diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

INTERNET E LE NUOVE FRONTIERE DI TUTELA DELLA PRIVACY

Autore: Redazione
In: Diritto civile e commerciale

Premessa
Il diritto alla privacy, elaborato dalla dottrina statunitense alla fine dell'Ottocento, nel corso di più di un secolo ha mostrato una natura multiforme, poliedrica, capace di modellarsi in relazione all'evoluzione dei costumi ed al frenetico progresso tecnologico.
Il c.d. "right to be let alone", così come definito dal giudice americano Cooley, grazie anche alla originale giurisprudenza nord-americana, è divenuto "one theme that pervades the entire constitutional structure", non solo negli Stati Uniti d'America, ma in tutti i Paesi con un regime democratico.
Essenziale, in tale processo di affermazione della privacy come diritto fondamentale, è stato il ruolo delle convenzioni internazionali in materia di diritti umani: ricordiamo la Dichiarazione Universale dei Diritti dell'Uomo, del 1948 (art.12), la Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, del 1950 (art.8), la Dichiarazione dei Diritti dell'Uomo in relazione ai mezzi di comunicazione di massa, del 1970 (art.1).
E' bene sottolineare come, sotto la spinta delle innovazioni tecnologiche, alla concezione di "privacy intimacy" che si riscontra nei documenti prima citati, si sia presto affiancata la nozione di "informational privacy", quale diritto dell'individuo di limitare e controllare la raccolta la registrazione e l'utilizzazione (soprattutto da parte di terzi) dei dati a carattere personale. E in tal senso si sono orientati l'Unione Europea (Direttiva 95/46), il Consiglio d'Europa (Convenzione Dati – 1981) e i singoli Stati, questi ultimi per lo più in attuazione degli impegni transnazionali.

Internet e le nuove esigenze di tutela della privacy.
Grazie alla corposa normativa comunitaria sulla privacy degli ultimi anni, l'Unione Europea è oggi la regione con il più alto livello di protezione dei dati personali al mondo.
Tuttavia lo sviluppo esponenziale dei mezzi di comunicazione telematica e, particolarmente, della rete mondiale Internet, sta via via mettendo in crisi gli strumenti normativi, approntati a livello nazionale e internazionale per tutelare il trattamento dei dati personali.
Internet è una rete telematica planetaria, costituita da milioni di computer interconnessi tra loro attraverso le normali reti di telecomunicazione; è utilizzata quotidianamente da milioni di utenti, che trasmettono una quantità enorme di dati, è una realtà globale, alla quale con molta difficoltà possono essere riferiti i parametri spaziali ai quali siamo stati sin qui abituati.
Le principali caratteristiche della "Rete delle reti" sono costituite da:
- la mancanza di un sistema di gestione dei dati telematici centralizzato;
- il libero accesso da ogni parte della Rete con strumenti e procedure di facile uso.

Diritto & Diritti ISSN 1127-8579

E’ subito evidente come, a queste condizioni, non possa esistere nessuna forma di controllo complessivo delle innumerevoli operazioni compiute momento per momento via Internet.
La Rete non è tuttavia una mera realtà tecnologica "asettica". Consentendo a milioni di individui di comunicare in tempo reale tra loro, al di fuori dei tradizionali mezzi di comunicazione e dei controlli insiti in questi, essa è divenuta ben presto "uno spazio sociale, uno spazio politico, uno spazio economico, uno spazio altamente simbolico, che permette nuove forme di rappresentazione del sé, incide sulle identità, consente nuove forme di espressione e di esperienza artistica", una nuova realtà mentale, che ci obbliga a ripensare le nostre categorie mentali.
Ma qual è la natura giuridica di Internet?
Sulla questione, sono state date le risposte più svariate, che possono così sintetizzarsi:
a) Secondo alcuni, Internet sarebbe un sistema, fondato su regole tecniche, che consentirebbe il collegamento tra un numero indefinito di soggetti che si trovano nelle stesse condizioni. Internet sarebbe un meta - territorio, dove i confini tra i vari Stati sarebbero non fisici, ma logici.
La dottrina indicata, ancorché originale, è tuttavia insoddisfacente, perché non spiega come i comportamenti di coloro che operano in Internet producano degli effetti nel mondo reale.
b) Secondo altri, che si agganciano alla teoria sub a), Internet sarebbe una realtà sovranazionale, più che transnazionale, riguardando tutte indistintamente le Nazioni dotate di infrastrutture di telecomunicazioni.
Tale teoria esamina le responsabilità dell'Internet Service Provider, del proprietario delle infrastrutture di rete, del gestore del sistema informatico, ma omette di affrontare la problematica della natura giuridica della Rete.
c) Secondo altri ancora, Internet sarebbe un procedimento di telecomunicazione al livello planetario, che supererebbe gli attuali termini di riferimento politico quali lo Stato nazionale, la sovranità limitata dal territorio, la definizione dei confini e degli attributi di potere tra Stato e Stato.
Tale teoria, ancorché generica, dà una rappresentazione realistica della Rete, cogliendo la sostanziale novità del fenomeno, che difficilmente può essere regolamentato ricorrendo unicamente alle categorie giuridiche tradizionali.
d) Va ricordata infine la teoria, secondo cui Internet sarebbe un luogo di infinita libertà, in cui gli utenti (i digital libertarians) potrebbero navigare nella più totale autonomia rispetto ad ogni autorità.
Tale prospettazione è caratterizzata da un’eccessiva connotazione utopistica, dimenticando che negli ultimi tempi i veri beneficiari della libertà di Internet non sono stati i singoli, ma le grandi multinazionali e gli apparati di controllo sociale dei governi.
In ogni caso, quale che sia la teoria accolta, Internet necessita di una sia pure minima regolamentazione per contenere ogni abuso e, quanto meno, identificare il foro competente in caso di conflitti d’interesse nell’ambito della Rete.
Tra i diritti degli utenti da salvaguardare assume particolare rilevanza quello che Rodotà chiama "il diritto all'autodeterminazione informativa", ossia la possibilità di controllare i processi di comunicazione che ci riguardano.
Nel sistema di circolazione planetaria delle informazioni, la privacy costituisce il "centro di gravità" attorno al quale si impernia il corretto utilizzo della Rete e il suo potenziale sviluppo.
Infatti, per usufruire di tutti i servizi che mette a disposizione Internet, dalla posta elettronica al commercio online (tanto per fare degli esempi concreti), è necessario che l'utente possa utilizzare i propri

Diritto & Diritti ISSN 1127-8579

dati personali con la sicurezza che essi non vengano raccolti e rielaborati per costruire un profilo personale, suscettibile di future probabili invasioni della sfera privata.
In tale ottica, da strumento di isolamento dagli altri, da diritto ad essere lasciato solo, quale era la sua antica nozione, la privacy diventa strumento di comunicazione.
Afferma, a tal proposito, Rodotà:
"A me serve avere tutela dell'anonimato, a me serve la tutela della riservatezza, della privacy, non per isolarmi ma per partecipare. Solo se sono certo del mio anonimato potrò partecipare senza timore di essere discriminato o stigmatizzato a gruppi di discussione in Rete su temi politicamente sgraditi al potere dominante in un certo momento. Solo se avrò la certezza di non essere discriminato, potrò denunciare gli abusi, magari nel luogo dove io stesso lavoro.
Ecco allora che la riservatezza non è un problema di silenzio, di isolamento dagli altri, ma è uno strumento di comunicazione. Allo stesso modo, nell'area del commercio elettronico, la riservatezza diventa lo strumento attraverso il quale, con fiducia, io accedo all'acquisto di beni o di servizi, avendo ad esempio la sicurezza che quelle mie informazioni non saranno ulteriormente utilizzate, fatte circolare, elaborate per costruire profili della mia personalità che potrebbero avere anche effetti discriminatori".

Internet e le nuove forme di intrusione nella privacy.
Le nuove tecnologie informatiche applicate alla Rete, permettendo con estrema facilità l'acquisizione e l'elaborazione dei dati concernenti le persone, consentono un'utilizzazione dei dati stessi "qualitativamente diversa dalla mera somma aritmetica che i vecchi strumenti consentivano, determinando una capacità di incisione della sfera giuridica del soggetto al quale le notizie si riferiscono, tale da non essere immaginabile in passato".
Quanto prima detto può essere dimostrato con un esempio concreto.
Tizio risulta iscritto a due gruppi di discussione (c.d. newsgroups), gestiti da soggetti diversi, di cui uno dedicato ad auto sportive, e l'altro al diritto.
Lo stesso soggetto ha pubblicato su un sito web di annunci economici gratuiti la ricerca di un'abitazione di lusso ed anche l'offerta di vendita di un'automobile di media cilindrata, indicando soltanto il proprio recapito telefonico.
La ricerca dell'abitazione di lusso attira l'attenzione degli specialisti dell'ufficio marketing di una società che propone investimenti finanziari di una certa consistenza i quali, individuate le generalità di Tizio tramite il suo numero del telefono, lanciano una ricerca in Rete.
Scoprono così che tale soggetto appartiene a due liste di discussione, sulla base di queste controllano velocemente gli Albi degli esercenti una professione legale e scoprono che Tizio è un avvocato, che ha raggiunto una buona posizione economica e che quindi gli può essere proposto un certo investimento.
Il tutto nel giro di qualche minuto!
In questo caso, l'utilizzo delle informazioni è stato effettuato per fini di direct marketing, ma si comprende benissimo che lo stesso tipo d'indagine (peraltro legittima, essendo stata effettuata con strumenti ordinari di ricerca, senza compiere alcuna criminale forzatura dei sistemi informatici altrui) potrebbe essere compiuta per fini meno commendevoli.
Se poi dalla "normalità" si passa alla "patologia", ci si accorge che i rischi per la privacy sono molto più grandi di quanto si possa pensare.

Diritto & Diritti ISSN 1127-8579

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

A – Dati concernenti gli abbonati ad un provider

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

I "transactional data" sono equiparabili sostanzialmente al traffico telefonico e rientrano nella normativa dettata dalla Direttiva CEE 97/66 e dalle norme nazionali attuative (in Italia, il D. Leg.vo n.171/1998).

Pertanto vanno mantenuti nel log (specie di registro elettronico del provider) per il tempo strettamente necessario per esigenze di fatturazione.

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

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

B - La posta elettronica

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

Concettualmente la posta elettronica va assimilata alla posta tradizionale circa le forme di tutela (tutela della corrispondenza).

Nei sistemi privati di posta elettronica i messaggi vanno direttamente al server (computer che raccoglie e smista i messaggi) e vi rimangono, fino a quando vengono letti.

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

Poiché tutti i messaggi di posta elettronica, anche se cifrati, contengono in chiaro l'indirizzo del mittente e quello del destinatario, si è pensato di approntare delle reazioni difensive, attivando gli "anonimous remailers", particolari server dotati di uno specifico programma, che consente di inviare la posta elettronica in maniera anonima.

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

C – I gruppi di discussione (c.d. newsgroups)

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

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

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

Negli USA tali dati vengono elaborati da apposite società, che poi vendono i risultati delle indagini a fini

Diritto & Diritti ISSN 1127-8579

commerciali.
La vulnerabilità della privacy di coloro che partecipano ai gruppi di discussione è stata l'oggetto principale dell'esempio concreto riportato al paragrafo precedente.
D – I servizi c. d. gratuiti
Esistono in Rete molti servizi (quali la distribuzione di programmi, la fornitura gratuita di pagine Web…) definiti come gratuiti, ma che tali non sono, perché, per consentire l'accesso, viene richiesta ad ogni utente la cessione di informazioni personali, che in questo modo diventano una vera e propria "merce" di scambio.
E – I Links
I documenti forniti dai server web sono generalmente composti da numerosi frammenti, ognuno dei quali è scaricato separatamente, potenzialmente anche da siti diversi.
In genere, nelle pagine web sono contenuti anche dei messaggi pubblicitari, scaricati da server appositi, che pagano il gestore della pagina per inserire gli annunci.
Nel momento in cui, nell'esaminare una pagina, l'utente "clicca" su un messaggio pubblicitario, generalmente scarica nel proprio computer e manda in esecuzione delle applet (piccoli programmi) java. Grazie a tale operazione, il gestore del server nel quale è memorizzato il messaggio pubblicitario è in grado di conoscere sia il tipo di client (programma che consente all'utente di navigare in Internet) utilizzato dall'utente, sia l'indirizzo IP del server tramite il quale l'utente si è collegato ad Internet, sia l'indirizzo del sito Web tramite il quale è stato letto il messaggio pubblicitario.
F – I cookies
Se si visita un sito Web, può accadere che il server di questo spedisca al client del visitatore e da questo al suo hard disk un pacchetto di dati contenenti alcune informazioni (quali l'indicazione del server mittente, una scadenza ed altri dati che interessano lo stesso server mittente).
In occasione delle visite successive, il server del sito Web chiede al client del visitatore di inviargli, sulla base delle istruzioni precedentemente impartite, dei piccoli file di testo, chiamati "cookies".
Questi, dal punto di vista tecnico, hanno la funzione di velocizzare il caricamento delle pagine web, facilitando il riconoscimento dell'utente.
Gli stessi cookies consentono tuttavia al server che li richiede di raccogliere dati sui siti e sulle pagine web precedentemente visitati dall'utente, potendo così ricostruire le abitudini e le preferenze di questo.
In sostanza, si tratta di una vera e propria "schedatura" all'insaputa dell'interessato (che molte volte ignora addirittura l'esistenza stessa di tali file), volta generalmente ad incrementare il "direct marketing", ma che contrasta pienamente con la tutela della privacy.
In conclusione, su Internet esistono numerose occasioni in cui, tramite appositi programmi, è possibile individuare i siti visitati da un utente della Rete, le sue scelte ed i suoi gusti, in una parola, penetrare con la massima facilità nella sua privacy.

Il commercio elettronico (e-commerce).
Un settore nel quale, più d'ogni altro, si combatte la battaglia della tutela della privacy è quello del commercio elettronico.
Questo è stato definito dalla commissione UE nella Comunicazione "Un'iniziativa europea in materia di commercio elettronico" [COM (97)157] come "lo svolgimento di attività commerciali e di transazioni per

Diritto & Diritti ISSN 1127-8579

via elettronica e comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica; la distribuzione on-line di contenuti digitali; l'effettuazione per via elettronica di operazioni finanziarie e di borsa; gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo delle Pubbliche Amministrazioni".
La definizione è molto ampia, comprendendo non soltanto gli scambi realizzati tra computers collegati in una rete telematica, quale Internet, ma tutte le fattispecie che implicano l'utilizzazione di strumentazioni elettroniche, indipendentemente dalle modalità e dalle procedure seguite.
Il commercio elettronico non si limita al contatto tra fornitore e compratore, ma s'estende alle fasi della trattativa e della negoziazione, della stipulazione del contratto e del pagamento dei prodotti o servizi acquistati e, nel caso di vendita di beni immateriali (quali software, informazioni ed altri servizi), anche della loro consegna.
Disciplinare il commercio elettronico con leggi nazionali è praticamente impossibile, poiché il traffico segue percorsi diversi, in relazione ai contratti stipulati dai venditori con i vari provider e da questi con altri provider.
In genere, gli utenti non si rendono neppure conto se il server al quale si connettono si trovi in Italia oppure all'estero, atteso che una pagina web può essere costituita da frammenti provenienti da server sparsi in tutto il mondo.
Peraltro, ove si voglia applicare una normativa nazionale a tutela dei dati personali, questa può essere facilmente elusa dal venditore, collocando il proprio server in un Paese con una legislazione più permissiva, e quindi più adatta alle proprie necessità.
Secondo una recente ricerca condotta un anno fa dall’IBM, negli Stati Uniti la preoccupazione maggiore della quasi totalità degli acquirenti di beni e servizi tramite il commercio elettronico è rappresentata proprio dall’insufficiente tutela della privacy.
E proprio tale timore ha determinato in tale Paese una diminuzione degli acquisti pro capite tramite la Rete.
Tutelare la privacy in maniera adeguata diventa così un’esigenza che, nata a livello individuale e sociale, viene ad avere rilevanti implicazioni anche in campo economico.
La necessità di un intervento efficace e tempestivo, che possa ridare fiducia, è ormai avvertita da tutti, anche perché la criminalità non sta certo a guardare.
Una recentissima fonte giornalistica ha evidenziato l'esistenza di un fenomeno molto inquietante, quello degli "ID theves" o ladri di identità.
Si tratta di criminali che riescono a procurarsi tutti i dati personali di un individuo (numeri di conto corrente, carta di credito e ogni elemento che possa identificare una persona), per assumerne l'identità nei confronti di banche, assicurazioni, negozi e chiedere prestiti o mutui, contrarre debiti, fare acquisti impunemente (negli USA circa 30.000 casi nell'ultimo anno).
Pare che su Internet esisterebbero addirittura dei siti che per 100 dollari renderebbero un buon numero di elementi capaci di caratterizzare un individuo.
La necessità di tutelare i dati personali su Internet quale condizione indispensabile per il commercio elettronico è stata riconosciuta dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali con documento del 23 febbraio 1999.

Diritto & Diritti ISSN 1127-8579

Come disciplinare la tutela dei dati personali su Internet.
Accertato che Internet è una realtà composita e policentrica, l'applicazione pura e semplice nei confronti degli utenti delle Rete delle norme sui dati personali e sulle telecomunicazioni, sin qui elaborate dalle singole nazioni e dall' UE, crea dei problemi difficilmente superabili.
Sino a quando il traffico Internet si svolge esclusivamente all'interno di uno Stato, è ovvio che si applicano le norme nazionali concernenti la protezione dati di quello Stato.
Tale situazione è tuttavia del tutto eccezionale, atteso che, nella quasi totalità dei casi, la trasmissione dei dati avviene (anche inconsapevolmente) utilizzando dei nodi collocati addirittura in altre zone del Pianeta.
Ciò, ovviamente, mette in crisi taluni concetti enunciati dalla normativa internazionale e nazionale, relativi alla protezione dati, come quelli di responsabile del trattamento, di trasferimento dei dati all'estero, del soggetto cui inviare l'informativa circa l'elaborazione dei dati e così via.
Mentre le utilizzazioni di Internet sono aperte a tutti e sono facilitate da procedure semplici, mancano degli efficaci sistemi di controllo.
Com'è stato evidenziato dal Consiglio di Stato francese in un'analisi svolta il 2 luglio 1998, "Internet e le reti numeriche sono soprattutto un nuovo spazio di espressione umana, uno spazio internazionale che trascende le frontiere, uno spazio decentralizzato che nessun operatore né alcuno Stato padroneggia interamente...
Da una parte la regolamentazione di origine statale deve ormai combinarsi con l'autoregolamentazione dei protagonisti, degli attori, dei servizi comunicativi;
d'altra parte, tenuto conto dei limiti inerenti ad ogni iniziativa puramente nazionale, spetta alla cooperazione internazionale tra gli Stati il far rispettare gli interessi pubblici in uno spazio largamente dominato dall'iniziativa privata...".
Nel documento prima richiamato troviamo indicate le due fonti dalla cui combinazione può scaturire un efficace normazione della "Rete delle Reti", la nuova "cyberlaw".
La prevalenza dev'essere data indubbiamente alla cooperazione internazionale che, tramite lo strumento dei Trattati, consente di:
- costruire sistemi di controllo efficaci per evitare e reprimere ogni abuso;
- individuare la normativa di tutela di volta in volta applicabile.
E' questa la strada preferita dall' UE, che con le proprie direttive ha inteso operare sia nel campo delle fonti sovranazionali, sia nell'ambito dei singoli diritti nazionali.
Secondo un'impostazione che si condivide, deve tuttavia trattarsi di una semplice regolamentazione di principio, che si limiti a porre poche regole fondamentali, quali:
- stabilire la legge da applicare per individuare il luogo dove è stato commesso il fatto, determinando di conseguenza la giurisdizione, e quindi la competenza di questo o quel giudice nazionale, con riferimento quindi anche al tempo dell'azione;
- stabilire delle regole procedurali minime sulla rilevanza e sul carattere delle prove;
- individuare alcune azioni da considerare comunque dannose o vietate, anche a prescindere da quanto previsto dalle legislazioni nazionali;
- stabilire i riferimenti giuridici per poter eseguire un eventuale condanna nei confronti di un soggetto straniero
A tale fonte, con funzione integrativa, deve affiancarsi l'elaborazione di codici di autodisciplina, informali

Diritto & Diritti ISSN 1127-8579

e per questo stesso in grado di essere aggiornati immediatamente (come le netiquettes statunitensi), per fronteggiare in maniera adeguata i problemi sempre nuovi proposti dall'uso delle tecnologie avanzate.
E' questa la soluzione preferita dagli USA, che sui codici di autoregolamentazione hanno costruito il loro sistema di tutela della privacy informatica, ancorché in maniera talvolta lacunosa, e quindi non del tutto soddisfacente.
Solo da tale sinergia dei trattati internazionali e dei codici di autodisciplina può venire la necessaria regolamentazione, per fare di Internet un luogo sicuro.
Quale che sia la soluzione preferita, un intervento che porti ordine nella circolazione delle informazioni all'interno della Rete è ormai necessario e non più rinviabile.

Le nuove tecnologie di controllo politico.
Al termine della nostra indagine sulle nuove forme di aggressione alla privacy, deve accennarsi brevemente a talune tecnologie di sorveglianza elettronica, con le quali vengono attuate vere e proprie forme di controllo politico sui sistemi di telecomunicazione.
A livello ufficiale, la questione è stata posta con uno "studio ad interim" della Omega Foundation di Manchester, denominato "Una valutazione delle tecnologie di controllo politico" (PE 166.499), presentato allo STOA - Scientific and Technological Options Assessment in data 18 dicembre 1997 ed alla Commissione sulle libertà civili e gli affari interni in data 27 gennaio 1998.
Nel predetto documento, sottoposto al Parlamento europeo in sessione ristretta nel settembre 1998 sotto forma di Sommario esecutivo aggiornato, vengono toccati vari argomenti, che possono così riassumersi:
A – Sviluppo delle tecnologie di sorveglianza
Viene evidenziato lo sviluppo di nuove tecnologie, dalle lenti a visione notturna ai microfoni parabolici in grado di captare conversazioni a voce ad oltre un chilometro di distanza, dalle reti di sorveglianza televisiva a circuito chiuso ai sistemi automatici di riconoscimento dei veicoli tramite il numero di targa, dai computer mobili in grado di intercettare le conversazioni trasmesse da telefoni mobili in un certo settore alla camera stroboscopica danese Jai, in grado di scattare centinaia di foto in pochi secondi, per fotografare individualmente tutti i partecipanti ad una manifestazione o ad una marcia.
Si chiarisce che tali tecnologie, nate originariamente per i settori della Difesa e dell' Intelligence, si sono rapidamente diffuse nei servizi di mantenimento dell'ordine pubblico ed anche nel settore privato.
B – Reti di intercettazione delle comunicazioni nazionali ed internazionali
Si afferma l'esistenza di due sistemi mondiali d'intercettazione, di cui il primo chiamato "ECHELON" (comprendente attività di strutture d'intelligence USA, quali la NSA e la CIA, ed inglesi, quali GCHQ ed M16) ed il secondo chiamato EU – FBI (comprendente varie agenzie di ordine pubblico, quali FBI e Polizie di Stato dell' UE).
Secondo il rapporto, ECHELON dispone di apparecchiature di ascolto e sorveglianza diffuse in tutto il mondo, che costituiscono un sistema puntato su tutti satelliti chiave Intelsat, utilizzati come infrastrutture di trasmissione satellitare per comunicazioni telefoniche, Internet, posta elettronica, fax e telex.
I siti di questo sistema sono situati negli USA, in Nuova Zelanda, in Australia, ad Hong Kong e nel Regno Unito.
Dalla massa indiscriminata delle informazioni raccolte vengono estratti gli elementi interessanti mediante l'utilizzo di sistemi di intelligenza artificiale come Memex, mediante l'utilizzo di parole chiave.

Diritto & Diritti ISSN 1127-8579

Sempre secondo il rapporto, le informazioni raccolte concernono non soltanto le eventuali attività terroristiche, ma anche le attività di carattere economico.
Secondo alcune informazioni giornalistiche, alcune società USA sarebbero state avvantaggiate per talune forniture all'estero mediante l'utilizzazione di notizie riservate raccolte tramite ECHELON.
Quanto al sistema EU – FBI, questo è stato creato in segreto nel dicembre 1996 dall'Unione Europea e dagli Usa, su sollecitazione di quest'ultimo Paese, per integrare il sistema ECHELON.
Si tratterebbe di una rete internazionale di posti d'ascolto telefonici nel quadro del "terzo pilastro" degli accordi di Maastrict, concernente la cooperazione nel campo giuridico e dell'ordine pubblico.
Di tale nuovo sistema, oltre i paesi dell' UE e gli Usa, farebbero parte anche l'Australia, il Canada, la Norvegia e la Nuova Zelanda.
A seguito della presentazione di tale documento, il Parlamento Europeo in data 16 settembre 1998 ha adottato una Risoluzione sulle relazioni transatlantiche e sul sistema ECHELON, con la quale, dopo aver riconosciuto l'importanza delle relazioni USA - UE a livello economico, politico e della sicurezza mondiale, ha affermato testualmente che:
"10. Recognises the vital role of international cooperation with regard to electronic surveillance in stopping and preventing the activities of terrorists, drug traffickers and organised criminals;
11. Further recognises, however, the vital importance of having democratically accountable systems of control with respect to the use of these technologies and the information obtained;
12. Asks for such surveillance technologies to be subject to proper open debate both at national and EU level as well as procedures which ensure democratic accountability;
13. Calls for the adoption of a code of conduct in order to ensure redress in case of malpractice or abuse;
14. Considers that the increasing importance of the Internet and worldwide telecommunications in general and in particular the Echelon System, and the risks of their being abused, require protective measures concerning economic information and effective encryption".
La problematica da ultimo esaminata riguarda certo i Governi, ma non va trascurato che la tutela dei dati personali riguarda soprattutto i singoli e le loro possibilità di accesso all'utilizzo degli strumenti informatici.

Conclusione. Le due anime della privacy.
L'indagine sin qui condotta ha consentito di individuare nuove esigenze di tutela in relazione all'uso crescente delle tecnologie informatiche e di Internet. E proprio l'evoluzione tecnologica, che nella trasmissione e rielaborazione dei dati compie continui ed incessanti progressi, richiede una rinnovata attenzione nei confronti della privacy, attesa la creazione di nuove e sempre più invadenti forme di intrusione nella vita privata.
La privacy, nata come "right to be let alone" (privacy-property), è divenuta ai giorni nostri il "diritto di controllare l'uso che altri facciano delle informazioni che mi riguardano" (informational privacy), potendo essere attuata, con estrema facilità:
a) l'utilizzazione persecutoria dei dati stessi;
b) la distorsione dell'identità sociale del soggetto, tale da comprometterne le relazioni con i soggetti frequentati quotidianamente;
c) la divulgazione indiscriminata di notizie, che impediscano al soggetto stesso di operare delle scelte in

Diritto & Diritti ISSN 1127-8579

maniera autonoma.
La sua efficiente tutela può essere garantita soltanto se si riconosce l'esistenza di un vero e proprio diritto alla privacy, che affonda le proprie radici nei Trattati internazionali (Dichiarazione universale dei diritti dell'uomo, Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali) ed al tempo stesso se si intensificano gli interventi normativi (sia di tipo istituzionale, sia di tipo spontaneo, quali i codici di autoregolamentazione) in materia di tutela del trattamento dei dati personali, in quanto i nuovi strumenti tecnologici sono in grado di creare sempre più penetranti forme di intrusione, senza che gli individui se ne rendano conto e senza che i singoli Stati siano in grado di tenere il passo con tale incessante evoluzione.
Trattasi in realtà di due aspetti tra loro complementari ed imprescindibili, perché non ha senso parlare di protezione dei dati personali se non si considera il valore giuridico fondamentale da tutelare, ossia la privacy.
Allo stesso modo la privacy non può essere intesa in maniera corretta ed adeguata, in tutte le sue necessarie implicazioni con riferimento alla società contemporanea, se non ci si rende conto della necessità di proteggere i dati personali.

Francesca Leotta
Dottore in Giurisprudenza

https://www.diritto.it/internet-le-nuove-frontiere-tutela-della-privacy/

Diritto & Diritti ISSN 1127-8579