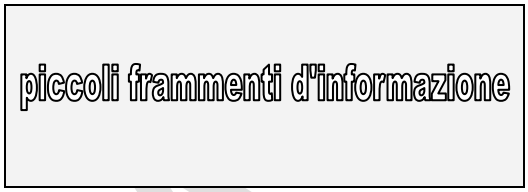
Privacy in internet: i cookies. "Piccoli frammenti d'informazione".

di M. Concetta De Vivo[*]

SOMMARIO: 1. Cosa sono i cookies. - 2. Tipi di cookies e sistemi di difesa. – 3. I casi di studio. – 4. Quadro normativo. – 5. Responsabilità del provider. – 6. Metodi di profilazione del consumatore. Il fenomeno del Datamining.

1. Il termine cookie (=biscottino) indica uno strumento informatico che, dietro un'apparenza innocua, nasconde potenzialità estremamente pericolose per la privacy dell'utente.



In concreto i cookies consistono in uno scambio di informazioni tra il server di un sito web ed il computer dell'utente che ne effettua la consultazione. Il "dialogo" che intercorre tra il client ed il sito visitato, viene generato dal server che ospita la risorsa consultata e depositato nel pc che si è collegato. I dati così registrati possono essere "richiamati", in un successivo contatto, permettendo il riconoscimento dell'utente (=client) a cui si riferiscono. La procedura è simile a quella posta in essere tra due persone che al loro primo incontro si presentano, cosicché la volta successiva, riconoscendosi, non hanno più alcun bisogno di ulteriori convenevoli .

(…)

Una caratteristica, poco nota, dei cookies è la data di scadenza (proprio come se si trattasse di un prodotto alimentare). Infatti, i programmi che lo installano sono obbligati ad impostare una data oltre la quale il browser del client potrà procedere alla ripulitura, ossia alla eliminazione dei cookies e dei dati in essi contenuti. È di questa estate la notizia che Google ha ridimensionato la data di scadenza dei propri cookies, passando da una durata di ben 31 anni (un cookie di oggi scadrebbe, dunque, nel 2038) ad una più accettabile, di 18/24 mesi (notizia pubblicata nel sito ufficiale di googleblog.blogspot.com del 14 marzo 2007). In Ue i dati verranno *anonimizzati* dopo 18 mesi anziché dopo 24, come avviene negli USA, dove sono tollerati per un lasso di tempo più lungo. Sostanzialmente il motore di ricerca più popolare del mondo ha promesso che i propri cookies si cancelleranno automaticamente nel caso in cui l'utente non dovesse più "ripassare" nel sito per almeno due anni.

---

[*] Bozza di lavoro pubblicato. Il saggio (in forma definitiva e piu' articolata) compare su volume: G. Biscontini e M.C. De Vivo (a cura di), Lezioni di Informatica. Percorsi di studio, ESI, 2007.

Le informazioni contenute nei cookies interessano sia le imprese, che su di essi hanno impiantato un'attività di rilevante profitto, sia gli hackers. Da un sondaggio effettuato dall'OWASP (l'Organizzazione Open Web Application Security Project, che si dedica alla diffusione della cultura per la sicurezza delle applicazioni web[1]) risulta, infatti, che la manipolazione dei cookies è uno degli attacchi più attuati dagli hackers, soprattutto nell'ambito del commercio elettronico.

In realtà, la funzione dei cookies non è poi così pericolosa, e consiste nell' identificare l'utente, riconoscendolo (se è già passato attraverso il sito) e favorendo in tal modo le risposte del server alle sue richieste. È proprio grazie alla identificabilità dell'utente che il server ospitante può abilitarlo a svolgere determinate operazioni all'interno del sito visitato.

Tuttavia, attraverso il monitoraggio degli accessi è possibile tracciare un profilo dell'utente, controllandone le "mosse" durante la navigazione e riuscendo, in tal modo, a "vedere" quali pagine visita (e con che frequenza), quali pagine non visita, i download che effettua e persino il tempo di permanenza nel sito.

Dalle premesse, appare logico dedurre che i cookies rientrano nell'àmbito del trattamento dei dati personali, anche se resta da stabilire in che tipo di dati personali possano "concretizzarsi". È dunque possibile applicare ad essi la regolamentazione prevista dal decreto legislativo n. 196/2003 (meglio noto come Codice della privacy) che nell'art. 4, lett. b), definisce il dato personale come "*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*". Pertanto, anche per essi, dovrebbe valere la previsione del consenso dell'utente che deve essere sempre preventivamente informato della installazione di cookies all'interno del suo computer.

[1] www.owasp.org

Per consenso informato si intende un consenso espresso, libero e consapevole, perché conseguenza di una serie di informazioni fornite al soggetto come previsto dall'art. 23 del d.lgs. n. 196/2003.

L'informativa dovrebbe, pertanto, rispettare le regole generali in materia, previste dal Garante, e cioè: essere consultabile prima della richiesta di registrazione, essere completa (ossia deve riguardare tutte le fasi del trattamento), contenere espressamente elencati i diritti d'accesso dell'interessato. Il termine "dovrebbe" è stato utilizzato volutamente, in quanto sorgono delle perplessità sulla possibilità della consultazione dell'informativa prima che accada qualsiasi "movimento" sospetto sul pc dell'utente, dato che i cookies sono acquisiti dal server nel momento stesso del contatto, e, dunque, prima ancora che vi sia un consenso espresso.

Per quanto riguarda la comparazione tra i cookies ed i dati sensibili questa non appare, poi, così improbabile, in quanto se è vero che un cookie preso singolarmente "testimonia" semplicemente un accesso ad una risorsa informatica, è vero anche che più accessi (=più cookies) a diverse risorse informatiche (o anche alla stessa risorsa informatica effettuata dallo stesso soggetto) finiscono con l'acquisire un "peso" ed una natura decisamente più complessa della semplice "testimonianza" informatica di avvenuto contatto. Inoltre, se i cookies vengono confrontati ed integrati con altre informazioni che riguardano l'utente, possono essere in grado di identificarlo e quindi diventare, automaticamente, rilevanti dal punto di vista della privacy. In tal caso i cookies finirebbero per trasformarsi in una ipotesi di dati sensibili ed essere regolamentati di conseguenza.

La normativa sui dati sensibili è particolarmente articolata, soprattutto in merito alla forma del consenso dell'interessato, consenso che deve essere espresso per iscritto. Su questo aspetto è lecito porsi il dubbio se il consenso fornito on line, attraverso moduli o formulari predisposti, possa essere assimilato ad una vera e propria sottoscrizione (si ricorda, tuttavia, che il nostro legislatore, sia nazionale sia comunitario, ha espressamente previsto la figura della firma digitale, proprio per ovviare alla mancanza della forma scritta in ambiente digitale. Sulla tematica delle firme elettroniche si rinvia alle indicazioni presenti in bibliografia).

Diversa è l'ipotesi dei c.dd. "dati anonimi" (come ad esempio i dati commerciali), ossia di quei dati attraverso i quali è impossibile risalire alla identità dell'utente/navigatore, ma che possono egualmente rappresentare un pericolo per la privacy dell'utente. Sull'argomento si rinvia alla parte dedicata al fenomeno del Data mining.

Riassumendo, si può dunque affermare che, al fianco dei classici Dati personali -

Dati sensibili - Dati non personali - Dati aggregati non personali o comunque identificabili, si pongono termini che il legislatore, in un primo momento, non aveva espressamente considerato, come ad esempio i cookies.

A questo punto è opportuno aprire una breve parentesi per ricordare le definizioni di "privacy" e di "dati".

Definire la "privacy" non è affatto semplice, anche se "semplicisticamente" si è soliti considerarla come il diritto del soggetto a vedere tutelata la propria sfera privata. In realtà "(…) non esiste alcuna definizione di *privacy* che ne contenga i molteplici ruoli ed interpretazioni, o che ne metta d'accordo i molti studiosi. Negli anni, la *privacy* è stata interpretata come controllo o come protezione; di un'ampia sfera privata o semplicemente dei propri dati personali; in senso puramente informativo o in senso decisionale. Ed ancora: la *privacy* è stata intesa come solitudine o come intimità, come anonimato o come riservatezza. Ed anche quando con *privacy* ci si riferisca al solo controllo sui propri dati personali, tale controllo è stato riferito alla raccolta, l'uso, o la divulgazione di tali dati." (A. Acquisti, Privacy, in Rivista di politica Economica, maggio-giugno 2005).

La definizione anglosassone "*the right to be left alone*" e cioè "il diritto ad essere lasciati (da) soli" rende molto bene il concetto di privacy, anche se lo lascia (volutamente) generico ed onnicomprensivo di molteplici aspetti: il diritto alla dignità umana, l'interesse alla riservatezza dei propri dati personali, la libertà da indebite influenze, il diritto a organizzare e controllare il proprio spazio di vita, sia esso fisico sia mentale o digitale. La sua definizione, spesso, è sfuggente ed ambigua anche per lo stesso soggetto a cui si riferisce. E così può accadere, ad esempio, che un individuo accetti che i propri movimenti telefonici vengano registrati dall'azienda telefonica, mentre non desideri assolutamente essere monitorato durante la navigazione in rete. Pertanto può affermarsi che "La *privacy* (…) è un concetto dalle molteplici, mutabili,ed a volte contraddittorie interpretazioni".

In riferimento alla definizione di "dato" (informativo) si deve puntualizzare che si intende per:

a) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (*ex* art. 4, lett. *b)*, d.lgs. n. 196 del 2003);

b) "dati sensibili" *"(...) i dati personali 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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale*" (*ex* art. 4, lett. *d)*, d. lgs. n. 196 del 2003);

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato (*ex* art. 4, lett. *c)*, d. lgs n. 196 del 2003);

e) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile; (*ex* art. 4, lett. *n)*, d. lgs n. 196 del 2003).

Alcuni tipi di dati, infine, vengono definiti "dati parasensibili" in quanto si collocano a metà strada tra i dati anonimi ed i dati sensibili ed hanno la caratteristica di recare, comunque, "pregiudizio ai diritti ed alle libertà dell'interessato". La tutela dalla pericolosità del trattamento di questi dati è espressamente prevista nell'art. 17 d.lgs. 196/2003, il quale recita: *"art. 17. Trattamento che presenta rischi specifici. - 1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei princìpi sanciti dal presente codice, nell'àmbito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare".* Sulla tutela della riservatezza dei dati personali si rinvia ai contributi citati nella bibliografia allegata, specialmente gli studi di R. BORRUSO.

Particolarmente dettagliato sull'argomento è lo studio svolto dal "Gruppo di lavoro per la tutela delle persone riguardo al trattamento dei dati personali" (parere n. 4/2007, consultabile nel sito www.privacy.it) che chiarisce, in modo articolato, il concetto "di dati personali".

È opportuno, comunque, ridimensionare il (legittimo) sospetto verso questi strumenti, che, di per sé, sono inidonei a creare danni , dato che, in origine, la loro funzione informatica era prevista solo per favorire l'utente nella navigazione. Questi

strumenti informatici non hanno l'attitudine ad arrecare danno all'utente, non possono, infatti, eseguire nessun tipo di script o contenere virus. Inoltre hanno altre utilità che non si esauriscono nel tracciare il comportamento dei consumatori, come ad esempio permettere la funzione di "riempimento del carrello" della spesa virtuale in siti commerciali, oppure abilitare un utente attraverso un login a svolgere delle attività in un sito web, e, ancora, personalizzare una pagina web sulla base delle preferenze dell'utente (è l'esempio del motore di ricerca Google). A volte la loro funzione consiste nel far saltare i filmati o le animazioni introduttive che spesso compaiono in alcuni siti prodotti in Flash (in questo caso i cookies vengono scritti "tramite alcune funzioni javascript", per essere successivamente recuperati ed attraverso il controllo della loro presenza, stabilito che la pagina è già stata visitata, evitare che il filmato introduttivo venga riproposto. Per approfondimenti v. il sito: flash.html.it).

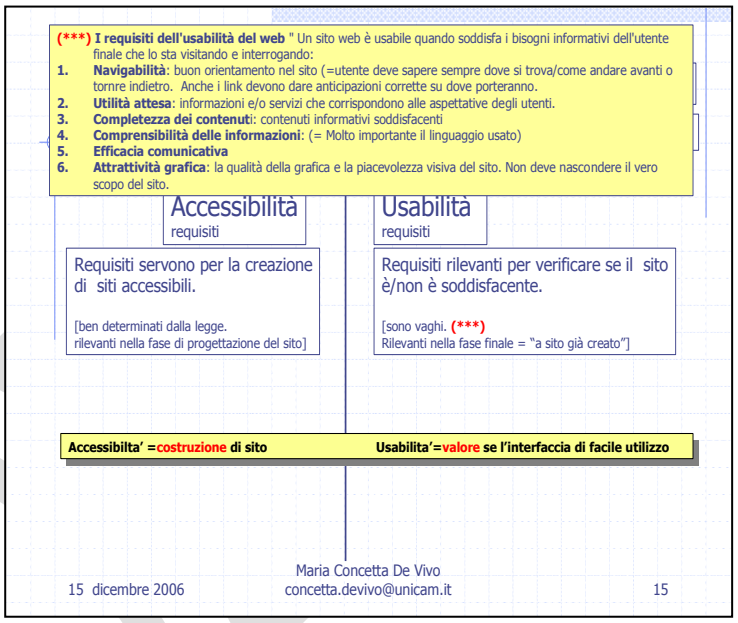
In realtà solo una delle funzioni dei cookies consiste nel tracciare i percorsi dell'utente. Il problema sta nel fatto che è proprio questa funzione ad essere sfruttata dalle società pubblicitarie, le quali ottengono, in questo modo, dati informativi sui gusti e le preferenze del navigatore, riuscendo ad elaborare proposte pubblicitarie che vengono destinate, in seguito, all'ignaro cliente.

Anche questa funzione, tuttavia, non è detto che sia poi così dannosa per l'utente. Si pensi alle ipotesi in cui una oculata pubblicità su determinati prodotti o servizi può essere di gradimento al destinatario finale, o a quei casi in cui la pubblicità mirata permetta al destinatario di tenersi costantemente aggiornato su prodotti o servizi che sono di suo gradimento. I cookies, in questi casi, garantiscono una personalizzazione dei servizi e delle offerte in Rete, favorendo, di fatto, le esigenze del consumatore.

Il monitoraggio effettuato durante la navigazione degli utenti, può, inoltre, essere utilizzato per la gestione ottimale di una risorsa web, nel senso che i dati contenuti nei cookies, possono essere sfruttati dal webmaster per comprendere in che modo il navigatore si muove all'interno di un sito, se ne è soddisfatto e, di conseguenza, se risulta effettivamente fruibile. In tal caso i cookies rappresenterebbero un sistema di valutazione del rispetto di quei canoni di usabilità che oggi sono espressamente previsti (anche se per ora solo in riferimento ai siti delle PA) dagli articoli 52 e 53 del d. lgs. n. 82/2005, altrimenti definito Codice dell'amministrazione pubblica digitale.

Art. 53. Caratteristiche dei siti. - 1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i principi di

__accessibilità__,_ nonché di elevata __usabilità__ e reperibilità, anche da parte delle persone __disabili__, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità. 2. Il CNIPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali. 3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.



Canoni che si rifanno ad esigenze di: **Navigabilità**, intesa come buon orientamento nel sito, per cui l'utente deve sapere sempre dove si trova/come andare avanti o tornare indietro nella fase della consultazione delle varie pagine web; **Utilità attesa,** per cui le informazioni e/o servizi debbono corrispondere alle aspettative degli utenti; **Completezza** dei contenuti, nel senso che i contenuti informativi debbono essere soddisfacenti per l'utenza; **Comprensibilità** delle informazioni, per cui, all'interno delle pagine web, si tende a favorire l'uso di un linguaggio semplice ed immediato; ed **Efficacia comunicativa**, al fine di predisporre una navigazione ottimale.

I requisiti che i siti istituzionali debbono possedere in riferimento alla privacy, sono previsti anche nel d.lgs. n. 196 del 2003. Secondo la normativa, è fatto obbligo al titolare del sito predisporre una sezione in cui risulti chiaramente ed in modo ben visibile l'informativa rivolta al navigante e che descriva le modalità di trattamento dei dati (da parte della PA). Più specificamente, deve risultare: chi è il titolare del trattamento dei dati, le modalità del trattamento, a chi sono comunicati i dati, quali sono i diritti dell'utente, se e come vengono impiegati dei cookies.

La sezione a cui si fa riferimento è denominata Policy o Disclaimer. Ormai tutti i siti, anche quelli di privati/professionisti e di imprese, ne possiedono una, ed è bene che l'utente la consulti sempre, prima di accedere al sito e, comunque, sempre prima di rilasciare qualsiasi

informazione che dal sito gli venga richiesta. Particolarmente interessante come esempio di Policy di un sito è quello predisposto dalla Warnerbros.it, reperibile al seguente url: www.warnerbros.it/main/privacy/privacy.html. Nel sito, la sezione "Privacy-policy" si raggiunge attraverso la consultazione della voce "Trattamento dati" e quindi > "Regolamento".
Per altri esempi di disclaimer o policy, si rinvia alla consultazione della documentazione proposta in allegato alla lezione.

2. I cookies possono essere classificati in due tipi:
Cookies generati e gestiti "da prime parti" (=ossia dal sito che si sta visitando);
Cookies generati e gestiti "da terze parti" (=ossia generati da un'altra risorsa che non è quella che si sta visitando, ma che viene raggiunta attraverso il sito contattato).

Per contrastare l'invasività dei cookies ci sono due modi: uno tecnico e l'altro giuridico. Su quello giuridico ci si soffermerà più avanti. Per quanto riguardo i vari accorgimenti "tecnici", invece, basta ricordare che il cookie può essere semplicemente disabilitato.

(…)

Attenzione. È bene sapere che la disattivazione dei cookies a volte può danneggiare lo stesso utente, poiché, se è stato precedentemente abilitato ad un determinato servizio proprio grazie al cookie, una volta che lo avrà cancellato non ne potrà più usufruire. Alcuni siti, inoltre, non permettono la navigazione all'interno di particolari sezioni a quegli utenti che hanno installato un blocco dei cookies. Di fatto, il navigatore che, con questa tecnica, vuol proteggersi dalla invasività dei cookies, pone dei limiti alla propria libertà di navigazione.

Alcuni esempi di disabilitazione dei cookies: il noto sito "Wikipedia" non permette, ad esempio, l'iscrizione di utenti che abbiano disabilitato l'installazione di cookies; i siti che fanno commercio elettronico, come Amazon, non permettono di mantenere il contenuto (=sostanzialmente di memorizzare gli ordini) nel "carrello della spesa"; il servizio "Google Personalized Search History" dell'omonimo Motore di ricerca, che immagazzina i dati inerenti alle ricerche, alle parole chiave delle ricerche e alle abitudini dell'utente, non riuscirà a funzionare se vengono disabilitati i cookies.

3. I casi di studio che hanno avuto ad oggetto i cookies incominciano ad essere numerosi. Di seguito se ne propongono un paio, abbastanza recenti, tra i più curiosi ed interessanti.

*"Chi ha paura di **Google**?". Google come al "Tentatore": pronto a soddisfare ogni tuo desiderio di fruitore e di produttore di comunicazione, in cambio "soltanto" della tua anima digitale, cioè i tuoi interessi, le tue passioni, le tue relazioni, la tua vita.*
[in Giornalismo d'altri di M. Tedeschini Lalli, 3 settembre 2007, http://mariotedeschini.blog.kataweb.it/]

Primo caso: Il caso Google ed i suoi cookies. -

Si fa fatica a credere che dietro la videata di questo diffusissimo motore di ricerca possa esserci qualche cosa di poco chiaro. La pervasività di questo colosso ha tuttavia suscitato remore e perplessità soprattutto in merito alla estrema facilità di gestione delle conoscenze raccolte ed utilizzate per fini di marketing. In realtà, un pò per la sua enorme diffusione ed un pò per la semplicità di consultazione, Google è riuscito a conquistare la maggioranza degli utenti di Internet. Wikipedia afferma che Google si occupa dell'80% di tutte le ricerche effettuate su Internet e che risulta essere il motore di ricerca più consultato su scala mondiale, con un'indicizzazione che supera gli 8 miliardi di pagine. Fino a poco tempo fa la sua interfaccia era volutamente pulita e proprio per questo particolarmente "rassicurante". Oggi la consultazione prevede una variante: iGoogle, fortunatamente personalizzabile.

Dietro alla semplice videata di Google si nasconde un'azienda che ha dichiarato nel 2006 un fatturato di 3,2 miliardi di dollari, mentre le stime per il 2007 prevedono che Google raccoglierà il 28,3% del fatturato pubblicitario statunitense investito su internet (Corrieredellasera.it del 1 febbraio 2007).

Ebbene, alla notizia (peraltro prevedibile) che anche questo motore di ricerca utilizza i cookies, c'è stato un coro unanime di proteste. Restano, comunque delle perplessità in merito all'effettivo pericolo per la privacy degli utenti. Infatti i cookies di Google servono "per memorizzare le impostazioni preferenziali di accesso al motore, così che l'esperienza di ricerca sia costante e ottimizzata", e perciò, sostanzialmente, per offrire un servizio migliore all'utente. È proprio grazie ad essi che il noto motore di ricerca mette a disposizione dei propri utenti servizi come **Google Maps**, che permette la creazione di mappe personalizzate; oppure il servizio di posta elettronica **Gmail –Google** o, ancora, il servizio gratuito **Google Analytics** predisposto per effettuare statistiche**.**

In seguito all'intervento delle Autorità garanti la privacy (del caso si sono occupate

sia la Commissione Europea sia l' Autorità garante europea - webnews.html.it/news/leggi/6083/lue-avverte-google-sia-garantita-la-privacy/ -) Google ha regolamentato l'attività di raccolta dati degli utenti, stabilendo una durata di registrazione dei cookies non superiore a 18 mesi (in Europa). La notizia è stata trattata anche dalle nostre testate giornalistiche, tra cui "la Repubblica.it", con un interessante articolo intitolato Privacy, Google accetta i rilievi "Conserveremo i dati per 18 mesi" (in www.repubblica.it 12 giugno 2007, sezione Tecnologia e Scienza).

Secondo caso: I cookie negli USA. - Negli Stati Uniti il fenomeno è conosciuto già dalla seconda metà degli anni '90. È in questo periodo che la Commissione Federale degli Stati Uniti per il commercio (Federal Trade Commission =FTC) inizia ad occuparsi dei primi casi di violazione della privacy e della tutela dell'utente in Internet. La FTC è una delle più attive organizzazioni, negli USA, preposta alla protezione dei consumatori ed a tematiche legate all'antitrust. Il suo sito è consultabile all'Url: www.ftc.gov, ed è possibile reperirvi i casi più interessanti di cui si è occupata.

In materia di violazione di privacy, il caso DoubleClick, è il più emblematico ed articolato che si conosca ad oggi. DoubleClick, infatti, da anni (dal 2000 ad oggi) è oggetto di "particolari attenzioni" da parte delle associazioni di utenti negli Usa. Dapprima a causa dell'acquisto, da parte dei suoi vertici, della società Abacus (2000), un'altra società leader nel campo della pubblicità online, e poi a causa del "suo" acquisto effettuato da Google (nel 2007). In entrambi i casi la fusione tra colossi del business, come era prevedibile, ha suscitato notevoli perplessità nel mondo dei consumatori/navigatori.

In seguito alla prima fusione (DoubleClick/Abacus) DoubleClick si è trovata nella condizione di poter visionare due milioni, circa, di profili-cliente derivanti dalle attività di commercio elettronico effettuate con la Abacaus.

L'unione fra il motore di ricerca più amato dai navigatori e la più potente società di pubblicità on line (Google/DoubleClick), invece, di fatto, ha creato un mostruoso database (di proprietà del motore di ricerca) particolarmente pericoloso per l'enorme mole di informazioni sugli utenti.

In entrambi i casi, dunque, le forti apprensioni delle associazioni di categoria risultano più che condivisibili.

Nei primi anni del 2000, proprio per contrastare questi pericoli, l'Epic (=Electronic Privacy Information Center)[2] presentò un reclamo alla Commissione del commercio

[2] www.epic.org Nel sito è possibile reperire documentazione particolarmente interessante, soprattutto legislativa, con particolare riferimento ai provvedimenti emanati dopo l'11 settembre 2001, c.d. "Patriot

federale per la tutela della privacy, facendo presente che l'operazione "DoubleClick/Abacus" comportava il superamento dei limiti accettabili in merito alla quantità di dati raccolti dagli inserzionisti sui propri utenti

Anche la Corte Distrettuale di New York, il 28 marzo 2001, è stata chiamata a giudicare in materia. Ma in entrambi i casi le due inchieste si sono concluse a favore di dell'operato di DoubleClick che è risultato legittimo. Infatti, il giudice Naomi Reice Buchwald della Corte distrettuale, chiamato ad accertarsi se DoubleClick avesse violato la privacy dei propri utenti attraverso l'installazione di cookies, trasgredendo così a ben tre leggi federali in materia di privacy e sicurezza telematica (l'Electronic Privacy Act, il Wiretap Act ed il Computer Fraud and Abuse Act), si è espresso riconoscendo la legittimità dell'uso dei cookies da parte della compagnia statunitense DoubleClick. Il procedimento aveva "riunito" ben tredici cause intentate contro DoubleClick nei vari stati degli Usa[3].

La fusione tra Google e DoubleClick ha messo in apprensione anche l'Europa, dove i consumatori non convinti che si sia difronte ad un semplice accordo commerciale, si sono mobilitati, attraverso le varie Associazioni (Altroconsumo[4] per l'Italia, l'Organización de Consumidores y Usuarios-OCU per la Spagna[5], VZBV[6] per la Germania e BEU[7]), ed hanno presentato una lettera di denuncia al Commissario per la Concorrenza UE, Neelie Kroes e, per conoscenza, ai Presidenti dell'Autorità per la garanzia dei dati personali, Francesco Pizzetti, e dell'Autorità garante della concorrenza e del mercato, Antonio Catricalà.

Anche il c.d. "Gruppo di lavoro Articolo 29" operante in Europa e da tempo impegnato nel controllo della privacy, ha ribadito il suo intento di controllare l'attività dei motori di ricerca, onde evitare possibili violazioni di privacy dell'utente, soprattutto attraverso l'uso (improprio) dei cookies[8].

Act", www.epic.org/privacy/terrorism/usapatriot che hanno creato, di fatto, forti limiti e deroghe alla privacy.

[3] V. nel sito www.dmnews.com/cms/dm-news/legal-privacy/14294.html, l'articolo titolato: Judge Dismisses Class-Action Cookie Lawsuit Against DoubleClick.

[4] www.altroconsumo.it/

[5] www.ocu.org

[6] www.vzbv.de/go/ - La Verbraucherzentrale Bundesverband e.V.-VZBV è un'associazione non governativa di consumatori che riunisce 38 associazioni.

[7] Il Bureau Européen des Unions des Consommateurs, www.beuc.org, è un'organizzazione europea che riunisce le associazioni di consumatori "e agisce a loro nome presso le istituzioni comunitarie" v. il sito Portale del consumatore, www.portaleconsumatore.it/consumatore/associazioni_dettaglio.php?id=44.

[8] Il Gruppo è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo

Secondo i legali di Google (tra cui l'avv. David Drummond) l'accordo che ha permesso l'acquisizione di DoubleClick non sarebbe neanche in contrasto con le leggi antitrust, in quanto le due società " sono complementari e non competono l'una con l'altra".

Negli USA, del caso è stata investita la FTC.

Sia sul caso "Google-DoubleClick" sia sul caso "DoubleClick-Abacus" sono stati versati fiumi di inchiostro da parte della stampa. Si rinvia, pertanto alla consultazione degli articoli segnalati in bibliografia.

Lo stesso Governo statunitense è risultato coinvolto nell' uso illegale di cookies permanenti, in quanto sembra che abbia tenuto sotto controllo i visitatori di alcuni siti web istituzionali, in palese contrasto con le leggi di garanzia per i cittadini. Secondo alcuni esperti, tale atteggiamento da parte del governo è "esplicitamente vietato da un'apposita legge del 2003 per la tutela della privacy" che vieta ai siti istituzionali di utilizzare i cookies c.dd. permanenti (v. in sitografia l'indicazione per reperire dell'articolo apparso su punto-informatico.it, USA controspionaggio a colpi di cookie, News, mercoledì 18 gennaio 2006). La reazione delle organizzazioni a difesa dei diritti individuali, particolarmente attive negli USA, è stata immediata ed ha dato origine ad un apposito servizio informativo curato dall'Aclu[9].

Proprio a causa delle potenzialità dei cookies, soprattutto nel campo pubblicitario, negli USA si sta cercando di elaborare una apposita legge in grado di disciplinare il fenomeno separatamente rispetto alla regolamentazione sulla privacy. Già nel 2004 la nostra Autorità garante per la privacy aveva dato notizia di queste intenzioni del legislatore statunitense (cfr. la newsletter n. 207 del 22-28 marzo 2004 - www.garanteprivacy.it/garante/doc.jsp?ID=897647; più specifica sull'argomento è una precedente newsletter che dedicò uno speciale in occasione della Conferenza Internazionale su *"Privacy, Cost to Resource – Privacy, da costo a risorsa"*, Roma, 5-6 dicembre 2002 , consultabile nel sito di www.interlex.it/675/newslett/nlspec.rtf). Per ora si è giunti, dopo alterne vicende, alla emanazione di una legge anti-spyware (nell'aprile 2007) che ha la finalità "di costringere software house ed agenzie pubblicitarie a notificare e richiedere il

---

indipendente, che si occupa della salvaguardia e della riservatezza dei dati. È un organismo in seno al quale le autorità nazionali di protezione dei dati collaborano all'attuazione della direttiva 95/46/CE. I suoi compiti sono descritti all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE. Cfr. il sito europeo ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

[9] Per approfondimenti., si rinvia al sito della Aclu www.aclu.org/safefree/nsaspying/index.html, nel quale è possibile consultare, in tutte le sue fasi, il "caso" ACLU v. NSA: The Challenge to Illegal Spying.

consenso dell'utente, così come avviene in Italia in base agli articolo 13 e 23 del D.Lgs.196/2003, prima di installare nel sistema del consumatore software anti-privacy" (notizia riportata dal sito di Anti-Phishing Italia, News 20.04.2007).

4. A seguito delle considerazioni sin qui esposte, sembra, dunque, che il quadro normativo relativo alla disciplina dei cookies sia quello previsto per il trattamento dei dati personali. Pertanto la normativa ad essi applicabile è quella predisposta per la tutela della privacy. Questo vuol dire che chi utilizza impropriamente i cookies rischia di rispondere dell'eventuale risarcimento del danno provocato nonché di eventuali sanzioni penali.

In uno dei precedenti paragrafi si è visto come è possibile difendersi, in pratica, dai cookies. A livello normativo, il problema è risolto attraverso il meccanismo del consenso del soggetto interessato. È essenziale, dunque, informare l'utente della raccolta dei dati che lo riguardano, anche quando questa avviene attraverso i cookies. In questo caso, il titolare del sito web che utilizza i cookies deve fornire una completa ed esaustiva informativa all'utente, *ex* art. 13 d. lgs. n. 196/2003, che lo avverta della presenza e del funzionamento dei *cookies*; fermo restando che, secondo il codice della privacy, nel caso di registrazione di dati sensibili occorre il consenso scritto dell'interessato e l' autorizzazione del Garante (*ex* art. 26 d.lgs. n. 196 del 2003). Pertanto, se si accetta l'ipotesi, precedentemente formulata, che i cookies potrebbero rientrare nell'ambito dei dati sensibili, anche per essi sarebbe necessario, oltre l'autorizzazione del Garante, il consenso scritto dell'interessato. Qualora si sia di fronte ad una "profilazione" attraverso gli strumenti elettronici, il Codice della privacy stabilisce l'obbligo di preventiva notifica al Garante (*ex* art. 37, co. 1, lett. d). Questi limiti sulla c.d. "profilazione" sono previsti sia per le aziende del territorio Ue sia per quelle che, pur essendo extracomunitarie, utilizzano strumenti che si trovano in territorio italiano o comunque che sia soggetto alla sua sovranità (*ex* art. 5 d. lgs. 196 del 2003).

Un altro principio a cui si deve fare riferimento è quello della "proporzionalità" della raccolta dei dati personali, per cui, laddove si ritenga superflua o inutile la memorizzazione/registrazione di particolari informazioni (=come ad esempio quelle inerenti allo stato di salute o alla sfera sessuale), la raccolta non deve essere consentita.

Tuttavia, nel caso in cui i cookies abbiano una funzione ed una finalità prevalentemente informatica non sembra sia necessario, riguardo al loro uso, l'obbligo di notificazione al Garante (v. in proposito la Deliberazione del Garante n. 1 del 31 marzo 2004). È ciò che accade nei c.dd. cookies di sessione, detti anche temporanei perché non

vengono "salvati" sul pc ma vengono cancellati immediatamente dopo la chiusura del collegamento (o meglio restano attivi finchè dura la connessione).

Conseguenza della mancata osservanza degli obblighi di legge è, oltre alla sanzione amministrativa, l'eventuale responsabilità civile per danni morali e patrimoniali (*ex* art. 15 d. lgs. 196 del 2003).

Il nocciolo del problema, dunque, è quello legato al trattamento dei dati che facilmente possono divenire oggetto di business. Un business a volte lecito e legale, come nel caso di forme di cessione volontaria (attraverso appositi contratti); altre volte, invece, illecito ed illegale, come nel caso in cui la cessione non sia volontaria (=è il caso in cui non venga predisposta una adeguata misura di protezione ed i dati vengano intercettati o rubati). Stesso discorso di legalità e di liceità si ha quando si è in presenza di una cessione c.d. "diretta" e cioè volta a soddisfare determinate finalità, di cui il soggetto interessato è stato messo, preventivamente ed adeguatamente, a conoscenza, mentre ad opposte conseguenze si giunge nell'ipotesi di forme di cessione "indiretta", che si ha nei casi in cui i dati vengano ceduti per uno scopo ma poi utilizzati per un altro fine, ignorando qualsiasi assicurazione o forme di garanzia e di sicurezza declamati negli appositi spazi web a ciò riservati (=disclaimer o policy. Vedere la documentazione allegata).

Alcuni Autori suddividono idealmente la regolamentazione in materia di privacy, a livello sia internazionale sia europeo, in due "filoni" di interventi normativi, convenzionalmente definiti come legislazione di I generazione e legislazione di II generazione.

Le Leggi di I generazione consistono in interventi normativi caratterizzati da una forte limitazione alla raccolta dei dati personali che si esprime nella previsione e regolamentazione di due sole fasi: quella dell'autorizzazione e quella del controllo della raccolta dei dati personali. Un atteggiamento, questo, dettato dal timore nei confronti degli strumenti informatici e della loro invasività. È di questo periodo la normativa svedese (*datalag*) del 1973 a cui si rifanno un pò tutti gli interventi normativi dell'epoca; la legge tedesca generale federale sulla protezione dei dati del '77 (c.d. BDSG '77); i vari DPA (=Data Protection Act) degli anni '80 e gli interventi delle Authority e delle Commissioni europee dei singoli Paesi, come, ad esempio, la Commision de l'informatique et des libertés.

Le Leggi di II generazione sono caratterizzate da un tipo di intervento atto a regolare in modo più articolato la raccolta ed il controllo dei dati personali. Una produzione normativa che, in realtà, subisce l'influenza di quelle aziende che intuiscono il business che

la raccolta dei dati informativi può creare.

Si può tentare di riassumere schematicamente i vari interventi in materia come segue:

Convenzione di Strasburgo. La Convenzione del Consiglio d'Europa del 28 gennaio 1981,entrata in vigore nel 1985 e ratificata in Italia nel 1989, è il risultato dell'esigenza di armonizzazione legislativa avvertita sia a livello internazionale sia a livello europeo, in grado di garantire ed uniformare in tutti gli Stati membri la protezione dei dati personali. All'epoca della sua formulazione era particolarmente avvertita l'esigenza di assicurare una regolamentazione del traffico transfrontaliero dei dati informatici, ispirandosi al principio della reciprocità.

Il c.d. Working Document . Una delle pietre miliari, per quanto riguarda la tutela delle persone ed al trattamento dei dati, è il Working Document approvato il 30 maggio 2002 (www.interlex.it/testi/pdf/wd5035.pdf) che tratta delle esigenze di tutela da parte degli utenti di Internet, della loro esigenza di privacy, del continuo attentato ad essa da parte di strumenti tipici dell'ambiente digitale quali: i cookie ed i software-spia e del problema legato alla giurisdizione (nel caso in cui il titolare del trattamento dei dati risulti residente fuori dall'Unione europea). Questo documento pur non presentando sostanziali novità nel settore e pur non essendo un atto normativo, grazie alla schematicità e sistematicità degli argomenti trattati, è il presupposto per lo sviluppo di alcune direttive successive, inerenti alle stesse tematiche.

Raccomandazione del 17 maggio 2001. Altro intervento rilevante per completare il quadro organico della regolamentazione della raccolta e tutela dei dati personali è la Raccomandazione relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea del 17 maggio 2001 (www.interlex.it/testi/racc010517.htm).

Direttiva europea del 95/46/CE. È da sempre è considerata la "madre di tutte le direttive" sulla protezione dei dati personali. In questo testo si tenta di armonizzare i diritti della persona con le esigenze delle imprese. Nel testo normativo viene contestualizzato il trattamento dei dati personali secondo principi di lealtà, liceità, adeguatezza, pertinenza, esattezza, aggiornamento, temporaneità (della registrazione), consenso informato, divieto di trattamento discriminatorio dei dati (e **dai** dati=si pensi alla raccolta di dati inerenti ai lavoratori sul posto di lavoro), controllo su tutte le procedure di raccolta e gestione dei dati, notificazione/autorizzazione presso l'apposita Authority, diritto d'accesso, diritto di opposizione e di ricorso da parte dell'interessato ai dati.

La Direttiva 2002/58/CE[10] "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche". Questo testo tratta espressamente di due fenomeni all'epoca poco conosciuti, i cookies e lo spyware. Infatti, nella Direttiva si legge:

> *Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.". (articolo 5, comma 3).*

Nel testo viene chiarito che l'uso dei cookies è consentito solo se accompagnato da una adeguata e chiara informativa, al fine di ottenere un consenso informato (vi deve essere la consapevolezza dello scopo della raccolta e del fine del monitoraggio dei dati) dall'interessato. Previsione che viene ripresa nell'articolo 24 dei Considerando:

> *"Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per*

[10] www.interlex.it/testi/02_58ce.htm

scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza."

nel quale viene più volte ribadito il principio che l'uso di tali dispositivi è consentito unicamente per scopi legittimi e che l'utente interessato deve comunque esserne a conoscenza.

Nell'articolo 25 dei Principi della Direttiva è inoltre specificato che:

" Tuttavia, tali dispositivi, per esempio i cosiddetti marcatori ("cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi".

in questo testo il legislatore europeo appare particolarmente lungimirante ed illuminato nel prevedere una regolamentazione che non si limiti a vietare bensì a prevedere l'ottimizzazione di uno strumento che, se opportunamente regolamentato, potrebbe portare anche utilità all'utente.

La normativa italiana in tema di privacy (e quella europea in genere) ha un approccio molto differente rispetto a quella statunitense. Mentre l'intervento del legislatore americano è decisamente "settoriale" (nel senso che "l'equilibrio tra protezione e scambio di dati è valutato di settore in settore" –settore bancario, medico o altri-), decentralizzato (le leggi che regolano la privacy sono molte e frammentate), espressione di una sostanziale autoregoalementazione e rispettoso dei principi del libero mercato; l'approccio del nostro legislatore è generalista (ossia indipendente dal settore di applicazione) e centralizzato (esiste un codice unico che regola la materia). In entrambi i casi, tuttavia, l'intento è identico e consiste nel "proteggere la *privacy* dell'individuo senza colpire i bisogni di flussi informativi" che è l'elemento tipico, presente in "ogni economia avanzata"[11].

L' Italia ha recepito nel proprio ordinamento le varie direttive europee sulla materia ed ha attuato la tutela e la regolamentazione dei dati personali attraverso una serie di normative che potremmo definire "a cascata".

- Dir.95/46/CE che tutela le persone fisiche rispetto al trattamento dei propri dati e ne disciplina la loro libera circolazione
- L. n. 675/96 che tutela i soggetti rispetto al trattamento dei dati personali (abrogata ed "assorbita" in altro testo successivo)
- d.l. 467/01 che ha novellato la l. n. 675/96
- d.lg.171/98 che tratta della privacy nel settore delle telecomunicazioni
-Dir 2001/31CE che si occupa specificamente del Commercio elettronico

In merito a questa disposizione comunitaria, data la sua importanza ai fini della regolamentazione del commercio elettronico, occorre aprire una breve parentesi.
La direttiva è stata recepita con d.lgs. n. 70 del 2003, il quale ha chiaramente stabilito degli obblighi informativi inerenti alle comunicazioni commerciali che debbono permettere, di fatto, una facile ed immediata identificazione sia del soggetto che la invia o che svolge attività commerciale, sia del contenuto e del fine della comunicazione (=se, cioè, si è in presenza di una pubblicità o di una comunicazione commerciale inerente ad offerte, premi, concorsi o giochi). Nella normativa è regolamentato un necessario consenso per il trattamento dei dati

[11] Per approfondimenti v. in bibliografia il saggio di A. ACQUISTI.

personali utilizzati per fini di marketing o comunque per fini commerciali o nel caso sia previsto il loro traffico o la loro comunicazione anche a terzi.

- Dir. 2002/58 CE che riguarda il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche;
- d.lgs. n. 196 del 2003, meglio conosciuto come il "Codice in materia di protezione dei dati personali" (che ha abrogato la l. 675/96);
- i vari Codici di condotta, come ad esempio quello dell'AIDIM (consultabile all'Url: www.aidim.it/codice_autodisciplina.pdf) e quello di Autoregolamentazione Tv e Minori (consultabile nel sito: www.comunicazioni.it).

In merito ai Codici di condotta sembra opportuno fare qualche breve puntualizzazione, rinviando, per un eventuale approfondimento, al materiale segnalato in bibliografia.

I "Codici di buona condotta" rappresentano una forma di autoregolamentazione/autodiscilplina, che è espressione di un consenso tra le parti (accade, cioè, che diversi soggetti - organizzazioni, associazioni, camere di commercio-, accomunati da stessi interessi ed obiettivi, predispongono delle "norme" regolamentari a cui si sottopongono) al fine di attuare una particolare tutela verso determinati soggetti che potrebbero risultare pericolosamente esposti ad abusi o violazioni. Sostanzialmente i codici di autodisciplina nascono dall'esigenza di "rassicurare" un soggetto-terzo.

In ambiente tecnologico, questa esigenza è particolarmente avvertita a causa della forte invasività degli strumenti utilizzati nelle relazioni interpersonali, soprattutto di tipo commerciale, e, pertanto, si è avvertita l'esigenza di fidelizzare il consumatore on line, offrendogli una serie di servizi che contemplano, fra le altre cose, anche la sicurezza ed il rispetto della sua persona. Una sicurezza ed un rispetto che vengono espressamente stigmatizzati nel Codice di condotta ed a cui gli aderenti liberamente si vincolano, predisponendo, a tal fine, una serie "di meccanismi di applicazione cogenti".

Spesso tali regole sono più limitative ed incisive della stessa disposizione normativa (laddove esiste). Questo perché i soggetti che pongono in essere i Codici

di condotta o che li sottoscrivono intendono rassicurare al massimo il "terzo" (=utente/consumatore) delle proprie intenzioni.

Gli interventi del legislatore, sia comunitario sia nazionale, in tema di Codici di condotta sono stati numerosi. In realtà il legislatore non ha fatto altro che prendere coscienza del valore fortemente etico di queste forme di autodisciplina volte a "responsabilizzare" ulteriormente il sistema economico, e che erano già consolidate prima del loro "riconoscimento" normativo, come prassi di mercato. I codici di condotta, infatti, anche prima del loro "riconoscimento" formale venivano sottoscritti da molte associazioni di imprenditori con l'intento di proporsi sul mercato come "erogatori eccellenti" di servizi altamente qualificati; servendosi, a volte, anche di enti definiti "certificatori", in grado di rilasciare dei "bollini di qualità" attestanti **non** la qualità dei beni o dei servizi erogati **bensì** la serietà con cui questi erano gestiti e proposti al pubblico.

Il legislatore, con il tempo, ha ritenuto, dunque, opportuno predisporre delle normative *ad hoc* che ne hanno, di fatto, riconosciuto ed incentivato l'uso.

Di seguito se ne elencano alcune:

- la l. n. 580/93 che ha promosso "la cultura dell'autodisciplina e dell'etica del mercato" attraverso il riordinamento delle Camere di Commercio;
- il d.lgs n. 185/99 che, in ossequio alle linee guida OCSE in materia di comunicazioni commerciali, ha incoraggiato l'elaborazione (da parte di organizzazioni imprenditoriali, professionali e dei consumatori) dei codici di condotta;
- la direttiva 2000/31/CE c.d. direttiva sul commercio elettronico;
- il d.lgs. n. 70/2003 di attuazione della precedente direttiva 2000/30/CE (artt. 7, 12, 18 e 20)
- il d. lgs. n. 196/2003, testo unico in materia di protezione dei dati personali (artt. 12, 16, 26, 61, 102, 106, 108, 111, 117, **118**, 119, **133**, 134, 135, **140**, 183, 185 – ALLEGATO A) contenente i Codici di deontologia e di buona condotta). In questo testo normativo, al fine di rendere più incisiva la portata dei Codici deontologici e di buona condotta, viene disposta la loro pubblicazione sulla GU.

Il contenuto dei "Codici" riguarda le regole sulla trasparenza (dei rapporti), sulla qualità (dei beni o dei servizi), sulle forme di garanzia e di responsabilità e sulla

previsione di risoluzione di controversie attraverso procedure più snelle e veloci (spesso a vantaggio del consumatore/utente).

Rientra nell' attività dell' Autorità Garante l'approvazione di codici di condotta elaborati dalle associazioni di categoria, così come espressamente stabilito nella Deliberazione del 20 luglio 2006 "Regolamento concernente la procedura per la sottoscrizione dei codici di deontologia e di buona condotta in materia di protezione dei dati personali" (G.U., 8 agosto 2006, n.183): "(…) *In particolare, occorre ricordare che il Garante Privacy ha il compito di: a) promuovere nell'ambito delle categorie interessate la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali; b) verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati; c) contribuire a garantirne la diffusione e il rispetto. La procedura di approvazione si articola nell'esame preliminare cui segue l'organizzazione dei lavori con la partecipazione, collaborazione e cooperazione dei soggetti appartenenti alle categorie interessate, nella successiva stesura di uno schema preliminare del codice oggetto di esame istruttorio per valutarne la conformità alla disciplina privacy, per poi giungere alla redazione dello schema finale del codice, all'ultima valutazione di conformità, alla sottoscrizione ed alla pubblicazione sulla Gazzetta Ufficiale. Il codice di buona condotta è infine comunicato al Ministero della giustizia ai fini della sua allegazione al Codice Privacy previo decreto ministeriale. Tra i più recenti codici ricordiamo quello per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti. Si attende il codice relativo al trattamento dei dati via internet e il codice relativo al trattamento dei dati dei lavoratori."*(www.filodiritto.com/)

I Codici hanno forza di legge solo tra le parti, come conseguenza della loro stessa natura di "accordo". Il consumatore/utente che contatta un'organizzazione/impresa che ha espressamente adottato un Codice di condotta ha, pertanto, il diritto di esigere da questa non solo il rispetto degli obblighi sottoscritti, bensì anche il rispetto di un più generico atteggiamento di correttezza e buona fede, poiché il suo "convincimento" viene fortemente condizionato proprio dalla presenza di "serietà e qualità" dei servizi/beni che il Codice di condotta dovrebbe attestare.

Il consumatore, inoltre, dev'essere informato dell'esistenza del codice al quale l'organizzazione/professionista ha aderito, e deve essere messo in grado di reperirlo e

consultarlo con facilità.

5. Il fenomeno dei cookies si riallaccia, dunque, al più complesso e generico aspetto della tutela del consumatore, più specificamente del consumatore on line, in considerazione della "tipologia" del soggetto debole (*weak*), pericolosamente esposto all'invasività sia tecnologica sia pubblicitaria/commerciale. Si pensi alle "figure" del minore/bambino o dell'anziano che esigono forme di protezione "avanzate" e per i quali appare particolarmente adeguata (ma non esclusivamente pensata) la figura del consenso consapevole, cioè di quel consenso che deve essere concesso con "la consapevolezza di ciò che si sta accordando perché si ha ben chiaro ciò che è stato richiesto".

Sulla figura del Consumatore è necessario ricordare, brevemente, alcuni aspetti che riguardano la sua peculiare evoluzione. La figura è passata, fra alterne vicende, dal concetto di "napoleonica codificazione" (Code Napoleon dell'800) del consumatore-forte, ossia dotato di un notevole potere negoziale, a quello di consumatore afflitto da una patologica debolezza, fortemente contestualizzato in una società dei consumi. È di questo periodo la produzione normativa vòlta ad una sua particolare tutela che sia in grado di ridimensionare le asimmetrie venutesi a creare tra i soggetti coinvolti negli scambi commerciali, ossia: il dovere d'informazione (per colmare la asimmetria informativa); la regolamentazione delle clausole abusive (per colmare la c.d. asimmetria contrattuale); le azioni collettive a difesa del consumatore (per colmare la c.d. asimmetria organizzativa).

Si giunge, infine, alla tipica figura del consumatore on line, che rappresenta, a mio avviso, un soggetto non più debole, bensì interattivo e particolarmente consapevole delle sue scelte e dei suoi diritti.

Di più: nel moderno panorama, il consumatore diventa portatore di interessi (*stakeholders*) verso l'impresa, senza anteporsi ad essa, ma spesso collaborando con essa, attraverso la segnalazione delle proprie esigenze, e a volte finanziandone alcuni processi.

Non a caso nasce, in questo periodo, l'Etica di impresa. Un'etica, cioè, basata sulla fidelizzazione della clientela; sul c.d. consumo equo e solidale; sull'attenzione riservata alla sicurezza dei prodotti; sui controlli di qualità (=attraverso il rilascio di

bollini di garanzia), sulla fiducia nelle nuove tecniche di marketing; sulla previsione di risoluzione di controversie più snelle ed indubbiamente più adeguate alle esigenze del consumatore (=come ad esempio gli ADR oppure gli ODR).

In questa nuova epoca, è l'impresa stessa che prende coscienza della sua "funzione di qualità", e che perciò si apre alle esigenze dei consumatori, che a loro volta diventano sempre più consapevoli dei propri diritti.

Nasce il consumatore "transazionale ed ecocompatibile" ed insieme a questa nuova tipologia di consumatore nasce una nuova figura di impresa, ben conscia della sua responsabilità sociale.

Nella raccolta dei dati personali via Internet assume un ruolo rivelante la figura del IP (=Internet Provider) che funge da "interfaccia amichevole" tra lo strumento tecnologico e l'elemento umano (=utente). È il Provider che, spesso, ha il carico più pesante in quanto quasi sempre coinvolto, più o meno direttamente, nella trattazione dei dati, e che pertanto deve informare l'utente delle tecniche invasive con cui è in contatto e delle adeguate misure di sicurezza prese per tutelare la sua privacy.

A volte la posizione del provider è regolamentata separatamente, o meglio, è regolamentata in base alla peculiarità del situazione di gestione dei dati in cui è coinvolto. È il caso della memorizzazione del contenuto di alcune comunicazioni, qualora queste risultino necessarie alla trasmissione. Memorizzazione a cui il provider è autorizzato, senza alcuna ulteriore formalità, ma consentita solo limitatamente ad un lasso di tempo determinato. Oppure è il caso della registrazione (=in un apposito registro elettronico) dei movimenti virtuali degli utenti effettuati dal provider per provare, eventualmente, l'avvenuto traffico in Internet e quindi la corretta esecuzione del contratto di accesso e/o fornitura di servizi.

Le regole di condotta dell' IP possono, dunque, schematizzarsi nelle seguenti indicazioni: rispetto del c.d. dovere di informativa (=che consiste nell'informare sulla natura dei dati che si intendono raccogliere, sui tempi, sulle modalità di trattamento e sulle finalità); richiesta del consenso dell'interessato che, in caso di dati sensibili, deve essere rilasciato per iscritto; la possibilità di raccolta/registrazione dati anche qualora non vi sia il consenso, purchè limitata ad esigenze probatorie sulla corretta esecuzione del contratto di accesso o erogazione dei servizi da parte dell'esercente (=provider o altro); notifica al Garante della Privacy del trattamento dei dati e relativa autorizzazione; adozione delle "adeguate" misure di sicurezza (sia minime sia idonee) a garanzia dei dati personali raccolti

e gestiti (come la installazione di adeguati sistemi hardware e software, la previsione di sistemi crittografici, o l'apposizione di adeguati firewall). La conseguenza comporta che, in caso di violazione o di non rispetto di queste regole, sussistono sanzioni penali, amministrative e civili (come il risarcimento del danno) nei confronti del provider.

Sostanzialmente si prevede che, in caso di inadempimento in riferimento all'adozione delle c.dd. misure minime di sicurezza per il trattamento dei dati personali, o in caso di altra forma di violazione che concretizzi un illecito, il provider (o chi si trova nelle sue stesse condizioni) può incorrere in sanzioni amministrative come previsto dal Codice della privacy, e cioè: a) da 5.000 a 30.000 euro per informativa omessa o non idonea (art. 161 d.lgs. n.196/20039; b) da 10.000 a 60.000 euro per notificazione omessa o incompleta (art. 163 d. lgs. n. 196/2003); c) da 4.000 a 24.000 euro per omessa informazione al garante (art. 164 d. lgs. n. 196/2003); d) da 5.000 a 30.000 per cessione dei dati (art. 162 d. lgs. n. 196/2003). Inoltre può incorrere in sanzioni penali fino a tre anni di reclusione per: a) falsa notifica e false informazioni al Garante (art. 168 d. lgs. n. 196/2003), b) trattamento illecito dei dati personali, c) illecita comunicazione a terzi, d) diffusione dei dati (art. 167 d. lgs. n. 196/2003), e) omessa adozione delle misure necessarie (art. 169 d. lgs. n. 196/2003), ed f) inosservanza dei provvedimenti del Garante (art. 170 d. lgs. n. 196/2003). Infine il soggetto dovrà rispondere civilmente attraverso l'obbligo di risarcimento danni qualora non sia in grado di dimostrare di aver adottato tutte le contromisure idonee per evitare il danno stesso (artt. 15 d. lgs. n. 196/2003 e 2050 c.c.).

6. Il fenomeno del Datamining è connesso, in qualche modo, a quello dei cookies, in quanto anch'esso riguarda il trattamento dei dati e delle informazioni. Nasce negli USA nel 1995 e in Italia si incomincia a parlarne nel 2001.

È dal Datamining che discende un fenomeno più complesso, ben conosciuto in ambiente imprenditoriale con la sigla Kdd (=per Knowledge discovery in database). Il Kdd consiste in una complessa procedura informatica che viene effettuata su una enorme mole di dati con il fine di estrapolarne ed elaborarne ulteriori informazioni. Questo processo viene definito di acquisizione di conoscenza da dati (=da qui l'acronimo inglese Kdd).

Il processo consiste in una fase iniziale di raccolta ed immissione dati (=c.d. input di dati grezzi) ed in una fase successiva di produzione di informazioni utili (c.d. output di dati) derivanti dalla elaborazione dei dati raccolti. Il procedimento abbastanza complesso si articola in varie fasi: a) nella selezione dei dati che vengono catalogati in insiemi secondo determinati criteri (ad esempio i database utili per il marketing conterranno tutte le informazioni che riguardano gli acquisti effettuati dai clienti, gli stili di vita, l'aspetto finanziario e i dati demografici); b) nella ripulitura; c) nella loro trasformazione, così che possano essere utilizzati (ad esempio da valori nominali in valori numerici); d) nella loro interpretazione, per poterne ricavare dati "diversi" (da quelli raccolti) che diventando, così, una nuova fonte di conoscenza.

È possibile applicare questo processo di trattamento dati in vari settori dell'attività umana, quali ad esempio le assicurazioni, le banche, la sanità e, non ultimo, il commercio elettronico. Nelle attività bancarie, ad esempio, il datamining trova un terreno fertile nelle analisi di credit risk, attraverso lel quali le banche valutano le varie richieste di credito e, secondo un punteggio assegnato ai clienti che fanno richieste di fido, in base alla classe di rischio che viene loro assegnata, decidono se concedere o meno il prestito.

È evidente il motivo per cui il fenomeno è stato oggetto di interesse, data la sua obiettiva utilità a fini di marketing. Infatti, dal processo di gestione delle informazioni raccolte, un'azienda può elaborare, con relativa semplicità, un profilo dettagliato dei propri clienti (o potenziali tali), valutare le opportunità di vendita, capire come fidelizzare il cliente, porre in essere un piano di crescita e di fatto diminuire i rischi e ottimizzare le risorse investite nell'attività d'impresa. Attraverso un'operazione di datamining i dati raccolti, opportunamente elaborati, possono, infatti, fornire previsioni su contenuti e prodotti di maggiore interesse per un particolare tipo di utenza.

Il fenomeno, di per sé, è lecito, poiché si basa su dati "anonimi" o comunque "anonimizzati". Ma anche qui il rischio di sfociare nella illiceità per violazione di privacy è molto forte.

Tempo fa, incuriosì molto un progetto del Mit, denominato Cheese (la notizia risale ad un articolo "datato", apparso sulla rivista telematica zewsnews.it e citato in sitografia), pensato per monitorare e registrare i movimenti, consci ed inconsci, del mouse, così da poter tracciare un profilo dell'utente

rivolto non solo a capirne i gusti ma addirittura a prevederne le mosse.
Il programma utilizzato (che non ha nulla di fantascientifico in quanto, a detta degli studiosi, ha lo stesso codice dello sript "OnMouseMove", conosciuto in ambiente Javascript e che sostanzialmente permette di raccogliere le coordinate del mouse in movimento) sarebbe in grado di analizzare le varie fasi della consultazione che l'utente pone in essere durante la visita ad una pagina web (più tecnicamente ad un file .html). Questo software di fatto è in grado di monitorare anche gli istanti di indugio del soggetto su di un link, o le scelte effettuate tra un link e l'altro, ed addirittura anche su parti bianche della pagina web, denotandone un eventuale fattore di stress. Fu spiegato dai programmatori che il software non faceva altro che tracciare e, quindi, registrare, i movimenti del mouse, col risultato di creare una mappa dei movimenti del visitatore, formata da migliaia di punti che si concentrano nell'area del sito maggiormente consultata. In questo modo, in base alla densità dei "puntini" registrati dal software, è facile comprendere quali sono le "parti" più gradite dall'ospite o prevedere eventuali richieste da parte del "consumatore".

Il progetto appariva (non se ne sa più nulla) indubbiamente inquietante soprattutto per lo sviluppo delle problematiche giuridiche che una tale prassi può sollevare, in quanto il software utilizzato non prevede (o almeno non prevedeva all'epoca) l'aggiunta o l'utilizzo di plug in o di strumenti tecnologici di cui l'utente potesse avvertire la presenza e di cui essere informato, ma utilizzava i dati, forniti del tutto incosciamente dall'utente, attraverso una raccolta statistica opportunamente rielaborata dei propri movimenti in Rete.

Questo caso emblematico, fa comprendere quanto sia difficile prendere una posizione chiara e decisa (ma che sia anche la più equilibrata possibile) di fronte al fenomeno della raccolta di dati, perché se è vero che, da un lato questa prassi risulta particolarmente utile, e non necessariamente nociva, per le aziende, per i siti che svolgono attività commerciale on line e per il marketing in genere, dall'altro appare evidente quanto possa essere pericolosa per l'utente/consumatore. Ritornando al caso Cheese, il test effettuato dal MIT su 17 soggetti scelti, evidenziò il pericoloso sviluppo delle potenzialità del sistema, quando si scoprì che il software riusciva a monitorare anche quei casi in cui alcuni dei soggetti studiati posizionavano il mouse in parti prive di link (zone bianche del sito visitato). Opportunamente interrogati su questa loro abitudine, i soggetti ammettevano la loro insicurezza e la loro paura di cliccare inavvertitamente su link sbagliati, dimostrandosi dei soggetti a rischio, ossia potenziali e/o latenti soggetti stressati e nervosi. Ebbene, si pensi per un attimo a come potrebbe essere sfruttata, in futuro, una simile

informazione da parte di industrie farmaceutiche che sarebbero in grado di proporre a questi "potenziali clienti", in tempo reale, medicinali antistress!

(…)

Documentazione allegata

Esempio di una sezione di Privacy-Policy presente in un sito.

LA PRIVACY POLICY DI QUESTO SITO

PERCHÈ QUESTO AVVISO

In questa pagina si descrivono le modalità di gestione del sito in riferimento al trattamento dei dati personali degli utenti che lo consultano.

Si tratta di un'informativa che è resa anche ai sensi dell'art. 13 d.lgs. n. 196/2003 a coloro che interagiscono con i servizi *web* della XXXXXXXXXXXXXXX S.r.l., accessibili per via telematica a partire dall'indirizzo:

http://www.xxxxx.it

corrispondente alla pagina iniziale del sito ufficiale della Società.

L'informativa è resa solo per il sito della XXXXXXXXXXX e non anche per altri siti *web* eventualmente consultati dall'utente tramite *link*.

L'informativa si ispira anche alla Raccomandazione n. 2/2001 che le autorità europee per la protezione dei dati personali, riunite nel Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE, hanno adottato il 17 maggio 2001 per individuare alcuni requisiti minimi per la raccolta di dati personali *on-line*, e, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine *web*, indipendentemente dagli scopi del collegamento.

IL "TITOLARE" DEL TRATTAMENTO

A seguito della consultazione di questo sito possono essere trattati dati relativi a persone identificate o identificabili.

Il "titolare" del loro trattamento è il Sig.XXXXXXXXXx, della XXXXXXXX S.r.l., che ha sede

in XXXXXXXX (Italia), Via XXXXXXXXXX n. XXXXXX Cap. XXXXXXXX

LUOGO DI TRATTAMENTO DEI DATI

I trattamenti connessi ai servizi *web* di questo sito hanno luogo presso la predetta sede della XXXXXXX e sono curati solo da personale tecnico della Società incaricato del trattamento, oppure da eventuali incaricati di occasionali operazioni di manutenzione.

Nessun dato derivante dal servizio *web* viene comunicato o diffuso.

I dati personali forniti dagli utenti che inoltrano richieste di invio di materiale informativo (bollettini, Cd-rom, *newslette*r, relazioni annuali, risposte a quesiti, atti e provvedimenti, ecc.) sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia a tal fine necessario (spedizionieri, tecnici, sviluppatori).

TIPI DI DATI TRATTATI

Dati di navigazione

I sistemi informatici e le procedure *software* preposte al funzionamento di questo sito *web* acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione *URI (Uniform Resource Identifier)* delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal *server* (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime

sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, allo stato i dati sui contatti *web* non persistono per più di sette giorni.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.

Specifiche informative di sintesi verranno progressivamente riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.

COOKIES

Nessun dato personale degli utenti viene in proposito acquisito dal sito.

Non viene fatto uso di *cookies* per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. *cookies* persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. *cookies* di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal *server*) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I c.d. *cookies* di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

FACOLTATIVITÀ DEL CONFERIMENTO DEI DATI

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali riportati nei moduli di richiesta (forms) alla XXXXXXX o comunque indicati nei

contatti per sollecitare l'invio di materiale informativo o di altre comunicazioni.

Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

Per completezza va ricordato che in alcuni casi (non oggetto dell'ordinaria gestione di questo sito) l'Autorità può richiedere notizie e informazioni ai sensi dell'art 157 del d.lgs. n. 196/2003, ai fini del controllo sul trattamento dei dati personali. In questi casi la risposta è obbligatoria a pena di sanzione amministrativa.

MODALITÀ DEL TRATTAMENTO

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

DIRITTI DEGLI INTERESSATI

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte alla XXXXXXXXXX S.r.l..

P3P

La presente informativa sulla *privacy* è consultabile in forma automatica dai più recenti *browser* che implementano lo *standard* P3P ("*Platform for Privacy Preferences Project*") proposto dal *World Wide Web Consortium* (www.w3c.org).

Ogni sforzo verrà fatto per rendere il più possibile interoperabili le funzionalità di questo sito con i meccanismi di controllo automatico della *privacy* disponibili in alcuni prodotti utilizzati dagli utenti.

Considerando che lo stato di perfezionamento dei meccanismi automatici di controllo non li rende attualmente esenti da errori e disfunzioni, si precisa che il presente documento, pubblicato all'indirizzo

htt://www.XXXXXXX.it/privacy.htm ,

costituisce la "*Privacy Policy*" di questo sito che sarà soggetta ad aggiornamenti (restano le varie versioni consultabili al medesimo indirizzo).

Esempio di una sezione di disclaimer presente in un sito e contente l'informativa sull'uso dei cookies.

INFORMATIVA AI SENSI DEL D.LGS N° 196/2003

Finalità del trattamento dei dati:

Ai sensi dell'art.130 comma 4 del Codice della Privacy, D.lgs. n. 196/2003, le Vostre coordinate di posta elettronica da Voi forniteci nel contesto dei nostri precedenti rapporti commerciali, o richiesti all'atto dell'iscrizione al sito e forniti in modo volontario, potranno essere utilizzate per l'invio di comunicazioni o materiale pubblicitario o per finalità di vendita diretta. Titolare del trattamento è la ns. impresa XXXXXX srl via XXXXXX, n. XXXX, Città: XXXXX (Italy) e per le finalità sopra indicate i dati suddetti verranno a conoscenza degli incaricati del ns. Ufficio marketing.

Modalità e sicurezza del trattamento dei dati:

I Vostri dati personali saranno trattati con l'ausilio di strumenti informatici e telematici adottando tutte le misure di sicurezza informatiche consigliate dalla legge per tutelare e garantire la riservatezza dei Vostri dati personali e ridurre, nei limiti del possibile, il pericolo dell'accesso abusivo, del furto o della manomissione dei Vostri dati personali. È impossibile, al contempo, navigare in rete senza essere "sorvegliati". La trasmissione dei Vostri dati personali a www.XXXX.it (e altri domini del gruppo) avviene quindi sempre sotto la Vostra responsabilità.
La procedura di iscrizione ai servizi non deve essere utilizzata con caselle di posta altrui. Siamo contrari a qualsiasi forma di violazione della privacy esercitata a danno di terzi, pertanto non è lecito utilizzare i meccanismi di iscrizione con indirizzi di posta elettronica diversi da quelli propri.

Conferimento dei dati:

Il conferimento dei Vostri dati personali è facoltativo in quanto i download del sito www.XXXXX.it (e altri domini del gruppo) sono accessibili a tutti, ad eccezione delle attività riservate agli utenti registrati all'area riservata.
Con l'iscrizione all'area riservata, acconsentite espressamente al trattamento dei Vostri dati personali.
Non verranno raccolti in nessun caso i Vostri dati "sensibili" (stato di salute, religione,

etc.).

Correzione/Aggiornamento dei dati personali:

Vi ricordiamo che potrete opporVi in ogni momento al trattamento in oggetto, mediante l'invio di una e-mail al seguente indirizzo: via XXXXXXX, città, XXXXXXX (Italy) e-mail: xxx@xxxxxxx.it o di un telefax n. XXXXXXXx, nonché esercitare tutti i diritti di cui all'art. 7 del d.lgs.vo n. 196/2003 (tra cui i diritti di accesso, rettifica, aggiornamento, cancellazione).

INFORMATIVA SULL'UTILIZZO DEI COOKIES

Nel sito www.XXXXXXX.it (e altri domini del gruppo) di proprietà della XXXXXX srl non si utilizzano i c.d. "cookies" persistenti di alcun tipo, né si tracciano gli indirizzi IP, né ci si avvale di altri sistemi analoghi di tracciamento duraturo degli utenti.
L'uso dei cookies di sessione (cioè temporanei che decadono alla chiusura del browser) è strettamente funzionale all'ottimizzazione della funzione del sito, e quindi a garantire la migliore navigazione nell'ambito del sito.
Altri siti a cui questo sito si può eventualmente "linkare" potrebbero contenere sistemi di tracciamento cui il titolare del sito è estraneo.

(…)