettere a rischio la propria privacy rispetto agli "immigrati digitali" con qualche anno di più.

Rischi dei Social Network

· Niente oblio su Internet.

Il concetto di oblio non esiste su Internet. I dati, una volta pubblicati, possono rimanerci per sempre – anche se sono cancellati dal sito "originario", possono esisterne copie presso soggetti terzi -. Inoltre, alcuni fornitori di servizi rifiutano di ottemperare (o non ottemperano affatto) alle richieste degli utenti di ottenere la cancellazione di dati e di interi profili.

· L'idea ingannevole di "comunità".

Il parallelo in realtà non regge perché nel cyberspazio la comunità può essere assai estesa.

· La raccolta di dati di traffico da parte dei fornitori di servizi di social network, i quali possiedono gli strumenti tecnici per registrare ogni singolo passo dell'utente sul loro sito e comunicare a terzi dati personali (di traffico) compresi gli indirizzi IP e i dati sull'ubicazione.
Ciò può avvenire, ad esempio, per finalità pubblicitarie, anche di tipo mirato.

· Rivelare più informazioni personali di quanto si creda.

Ciò accade molto spesso, soprattutto con riferimento alle fotografie.

· Utilizzo improprio dei profili utente da parte di soggetti terzi.

Si tratta, probabilmente, del rischio potenziale più grave per i dati personali. A seconda della configurazione (di default) sulla privacy e dell'utilizzo o meno di tale configurazione da parte degli utenti, i contenuti diventano accessibili, nel peggiore dei casi, all'intera comunità. Allo stesso tempo, sono assai scarse le salvaguardie oggi disponibili rispetto alla copia dei dati contenuti nei profili ed al loro utilizzo per costruire profili personali e/o ripubblicare tali dati.
Tuttavia, anche l'utilizzo "normale" dei dati contenuti nei profili può incidere gravemente sulle loro possibilità di carriera. Un esempio riguarda l'abitudine da parte dei dirigenti del personale di società di consultare i profili dei candidati all'assunzione e/o dei dipendenti. Sembrerebbe che già oggi i due terzi dei dirigenti ammettano di utilizzare i dati ricavati da servizi di social network per verificare e/o completare i curricula dei candidati.

Alla luce delle considerazioni svolte, il Gruppo di lavoro ex art. 29 della Direttiva 46/95 ha formulato diverse raccomandazioni:

1) Prevedere la possibilità di ricorrere a pseudonimi (a mio parere abbastanza inutile nell'ottica di funzionamento dei social network);
2) Obbligare i fornitori ad adottare un approccio trasparente nell'indicare le informazioni necessarie per accedere al servizio;
3) Introdurre l'obbligo di notifica di eventuali violazioni dei dati;
4) Potenziare le tematiche connesse alla privacy nel sistema educativo;
5) Garantire la massima trasparenza nell'informare gli utenti. Occorre ripensare alle modalità con cui si informano gli utenti. Oggi l'informativa fa parte generalmente delle "condizioni di prestazione del servizio", che solo una bassissima percentuale degli utenti scarica veramente;
6) L'informativa resa all'utente deve prendere in considerazione anche i dati relativi a soggetti terzi, indicando anche ciò che agli utenti è permesso fare con i dati relativi a terzi eventualmente contenuti nei profili. Particolare importanza rivestono le foto che in grandi quantità figurano nei profili-utente e mostrano spesso altre persone (spesso indicate con nome e cognome);
7) Prevedere impostazioni di default orientate alla privacy. È noto che soltanto una minoranza degli utenti che si iscrivono ad un servizio modifica le impostazioni di default relative alla privacy. Dovrebbe, invece, essere obbligatorio per i fornitori selezionare impostazioni che offrano per default un livello elevato di privacy. In ogni caso, per default non dovrebbe essere consentita l'indicizzazione dei profili-utente da parte dei motori di ricerca;
8) Migliorare il controllo da parte degli utenti sull'utilizzo dei dati contenuti nei loro profili;
9) Creare strumenti che consentano agli utenti di controllare l'utilizzo dei dati contenuti nei loro profili da parte di soggetti terzi;
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.

Susanna Svaluto
Università di Padova - Facoltà di Scienze Politiche, Relazioni Internazionali e Diritti Umani

Una convivenza forzata

La questione della privacy era vissuta, alla fine degli anni '90, come un attacco alla libertà di stampa e lo stesso sentimento è ricomparso con la discussione del decreto legge 259 del 2006, il quale ha suscitato ampie critiche in relazione al tema delle intercettazioni.

Nel 1996 viene istituita la figura del Garante della Privacy, la cui azione è volta a promuovere e a garantire la tutela dei dati personali in qualsiasi ambito. L'evoluzione del suo ruolo nel giornalismo è riassunta nel documento " Privacy e giornalismo", un progetto nel quale si ripercorrono le tappe che sanciscono il rapporto tra diritto di privacy e libertà di stampa. Il Garante rappresenta, inoltre, il simbolo dello sviluppo di una cultura e di una società sempre più consapevole dei propri diritti e, di conseguenza, sempre più decisa a farli valere.

Il rapporto tra libertà d'informazione e tutela della privacy presenta un confine molto labile e, spesso, sfocia in un conflitto. È abbastanza diffusa l'opinione che ad una maggiore tutela della riservatezza si accompagni un'attività di censura più o meno grave, anche se nessuna richiesta di censura è mai stata accolta, secondo quanto è riferito nel documento "Privacy e giornalismo", a cura di Mauro Paissan. La questione libertà di stampa / diritto di privacy iniziò ad essere effettivamente disciplinata negli anni '90. Mentre in molti Paesi europei una legge sulla protezione dei dati personali era già stata promulgata, prima fra tutte la Germania, nel 1970, in Italia ciò è avvenuto con l'approvazione della legge n. 675 del 31/12/1996, solo a seguito di un richiamo da parte dell'Unione Europea. A questo proposito, tale ritardo fece scaturire come pena la temporanea esclusione dall'Accordo di Schengen. La legge, entrata in vigore l'anno successivo, prevedeva, peraltro, l'istituzione del Garante della Privacy. Questa figura, che trova il suo corrispettivo anche a livello europeo (GEPD), si pone come intermediario tra coloro che ritengono di aver subito una lesione del diritto di privacy e coloro che, al contrario, dovrebbero averlo violato. Per quanto riguarda i mezzi d'informazione, l'istituzione del Garante interrompe un po' quella che era una prassi tipica, cioè ritenere il mondo del giornalismo al di fuori di queste dinamiche ed esente da sanzioni. I giornalisti godevano, infatti, di un'ampia libertà. In riferimento a questo ruolo, è importante sottolineare l'introduzione del Codice deontologico del 1998, che rappresenta un documento nel quale sono fissate le linee guida dell'attività di giornalisti e non: vi sono ricompresi, infatti, anche coloro che risultano iscritti nell'elenco dei pubblicisti e dei praticanti. Di conseguenza, sono soggetti al Codice anche coloro che, in maniera occasionale, tramite articoli, saggi, ma anche fotografie, esprimono una "manifestazione di pensiero". Il Codice è stato pensato, innanzitutto, per adeguarsi ad una normativa europea vigente, ma, allo stesso tempo, con lo scopo di porre dei principi che non si limitassero a dettare delle regole interne, la cui violazione sarebbe stata oggetto di mere sanzioni disciplinari da parte dell'Ordine, ma una vera fonte giuridica applicabile ad ogni persona intenzionata a fare informazione.
La legge 675/96 è stata abrogata, ma il suo contenuto è confluito nel Codice della Privacy, istituito con il D. Lgs. 196/2003. In esso sono disciplinati, oltre alle regole generali per il trattamento dei dati e le disposizioni specifiche per i singoli settori (giudiziario, sanitario, giornalistico, ecc.), anche i diritti e le modalità a cui l'interessato può far riferimento nell'ipotesi di trattamento illegittimo dei suoi dati.
Le norme internazionali, come evidenziato, giocarono un ruolo rilevante nell'evoluzione della legislazione interna. L'ordinamento italiano, infatti, rimanda alla Convenzione dei diritti e delle libertà fondamentali del 1950, la quale evidenzia la possibilità di limitare la libertà d'espressione in quanto "l'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario." (art. 10.2).
La normativa è tuttora in evoluzione a fronte anche della diffusione di altri mezzi di comunicazione, come internet. L'attività legislativa in questo ambito era vissuta, alla fine degli anni '90, come un attacco alla libertà di stampa e lo stesso sentimento è ricomparso con la discussione del decreto legge 259 del 2006, il quale ha suscitato ampie critiche in relazione al tema delle intercettazioni. La questione che si poneva, e che si pone tuttora (sono attualmente in discussione altri disegni di legge al riguardo), concerne il fatto se queste debbano essere pubblicate o meno e, in caso affermativo, in che momento e in che quantità. La disputa, sorta nel 2006, si soffermava sugli ultimi due quesiti. Il Garante aveva dovuto più volte richiamare i mezzi d'informazione

in seguito alla pubblicazione di intercettazioni che non rispettavano i limiti imposti dalla legge. Più volte era, infatti, capitato che le conversazioni pubblicate comprendessero dialoghi tra l'indagato e terzi estranei al fatto, o che venissero pubblicate prima che il sospettato avesse ricevuto l'informazione di garanzia. In ragione di queste diverse violazioni, il Garante, con la decisione 1299615 del 26 gennaio 2006, ha disposto che "nel riportare le trascrizioni di intercettazioni telefoniche, i mezzi di informazione devono valutare più attentamente l'effettiva essenzialità di quanto pubblicato". Quindi, quello che si ritiene importante nella trascrizione di una notizia è che essa si limiti il più possibile all'enunciazione dell'essenziale. Tuttavia, il pubblico appare sempre più interessato agli aspetti scandalistici di un fatto pubblicato, sia esso politico, di cronaca o di spettacolo. L'attenzione sembra diretta più alla vita personale dei soggetti pubblici piuttosto che al ruolo che ricoprono nella società, e diventa ancora più elevata attorno a questioni scabrose. Vi è proprio una continua ricerca dello scandalo. Così, per quanto riguarda i fatti di cronaca, questo "desiderio di conoscenza" viene saziato con l'organizzazione di autobus diretti a vedere il "mostro" che ha ucciso Sarah Scazzi, mentre, in politica, con il passare in rassegna tutti i numeri di "burlesque" avvenuti in casa Berlusconi. È quanto di più lontano dall'"essenzialità" dell'informazione. Si crea un circolo vizioso: i giornalisti si concentrano sempre più sugli aspetti privati dei soggetti "credendo" sia questo che il pubblico richiede. I politici, dal canto loro, rimangono coinvolti in dibattiti sulla rettitudine morale che dovrebbe loro appartenere, e il pubblico si nutre di questa mala informazione venendo accusato di essere esso stesso a richiederla. Purtroppo, è difficile stabilire chi abbia "cominciato il gioco", se quindi sia il pubblico ad essere interessato solo alla vita personale e, di conseguenza, giornalisti e politici si adeguino, o se siano i giornalisti ad aver deciso che la vita privata debba essere condivisa e giudicata da tutti, ovvero, se siano piuttosto i politici a ricercare dei diversivi per intrattenere popolo e giornali e distrarli dalle questioni veramente importanti. In realtà, poco importa come si sia evoluta la situazione, le conseguenze sono negative per tutte le parti in gioco. Con questo atteggiamento, sia la classe politica, sia la classe giornalistica, suscitano nel popolo un sentimento di sfiducia che ha condotto ad una riconsiderazione in senso negativo del loro ruolo.

Per rispondere alla legge delle vendite, dell'audience, dello scandalo a tutti i costi, diversi giornalisti si sono dimenticati che il loro compito, oltre che informare, è anche quello di educare. Nel ruolo che rivestono, non si limitano a riferire la notizia, non compiono un lavoro neutro. Lo dimostra, in primo luogo, il fatto che sono loro stessi a decidere cosa diventerà notizia, cosa sia, quindi, rilevante e cosa possa, invece, rimanere in disparte. Nella stesura di un articolo, poi, a seconda delle scelte stilistiche, linguistiche e di contenuto, si traccia una direzione d'interpretazione. Questo tipo di influenza appare evidente nei fatti di cronaca. Se si prendono in considerazione casi come quelli avvenuti a Garlasco, Cogne, Perugia, l'influenza dei giornalisti risulta notevole. Le parole utilizzate per descrivere le situazioni trasformano ipotesi in sentenze. Così, un indagato diventa un probabile colpevole. Al fine di sostenere la tesi, si cercano incongruenze dove non ve ne sono, si scava a fondo cercando degli indizi di colpevolezza senza preoccuparsi dei limiti da rispettare, senza ipotizzare, anche solo per un secondo, che la persona di cui si sta invadendo la sfera privata senza remore possa essere innocente. E tanto più accanimento e sforzo viene impiegato nella ricerca di qualche scheletro nell'armadio, tanto meno impegno affiora nel ristabilire la reputazione di un uomo dichiarato, infine, innocente. Questa usurpazione di diritti non può rimanere impunita. La libertà di un individuo finisce dove inizia quella di un altro. Anche la libertà di stampa ha un limite che non deve essere avvertito come censura, ma quale diritto ad avere una buona stampa, a ricevere un'informazione che non si "compiaccia" davanti al "disastro umano". A tale proposito, qualcuno che poteva essere definito un rivoluzionario, qualcuno che, indubbiamente, della libertà di parola aveva fatto il suo pane quotidiano, e che, proprio per la sua irriverenza, era stato censurato, in una canzone tra le più entusiasmanti, rivolto ai giornalisti, affermava: "avete troppa sete e non sapete approfittare delle libertà che avete, avete ancora la libertà di pensare, ma quello non lo fate e in cambio pretendete la libertà di scrivere". Era Giorgio Gaber.

Michele Iaselli
Presidente Associazione nazionale difesa privacy

Diritto all'oblio

Mettere i propri dati a disposizione del mondo intero comporta rischi che nessuno espone chiaramente, in particolare ai giovani che saranno i primi a pagare il conto di una società grossolanamente globalizzata.

Diverse sono ormai le definizioni o, meglio ancora, i significati attribuiti dalla dottrina del diritto all'oblio, concetto tornato prepotentemente alla ribalta in ambito internazionale, e principalmente europeo, con l'avvento della Rete.

In sintesi, possiamo definire il diritto all'oblio come il diritto di un individuo ad essere dimenticato, meglio, a non essere più ricordato per fatti che in passato furono oggetto di cronaca. Il suo presupposto è che l'interesse pubblico alla conoscenza di un fatto è racchiuso in quello spazio temporale necessario ad informarne la collettività e che, con il trascorrere del tempo, si affievolisce fino a scomparire. In pratica, con il trascorrere del tempo, il fatto cessa di essere oggetto di cronaca per riacquisire l'originaria natura di fatto privato(1).

In realtà, l'oblio è un diritto che va oltre la tutela della privacy e che, ad oggi, non trova ancora legittimazione nell'ordinamento nazionale ed europeo.

Frutto di elaborazioni dottrinarie, giurisprudenziali (2) e principalmente delle Autorità Garanti europee, è da intendersi quale diritto dell'individuo ad essere dimenticato; diritto che mira a salvaguardare il riserbo imposto dal tempo ad un notizia già resa di dominio pubblico.

Come fondamento normativo del diritto all'oblio, il nostro Codice della Privacy prevede che il trattamento non sia legittimo qualora i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo superiore a quello necessario agli scopi per i quali sono stati raccolti o trattati (art. 11 D.Lgs. n. 196/2003). Lo stesso interessato ha il diritto di conoscere, in ogni momento, chi possieda i suoi dati personali e come li adoperi, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione (art. 7 D.Lgs. n. 196/2003).

Storicamente, il problema del diritto all'oblio nasce in rapporto all'esercizio del diritto di cronaca giornalistica. Presupposto perché un fatto privato possa divenire legittimamente oggetto di cronaca è l'interesse pubblico alla notizia. La collettività va informata con tempestività, in modo da poter conoscere l'accaduto in tempo reale e con completezza, così da fornirle una visione chiara del fatto. Se viene scoperto un giro di corruzione, è possibile che la notizia debba essere divulgata a più riprese, secondo gli sviluppi graduali della vicenda. Il pubblico dovrà conoscere i soggetti coinvolti nella vicenda, la loro posizione istituzionale, in cosa consistevano i "favori" eseguiti in cambio di denaro, le conseguenze del reato sul funzionamento dell'istituzione interessata e sulla pelle dei cittadini onesti, ecc. Poi, potranno seguire dibattiti sulla vicenda. La diffusione della notizia dovrà, insomma, perdurare necessariamente nel tempo. Ma, una volta che del fatto il pubblico sia stato informato con completezza, cessa l'interesse pubblico, in quanto la collettività ha ormai acquisito il fatto. Non vi è più una notizia. Riproporre l'accadimento sarebbe inutile poiché non sussisterebbe più un reale interesse della collettività da soddisfare. Non solo inutile per la collettività, ma anche dannoso per i protagonisti in negativo della vicenda. Qui la reputazione dei soggetti subirebbe un'ulteriore lesione. E se la lesione è inizialmente giustificata dall'esigenza di informare il pubblico su fatti nuovi, non lo è più dopo che la notizia risulta ampiamente acquisita. A partire dalla sua completa acquisizione, sorgono i presupposti del diritto all'oblio (3).

Il diritto all'oblio è, quindi, la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca. Come non va divulgato il fatto la cui diffusione (lesiva) non risponda ad un reale interesse pubblico, così non va riproposta la vecchia notizia (lesiva) quando ciò non sia più rispondente ad un'attuale esigenza informativa.

Ma, indubbiamente, l'attività giornalistica è stata modificata dallo sviluppo di Internet. La possibilità di raccogliere, incrociare, scambiare ed archiviare informazioni personali si è enormemente accresciuta, consentendo una straordinaria circolazione e diffusione di conoscenze e di opinioni. Questo ha reso anche estremamente difficile esercitare un controllo sulla qualità delle informazioni personali diffuse. In rete circolano notizie vere, non vere, vere solo parzialmente, notizie talmente vecchie la cui riproposizione pone seri problemi all'interessato (4).

Ogni giorno, milioni di utenti devono difendere la propria reputazione elettronica spesso non conoscendone modalità, leggi e contromisure necessarie.

Mettere i propri dati a disposizione del mondo intero comporta rischi che nessuno espone chiaramente, in particolare ai giovani che saranno i primi a pagare il conto di una società grossolanamente globalizzata.

Dopo aver visionato i curriculum forniti dagli aspiranti ad un posto di lavoro, la maggior parte delle aziende effettua controlli incrociati sui social network, "spiando" le abitudini quotidiane degli ignari candidati, i quali, innocentemente, eccedono spesso nella trasparenza delle loro biografie.

Il desiderio di apparire, stupire ed essere protagonisti ad ogni costo si trasforma in un'arma pericolosa e la schedatura volontaria di massa garantisce ai massimi sistemi accurate indagini di mercato ed analisi com-

portamentali vendute a carissimo prezzo alle multinazionali di produzione.
Le legittime richieste di cancellazione o aggiornamento devono anche tener conto dei diversi luoghi virtuali in cui tali informazioni compaiono: sul sito, sulla copia cache della pagina web, sui titoletti che costituiscono il risultato dell'estrazione tramite motore di ricerca. Ognuno di questi luoghi ha un titolare di trattamento diverso e, per i gestori dei motori di ricerca extraeuropei, c'è l'ostacolo della disciplina applicabile. Una volta entrati nel circuito elettronico della rete, insomma, è davvero difficile far valere i propri diritti (5).
L'applicazione di questi principi, riconosciuti ormai anche a livello di Costituzione europea, trova ostacoli seri, a volte anche di difficile soluzione, quando il trattamento dei dati personali avviene sul web. Ed è proprio in ambito comunitario che, di recente, è stata affrontata la problematica del diritto all'oblio. Il 25 gennaio scorso, la Commissione ha proposto una riforma globale della normativa UE del 1995 in materia di protezione dei dati che contiene, fra le altre misure, anche quella del cosiddetto ''diritto all'oblio'': chiunque potrà cancellare definitivamente dal web i propri dati se non sussistano motivi legittimi per mantenerli.
In particolare, la riforma punta a creare un insieme di norme stabile e coerente che permetta, da una parte, la crescita del business virtuale nel Vecchio Continente (''i dati personali sono la valuta del mercato digitale'', ha affermato la Reding in conferenza stampa) e, dall'altra, di tutelare al meglio la privacy degli utenti sul web.
La proposta si articola in una direttiva e in un regolamento e prevede sanzioni fino ad un milione di euro o fino al 2% del fatturato di un'azienda. Passerà ora al vaglio del Parlamento europeo e dei singoli Stati.
Tra coloro sui quali la norma avrà certamente un impatto ci sono i social network: da oggi, spetterà a loro l'onere di provare che la conservazione di una certa informazione è necessaria e non all'utente dimostrare il contrario.
A questo punto, dopo aver esaminato diversi aspetti del diritto all'oblio, avuto riferimento in particolare al mondo della Rete, è opportuno capire quale sia il vero significato di tale diritto. La richiesta del riconoscimento del diritto all'oblio ci porta ad affrontare questioni non solo tecniche, ma anche di carattere sociale ed umano. Confondere privacy e diritto all'oblio è un rischio, soprattutto se fatto con lo spirito di promuovere un tema importante: quello della consapevolezza di come i nostri dati vengano utilizzati dagli attori che gestiscono i servizi da noi quotidianamente sfruttati. Come ben sappiamo, Facebook, Twitter, Google, ecc. sono ben lungi dall'offrire, come moderni benefattori digitali, servizi gratuiti ai loro utenti. Tutt'altro: l'accesso a Facebook, la mail di Google, l'uso di Twitter sono pagati a caro prezzo. Da tempo questi colossi del web stanno annunciando nuove regole della privacy che, guarda caso, sembrano "particolarmente" rispettose dei diritti degli utenti. Ma, come è noto, la stessa Unione Europea ha manifestato una certa diffidenza verso queste politiche di privacy. D'altronde, come si può pensare che, in questo particolare periodo storico, colossi come Google, Facebook, Yahoo! possano rinunciare all'immenso patrimonio a loro disposizione costituito da milioni di dati personali spendibili per soddisfare le esigenze di marketing di milioni di aziende? È chiaro che questa grande pubblicità del cambiamento serve per illudere su una trasformazione che non potrà mai esserci, anche se si farà di tutto per farla sembrare tale. Provider come Google mettono a disposizione degli utenti tantissimi servizi e sarà fin troppo facile ottenere il consenso ad utilizzare i dati personali dei navigatori in cambio di qualche utile applicazione. Non possiamo pensare che Google non approfitti della situazione. Il problema è che questo consenso non sarà sempre consapevole. Spesso, sarà conseguente ad un'informativa non troppo chiara o, comunque, troppo generica. In tale ottica, è tutto molto semplice: alcuni operatori ci offrono dei servizi e noi li paghiamo con delle informazioni. A complicare le cose, non è il fatto in sé, quanto, piuttosto, la constatazione che, spesso, le persone che usano tali servizi lo fanno nella beata convinzione di usare servizi gratuiti. Ed è questo il vero problema. Non percepire la contropartita composta dal valore delle proprie informazioni. La privacy rappresenta, quindi, il sacrosanto diritto alla riservatezza che si esprime nella possibilità di scegliere se condividere o meno le proprie informazioni personali; il diritto all'oblio rappresenta, invece, quel fenomeno per il quale, dopo averle condivise, quelle informazioni, prima o poi, debbano scomparire. E, nell'era di Internet, quel "poi" è posto sempre più in là. Ma, mentre la privacy è un diritto (pur mutevole nel tempo) di valore assoluto, può dirsi lo stesso del "diritto" all'oblio?

(1) FINOCCHIARO G., La memoria della Rete ed il diritto all'oblio, in Il diritto dell'informazione e dell'informatica, Milano, 3/2010
(2) In Italia assumono rilevanza alcune decisioni della Corte di Cassazione come Cass., 9/4/1998, n. 3679; Cass., 25/6/2004, n. 11864 e, da ultimo, Cass., 05/04/2012, n. 5525
(3) http://www.difesadellinformazione.com/113/il-diritto-all-oblio/
(4) FIDELIO A.- GUASTELLA S., Motori di ricerca e diritto all'oblio in Rivista di diritto, economia e gestione delle nuove tecnologie, Milano, 4/2005
(5) PAISSAN M., "Privacy e Giornalismo", Roma, 2008

Luca Bolognini
Avvocato, Presidente dell'Istituto Italiano per la Privacy

Una questione informatica

Siamo nelle mani degli algoritmi. Formule di calcolo, stabilite a priori da qualche ottimo programmatore, che organizzano, indicizzano, ordinano le informazioni. L'"automatizzazione" della gestione dei dati rischia di produrre impatti pesanti sulla dignità e sulla libertà degli individui.

Potrà piacere o meno, come idea, ma siamo fatti anche di dati, cioè elementi non "nostri". Elementi altrui, terzi, come le ombre che non ci appartengono, ma che ci rappresentano, in qualche modo, sul muro. Dopo il soma e la psiche, la terza dimensione è l'informazione che ci proietta verso (e ci fa relazionare con) l'esterno. La "privacy", allora, potrebbe essere intesa, in senso lato, come una "disciplina giuridica del Sé" (non me ne vogliano gli psicoanalisti, licenza poetica). Tant'è. Sta di fatto che, ormai, l'identità personale è composta anche (se non solo, vista da fuori) dai dati che circolano e sono reperibili su di noi e malgrado noi: non conta la sostanza, a volte, e nemmeno l'apparenza che diamo di noi stessi, se l'apparenza organizzata da altri soggetti (motori di ricerca, in primis) ci assegna una diversa misura, qualità, immagine e fama. Puoi dire quello che vuoi di te, ma, alla fine, ciò che conta sarà il "quadretto" di informazioni reso disponibile dal motore di ricerca e non da te. Stiamo parlando di identità sociale, ma anche di identità civile.

Siamo nelle mani degli algoritmi (bene ne ha parlato, di recente, anche Evgeny Morozov). Formule di calcolo, stabilite a priori da qualche ottimo programmatore, che organizzano, indicizzano, ordinano le informazioni. C'è una bella differenza se la notizia di un convegno a cui hai partecipato come relatore si trova in prima o in sesta pagina dei risultati, in una ricerca su Internet. Così come il massimo rilievo, primo risultato, assegnato a quella foto in cui festeggiavi un compleanno con un cappello da stregone in testa e il sigaro in bocca potrebbe mettere in secondo piano il fatto che sei un serissimo professore universitario di medicina.
Al di là delle ironie, questa "automatizzazione" della gestione dei dati rischia di produrre impatti pesanti sia sulla dignità e sulla libertà degli individui, in relazione al trattamento di dati che li riguardano come soggetti passivi, sia, al contrario, sulla loro capacità di informarsi come soggetti attivi. Andiamo con ordine, cercando di chiarire con semplicità perché si rivelino dei rischi, che andrebbero affrontati e ridotti con lungimiranza.

Libertà e dignità, prima di tutto. In un suo editoriale italiano, Morozov citava il caso della cosiddetta "polizia predittiva", la tecnica, sempre più diffusa tra le autorità che svolgono indagini e si occupano della pubblica sicurezza in molti Paesi del mondo, non solo in quelli più sviluppati, grazie alla quale si riesce a prevedere statisticamente quali siano le zone (territoriali, per esempio i quartieri) più colpite da quali crimini, o chi siano gli individui più propensi a delinquere e dunque da tenere sotto controllo, e così via. Queste "predizioni" non sono frutto di portentose sfere di cristallo messe davanti a magici ispettori, bensì (solo) risultati di calcoli automatizzati basati su algoritmi complessi. Questi algoritmi consentono alla polizia di elaborare miliardi di dati, effettuare profilazioni e stabilire gradi di probabilità o tendenze. In sostanza, come giustamente ricordava Morozov in quell'articolo, la polizia non fa altro che applicare alla sicurezza ciò che i grandi operatori del web applicano da anni ai consumatori on-line, analizzando le loro navigazioni e preferenze, e pronosticando (invogliando, personalizzando) i loro acquisti futuri.
Internet, per questo tipo di analisi predittive, è lo strumento perfetto: per questa ragione si stanno facendo strada accordi tra grandi operatori privati (social networks, motori, provider di vario genere) ed autorità di polizia dei vari Paesi interessati. In poche parole, al social network viene delegata una parte di attività di polizia, e tutti quanti veniamo analizzati e profilati in automatico, non solo per scopi commerciali, ma anche per capire se siamo dei (potenziali?) criminali. Tutto ciò avviene in silenzio e spesso non ce ne accorgiamo. Beninteso, gli obiettivi di sconfiggere pedofilia, terrorismo e altre atrocità sono irrinunciabili e sarebbe scellerato metterli in discussione, ma ogni azione di prevenzione e contrasto deve muoversi nel rispetto dei diritti fondamentali dell'essere umano.
La Storia ha insegnato quanto le profilazioni siano pericolose, anche (o a maggior ragione) se legate a chissà quali buone intenzioni. Una profilazione automatizzata, per funzionare, ha bisogno di tre fasi fondamentali: la prima, in cui è necessario raccogliere la massima quantità e qualità di dati relativi ad ogni singolo individuo (che significa archiviare una miriade di informazioni precise e contestualizzate su gusti, preferenze, idee, spostamenti, ecc., cioè formare un dossier di per sé "esplosivo" per la dignità e la libertà di una persona). La seconda fase è quella dell'elaborazione di questa miriade di dati, che avviene grazie ad un software che ragiona sulla base del (famigerato) algoritmo predeterminato da "qualcuno". La terza fase, rischiosa per la dignità, soprattutto, consiste nella riconduzione di quello specifico individuo, unico ed irripetibile come ogni persona umana, ad un "profilo" più generale, meno unico, appunto, al quale apparterranno anche altri individui. In questa terza fase si semplifica l'identità del singolo e lo si "assegna" ad un gruppo più vasto di soggetti, così forzando e superando la sua speciale peculiarità.

Se immaginiamo che tutto questo venga svolto da un'impresa privata per il solo scopo di fornirci pubblicità personalizzata, dopotutto non ci allarmiamo più di tanto (sebbene questo continuo "ricevere indietro in offerta" ciò che noi già amiamo e preferiamo potrebbe non rivelarsi un toccasana per l'evoluzione). Se pensiamo che siano gli Stati, con le loro polizie, a sviluppare queste analisi, qualche timore in più lo sentiamo crescere in noi. Se, poi, veniamo a sapere che la polizia di uno Stato ha sottoscritto un accordo con questo o quel social network o motore di ricerca, delegando ai privati la funzione di analizzarci e profilarci per finalità di pubblica sicurezza, quel brivido diventa febbre. In Democrazia, tutto questo non può e non deve accadere senza che vi sia totale trasparenza pubblica, sia sugli accordi, sia sugli algoritmi utilizzati, ovviamente. Di più, aggiungo io, senza che vi sia l'ordine di un magistrato che con-

senta alle polizie di effettuare, magari con l'aiuto dei privati, siffatte analisi profilanti sul web. La febbre sale, e di molto, se pensiamo che certe "alleanze" tra grandi operatori privati di Internet e delle telecomunicazioni potrebbero stringersi anche in Paesi non democratici, dittatoriali, spesso incuranti dei diritti umani (scenario reso ancora più realistico dalla prospettiva, a mio parere non auspicabile, che al prossimo ITU di Dubai, dicembre 2012, la governance di Internet finisca per cadere sotto la competenza dell'ONU).

Venendo al secondo ordine d'impatti, quello che vede l'individuo come soggetto attivo e capace di informarsi su ciò che è "altro da sé", come direbbe Baudrillard, il tema appare altrettanto rilevante. Un algoritmo di un motore di ricerca o di un social network – pur non assurgendo questi ad attività editoriali, poiché non creano, né modificano i contenuti organizzati prodotti da altri utenti – può comunque dipingere un quadro non necessariamente oggettivo della realtà: potrebbe dare più peso e maggiore visibilità ad un dato piuttosto che ad un altro; potrebbe condannare all'oblio una notizia e renderne immortale un'altra; potrebbe mostrare una critica cento risultati prima di un'altra di senso opposto. Potrebbe, un algoritmo, intervenire sulla cultura diffusa, favorendo o sfavorendo linee di pensiero, politiche, economiche o filosofiche. Che strumento formidabile di pressione sul popolo, se intervenissero (il congiuntivo imperfetto è ironico) degli accordi tra questo o quel Paese non democratici ed un motore di ricerca: gli utenti formerebbero le proprie coscienze vedendo solo certi risultati e non altri, o almeno alcuni dati prima e meglio di altri. I cittadini conoscerebbero l'identità di altre persone (per esempio, oppositori a questo o a quel regime) secondo un quadro composto da informazioni incomplete o viziate. La libertà di informazione (che è libertà di informarsi e di informare, anche su di sé) sarebbe, insomma, prigioniera.

Una possibile soluzione a questi problemi, ma solo in contesti democratici, potrebbe essere la "certificazione degli algoritmi": nessuna "disclosure" indiscriminata, nessuna pubblicazione degli algoritmi delle imprese private (quelli usati dalle polizie, invece, sì, andrebbero resi pubblici e trasparenti), quindi nessuna violazione dei segreti e dei vantaggi concorrenziali. Basterebbe solo l'obbligo di sottoporre gli algoritmi via via adottati, nel segreto amministrativo, alle autorità garanti per la data protection dei vari Paesi, così da farne valutare l'effettiva neutralità informativa. Se i big di Internet si rendessero "parti diligenti" in quest'ottica, otterrebbero due risultati in un colpo solo: allontanerebbero dagli Stati la tentazione di considerare i motori di ricerca ed i social network dei veri e propri editori, cosa che non sono, e, insieme, darebbero esempio di affidabilità ai propri utenti.

Già, perché non solo gli individui e le persone accusano problemi di identità nel mondo tecnologico: anche le nuove imprese, in particolare quelle che trattano dati e operano sul web, vengono spesso comprese – in particolare dai regolatori pubblici – per ciò che non sono e non possono essere. Poliziotti virtuali, per esempio.

Sempre in tema di algoritmi che elaborano dati personali, molto ha fatto discutere in Italia, di recente, l'istituzione o, meglio, il potenziamento del sistema informatico di analisi delle spese e dei movimenti di conto corrente per finalità di contrasto all'evasione fiscale, introdotto con un decreto del dicembre 2011. Si tratta di una norma che legittima l'amministrazione fiscale ad elaborare automaticamente i dati di entrate ed uscite bancarie e le transazioni elettroniche di tutti i cittadini. Grazie a questo sistema, si punta a trovare incongruenze che conducano a scovare evasori fiscali. In sostanza, la norma legittima lo Stato italiano a monitorare ed a setacciare i movimenti finanziari privati di chiunque, automaticamente ed a priori. Si mettono sotto controllo tutti per acciuffare alcuni furbi. L'emergenza dell'evasione, in Italia, è tale da far tollerare all'opinione pubblica ed alla politica quello che, a giudizio di chi scrive, sembra comunque un grande errore, malgrado i fini nobili, per eccesso di sproporzione nel trattamento dei dati dei cittadini e per la mancanza di una "data di scadenza" entro la quale far cessare questa misura invasiva ed eccezionale.

C'è un articolo "salva-libertà" nella Direttiva europea del '95 in materia di protezione dei dati personali: riconosce a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o eserciti effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc. Una siffatta decisione, basata su questo genere di trattamenti, tra i quali rientrano tutte le profilazioni automatizzate, può essere assunta solo se autorizzata da una legge che precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata. Quell'articolo è recepito nell'art.14 del nostro Codice della Privacy. Non vedo traccia, tuttavia, di precisazioni su "provvedimenti atti a salvaguardare un interesse legittimo della persona interessata" nel testo che introduce il monitoraggio massivo anti-evasione made in Italy. In Germania, nel 2010, per il tentativo del Governo di avviare un analogo sistema, soprannominato ELENA, si riempirono le piazze di cittadini furenti e l'idea fu abbandonata.

La nostra identità, dunque, fatta anche di rappresentazioni "altre da sé" che chiamiamo "dati" e la nostra sfera privata sono sempre più in balia degli algoritmi che ne decidono le sembianze, l'estensione, l'accessibilità e la conoscibilità, persino la valutazione, nel bene e nel male. Questi algoritmi sono frutto di intelligenza quando vengono ideati ed assegnati al programma. Ma costituisce intelligenza vera, dopo l'invenzione, ciò che si ripete, sempre uguale a se stesso e che, ripetendosi, incide sulle vite di persone vive, umane, imperfette ed imprevedibili, diverse da quelle immaginate all'atto dell'invenzione algoritmica? Non resta che rileggersi il pensiero del giudice Louis Brandeis, uno dei padri americani del diritto alla privacy: "L'esperienza dovrebbe insegnarci a vigilare per difendere la libertà quando le intenzioni del Governo sono buone. Gli uomini nati liberi sono naturalmente pronti a respingere violazioni della loro libertà da parte di governanti mossi da fini malvagi. I pericoli più gravi per la libertà si nascondono in abusi insidiosi compiuti da uomini zelanti, bene intenzionati, ma privi di intelligenza".

Marco Simoni
Economista, politologo, docente alla London School of Economics
Sergio de Ferra
Docente di International Economics alla London School of Economics

La crescita digitale

Come Internet crea lavoro, come potrebbe crearne di più. Gli effetti occupazionali di Internet si amplificano se, nel contempo, cresce il capitale umano del Paese. Saranno i giovani a farci conoscere le opportunità e i rischi della digitalizzazione.

italiafutura

Il rapporto "Crescita digitale" intende contribuire alla discussione pubblica sul legame tra crescita economica e nuove tecnologie e i modi per massimizzarne l'impatto. Nasce, insomma, per rispondere ad una semplice domanda: quanti posti di lavoro, in particolare giovanile, si creerebbero in Italia con una maggiore e migliore diffusione di Internet? Si stima che Internet abbia già creato 12.700 nuovi posti di lavoro nel nostro Paese (DAG, Sviluppare l'economia digitale in Italia: un percorso per la crescita e l'occupazione) e che l'internet economy abbia rappresentato il 2% del PIL nel 2010 (BCG, Fattore Internet. Come Internet sta cambiando l'Economia italiana, The Boston Consulting Group, 2011). Ma non era ancora stato realizzato uno studio che misurasse puntualmente il potenziale occupazionale della rete, forse perché fino al 2007 c'è stata una scarsa disponibilità di dati: anche solo cinque anni fa l'esplosiva espansione di Internet non era sufficiente a stimare il suo effetto occupazionale in maniera solida. Il rapporto Crescita digitale tenta di colmare questa lacuna.

Le risposte del rapporto

Le risposte fornite dal rapporto sono molto chiare: a) la diffusione di Internet esercita un impatto positivo "puro" sull'occupazione, soprattutto su quella giovanile, indipendentemente da altre concause, come la crescita economica, il livello di tassazione sul lavoro, il cambiamento della competitività internazionale. In particolare, si è cercato di valutare quanti occupati in più o in meno si otterrebbero nella fascia d'età tra i 15 ed i 64 anni e quanti nella fascia tra i 15 ed i 24 anni, se l'indice di diffusione di Internet aumentasse del 10%. I dati presi in considerazione per fornire una risposta a queste domande si riferiscono a 28 Paesi dell'OCSE su un periodo di dodici anni (dal 1999 al 2010). I risultati ottenuti mostrano che in un ipotetico Paese medio, l'aumento della diffusione di Internet del 10% comporta un aumento dell'occupazione complessiva di 0,44 punti percentuali ed un aumento dell'occupazione giovanile di 1,47 punti percentuali. Questo risultato è valido per tutte le economie avanzate ed è particolarmente rilevante per Paesi come l'Italia, che scontano un ritardo sia per quanto riguarda la diffusione di Internet, sia per quanto riguarda gli altri fattori che consentono di cogliere le opportunità delle nuove tecnologie. Il rapporto ha cercato, inoltre, di analizzare quale sarebbe la condizione occupazionale attuale se l'Italia fosse stata capace di garantire la stessa diffusione di Internet riscontrata in Francia, un Paese a noi vicino e comparabile dal punto di vista della dimensione e dello sviluppo, oppure come l'Olanda, Paese tra i migliori performer. Se l'Italia, nel 2010, fosse stata in grado di pervenire alla stessa diffusione Internet della Francia, ci sarebbero circa 200.000 occupati in più nella fascia d'età tra i 15 ed i 64 anni, di cui 100.000 nella fascia 15-24. Se, poi, fosse stata in grado di raggiungere i livelli dell'Olanda, gli occupati in più sarebbero oltre 275.000, di cui oltre 140.000 giovani. Se, da un lato, la posizione arretrata del nostro Paese in tutte le classifiche internazionali che misurano lo sviluppo in vari ambiti determinanti per cogliere le opportunità delle nuove tecnologie - livello di formazione del capitale umano, facilità di fare impresa e di accedere al credito - è una delle cause dell'attuale situazione di sofferenza economica, da un'altra prospettiva essa indica molto chiaramente la direzione da seguire. La strada dello sviluppo digitale è a portata di mano e ha dimostrato di poter fornire risultati importanti in tempi relativamente brevi. b) Gli effetti occupazionali di Internet si amplificano se, nel contempo, cresce il capitale umano del Paese: crescono, cioè, i livelli di formazione volti alla creazione di una cultura digitale e, allo stesso tempo, vengono implementate politiche per far crescere l'ecosistema digitale nel suo complesso.

Le fonti della crescita digitale. Essere "preparati"

Se un Paese, le sue imprese ed i suoi cittadini, non sono sufficientemente pronti ad integrare Internet nella loro economia, gli investimenti in tecnologia esercitano un impatto molto minore. Nella classifica di un indice composito che misura quanto i diversi Paesi europei siano preparati a trarre vantaggio dal potenziale di Internet, l'Italia è posizionata sotto la media, molto distante dai piani alti della classifica. Nuovamente: questo indice rappresenta una condizione di attuale difficoltà, ma suggerisce anche delle importanti potenzialità, dato che, intervenendo sui fattori che limitano la nostra "preparatezza", si possono ottenere risultati molto positivi sulla crescita.

Un ecosistema favorevole

Naturalmente, accanto ai fattori moltiplicativi dovuti al contesto di riferimento, la crescita digitale è favorita e stimolata dallo sviluppo diretto di settori legati all'uso delle nuove tec-

nologie. In altre parole, gli effetti di creazione di nuova occupazione e di crescita economica dipendono anche dallo sviluppo di un'industria dedicata a sviluppare servizi e prodotti legati ad Internet, che possono fungere da traino ed accompagnare i settori più tradizionali nell'economia digitale. A svolgere un ruolo fondamentale nel promuovere l'impatto positivo di Internet, oltre al capitale umano, sono, in particolare, una struttura dei finanziamenti vicina alle necessità d'impresa (e, nel caso delle aziende ICT, vicina alle necessità delle startup) ed il bisogno di regimi regolamentari semplici. Leggendo i dettagli della classifica della Banca Mondiale, si capisce bene quale debba essere la principale preoccupazione di ogni nuovo giovane imprenditore in Italia: non solo il peso, ma anche il livello di complicazione del sistema fiscale che lo costringe ad effettuare ben 15 pagamenti l'anno, e passare in media circa 285 ore l'anno, oltre un mese e mezzo a tempo pieno, a risolvere problemi fiscali. In altre parole, un geniale startupper italiano non avrebbe modo o tempo di concentrarsi sullo sviluppo delle sue idee o sulle strategie di mercato perché passerebbe gran parte del tempo a risolvere problemi burocratici... Per questa ragione, va proseguita la strada, già iniziata dall'attuale Governo, di semplificazione della vita di imprese giovani. In particolare, una spinta verso la digitalizzazione degli adempimenti burocratici e fiscali può diventare doppiamente efficace in questo senso, essendo sia una semplificazione in sè, sia una spinta all'utilizzo del digitale da parte delle aziende tradizionali.

Un volano per tutti

Una delle ragioni per cui non risulta agevole misurare l'impatto di Internet è legata proprio alla sua pervasività. Internet cambia il modo in cui le aziende operano, interagiscono le une con le altre, e la rivoluzione digitale sta trasformando il modo in cui si producono le cose. In altre parole, oltre ai fattori già discussi, l'impatto di Internet sull'economia presenta due effetti analiticamente distinti. Da un lato, migliora la produttività delle aziende che si dotano di strumenti web, con guadagni stimati tra

il 5% e il 10%; dall'altro, fa nascere nuove opportunità anche nella old economy. Per rafforzare questi fenomeni, si possono identificare, sfruttando la scala locale di parte dell'industria italiana, specifici sostegni alla digitalizzazione delle aziende, specialmente quelle che la sfrutterebbero al fine di incrementare la loro esposizione internazionale. Infatti, e questo vale specialmente per l'Italia, in cui gran parte della produzione avviene nelle piccole e medie imprese, è possibile favorire, tramite la digitalizzazione, economie di scala che consentano di superare gli svantaggi della dimensione ridotta. Il web, in sostanza, può portare i distretti ad assumere un nuovo ruolo nella crescita dell'economia locale e nella sua esposizione internazionale, favorendo la specializzazione locale grazie alla possibilità di un enorme ampliamento dei mercati di riferimento.

Capitale e lavoro: tornare al territorio

In Italia, l'innovazione va realizzata anche partendo dalle realtà dinamiche e produttive, ancora largamente organizzate in distretti locali. Sul capitolo dell'innovazione delle imprese non appare dunque ipotizzabile l'adozione di scorciatoie statali basate su finanziamenti a pioggia. Al contrario, è fondamentale l'intervento di mediazione e coordinamento degli attori locali: non solo i poteri pubblici, ma le banche, le camere di commercio, gli enti di formazione, i sindacati, etc. Una stretta cooperazione con gli enti di formazione può favorire, poi, l'ingresso nelle aziende di una nuova generazione di "nativi digitali", in grado di stimolare l'innovazione. Molto spesso, infatti, ci si trova di fronte ad un blocco di natura culturale. Inserire, anche per poche settimane, "nativi digitali" all'interno delle PMI può diventare un modo per far scattare l'interesse verso il mondo digitale e, allo stesso tempo, dotare queste ultime di strumenti di base. Possono essere proprio i giovani ad accompagnare le aziende a scoprire le opportunità offerte dalla digitalizzazione.

Giovanna Mascheroni
Ricercatrice Università Cattolica del Sacro Cuore
Referente nazionale EU Kids Online (www.eukidsonline.net)

I social network

I dati della ricerca "EU Kids Online" confermano la grande popolarità dei social network fra adolescenti e, in modo più sorprendente, pre-adolescenti europei: il 59% dei ragazzi europei di 9-16 anni possiede un profilo personale su un social network.

I social network sono le piattaforme web 2.0 più popolari fra giovani e giovanissimi, per i quali rappresentano pratiche comunicative quotidiane per la gestione delle relazioni interpersonali e la costruzione della propria identità. Il social networking offre ai ragazzi opportunità sul piano relazionale, identitario e culturale: l'opportunità di mantenersi in contatto con i legami personali, estendere la propria rete sociale, condividere conoscenze ed interessi con i pari, sperimentare la propria identità e via dicendo. Tuttavia, l'uso dei social network da parte dei più giovani – spesso anche sotto i limiti di età consentiti dagli stessi provider – solleva preoccupazioni fra i decisori politici, i genitori, gli insegnanti e, più in generale, nell'opinione pubblica. Si teme, infatti, che la comunicazione negli ambienti digitali costituisca l'occasione per contatti rischiosi - come l'adescamento a scopo sessuale da parte di adulti ed azioni di cyberbullismo da parte di coetanei – o altre esperienze negative quali l'uso improprio di dati personali, ad esempio il furto di identità o il frape. È opinione comune anche che i ragazzi non possiedano un senso della privacy e che i social network, consentendo un numero ampio di contatti, impoveriscano, di fatto, il valore dell'amicizia.

Adottando un approccio "child-centred", critico e comparativo, la ricerca EU Kids Online – finanziata dal Safer Internet Plus Programme della Commissione Europea - analizza le pratiche on-line, le opportunità ed i rischi di internet di oltre 25.000 ragazzi europei di età compresa fra i 9 ed i 16 anni, e dei loro genitori, residenti in 25 Paesi. In particolare, per quanto riguarda i social network, sono stati raccolti dati relativi alla loro diffusione, agli usi relazionali (numero e natura dei contatti, anche in confronto ad altre pratiche comunicative on-line), alla gestione della privacy ed al tipo di informazioni personali usate per la costruzione del proprio profilo on-line.

I dati della ricerca confermano la grande popolarità dei social network fra adolescenti e, in modo più sorprendente, pre-adolescenti europei: il 59% dei ragazzi europei di 9-16 anni possiede un profilo personale su un social network. La pratica è più diffusa nei Paesi nordici, in particolare Paesi Bassi (80%), Lituania (76%) e Danimarca (75%); i livelli minimi si registrano in Romania (46%) e Turchia (49%), mentre l'Italia si assesta poco sotto alla media europea, con il 57% dei ragazzi che mantengono un profilo on-line in modo continuativo. L'uso dei social network cresce con il crescere dell'età: solo il 26% dei ragazzi europei di età compresa tra i 9 ed i 10 anni, ed il 19% dei coetanei italiani, possiede un profilo su un social network, percentuale che sale, rispettivamente, all'82% ed all'80% degli adolescenti europei ed italiani di 15-16 anni.

Uno dei principali fattori di rischio dei social network viene identificato nell'ampiezza e nella natura dei contatti on-line: si teme, cioè, che i ragazzi abbiano un numero spropositato di contatti e che questi siano in larga parte estranei.

I dati EU Kids Online aiutano a ridimensionare le paure, in primo luogo in relazione al numero medio di contatti on-line: più della metà (51%) dei ragazzi europei ha meno di 50 amici sui social network, un terzo (31%) possiede un numero di contatti compreso fra 11 e 50 e meno di un terzo supera i 100. Solo il 9% dei ragazzi intervistati ha dichiarato di avere una cerchia sociale di oltre 300 contatti. Ci sono, tuttavia, delle differenze cross-nazionali piuttosto evidenti, che vedono ai lati opposti dello spettro la Romania – dove il 63% dichiara meno di 50 contatti e solo l'8% supera i 100 amici – e l'Ungheria – dove, all'opposto, si abbassa il numero di chi ha meno di 50 contatti (il 30%) e si alza, invece, quello di chi è in contatto con oltre 100 amici (46%). L'Italia si allinea maggiormente con il dato europeo, con il 47% dei ragazzi che è in contatto con meno di 50 amici, ed il 34% che ha più di 100 contatti.

Rispetto alla natura dei contatti on-line, i dati confermano quanto già evidenziato da altre ricerche empiriche sugli utenti di social network: vengono usati prevalentemente per restare in contatto con persone conosciute. Il 78% dei ragazzi intervistati (ed il 69% dei coetanei italiani) afferma, infatti, di usare i social network per mantenere e consolidare i legami con la propria rete amicale. In confronto ad altri mezzi di comunicazione interpersonale, tuttavia, i social network consentono di ampliare la propria sfera relazionale: ciò avviene sia attingendo alle liste dei contatti dei nostri amici, sia attraverso l'acquisizione di nuove amicizie. La prima modalità di espansione delle

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Servizio relazioni con i mezzi di informazione

Privacy: cittadini più tutelati nell'uso dei dati da parte di regioni e aziende sanitarie

Maggiori tutele per i cittadini nell'uso dei dati da parte della Pa. Quando trattano a fini amministrativi i dati sensibili e giudiziari delle persone - ad esempio a fini di monitoraggio della spesa sanitaria, di accertamento dell'idoneità al lavoro o di concessione di benefici – le regioni, gli enti regionali e provinciali, le aziende sanitarie devono rispettare precise garanzie a tutela della privacy. È quanto ha chiesto il Garante per la protezione dei dati nel dare parere favorevole sullo schema tipo di regolamento predisposto dalla Conferenza delle regioni e delle province autonome. Lo schema tipo aggiorna quello adottato nel 2006 con il quale sono stati individuati i dati sensibili (salute, vita sessuale, sfera religiosa, appartenenze politico-sindacali, origine etnica) e giudiziari (condanne, carichi pendenti etc.) che possono essere raccolti e utilizzati da regioni, province autonome, asl, enti e agenzie regionali e provinciali, enti vigilati, e le operazioni che con tali dati si possono effettuare.
La revisione dello schema tipo di regolamento del 2006 nasce dalla necessità di garantire un più ampio quadro di tutele rispetto ai flussi crescenti di dati che vengono scambiati tra le pubbliche amministrazioni nell'ambito delle loro attività istituzionali, anche in ragione delle nuove competenze acquisite e della necessità di verifica del buon andamento dell'attività amministrativa.
Nel dare il suo via libera, l'Autorità ha dato indicazioni alla Conferenza delle regioni e delle province autonome perché lo schema venga integrato con specifiche garanzie.
L'Autorità ha chiesto, ad esempio, che ai fini del monitoraggio e valutazione dell'efficacia dei trattamenti sanitari erogati, le Regioni, una volta acquisiti i dati dalle Asl, adottino un sistema di codifica che non consenta l'identificazione diretta del soggetto interessato. Inoltre ha ritenuto che non fosse indispensabile l'utilizzo di dati sensibili, quale l'adesione a partiti, sindacati, associazioni religiose, per finalità di programmazione, gestione e valutazione dell'assistenza sanitaria.
Il lavoro di revisione portato a termine è frutto di un complesso e proficuo lavoro di collaborazione del Garante con la Conferenza delle regioni e delle province autonome, che ha visto presenti tutte le amministrazioni interessate.
Lo schema tipo, è bene ricordarlo, semplifica gli adempimenti di regioni, asl, agenzie ed enti vigilati provinciali e regionali poiché evita che i singoli regolamenti previsti per legge, se adottati in conformità alla versione aggiornata dello schema tipo, debbano essere sottoposti al parere del Garante.

Roma, 26 luglio 2012

cerchie sociali è di gran lunga prevalente: il 34% dei ragazzi europei ed il 42% dei ragazzi italiani usa i social network per stabilire un contatto con i legami latenti, amici o familiari di persone che già appartengono alla propria rete amicale. Includono nella propria cerchia relazionale persone mai incontrate off-line, rispettivamente, il 12% dei giovani europei e l'11% dei loro coetanei italiani. Il contatto con sconosciuti nei social network è inferiore rispetto alle chat, agli ambienti di gioco multi-utente ed ai mondi virtuali, e riguarda principalmente coetanei. Ciononostante, la pratica di networking solleva preoccupazioni in merito alla privacy ed alla sicurezza on-line dei minori.
La privacy è il frutto di processi di negoziazione fra l'esigenza di proteggere informazioni personali e quella, opposta, di condividerle per dare forma alla propria identità ed entrare in relazione con gli altri. Nei social network la privacy è strettamente dipendente dalle impostazioni abilitate dai diversi provider, che impongono scelte standard rispetto alla visibilità del profilo e dei contenuti che decidiamo di condividere on-line ed ai confini delle relazioni sociali.
Contrariamente all'idea che gli adolescenti siano disinteressati alla propria privacy, la maggior parte dei ragazzi europei (43%) sceglie un profilo privato, il 28% ha un profilo parzialmente privato, cioè accessibile anche agli amici degli amici e poco più di un quarto (il 26%) ha un profilo pubblico. Permangono, tuttavia, notevoli differenze fra i diversi Paesi europei: il numero di ragazzi dotati di un profilo pubblico è più bassa in Irlanda e Regno Unito (10%), Nazioni che hanno adottato da più tempo campagne di sensibilizzazione su questo tema. In Italia, la percentuale dei ragazzi che dispongono di un profilo pubblico aumenta (34%), mentre diminuisce la percentuale di chi sceglie di impostare il proprio profilo come privato (36%). In linea con la media europea, invece, il dato relativo ai profili parzialmente privati. A livello europeo, sono le ragazze (48% rispetto al 38% dei coetanei maschi) ed i giovani di famiglie di status socio-economico più elevato (48% contro il 43% dei ragazzi di background socio-economico inferiore) ad avere più probabilità di impostare come privato il proprio profilo. Rispetto all'età, la media europea non registra forti differenze fra i ragazzi di fasce di età diverse nella protezione della privacy. In Italia, invece, i ragazzi di 9-12 anni hanno più probabilità di avere un profilo pubblico (39%) rispetto agli adolescenti. Per i ragazzi più piccoli, spesso, il profilo pubblico non è una scelta consapevole, bensì la conseguenza dell'incapacità di modificare le impostazioni di privacy del proprio profilo: il 42% dei ragazzi italiani, ma solo un quinto dei ragazzi di 11-12 anni, dichiara di possedere queste competenze.
La natura pubblica o privata del profilo si combina con le informazioni personali condivise on-line dando forma a specifiche configurazioni della privacy. Fra le informazioni identificative più frequentemente inserite nei propri profili ci sono una fotografia che li ritrae fedelmente, inclusa dal 75% dei ragazzi europei e dal 77% dei coetanei italiani; il cognome, che viene dichiarato, rispettivamente, dal 64% e dal 67%; la scuola frequentata, indicata dal 43% degli intervistati europei e dal 39% del campione italiano. Inoltre, più della metà degli intervistati – il 61% del campione ed il 52% dei ragazzi italiani – dichiara l'età reale nel profilo. La pratica di indicare un'età falsa riguarda solo il 16% dei ragazzi europei ed il 20% dei coetanei italiani, ma è più diffusa fra i ragazzi più piccoli, che hanno un'età inferiore al limite imposto dal social network. Al contrario, altre informazioni, come l'indirizzo di casa ed il numero di telefono, sono ritenute sensibili: solo l'11% dei ragazzi europei ed il 14% dei ragazzi italiani rende pubblico il proprio indirizzo di casa nel profilo, dimostrando un forte senso di privacy. Ancor più bassa la percentuale di chi condivide il proprio numero di telefono, pari al 7% in Europa ed al 4% in Italia.
I dati qui presentati smentiscono alcune convinzioni diffuse - che su internet i ragazzi siano in contatto prevalentemente con sconosciuti e che non si preoccupino assolutamente della propria privacy – e suggeriscono l'importanza di politiche di sensibilizzazione agli usi responsabili della rete e di promozione della sicurezza on-line soprattutto in Paesi, come l'Italia, caratterizzati da un livello di digital literacy inferiore alla media europea.

Walter Paolicelli
Avvocato, specialista in diritto delle nuove tecnologie e computer crimes.
www.studiopaolicelli.it

Come difenderci da noi stessi

Mi torna alla mente un caso particolarmente singolare di cui mi sono occupato tempo addietro e riguardante proprio la fuga di dati sensibili dall'interno di una struttura sanitaria italiana.

Il concetto di privacy, risalente a circa un secolo addietro, è stato coniato al fine di evidenziare uno degli aspetti più importanti della libertà individuale. Nel corso del tempo, tale terminologia ha assunto dimensioni più o meno indefinite, ma solo negli ultimi anni il legislatore si è accorto dei pericoli legati alla dispersione dei dati personali.
E il cittadino si è reso conto del pericolo che rappresenta per se stesso?
Probabilmente, questa domanda potrebbe apparire senza alcun senso se non letta alla luce delle considerazioni che seguono. Inutile ricordare che, dal presente articolo ad ogni altra attività che ci accingiamo a compiere quotidianamente, lo strumento informatico resta sempre e comunque il protagonista. Quotidianamente riveliamo alle macchine una quantità infinita di informazioni circa le nostre attività lavorative, le nostre vite private, il nostro tempo libero. Migliaia di informazioni che lasciano irrimediabilmente traccia di sé all'interno dei pc domestici, aziendali, in rete e nei server di chissà quale ditta che si presta ad offrire servizi di archiviazione remota dei contenuti. Non è possibile sapere con certezza quale percorso effettuino i nostri dati una volta immessi nel sistema, sia che si tratti di una rete privata, sia che si tratti di pubblica amministrazione. Attualmente, troppi soggetti senza alcun controllo possono entrare in contatto con i dati informatici.
Rileggendo le righe che precedono, si intravede la risposta alla domanda circa il pericolo che rappresentiamo per noi stessi. Come si diceva, il legislatore si è affrettato a definire un testo normativo che potesse porre le basi per la tutela della privacy di ciascun cittadino, affiancando alla violazione delle suddette norme sanzioni più o meno gravi. Tuttavia, quanto previsto normativamente non poteva prevedere l'incalzante diffusione degli strumenti informatici e l'impossibilità materiale di rincorrere i dati personali una volta immessi nel circuito informatico mondiale. Se ci pensiamo bene, quelle decine di migliaia di mail e banner pubblicitari che riceviamo quotidianamente all'interno della nostra posta elettronica o all'interno della pagine web che visitiamo più spesso sembrano coniate appositamente per noi. A volte riproducono esattamente ciò che riguarda le nostre preferenze lavorative, hobbystiche e sessuali! Ma com'è possibile tutto questo? Potrei rispondere che qualcuno si sia appropriato dei nostri dati e abbia realizzato un profilo commerciale poi rivenduto a qualche agenzia pubblicitaria. Oppure, potrei affermare che siamo stati noi stessi ad acconsentire che il gestore di posta elettronica al quale siamo abbonati "gratuitamente" inviasse informazioni personali a società "terze" per fini commerciali. Ancora, potrei rispondere che, ogni qualvolta ci affacciamo in rete, seminiamo tracce del nostro passato, presente e, perché no?, anche del nostro futuro.
L'esperienza professionale da me accumulata negli ultimi anni, tra l'altro, ha portato alla luce altri aspetti inquietanti della fragilità della nostra privacy. Un numero sempre maggiore di personaggi dello spettacolo, imprenditori, dirigenti d'aziende pubbliche domanda il nostro aiuto per questioni relative alla tutela della propria riservatezza. In numerosi casi, piuttosto, coloro i quali dovevano essere considerati le vittime di questi abusi, sono stati invece perseguiti come colpevoli!
A tal proposito, mi torna alla mente un caso particolarmente singolare di cui mi sono occupato tempo addietro e riguardante proprio la fuga di dati sensibili dall'interno di una struttura sanitaria italiana. Tutto nacque dalla denuncia presentata da un cittadino circa il presunto furto di dati sensibili da parte di alcuni addetti ai lavori. Le indagini appurarono non solo che nessun dato era stato prelevato abusivamente, bensì che gli stessi soggetti denunciati erano stati, a loro volta, vittime di violazione della propria privacy presso la struttura in cui lavoravano.
I fatti appena narrati, volutamente semplificati, si verificavano a causa di una situazione "informatica" a dir poco sconcertante: i punti di accesso al server centrale risultavano non protetti da credenziali di accesso e, comunque, non conformi alle vigenti normative in materia di tutela dei dati personali. Chiunque si fosse trovato nei pressi delle suddette postazioni avrebbe potuto accedervi sfruttando le credenziali immesse da altri. Inoltre, nessuno dei dipendenti della suddetta azienda sanitaria era stato formato ed informato circa modalità di utilizzo, pericoli e quant'altro necessario al corretto svolgimento delle proprie mansioni per mezzo delle postazioni informatiche loro affidate.
Tutto questo è possibile a causa dell'impreparazione, innanzi tutto di coloro i quali sono deputati all'organizzazione ed alla gestione delle strutture aziendali e, successivamente, degli utenti tutti, nei confronti di una tecnologia che si evolve molto più velocemente di quanto si pensi. Ogni settimana vengono offerti nuovi servizi tele-

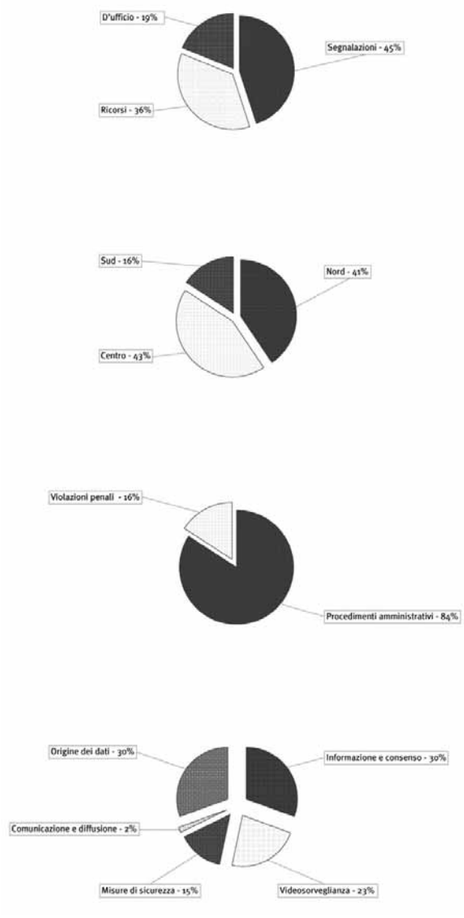
Dalla privacy alla diagnosi

Quando il cittadino si affida ad un ospedale per risolvere un problema di salute, probabilmente, l'ultimo dei suoi pensieri sarà la gestione della privacy o le modalità di trattamento dei dati personali. Ma, di certo, l'importanza che si attribuisce oggi a queste informazioni è grandissima ed il D.Lgs. 30/06/2003, n. 196, la cosiddetta "legge sulla privacy", è diventata una tappa fondamentale per la tutela dei diritti della persona. Attraverso questa legge viene attentamente stabilita la modalità di gestione di tutte le informazioni personali. In vigore dal 1° gennaio 2004, questa ha, di fatto, abrogato la precedente L. 675/96. Le informazioni inerenti lo stato di salute sono di particolare delicatezza e vengono comprese nei cosiddetti "dati sensibili": non possono essere liberamente diffuse. Durante la permanenza del cittadino all'interno di una struttura ospedaliera, tutti i dati che lo riguardano vengono complessivamente riversati su un unico documento. La cartella clinica lo accompagnerà nel suo percorso sanitario. E' il diario del decorso della malattia ed è giuridicamente considerata un atto pubblico di "fede privilegiata" perché proveniente da un pubblico ufficiale (il medico), ma anche perché esemplifica il trattamento e contiene notizie individualizzanti un determinato soggetto. Vi sono contenuti il decorso della malattia e tutti i referti clinici rilevanti. La cartella clinica deve contenere: a) il consenso da parte del paziente al trattamento dei dati; b) l'inquadramento clinico; c) l'anamnesi completa; d) i referti di indagini di laboratorio e strumentali; e) il consenso per emotrasfusioni ed interventi diagnostico-terapeutici; f) eventuali verbali operatori; g) la lettera di dimissione.
L'art. 23 del Nuovo Codice di Deontologia Medica prevede che la cartella clinica debba essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica. Secondo il Garante della privacy, la cartella clinica cartacea deve essere leggibile. Se illeggibile a causa della grafia del redattore, dovrà essere trascritta in modo che le informazioni contenute diventino chiare. Il Direttore dell'Unità Operativa è responsabile della compilazione della cartella clinica, della sua conservazione e della sua riservatezza. Durante il periodo di degenza deve essere conservata nello studio del Direttore o in una stanza apposita, in modo che nessuno possa consultarla, tranne i medici del reparto o gli specialisti chiamati per eventuali consulenze. Il medico non può rivelare ad altre persone le condizioni di salute di un paziente se questo non ne fa espressamente richiesta; l'illegittima divulgazione del contenuto della cartella clinica costituisce reato penalmente perseguibile per violazione di segreto professionale e d'ufficio. La cartella clinica viene conservata illimitatamente nell'archivio centrale della struttura ed è in qualsiasi momento recuperabile per consultazione o copia da parte dei soggetti autorizzati. Il Direttore Sanitario si fa garante penalmente e civilmente della buona e corretta conservazione. Fermo restando il valore legale intrinseco della cartella cartacea, l'informatizzazione della società e le necessità pratiche della gestione dei dati sanitari hanno portato alla legalizzazione dell'utilizzo anche della cartella clinica elettronica. Con l'introduzione del Decreto sulla Semplificazione, la Sanità diventa informatizzata per rendere il SSN più efficiente e ridurre la burocrazia ed i costi. L'emendamento sulle semplificazioni approvato dalla Commissione Affari Costituzionali e Attività Produttive della Camera, in vigore dallo scorso 12 febbraio, introduce di fatto l'utilizzo della cartella clinica elettronica. Anche la Commissione Europea ha approvato delle linee guida che gli Stati membri dovranno rispettare e garantire da quando la cartella clinica digitale viene adottata dai propri SSN. Attraverso queste linee-guida, si raccomanda di: utilizzare i dati sensibili archiviati solo per scopi medici, con l'obbligo della segretezza e della privacy del paziente; rispettare la decisione autonoma del paziente in merito alle modalità di utilizzo dei dati; riservare l'accesso al fascicolo sanitario da parte del paziente tramite card elettronica, mentre, per gli operatori sanitari, sarà necessario un sistema di autenticazione che identifichi anche il loro ruolo; utilizzare le informazioni solo per ricerche scientifiche o statistiche; effettuare trasferimenti informatici ad istituzioni mediche extra UE solo in forma anonima o con pseudonimo; adottare sistemi di sicurezza che consentano l'accesso solo a persone autorizzate.
In Italia, l'uso della cartella clinica elettronica nel SSN è diventato legge il 6 marzo scorso.
La legge sulla privacy ha indubbiamente trasformato il tradizionale diritto alla riservatezza in ambito sanitario in diritto alla protezione dei dati personali, ma ciò che conta è che la condivisione di prassi sanitaria e legale serva a tutelare sempre il rispetto e la dignità di ognuno.

Antonio Irlando
Dirigente Medico ASS4 Medio Friuli

matici ai cittadini che ne approfittano senza neanche domandarsi il perché della gratuità degli stessi. Tanto per fare un esempio, il fenomeno dei social network parla da sé. Milioni di persone hanno diffuso in rete fotografie personali, informazioni, dichiarazioni, senza preoccuparsi di chi possa accedervi e dell'uso che vi si possa farne.
Il quadro che si presenta ai nostri occhi è a dir poco sconcertante. Non è possibile ricostruire il percorso dei nostri dati personali, ma solo cercare di limitare i danni.
Dal punto di vista dell'utente, occorre seguire semplici regole affinché possiamo tutelare quel che resta della propria privacy. Dal punto di vista dell'ente (pubblico o privato), occorre affidarsi a consulenti i quali, grazie agli strumenti normativi e tecnologici esistenti, riescano a prevenire situazioni come quelle appena narrate e, comunque, ad ottenere la giusta tutela per ciascun soggetto.

Relazione 2003
Attività Garante - Atti e provvedimenti



Valeria Vilardo
Giornalista Freelance

Il potere della mente sulle menti

Spiati dai satelliti, filmati dalle telecamere, sorvegliati su internet ed incollati alle TV. Dov'è finita la privacy nel 2012? Esiste ancora un barlume di intimità in un mondo dai riflettori accesi 24 ore su 24?

Nel tardo XVIII secolo, il filosofo inglese Jeremy Bentham progettò il Panopticon. Si trattava di un edificio istituzionale a forma circolare, dotato di una "inspection house" posta al centro, una sorta di torre. Da essa, i capi dell'istituzione potevano sorvegliare tutti gli internati senza che questi riuscissero a capire se venivano controllati o meno. In questo modo, nel dubbio, essi agivano secondo le ferree regole dell'istituzione stessa. Bentham descrisse il Panopticon come "un nuovo modo di ottenere il potere della mente sulle menti". Concepì un carcere modello - secondo lui - molto più economico e funzionale della deportazione dei condannati in lontane isole coloniali. Un solo guardiano, collocato nella torre centrale, poteva controllare i detenuti in tutte le celle. Queste erano edificate in cerchio, con la porta nella parte interna ed una finestra sulla parete esterna dalla quale filtrava la luce. I detenuti non potevano vedere gli altri carcerati, né – grazie ad un ingegnoso gioco di luce e controluce - il guardiano, il quale possedeva, invece, una completa vista sulla loro vita all'interno delle celle ed anche sull'attività dei secondini suoi sottoposti. I prigionieri non sapevano mai se il guardiano li stava osservando o meno. Da qui il nome "Panopticon", colui che può vedere tutto.
Il progetto di Bentham è stato ripreso e riportato all'attualità dal libro di Michel Foucault "Sorvegliare e punire", 1975, dedicato alle istituzioni carcerarie. La visibilità (che assicura il funzionamento del potere), la sorveglianza (che diventa prevenzione perché evita il ripetersi della colpa), la punizione (che assicura la modifica del comportamento che a suo tempo generò la colpa) costituiscono forme del potere moderno. Ogni superiore spia i suoi sottoposti ed è a sua volta spiato ed osservato all'interno di istituzioni che tendono sempre più ad essere totalizzanti, chiuse, disciplinari. Il Panopticon diventa una metafora della modernità. La visione panottica è differenziale, asimmetrica: uno solo vede tutto e tutti gli altri non vedono niente. Per questo si presta perfettamente ad esemplificare il controllo sociale. Il Panopticon viene però spesso evocato anche in una delle più serrate critiche alla società attuale: quella che la accusa di essere, sotto una patina di Democrazia formale, una società del controllo che osserva continuamente - accampando motivazioni di "sicurezza", "lotta al terrorismo" e simili - la vita dei comuni cittadini, utilizzando forme tecnologiche meno evidenti e rozze di quelle usate dai totalitarismi degli anni '30. Di questa attività di controllo si presentano generalmente due varianti, tra loro, peraltro, connesse: la prima mostra un carattere primariamente visivo e si materializza nell'enorme diffusione di telecamere di sorveglianza poste a presidio di spazi pubblici e privati e di satelliti in grado di localizzare qualunque punto della Terra; la seconda è legata, invece, alla presenza di grandi quantità di banche dati, raccolte per gli scopi più vari (anagrafe, conti correnti bancari, carte di credito, navigazione in Internet). Opportunamente incrociate, queste sono in grado di ricostruire anche gli aspetti più nascosti della vita dell'individuo se non interviene una valida tutela della privatezza, della "privacy". Nella prima, il punto centrale è la visibilità, premessa del riconoscimento; nella seconda, invece, è la tracciabilità, la ricostruzione dei nostri percorsi telematici. Notiamo, per inciso, che la videosorveglianza confina ormai con la televisione e con YouTube ed ha fornito amplissimo materiale a trasmissioni televisive ed a film.
Un'applicazione tecnologica del Panopticon è la televisione bidirezionale di "1984", di George Orwell (nome d'arte di Eric Blair), il più famoso romanzo distopico del '900. Ambientato nell'anno indicato dal titolo, immagina che il mondo sia diviso, dopo una lunga guerra nucleare, in tre grandi Stati, continuamente in lotta fra loro. Londra fa parte dell'Oceania: è una città incessantemente colpita dalle bombe, semidistrutta, in miseria. L'Oceania non conosce più la Democrazia ed è retta da una spietata dittatura di tipo socialista, il cui leader distante, il Grande Fratello, appare ossessivamente in grandi cartelloni, mentre le sue affermazioni sono riprodotte ovunque. Nella società descritta da Orwell, ciascun individuo è tenuto costantemente sotto controllo dall'autorità. Lo slogan "Il Grande Fratello vi guarda" ricorda continuamente agli abitanti che il Grande Fratello si situa al vertice della piramide gerarchica (tratto da Mediastudies, Università degli Studi Roma Tre).
Fantasia o realtà? Questo è più o meno ciò che sta accadendo nel mondo, a causa di una sempre più intrusiva sorveglianza dei cittadini da parte dei Governi, delle multinazionali del potere e delle istituzioni, attraverso un sistema che coinvolge i cittadini stessi nel raccogliere dati ed informazioni sulla popolazione. Va menzionato, a tale riguardo, il film The Truman Show, nota pellicola diretta nel 1998 da Peter Weir ed interpretata da Jim Carrey (premiato con un Golden Globe). Questo film affronta un tema già trattato nel famoso "Vanilla Sky", considerando come mondo fittizio una realtà creata ad hoc intorno ad un solo essere umano allo scopo di allestire un grandissimo show televisivo. Si tratta di un'estremizzazione del reality show, del grande fratello. Truman Burbank (Jim Carrey) vive su un'isola e conduce un'esistenza normalissima. Ha una grande paura del mare, cosa che gli impedisce di andarsene. Ma, ad un certo punto, accadono avvenimenti insoliti che lo porteranno a scoprire l'atroce verità: tutta la sua vita, fin dalla nascita, è stata seguita da un complesso sistema di telecamere che hanno mostrato al mondo, in diretta, ventiquattro ore su ventiquattro e sette giorni su sette, ogni momento della sua esistenza, da quando ha mosso i primi passi ai suoi primi baci, dalle gioie alle sofferenze, senza alcuna censura. The Truman Show mostra una prospettiva davvero inquietante sul controllo delle vite e delle menti: c'è l'inganno e la riduzione in schiavitù di un individuo al servizio dello spettacolo.
Una prospettiva così estrema non è poi tanto lontana dalla realtà. Basta riflettere sulla spettacolarizzazione che contraddistingue la nostra contemporaneità: tutto ciò che può trasformarsi in share viene filmato e trasmesso, senza alcun pudore o rispetto per le persone. Vengono intervistati padri che hanno appena perso un figlio, con primi piani sugli occhi gonfi di lacrime. Le televisioni offrono continuamente immagini dell'orrore, corpi sanguinanti macerati e straziati da bombe, pistole. Violenza trasmessa in un circolo che riproduce violenza. La sofferenza diventa merce e tanto più questa sofferenza è spettacolare, meglio è. In Italia si potrebbe affermare che questo processo di spettacolarizzazione delle tragedie umane abbia avuto inizio nel giugno del 1981, quando il caso di Alfredino Rampi, precipitato in un pozzo artesiano largo appena 30 centimetri, fruì di una copertura mediatica senza precedenti. Questo caso si può considerare il primo ed involontario reality della storia televisiva italiana: un Big Brother che risponde alla fame di informazione, alla bulimia giornalistica ed alla ricerca del macabro, dello scabroso, che caratterizza il peggiore giornalismo sensazionalista di oggi.

Ministero della Giustizia
Dipartimento Dell'amministrazione Penitenziaria
Direzione della Casa Circondariale Trieste
Via Coroneo, 26 - 34124 Trieste - Tel. 040635044 - Fax.040635008

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
Progetto realizzato con il finanziamento della Regione Autonoma Friuli Venezia Giulia

Genitori detenuti e professori dei propri figli a colloquio attraverso Skype

Il progetto finanziato dalla Regione Friuli Venezia Giulia *"Genitori detenuti e professori dei propri figli a colloquio attraverso Skype"* è stato promosso dall'associazione di volontariato

@uxilia Onlus, rappresentata dal Presidente, dr Massimiliano Fanni Canelles, in collaborazione con la Casa Circondariale di Trieste, diretta dal dr Enrico Sbriglia.
La realizzazione del progetto rappresenta una sperimentazione a livello nazionale, e forse europeo, attraverso la quale al detenuto viene offerta la possibilità di colloquiare con i professori del figlio minore frequentante la classe prima della scuola secondaria inferiore.

Obiettivo del progetto è quello di sostenere la relazione genitore-figlio quando il primo si trovi in stato di detenzione.
Grazie alla collaborazione attiva del Direttore della Casa Circondariale, dr Enrico Sbriglia, e dell'Ufficio dell'Area Educativa, è stato possibile individuare il detenuto interessato al progetto.
Il soggetto che ha aderito all'iniziativa è stato M.T., padre di un ragazzo che frequenta la classe prima di una scuola secondaria inferiore sita in provincia di Udine.
La videocomunicazione Skype ha rappresentato lo strumento attraverso il quale il detenuto ha potuto prendere parte in modo diretto alla vita di suo figlio e gli ha permesso di esprimere una sensibilità che il sentire comune solitamente non attribuisce alle persone sottoposte a regime carcerario. Grazie al contributo dell'associazione @uxilia Onlus, della Casa Circondariale di Trieste e dell'Istituto Scolastico, la Regione Friuli Venezia Giulia ha offerto un'occasione unica nel suo genere, promuovendo il dialogo interistituzionale e quello tra persone che appartengono a mondi diversi. Si è inteso sottolineare, infine, che una condanna gravante su una persona non nega alla stessa la possibilità di esercitare i suoi diritti di uomo e di padre. Il legame padre-figlio, se non limitato dalla legge, è unico e va tutelato nelle sue manifestazioni al fine di garantire al minore una vita quanto più serena e "normale".