ARTICOLO 29 - GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI

5063/00/IT/DEF.
WP 37

Documento di lavoro

Tutela della vita privata su Internet
- Un approccio integrato dell'EU alla protezione dei dati on-line-

adottato il 21 novembre 2000

Il Gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo indipendente di consulenza dell'UE per la protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE. Il servizio di segretariato è fornito da:

Commissione europea, DG Mercato Interno, Unità Libera circolazione delle informazioni e protezione dei dati.
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgio - Ufficio: C100-2/133
Indirizzo Internet: www.europa.eu.int/comm/dg15/en/media/dataprot/index/htm

CAPITOLO 1: INTRODUZIONE

Il presente documento intende offrire un approccio comunitario integrato alla protezione dei dati on-line. Il termine "integrato" sottolinea il fatto che questa analisi parte principalmente dai testi sia della direttiva generale sulla protezione dei dati (direttiva 95/46/CE) sia della direttiva sulla tutela della vita privata e le telecomunicazioni (direttiva 97/66/CE), ma tiene in considerazione e riunisce altresì tutti i pareri e documenti sinora adottati dal Gruppo di lavoro su taluni temi critici correlati all'argomento in questione[1].

In varie occasioni in passato, il Gruppo di lavoro, nel discutere le priorità riguardanti l'attività futura, ha confermato la necessità di affrontare le tematiche relative alla protezione dei dati correlata all'uso di Internet. Per trattare tali temi in modo sistematico ed efficace, è stata istituita nel 1999 la cosiddetta Internet Task Force (ITF), la cui finalità principale è riunire le risorse e competenze delle varie autorità per la protezione dei dati al fine di contribuire all'interpretazione e l'applicazione uniformi del quadro giuridico esistente in questo settore. L'ITF ha elaborato vari documenti, che sono stati adottati dal Gruppo di lavoro nel corso degli ultimi due anni. Dall'inizio del 2000, l'ITF ha intensificato i propri incontri allo scopo di elaborare un documento di sintesi che possa servire da riferimento per affrontare le tematiche attuali e, per quanto possibile, future relative alla tutela della vita privata su Internet.

L'obiettivo principale di questo documento è offrire un primo approccio al problema della tutela della vita privata on-line, che possa servire a sensibilizzare il pubblico sui rischi per la vita privata correlati all'uso di Internet e che possa, al contempo, agevolare l'interpretazione delle due direttive in questo settore. Il Gruppo di lavoro è conscio del fatto che la tutela della vita privata rappresenta una delle maggiori preoccupazioni degli utenti del web[2]. Per il Gruppo di lavoro è pertanto particolarmente importante affrontare questo tema ed esso è consapevole del fatto che alcune questioni controverse, che sollevano un particolare dibattito, potrebbero richiedere interventi futuri.

- Questo documento non si propone di essere completo in sé, ma intende illustrare le situazioni più tipiche in cui gli utenti Internet possono imbattersi utilizzando i servizi

[1] In particolare: parere 1/98: Piattaforma per le preferenze in materia di protezione della vita privata (P3P) e la norma aperta per i profili (OPS), adottato dal Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali il 16 giugno 1998; documento di lavoro: Trattamento dei dati personali in Internet, adottato dal Gruppo di lavoro il 23 febbraio 1999, WP 16, 5013/99/IT/def.; raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware, adottata dal Gruppo di lavoro il 23 febbraio 1999, 5093/98/IT/def., WP 17; raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni, adottata il 3 maggio 1999, 5005/99/def., WP 18; parere 3/99 relativo all'informazione del settore pubblico e la protezione dei dati personali, adottato dal Gruppo di lavoro il 3 maggio 1999; raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei *fornitori di servizi Internet* a fini giudiziari, adottata il 7 settembre 1999, 5085/99/IT/def., WP 25; parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali presentato dall'Internet Task Force, adottato il 3 febbraio 2000, 5007/00/IT/def., WP 28; parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni, presentato dall'Internet Task Force, adottato il 3 febbraio 2000, WP 29, 5009/00/IT/def.; parere 5/2000 sull'uso degli elenchi pubblici per i servizi di ricerca derivata o a criteri multipli (elenchi derivati), WP 33, adottato il 13 luglio 2000 e il parare 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 COM (2000) 385, adottato il 2 novembre 2000, WP 36.

[2] Secondo quanto è emerso da una studio semestrale recentemente pubblicato dalla Markle Foundation. V. articolo di AARON, D., *A Euro-American proposal for privacy on the Net,* Washington Post, 2 agosto 2000.

disponibili in rete (come posta elettronica, navigazione, ricerca, gruppi di discussione, ecc.). In considerazione del suo carattere generale, esso non si occupa di temi specifici che potrebbero richiedere un ulteriore approfondimento da parte del Gruppo di lavoro in futuro, tra cui il controllo della posta elettronica dei dipendenti sul posto di lavoro. Il presente documento di lavoro di basa sull'attuale stato dell'arte di Internet che, per sua natura, è un fenomeno molto dinamico ed in continua evoluzione.

Per agevolare la lettura, il documento di lavoro riporta all'inizio una descrizione tecnica di base nonché le questioni giuridiche di carattere generale. In seguito, vengono descritti separatamente tutti i vari servizi Internet affrontando, in ogni capitolo, sia i temi tecnici che giuridici in gioco. Un capitolo specifico è dedicato alle misure e tecnologie intese al miglioramento della tutela della vita privata che possono essere utilizzate per accrescere la tutela della vita privata degli utenti Internet. L'ultimo capitolo contiene le conclusioni.
Al documento è stato accluso un glossario di termini tecnici per consentire ai lettori di comprendere i concetti tecnici utilizzati nel testo del documento. Tutte le parole in corsivo sono riportate nel glossario.

L'ITF ha scelto deliberatamente di mantenere, nel testo del documento, un certo grado di sovrapposizione al fine di consentire una lettura selettiva da parte dei lettori particolarmente interessati ad un determinato argomento. A tale scopo, sono state mantenute nel testo alcune descrizioni supplementari, talvolta ripetitive, per facilitare la consultazione dei vari capitoli.

L'attività dell'Internet Task Force è stata coordinata da Peter HUSTINX, presidente dell'autorità olandese per la protezione dei dati. La versione consolidata del documento di lavoro è stata predisposta da un gruppo redazionale nominato in seno all'ITF e composto da Diana ALONSO BLAS (Autorità olandese per la protezione dei dati) e Anne-Christine LACOSTE (Autorità belga per la protezione dei dati). Il lavoro svolto dal gruppo redazionale ha riguardato, in particolare, la strutturazione e la verifica della coerenza dell'intero documento, l'integrazione e l'ulteriore sviluppo di altri temi giuridici ed informazioni tecniche, nonché i commenti pervenuti da altre delegazioni, l'elaborazione del glossario tecnico e le conclusioni.

I delegati delle autorità per la protezione dei dati di sei paesi hanno partecipato alle varie fasi dell'attività dell'Internet Task Force, preparando i documenti che sono serviti da base per una serie di capitoli, commentando i contributi di altri membri dell'ITF e contribuendo alle discussioni nel corso dei cinque incontri dell'ITF del 2000.
In particolare, le seguenti persone meritano di essere citate: Anne-Christine Lacoste e Jean-Marc Dinant (Belgio), Ib Alfred Larsen (Danimarca), Marie Georges (Francia), Angelika Jennen e Sven Moers (Germania), Emilio Aced Félez (Spagna) e Diana Alonso Blas, Ronald Hes e Bernard Hulsman (Paesi Bassi). L'ITF desidera ringraziare, per l'aiuto e l'assistenza, Christine Sottong-Micas (segreteria del Gruppo di lavoro istituito dall'articolo 29, Commissione europea) e Karola Wolprecht (sessione di formazione 1999/2000 presso la Commissione europea).

CAPITOLO 2: DESCRIZIONE TECNICA DI INTERNET

I. Elementi fondamentali

Internet è una rete di computer che comunicano tra loro in base al Transport Control Protocol/Internet Protocol (TCP/IP)[3]. Si tratta di una rete internazionale di computer interconnessi, che consente a milioni di persone di comunicare tra loro nel "cyberspazio" ed accedere ad enormi quantità di informazioni da ogni parte del mondo[4].

Dal punto di vista storico, il predecessore di Internet è la rete militare ARPAnet (1969). L'idea di base era realizzare una rete digitale transamericana, che consentisse ai computer dei fornitori dell'esercito e delle università che conducevano attività di ricerca correlate alla difesa di comunicare tra loro attraverso canali ridondanti, anche nel caso in cui alcune porzioni della rete venissero danneggiate durante la guerra[5].

I primi programmi di posta elettronica hanno fatto il loro esordio nel 1972. Nel 1985, la American National Science Foundation ha realizzato la rete NSFNET per collegare sei centrali di supercomputer statunitensi. Alla fine degli anni '80, questa rete è stata trasferita ad un gruppo di università denominato MERIT. La rete si aprì sempre di più alle istituzioni non universitarie e alle organizzazioni non statunitensi. Nel 1990, Tim Berners Lee, che lavorava presso il CERN di Ginevra, ha progettato il primo browser e applicato il concetto di *collegamento ipertestuale*, cui da allora continua ad aggiungersi una serie di nuovi servizi e funzionalità.

E' tuttavia necessario tenere presente che il TCP/IP resta tuttora il *protocollo* principale utilizzato per la trasmissione dei dati attraverso Internet e che tutti i servizi si basano su di esso. Questo *protocollo* è stato progettato in modo che fosse molto semplice da impostare ed è indipendente da qualsiasi particolare computer o sistema operativo.

In Internet, ogni computer è identificato da un unico indirizzo IP numerico nella forma di A.B.C.D. dove A, B, C e D sono numeri da 0 a 255 (ad esempio, 194.178.86.66).

Una *rete TCP/IP* si basa sulla trasmissione di piccoli pacchetti di informazioni. Ogni pacchetto comprende l'indirizzo IP del mittente e del destinatario. Questa rete è priva di connessioni. Ciò significa che a differenza, ad esempio, della rete telefonica, non è necessaria alcuna connessione preliminare tra due dispositivi perché le comunicazioni possano iniziare. Significa inoltre che sono possibili, contemporaneamente, molte comunicazioni con molti interlocutori diversi.

Il Sistema dei nomi di dominio (*Domain Name System - DNS)* è un meccanismo che consente di assegnare dei nomi ai computer identificati dall'indirizzo IP. Questi nomi assumono la forma di <nome>.primo livello dove il <nome> è una stringa costituita da una o più stringhe secondarie separate da un punto. Il dominio di primo livello può essere un dominio generico come “com” per i siti web commerciali o “org” per le

[3] Gli aspetti tecnici descritti nel presente documento sono stati notevolmente semplificati per renderli comprensibili ai profani. Per maggiori particolari, vedere la *comunicazione della Commissione al Parlamento europeo e al Consiglio "L'organizzazione e la gestione di Internet- Aspetti di politica internazionale ed europea"*, 1998- 2000, COM (2000) 202 def., 11 aprile 2000.

[4] Vedere la sentenza Reno contro ACLU del 26 giugno 1997, Corte suprema degli Stati Uniti, disponibile su www2.epic.org/cda/cda_decision.html

[5] Vedere la sentenza Reno contro ACLU del 26 giugno 1997.

organizzazioni senza scopo di lucro, oppure un dominio geografico come “be” per il Belgio.
Il *DNS* è a pagamento e le società o i singoli che desiderano un nome di dominio devono identificarsi. Alcuni strumenti pubblici in rete consentono di risalire al collegamento tra il nome di dominio e la società, nonché tra l'indirizzo IP e il nome di dominio. Un nome di dominio non è indispensabile per collegare un computer a Internet. I nomi di dominio sono dinamici. Un unico computer Internet può avere uno o più nomi di dominio (o non averne affatto), ma un nome di dominio specifico corrisponde sempre ad un particolare indirizzo IP.

Attualmente esiste un numero limitato di indirizzi IP. Tale numero dipende dalla lunghezza del campo assegnato all'indirizzo IP nel *protocollo*[6]. In Europa, gli indirizzi IP vengono assegnati, mediante una procedura internazionale[7], ai fornitori di accesso Internet i quali li riassegnano ai rispettivi client, organizzazioni o singoli. Utilizzando uno strumento di ricerca disponibile al pubblico come http://www.ripe.net/cgi-bin/whois, è possibile identificare il responsabile dell'allocazione di un determinato indirizzo IP.

Si tratterà di solito:

- del gestore di una LAN (Local Area Network) collegata ad Internet (ad esempio, una PMI o un'amministrazione pubblica). In tal caso, il gestore in questione dovrà utilizzare probabilmente un regime di indirizzi IP fissi e conservare un elenco della corrispondenza intercorsa tra i computer e gli indirizzi IP. Se il soggetto in questione utilizza il *Dynamic Host Configuration Protocol* (DHCP[8]), il programma *DHCP* terrà in genere un registro contenente il numero di scheda Ethernet. Questo numero internazionale esclusivo identifica un determinato computer all'interno della LAN.

- di un fornitore di accesso Internet, che abbia stipulato un contratto con un abbonato Internet. In questo caso, il fornitore terrà in genere un logfile con l'indirizzo IP allocato, il numero di identificazione dell'abbonato, la data, l'ora e la durata di allocazione dell'indirizzo. Inoltre, se l'utente Internet utilizza una rete di telecomunicazione pubblica (telefono cellulare o fisso), il numero chiamato (e la data, l'ora e la durata) saranno registrati dalla società telefonica a scopo di fatturazione.

- del titolare del nome di dominio, che potrebbe essere il nome di una società, il nome di un dipendente di una società o un privato cittadino.

In questi casi, con l'aiuto del responsabile dell'allocazione, un utente Internet (ossia i relativi dati anagrafici: nome, indirizzo, numero di telefono, ecc.) può essere identificato mediante strumenti ragionevoli.

Un *router* è un dispositivo importante che fornisce i percorsi per le *reti TCP/IP*.

---

[6] E' attualmente in fase di sviluppo la versione aggiornata (IP versione 6) del sistema di indirizzamento IP, basata su numeri aventi una lunghezza di 128 bit.

[7] La Internet Corporation for Assigned Names and Numbers (ICANN) è un'organizzazione senza fini di lucro istituita per assumersi la responsabilità dell'allocazione degli spazi di indirizzo del protocollo IP (http://www.icann.org). In Europa, lo spazio di indirizzo è gestita dall'organizzazione RIPE (Réseaux IP Européens) (http://www.ripe.net). Per ulteriori particolari sul processo evolutivo dei nomi di dominio Internet, v. la comunicazione della Commissione di cui alla nota 2.

[8] Il *protocollo* Dynamic Host Configuration (DHCP) è un protocollo Internet che consente di automatizzare la configurazione dei computer che usano il TCP/IP. Il DHCP può essere utilizzato per assegnare indirizzi IP in automatico (http://www.dhcp.org).

Ciò significa che il percorso TCP/IP è dinamico, in funzione dei guasti o del sovraccarico di alcuni percorsi o collegamenti. Può inoltre essere utilizzato come 'parete tagliafuoco' tra un'organizzazione e Internet e può garantire, in particolare, che da un determinato fornitore di servizi Internet possano derivare solo indirizzi IP autorizzati.

E' importante osservare che la velocità di trasmissione è l'unico e il principale criterio di instradamento nelle reti TCP/IP. Con le informazioni che circolano quasi alla velocità della luce, può essere più conveniente, in presenza di un ingorgo di rete a Parigi, instradare i pacchetti TCP/IP da Londra a Madrid via New York. Alcuni strumenti consentono all'utente della rete di conoscere il percorso tra due punti, che tuttavia può cambiare teoricamente ogni secondo, anche durante il trasferimento di una sola pagina web.

Protocolli più sofisticati che utilizzano il protocollo TCP/IP

Oltre al protocollo TCP/IP, è stata studiata una serie di *protocolli* per la fornitura di alcuni servizi. Fondamentalmente, i *protocolli* più diffusi sono:

- HTTP (HyperText Transport Protocol) usato per la navigazione,
- FTP (File Transfer Protocol) usato per trasferire i file,
- NNTP (News Network Transport Protocol) usato per accedere ai gruppi di discussione in rete (newsgroup),
- SMTP (Simple Mail Transport Protocol) e i *protocolli* POP3 (usati per inviare e ricevere messaggi di posta elettronica).

Strati e gerarchia dei protocolli di un processo di comunicazione Internet

<table>
<tr><td>HTTP
usato per navigare ed effettuare ricerche</td><td>SMTP
usato per inviare la posta elettronica</td><td>POP3
usato per scaricare messaggi di posta elettronica dal server di posta al client</td><td>NNTP
usato per trasferire notizie</td><td>FTP
usato per scaricare o caricare i file</td><td>Ecc.
Sono in uso o in fase di sviluppo molti altri protocolli di primo livello</td></tr>
<tr><td colspan="6">TCP/IP</td></tr>
<tr><td>PPP
usato dai modem sulle linee telefoniche</td><td>X-75
usato dall'adattatore di terminale sulle linee ISDN</td><td>ADSL
usato da un modem ADSL sulle linee telefoniche standard</td><td>ETHERNET
usato dalle schede LAN su una Local Area Network</td><td colspan="2">Ecc.
Sono in uso o in fase di sviluppo molti altri protocolli di secondo livello</td></tr>
</table>

- Questi *protocolli* sono necessari poiché il *protocollo* TCP/IP permette solo la trasmissione di blocchi di informazioni da un computer all'altro. Il computer che fornisce un servizio è chiamato SERVER. Il computer che utilizza un servizio è chiamato CLIENT. Per fornire un servizio tecnico, sia il client che il server utilizzano lo stesso protocollo, cioè le stesse regole di comunicazione. Internet viene spesso definita una rete client/server. E' importante osservare che il protocollo TCP/IP viene sempre utilizzato da

ogni servizio sopra citato, indipendentemente dal tipo usato. Ciò significa che, quando si utilizzano i servizi presenti sul web, saranno presenti rischi per la vita privata correlati al *protocollo* TCP/IP.

• Per evitare malintesi relativi al significato generale della parola "servizio", in questo documento il termine *protocollo* sarà usato per designare i protocolli HTTP, FTP, NNTP e altri servizi disponibili su Internet.

Un *proxy* server è un server intermedio tra l'utente Internet e la rete. Funge da *web cache*, migliorando sensibilmente il tasso di visualizzazione delle informazioni (ad esempio, la visualizzazione di pagine web). Molte grandi organizzazioni o fornitori di accesso Internet hanno già adottato questa soluzione. Le pagine, le immagini o i logo scaricati dall'esterno da parte di un membro di un'organizzazione vengono memorizzati in una memoria cache nel *proxy* e verranno messi immediatamente a disposizione anche degli altri membri dell'organizzazione.

II. GLI ATTORI COINVOLTI IN INTERNET

Occorre osservare che una società o un singolo possono svolgere ruoli diversi in relazione a Internet e potrebbero quindi eseguire, contestualmente, vari trattamenti di dati (ad esempio, la registrazione delle connessioni da parte di un operatore di telecomunicazioni e la memorizzazione da parte di un *fornitore di servizi Internet* dei siti web visitati), che comportanto l'applicazione dei principi sulla tutela della vita privata.

Operatore di telecomunicazioni

In Europa, l'infrastruttura di telecomunicazioni è de facto monopolio degli operatori di telecomunicazioni tradizionali. Tuttavia, questa situazione si sta evolvendo. Inoltre, tale monopolio si riduce spesso ai cavi o alle fibre ottiche, mentre per le comunicazioni senza fili e le tecnologie emergenti come *WAP, UMTS*, ecc., tra i vettori nazionali sta facendo capolino la concorrenza.

L'operatore di telecomunicazioni tradizionale, tuttavia, è ancora un attore importante poiché fornisce le comunicazioni di dati tra l'utente della rete e il fornitore di accesso Internet.

L'operatore di telecomunicazioni elabora le informazioni sul traffico a fini di fatturazione, tra cui il numero chiamante e la relativa localizzazione (per i telefoni mobili), il numero chiamato, la data, l'ora e la durata della comunicazione[9].

Fornitore di accesso Internet

Il fornitore di accesso Internet fornisce, solitamente su base contrattuale, una connessione TCP/IP a:

- i singoli che utilizzano un modem o un adattatore di terminale (ISDN). In questo caso, l'abbonato riceverà un indirizzo IP per la durata della connessione, che sarà probabilmente diverso alla connessione successiva. Si tratta di un indirizzo IP di tipo dinamico.

[9] Il periodo di trattamento e memorizzazione di tali dati è soggetto a severe norme giuridiche, come spiegato in seguito.

Per le connessioni effettuate da una linea ADSL o da un cavo video, solitamente l'indirizzo IP sarà di tipo statico, sempre che tali connessioni siano permanenti.

Per ottenere una connessione, il singolo[10] deve stipulare un contratto (dove l'abbonamento è gratuito) e fornire il proprio nome, indirizzo e altri dati personali. L'utente riceverà un proprio nome utente (una UserId che potrebbe essere uno pseudonimo) e una password, che impediranno l'uso dell'abbonamento da parte di terzi. Quanto meno per motivi di sicurezza, sembra che, di solito, i fornitori di accesso Internet "registrino" sistematicamente la data, l'ora, la durata e l'indirizzo IP dinamico fornito all'utente Internet in un apposito file. Finché sarà possibile collegare il registro all'indirizzo IP di un utente, tale indirizzo deve essere considerato alla stregua di un'informazione personale;

- le organizzazioni che usano una connessione telefonica o, più spesso, una linea affittata alla sede della società. Questa linea in affitto verrà fornita normalmente dall'operatore di telecomunicazioni tradizionale. Il fornitore di accesso Internet fornirà alla società gli indirizzi IP e utilizzerà un *router* per garantire che gli indirizzi vengano rispettati.

I fornitori di accesso Internet possiedono una o più linee in affitto (doppino incrociato, fibra ottica, collegamento satellitare) collegate ad altri fornitori di accesso Internet più grandi.

Fornitore di servizi Internet

I *fornitori di servizi Internet* forniscono servizi ai singoli e alle aziende sul web. Essi possiedono o affittano una connessione TCP/IP permanente e utilizzano server costantemente connessi a Internet. Di norma, essi forniscono l'ospitalità web (pagine web memorizzate sul proprio server web), l'accesso ai gruppi di discussione (newsgroup), l'accesso a un server FTP e la posta elettronica. Tutto ciò prevede l'uso dei *protocolli* HTTP, NNTP, FTP, SMTP e POP3 da parte di uno o più server.

Le imprese che operano in qualità di fornitori di accesso Internet offrono spesso anche servizi di *fornitori di servizi Internet*. Ecco perché il termine *fornitori di servizi Internet* viene utilizzato spesso anche in riferimento ai fornitori di accesso Internet. Ma, da un punto di vista concettuale, le regole sono diverse. Infatti, il fornitore di accesso Internet, fungendo da porta di accesso a Internet, instraderà tutto il traffico proveniente dall'abbonato Internet, mentre il *fornitore di servizi Internet* sarà al corrente solo di ciò che accade sui propri server[11]. In questo documento, il termine *fornitore di servizi Internet* viene generalmente utilizzato includendo i fornitori di accesso Internet. Il termine fornitore di accesso Internet, invece, viene usato solo quando è chiaro che si tratta di accesso ad Internet; in tutti gli altri casi, viene utilizzato il termine generico di *fornitore di servizi Internet*.

Da un punto di vista tecnico, è la presenza di server dotati di *protocolli* ad essere decisiva ai fini della raccolta di dati personali. Di solito, nel caso dei server HTTP, viene sistematicamente creato per default un registro o un logfile che può contenere, integralmente o in parte, i dati presenti nell'intestazione di richiesta HTTP (*browser chattering*) e l'indirizzo IP. Il registro è una prassi standard e viene creato da ogni server.

[10] Anche le piccole imprese possono stipulare tali contratti, ma tali casi non vengono presi in considerazione nel presente documenti.

[11] Il presente documento non si occuperà dei *fornitori di servizi Internet* in quanto fornitori di contenuti sebbene alcuni di essi svolgano questa funzione in talune circostanze (ad esempio, alcuni *fornitori di servizi Internet* possiedono un proprio *sito portale*).

Utente

L'utente Internet può essere un singolo che accede alla rete da casa propria, utilizzando di solito una connessione TCP/IP temporanea (e quindi un indirizzo IP dinamico) attraverso un modem, un adattatore di terminale (ISDN) o una connessione permanente (quindi un indirizzo IP statico) attraverso una linea ADSL, la televisione via cavo, ecc. E' inoltre possibile, anche se in genere più costoso, connettersi mediante un telefono mobile.

Qualora l'abbonato fornisca un'identità falsa o utilizzi l'identità di un altro utente (inserendo, di solito, il nome utente e la password di un terzo), è possibile risalire al titolare della linea cui è stato assegnato un determinato indirizzo IP confrontando queste informazioni con le informazioni contenute nel registro del fornitore di accesso Internet. E' quel che fa solitamente la polizia per individuare le intrusioni illecite nei computer collegati a Internet.

Lo stesso vale per l'utente che utilizza una rete LAN o Intranet.

L'utente può essere inoltre un'organizzazione, un'amministrazione pubblica o una società, che usano Internet non solo per fornire o reperire informazioni, ma anche per raccogliere dati ai fini delle proprie funzioni o attività (procedure amministrative, vendita di beni o fornitura di servizi, pubblicazione di elenchi, piccoli annunci, invio di questionari, ecc.).

III. SERVIZI DISPONIBILI SU INTERNET[12]

Chiunque abbia accesso a Internet può utilizzare una vasta gamma di metodi di comunicazione e reperimento delle informazioni. Tra i più comuni figurano la posta elettronica (v. capitolo 4), i gruppi di discussione e le chat room (v. capitolo 6), nonché il World Wide Web (v. capitolo 5).

Tutti questi metodi possono essere usati per trasmettere testi; la maggior parte è in grado di trasmettere suoni, fotografie e immagini in movimento. Nel complesso, questi strumenti costituiscono un supporto unico, conosciuto agli utenti con il nome di "cyberspazio", accessibile a tutti, in ogni parte del mondo, attraverso Internet.

Posta elettronica

La posta elettronica consente a una persona di inviare ad un'altra persona, o a un gruppo di destinatari, un messaggio elettronico. In genere, il messaggio viene memorizzato elettronicamente su un server, in attesa che il destinatario controlli la propria casella di posta, e talvolta segnala il proprio arrivo mediante un apposito avviso.

Gruppi di discussione (newsgroup)

I gruppi di discussione permettono di condividere informazioni o esprimere pareri su argomenti specifici. Sono costituiti, di solito, da gruppi di partecipanti regolari, i cui messaggi possono essere letti anche da altri. Esistono migliaia di gruppi simili destinati a promuovere lo scambio di informazioni o di opinioni su un particolare argomento. Ogni giorno, vengono inviati oltre 100.000 nuovi messaggi.

[12] Per una descrizione particolareggiata di questi servizi, vedere la sentenza Reno contro ACLU del 26 giugno 1997.

Chat room

Due o più persone che desiderano comunicare direttamente possono accedere a una chat room per avviare un dialogo in tempo reale, digitando messaggi che appaiono quasi immediatamente sullo schermo del computer degli interlocutori.

World Wide Web

Il metodo di comunicazione Internet più conosciuto è il World Wide Web, che consente agli utenti di cercare e reperire informazioni memorizzate in computer remoti. In parole povere, il web è costituito da una vasta gamma di documenti memorizzati in vari computer di tutto il mondo.

Navigare sul web è relativamente semplice. Un utente può digitare l'indirizzo conosciuto di una pagina o inserire una o più parole chiave nel "motore di ricerca" commerciale nel tentativo di localizzare siti sull'argomento di interesse. Generalmente, gli utenti esplorano una determinata pagina web o passano ad un'altra cliccando con il "mouse" del computer su una delle icone o dei collegamenti (link) presenti sulla pagina. Il web è pertanto paragonabile, dal punto di vista del lettore, a una vasta biblioteca comprendente milioni di pubblicazioni immediatamente disponibili e indicizzate, o a un enorme centro commerciale che offre beni e servizi (v. capitolo 7).

Qualsiasi persona o organizzazione in possesso di un computer collegato a Internet può "pubblicare" o raccogliere informazioni (v. capitoli 6, 7 e 8). Tra coloro che pubblicano o raccolgono dati figurano gli organismi governativi, le istituzioni educative, i soggetti commerciali, i gruppi di interesse e i singoli, i quali possono decidere di rendere disponibile il proprio materiale all'intero bacino di utenza Internet o di limitarne l'accesso ad un gruppo selezionato.

IV. Rischi per la vita privata[13]

Rischi per la vita privata inerenti all'uso del protocollo TCP/IP

Poiché Internet è stata considerata, sin dal suo esordio, una rete aperta, vi sono molte caratteristiche dei *protocolli* di comunicazione che, più per caso che per vera e propria natura, possono dar luogo ad interferenze nella vita privata degli utenti Internet.

Per quanto riguarda il protocollo TCP/IP, vi sono tre caratteristiche che sembrano rappresentare una potenziale interferenza nella vita privata.

- Il **percorso** seguito dai pacchetti TCP/IP è dinamico e segue la logica delle prestazioni. In teoria, esso può cambiare durante il trasferimento di una pagina web o la trasmissione di un messaggio di posta elettronica, ma in pratica rimane ampiamente statico. Nelle telecomunicazioni, le prestazioni sono legate più alla congestione della rete che alla distanza fisica tra i nodi di telecomunicazione (*router*). Ciò significa che la via "più breve" tra due città dello stesso paese europeo può passare attraverso un paese extracomunitario, che può essere dotato o meno di un adeguato regime di protezione dei dati[14]. Pur conoscendo il percorso seguito in un determinato momento, l'utente Internet medio non dispone di mezzi ragionevoli per poterlo modificare.

- A causa del fatto che la traduzione tra il nome di dominio e l'indirizzo numerico IP avviene attraverso un **server DNS,** la cui funzione è garantire tale traduzione, il server

[13] La CNIL francese dispone, all'interno del proprio sito web, di una sezione dal titolo "vos traces", che consente agli utenti Internet di visualizzare le tracce da essi lasciate utilizzando la rete. Questa sezione è disponibile in francese, inglese e spagnolo. V. www.cnil.fr

[14] Per maggiori particolari su questo argomento, v. il capitolo 2.

DNS riceve e può tenere traccia di tutti i nomi del server Internet che l'utente Internet ha tentato di contattare. In pratica, tali server DNS vengono mantenuti, principalmente, dai fornitori di accesso Internet, i quali hanno la capacità tecnica di conoscere molte più cose, come descriveremo nei prossimi capitoli.

- Il comando **ping**, disponibile in tutti i sistemi operativi, consente a chiunque sia presente su Internet di sapere se un determinato computer è acceso e connesso a Internet. Si tratta di un comando che prevede la digitazione delle lettere PING seguite dall'indirizzo IP (o dal nome corrispondente) di un computer selezionato. Di solito, l'utente del computer "preso di mira" non sa che qualcuno ha tentato di scoprire se era connesso a Internet in un determinato momento e non ne conosce i motivi.

Occorre osservare che le connessioni Internet permanenti via cavo o ADSL presentano gli stessi rischi.

Sebbene questi trattamenti di dati siano leciti e, in base alle circostanze, inevitabili per il buon funzionamento della rete Internet, l'utente Internet deve sapere che essi avvengono e deve conoscere le misure di sicurezza disponibili.

Rischi per la vita privata inerenti all'uso dei protocolli di primo livello

Questa sezione è incentrata su tre caratteristiche quasi sempre presenti quando viene implementato il *protocollo* HTPP nei browser più diffusi. Occorre osservare che una combinazione di queste caratteristiche può avere gravi conseguenze per la vita privata degli utenti Internet.

Il *protocollo* HTTP è di importanza strategica poiché è il *protocollo* principale usato sul web e può offrire servizi come la posta elettronica o i gruppi di discussione, che sinora erano stati in genere forniti da protocolli di primo livello specializzati, come POP3, SMTP o NNTP[15].

Browser chattering

E' generalmente noto che inserire l'indirizzo "http://www.website.org/index.htm" significa "mostrami la pagina chiamata "index.htm" del server www.website.org usando il *protocollo* HTTP". Si può pensare che vengano trasmessi al sito web solo l'indirizzo IP del navigatore e il file da visualizzare. Ma non è così.

La tabella che segue riporta alcuni dei dati che vengono trasmessi sistematicamente nell'intestazione HTTP nel corso di una richiesta HTTP (browser chattering automatico) e che sono quindi disponibili al server:

[15] V. DINANT, Jean-Marc, Law and Technology Convergence in the Data Protection Field? *Electronic threats to personal data and electronic data protection on the Internet*, Progetto ESPRIT 27028, Piattaforma sugli aspetti giuridici del commercio elettronico.

HTTP Var.	*Opera 3.50*	*Netscape 4.0 F*	*Explorer 4.0 Regno Unito*
GET	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0
Agente utente:	Mozilla/4.0(compatible; Opera/3.0; Windows 95) 3.50	Mozilla/4.04 [fr] (Win95; I ;Nav)	Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
Formati accettati:	image/gif, image/x-xbitmap, image/jpeg, /	Image/gif, image/x-xbitmap, image/jpeg	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, /
Pagina di riferimento:		Where.were.you/doc.htm	Where.were.you/doc.htm
Lingua :		Fr	fr-be

La definizione tecnica di questi campi può essere reperita nella RFC 1945 per il *protocollo* HTTP 1.0 o nella RFC 2068 per il *protocollo* HTTP 1.1.

- La prima riga è l'unica indispensabile.
- Alla riga dei formati accettati, ogni browser indica che l'utente Internet sta usando Windows 95. Ci si potrebbe chiedere perché. Netscape aggiunge che la versione del browser è in francese. Ogni browser fornisce l'identificazione del proprio nome, della propria versione e della propria sottoversione.
- Nella descrizione dei formati accettati, Microsoft informa ogni sito che sul computer dell'utente Internet sono installati i programmi PowerPoint, Excel e Word.
- "Opera" non rivela la pagina di riferimento.
- "Opera" non rivela la lingua parlata. Netscape rivela che l'utente Internet è di lingua francese. Microsoft rivela che l'utente Internet è un belga francofono.

Collegamenti ipertestuali invisibili

I collegamenti ipertestuali invisibili sono il valore aggiunto di Internet. Essi consentono di sfogliare, da un continente all'altro, premendo semplicemente il tasto del mouse. Ciò che non appare agli occhi dell'utente comune è che il software di browsing tradizionale permette di includere nella richiesta HTTP un comando di scaricamento delle immagini da inserire nel codice di pagina HTML. Non è necessario localizzare queste immagini nello stesso server di quello che ha ricevuto la chiamata originaria relativa ad una determinata pagina web.

In questo caso, la variabile HTTP_REFERER contiene l'indicazione della pagina di riferimento, cioè la pagina principale in cui verranno localizzate le immagini. In altre parole: se un sito web contiene, nella propria pagina web HTML, un collegamento invisibile ad un'immagine localizzata nel sito web di una società di 'cybermarketing', quest'ultima conoscerà la pagina di riferimento prima di inviare il banner pubblicitario. Durante una ricerca in un motore di ricerca, il nome della pagina web compenderà le parole chiave inserite.

Cookie

I *cookie* sono dati che possono essere memorizzati in file di testo sul disco fisso dell'utente Internet e conservati in copia dal sito web. Rappresentano una componente standard del traffico HTTP e, in quanto tali, possono essere trasportati, senza ostacoli, con il traffico IP.

Un *cookie* risiede sul disco fisso dell'utente e contiene informazioni personali che possono essere rilette dal sito web che le ha depositate o da chiunque conosca il formato dei dati del sito web in questione. Un *cookie* può contenere tutte le informazioni che il sito web desidera includervi: pagine visualizzate, annunci pubblicitari selezionati, numero di identificazione dell'utente, ecc.[16]. In alcuni casi, possono essere utili per fornire un determinato servizio attraverso Internet o per agevolare la navigazione da parte dell'utente Internet. Ad esempio, alcuni siti web personalizzati utilizzano i *cookie* per identificare gli utenti ogniqualvolta essi vi accedono ed evitare che debbano registrarsi di nuovo per controllare le proprie notizie.

Il SET-COOKIE si trova nell'intestazione di risposta HTTP[17], cioè nei *collegamenti ipertestuali* invisibili. Se viene stabilita una scadenza[18], il *cookie* verrà memorizzato sul disco fisso dell'utente Internet e ritrasmesso al sito web che lo ha originato (o ad altri siti web dello stesso sottodominio) per la durata prefissata. Questa ritrasmissione assumerà la forma di un campo COOKIE, che farà parte del browser chattering descritto in precedenza.

Unendo il browser chattering e i *collegamenti ipertestuali* invisibili, una società di 'cybermarketing' può, per default, conoscere tutte le parole chiave inserite da un determinato utente Internet nel motore di ricerca in cui la società sta effettuando la propria pubblicità, il computer, il sistema operativo, la marca del browser dell'utente Internet, l'indirizzo IP dell'utente, nonché l'ora e la durata delle sessioni HTTP. Questi dati grezzi consentono, se combinati con altri dati disponibili alla società, di ricavarne altri quali[19]:

1. Il paese in cui vive l'utente Internet.
2. Il dominio Internet cui appartiene l'utente.
3. Il settore di attività della società presso cui è occupato l'utente Internet.
4. Il fatturato e le dimensioni della società presso cui è occupato l'utente Internet.
5. Le funzioni e la qualifica del navigatore all'interno della società.
6. Il fornitore di accesso Internet.
7. Il tipo di siti web generalmente visitati.

Il *cookie* consente di inviare sistematicamente un identificativo permanente ed esclusivo insieme ad ogni richiesta di informazione, mentre l'indirizzo IP è un identificativo relativamente debole poiché può essere nascosto dai *proxy* e, a causa della propria natura dinamica, non è affidabile per gli utenti Internet che accedono alla rete via *modem*. Molte

[16] V. il libro di HAGEL III, J. e SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information*, Harvard Business School Press, 1999, p. 275.
[17] Dal punto di vista tecnico, è anche possibile creare i *cookie* in JavaScript o nei campi <META-HTTP EQUIV> presenti nel codice HTML.
[18] I *cookie* privi di scadenza fissa sono denominati "cookie di sessione" e scompaiono quando il browser viene scaricato o al termine della sessione.
[19] GAUTHRONET, Serge , "On-line services and data protection and the protection of privacy", Commissione europea, 1998, p. 31 e 92 disponibile su http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm

società di 'cybermarketing' hanno già messo in atto tale sistema di identificazione invisibile del cliente (elaborazione di profili)[20].

I rischi per la vita privata connessi all'implementazione del protocollo HTTP nei browser comuni

La combinazione del browser chattering, dei *collegamenti ipertestuali* invisibili e dei *cookie* consente di mettere in atto un sistema di identificazione invisibile (elaborazione di profili) di ogni singolo utente Internet che utilizza un browser installato per default. Questo sistema di identificazione non è in sé collegato al *protocollo* HTTP, secondo quanto definito dal W3C[21]. Inoltre, durante l'implementazione del protocollo HTTP[22], la definizione del *protocollo* HTTP 1.1 ha espressamente richiamato l'attenzione dell'industria su eventuali temi relativi alla tutela della vita privata:

– "*Having the user agent describe its capabilities in every request can be both very inefficient (given that only a small percentage of responses have multiple representations) and a potential violation of the user's privacy*" [page 68]
– "*It may be contrary to the privacy expectations of the user to send an Accept-Language header with the complete linguistic preferences of the user in every request"* [page 98]
– *" The client SHOULD not send the From header[23] field without the user's approval, as it may conflict with the user's privacy interests or their site's security policy. It is strongly recommended that the user is able to disable, enable, and modify the value of this field at any time prior to a request*." [page 118]

"*HTTP clients are often privy to large amounts of personal information (e.g. the user's name, location, mail address, passwords, encryption keys, etc.), and SHOULD be very careful to prevent unintentional leakage of this information via the HTTP protocol to other sources. We very strongly recommend that a convenient interface be provided for the user to control dissemination of such information, and that designers and implementers be particularly careful in this area. History shows that errors in this area are often both serious security and/or privacy problems, and often generate highly adverse publicity for the implementer's company*." [page 143][24]

(N.d.T.

- *"Far descrivere all'agente utente le proprie capacità in ogni richiesta può essere sia molto inefficace (poiché solo una piccola percentuale delle risposte è dotata di rappresentazioni multiple) sia una potenziale violazione della vita privata dell'utente in questione." [pag. 68]*

[20] Solo per DoubleClick, oltre 26 milioni di utenti Internet nel mese di marzo 1997 (GAUTHRONET, op. cit., p. 86) e oltre un miliardo di banner di cybermarketing scaricati ogni mese fuori dagli Stati Uniti (ibid., p. 96). Attualmente vengono inviati ogni giorno oltre 500.000.000 di banner pubblicitari per ogni singola società di cybermarketing.
V.http://www.doubleclick.net/company_info/investor_relations/financials/analyst_metrics.htm
[21] Il World Wide Web Consortium è un'organizzazione senza fini di lucro ospitato presso Inria (Francia), MIT (USA) e l'università di Keio (Giappone). I membri del consorzio sono, in particolare, Microsoft, AOL, Netscape e Center for Democracy and Technology (http://www.w3.org/Consortium/Member/List). IL consorzio si occupa di elaborare nome tecniche non obbligatorie ma *de facto* intese a garantire l'interoperabilità dei computer su Internet.
[22] http://www.w3.org/Protocols/rfc2068/rfc2068 . Il numero di pagina tra parentesi si riferisce alla numerazione del W3C.
[23] Il campo dell'intestazione ("From header") consente di inserire il nome della pagina di riferimento.
[24] Nella RFC 2068, il termine "vita privata" è citato 18 volte.

- *"L'invio, in ogni richiesta, di un'intestazione Accept-Language con le preferenze linguistiche complete dell'utente può essere contraria alle esigenze di riservatezza dell'utente." [pag. 98]*
- *"Il client non DEVE inviare il campo dell'intestazione ("From header") senza l'approvazione dell'utente poiché ciò può essere in conflitto con gli interessi di riservatezza dell'utente ovvero con la clausola di sicurezza del relativo sito. Si raccomanda vivamente che l'utente possa disabilitare, abilitare e modificare il valore di questo campo in qualsiasi momento prima della richiesta." [pag. 118]*
- *I client HTTP sono spesso a conoscenza di grandi quantità di informazioni personali (ad esempio, il nome dell'utente, la località, l'indirizzo di posta, le password, le chiavi di cifratura, ecc.) e DEVONO essere molto attenti ad impedire la fuga accidentale di tali informazioni attraverso il protocollo HTTP verso altre fonti. Si raccomanda vivamente di prevedere un'interfaccia comoda che consenta all'utente di controllare la diffusione di tali informazioni e che i progettisti e gli implementatori operino con un'attenzione particolare in questo campo. La storia mostra che gli errori commessi in questo campo comportano spesso gravi problemi di sicurezza e/o di riservatezza, e rappresentano spesso una pubblicità molto negativa per la società di implementazione." [pag. 143]*).

V. Alcune considerazioni di carattere economico

Negli ultimi anni, Internet ha sostenuto una crescita straordinaria. Il numero di host computer (quelli che memorizzano le informazioni e collegano le comunicazioni) è passato da circa 300 nel 1981 a circa 9.400.000 nel 1996. Circa il 60% di questi host computer è situato negli Stati Uniti. Nel 1996, circa 40 milioni di persone usavano Internet mentre le previsioni erano di circa 200 milioni di persone entro il 2000[25]. Si prevede che entro il 2005, metà della popolazione europea sarà connessa a Internet[26].

In molti paesi europei, l'abbonamento ad Internet è gratuito ma l'abbonato deve pagare all'operatore di telecomunicazioni l'uso della linea. Il fornitore di accesso Internet o il *fornitore di servizi Internet* verrà rimborsato dall'operatore di telecomunicazioni della tariffa di retroconnessione, in base alla durata della chiamata locale effettuata dall'abbonato Internet. Ciò significa che anche nei casi in cui l'utente sia titolare di un abbonamento gratuito ad Internet, egli dovrà comunque sostenere le spese delle linee telefoniche utilizzate. Ciò andrà a beneficio sia del fornitore di accesso/*fornitore di servizi Internet* sia degli operatori di telecomunicazione.

Anche i produttori software beneficeranno dell'uso di Internet poiché, sebbene essi mettano i propri prodotti a disposizione dell'utente gratuitamente (freeware, browser, ecc.), essi non ricevono alcun compenso per l'uso dei propri software da parte dei server dei siti web.

Il marketing diretto è una delle principali attività di lucro presente sul web. Le società di 'cybermarketing' inseriscono nelle pagine web i propri banner, spesso in modo tale che la raccolta di dati personali risulti ampiamente invisibile alla persona interessata. Grazie all'uso dei collegamenti invisibili, unitamente al browser chattering e ai *cookie*, società di marketing sconosciute sono in grado di elaborare i profili degli utenti in modo biunivoco. Una sola società di 'cybermarketing' potrebbe inviare, ogni giorno, circa mezzo miliardo

[25] V. la sentenza Reno contro ACLU del 26 giugno 1997.
[26] Comunicato stampa della Commissione europea, *Commission welcomes new legal framework to guarantee security of electronic signatures*, 30 novembre 1999.

di banner personalizzati sul web. Le società di marketing diretto finanziano molti motori di ricerca.

Inserendo un *collegamento ipertestuale* invisibile nelle pagine web delle società di 'cybermarketing', i comuni siti web (e, in particolare, i motori di ricerca) istruiranno i comuni browser, come Netscape e Internet Explorer, di aprire una connessione HTTP indipendente con il server HTTP della società di 'cybermarketing'. Come spiegato in precedenza, il browser, nel dare seguito alla richiesta HTTP, comunicherà automaticamente vari dati quali: l'indirizzo IP, la pagina di riferimento (nel caso di un motore di ricerca, questa variabile contiene le parole chiave inserite da chi effettua la ricerca), la marca, la versione e la lingua del browser in uso (ad esempio Internet Explorer 4.02, olandese, tipo e sistema operativo usati: Windows 2000, Linux 2.2.5, SO Mac 8.6 ecc.) e, ultimo ma non meno importante, il *cookie* identificativo (ad esempio, UserId=342ER432) che potrebbe essere già stato depositato dalla società di 'cybrmaketing' attraverso *collegamenti ipertestuali* invisibili precedenti.

L'utente Internet medio generalmente non sa che, inserendo un URL (Unified Resource Locator), molti banner che appariranno sullo schermo non appartengono al sito web visitato. Gli utenti non sanno nemmeno che, scaricando un banner, il loro browser trasmetterà sistematicamente un identificativo esclusivo, l'indirizzo IP e l'URL completo della pagina web visitata (comprese le parole chiave inserite nei motori di ricerca e il nome degli articoli di stampa consultati in linea). Tutti questi dati possono essere uniti per elaborare un profilo globale di un cittadino che naviga da uno sito all'altro, grazie all'identificativo esclusivo memorizzato nel *cookie*.

Si ritiene che la raccolta di informazioni sugli utenti negli ambienti on-line abbia un'importanza economica e strategica. Il seguente paragrafo, tratto da una famosa pubblicazione americana[27], illustra questo concetto: *Troppe aziende, tra cui molte delle imprese innovative emergenti su Internet, non si sono concentrate abbastanza sul valore dell'elaborazione di profili degli utenti. I vincitori e i perdenti di questa nuova era saranno determinati da chi è in possesso di profili dei clienti on-line.*

Vale la pena di ricordare che la raccolta dei dati di utenti Internet è di solito gratuita per la società, poiché gli utenti spesso forniscono le informazioni spontaneamente, ad esempio compilando dei moduli. I siti web utilizzano spesso programmi di fedeltà, come giochi, questionari, notiziari, che implicano la fornitura di dati personali da parte di chi visita il sito.

Casi recenti confermano il valore crescente attribuito dalle imprese ai profili degli utenti. Elenchi di clienti vengono venduti o scambiati, per lo più attraverso la fusione di società di TI, che incrementano in tal modo la precisione e il numero dei profili utilizzabili.

Avranno luogo, alla fine, acquisizioni basate sui dati dei consumatori, in cui la risorsa primaria acquistata saranno proprio tali dati (…). Oggi, i dati dei consumatori rappresentano la valuta del commercio elettronico in parecchi modi. I clienti sono preziosi perché hanno dimostrato di essere acquirenti e hanno fatto i loro acquisti in un negozio competitivo (…) I nomi contenuti in una base di dati consentono ad una società di ridurre i costi di marketing per acquisire nuovi clienti, che di solito corrispondono a circa 100 dollari a cliente[28].

I dati degli utenti vengono messi in vendita quando una società Internet fallisce. Recentemente, una società di vendita di giocattoli ha incluso nella liquidazione dell'azienda la vendita dei profili dei propri clienti. Questi profili erano stati raccolti dagli

[27] V. il libro "Net Worth" (op cit), pag. xiii (prefazione).
[28] Citazione da M. HALPERN e HARMON, *E-mergers trigger privacy worries* di Deborah KONG, http://www.mercurycenter.com/svtech/news/indepth/docs/consum012400.htm

utenti in conformità alla disposizione sulla vita privata che nessuna informazione sarebbe mai stata divulgata a terzi senza il loro esplicito consenso. I profili comprendono i nomi, gli indirizzi, le informazioni sulla fatturazione, le informazioni sul comportamento in fatto di acquisti, nonché i profili dei familiari con i nomi e le date di nascita dei figli.

TRUSTe, che aveva approvato la politica sulla vita privata della società, ha annunciato l'8 agosto 2000 di avere depositato, presso il Tribunale fallimentare degli Stati Uniti, un'istanza di opposizione all'accordo della Commissione federale del commercio (Federal Trade Commissione - FTC) con la società relativo alle condizioni di liquidazione del patrimonio[29].

Un'esauriente politica in materia di protezione dei dati deve tener conto di una scelta equilibrata tra gli interessi economici e i diritti umani. Due grandi questioni rimangono irrisolte.

- Sinora è stata raccolta su Internet una grande quantità di dati personali relativi a molti utenti Internet senza il precedente assenso e/o consenso dell'interessato, principalmente a causa degli effetti collaterali invisibili della tecnologia Internet. E' prevedibile che, nei prossimi anni, sempre più dati personali verranno scambiati a scopo di lucro[30]; ma dove può arrivare l'utente Internet di questo passo? Che tipo di dati personali possono essere divulgati da parte della persona interessata, per quanto tempo e in quali circostanze?
- Se il finanziamento di siti web particolari (come i motori di ricerca) proviene principalmente dal settore del 'cybermarketing', si potrebbe essere tentati di utilizzare sistemi di elaborazione di personalizzati per garantire che i servizi precedentemente gratuiti escludano le persone che non dispongono di un reddito sufficiente, che non hanno risposto a centinaia di banner pubblicitari o che desiderano tutelare la propria vita privata.

VI. Conclusioni

- Internet è stata concepita come una rete aperta a livello mondiale (www) attraverso la quale poter condividere informazioni. E' tuttavia necessario stabilire un equilibrio tra la "natura aperta" di Internet e la tutela dei dati personali dei relativi utenti.
- Su Internet vengono rilevate enormi quantità di dati relativi agli utenti, spesso senza che essi ne siano a conoscenza. Questa mancanza di trasparenza nei confronti degli utenti Internet deve essere affrontata per conseguire un buon livello di protezione dei dati personali e degli utenti.
- I protocolli sono strumenti tecnici che, di fatto, determinano le modalità di raccolta e trattamento dei dati. Anche i browser e i programmi software svolgono un ruolo importante. In alcuni casi, essi includono un identificativo che consente di collegare l'utente Internet alle proprie attività sulla rete. E' pertanto responsabilità di chi si occupa della progettazione e dello sviluppo di questi prodotti offrire agli utenti prodotti conformi alle norme sulla vita privata. A tale proposito, è importante citare che l'articolo 14 del progetto di direttiva sulle telecomunicazioni del 12 luglio 2000 stabilisce che, all'occorrenza, la Commissione adotta misure dirette a garantire che le apparecchiature tecniche incorporino i dispositivi di protezione necessari per garantire la tutela dei dati personali e della vita privata di utenti e abbonati.

[29] http://www.truste.org/users/users_investigations.html
[30] V. ad esempio il dibattito relativo agli infomediari nel capitolo 9.

CAPITOLO 3: APPLICAZIONE DELLA LEGISLAZIONE SULLA PROTEZIONE DEI DATI

I. Considerazioni giuridiche di carattere generale

Il punto di partenza per l'analisi giuridica di tutti i vari fenomeni, che verrà svolta nei capitoli che seguono, è rappresentato dal fatto che entrambe le direttive sulla protezione dei dati (direttive 95/46/CE e 97/66/CE) si applicano, in linea di principio, ai dati personali trattati su Internet[31].

Tutte le considerazioni di carattere giuridico oggetto del presente documento si basano sull'interpretazione di queste direttive, nonché sui documenti adottati dal Gruppo di lavoro e, in alcuni casi (se indicato in questo senso) sulla giurisprudenza della Corte europea dei diritti umani.

I dati personali su Internet

Come già menzionato in questo documento, i fornitori di accesso Internet e i gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP poiché, normalmente, essi "registrano" in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet. Lo stesso dicasi per i *fornitori di servizi Internet*, i quali detengono un registro sul server HTTP. In questi casi, non vi è dubbio sul fatto che si possa parlare di dati personali ai sensi dell'articolo 2(a) della direttiva[32].
In altri casi, è possibile che un terzo venga a conoscenza dell'indirizzo IP dinamico di un utente, ma senza essere in grado di collegarlo ad altri dati relativi a tale persona, che ne renderebbero possibile l'identificazione. E' ovviamente più facile identificare gli utenti Internet che utilizzano indirizzi IP di tipo statico.

Tuttavia, esiste in molti casi la possibilità di collegare l'indirizzo IP dell'utente ad altri dati personali (disponibili al pubblico o meno) che lo identifichino, segnatamente se si utilizzano strumenti di trattamento invisibili per raccogliere dati supplementari relativi all'utente (ad esempio, utilizzando *cookie* contenenti un identificativo esclusivo) o sistemi di *datamining (estrazione di dati)* moderni collegati a grandi basi di dati contenenti dati personalmente identificabili relativi agli utenti Internet.

Pertanto, sebbene potrebbe non essere possibile identificare un utente, in qualsiasi caso e da parte di tutti gli attori Internet, dai dati trattati su Internet, questo documento presuppone che esista la possibilità di identificare l'utente Internet in molti casi e che su Internet vengano pertanto trattate grandi masse di dati personali cui si applica la direttiva sulla protezione dei dati.

Applicazione delle direttive

Secondo quanto già dichiarato dal Gruppo di lavoro in passato, la direttiva generale sulla protezione dei dati 95/46/CE si applica a qualsiasi trattamento di dati personali che rientra nel relativo ambito di applicazione, indipendentemente dai mezzi tecnici utilizzati.

---

[31] V. il documento di lavoro WP 16: *Trattamento dei dati personali su Internet*, adottato dal Gruppo di lavoro il 23 febbraio 1999, 5013/99/IT/def.
[32] V. anche il considerando 26 nel preambolo della direttiva.

Pertanto, il trattamento dei dati personali su Internet deve essere considerato alla luce di questa direttiva[33]. La direttiva generale si applica quindi in tutti i casi e a tutti i vari attori di cui si è parlato nella prima parte del presente capitolo (descrizione tecnica).

La direttiva specifica 97/66/CE sulla tutela della vita privata e dei dati personali nel settore delle telecomunicazioni approfondisce ed integra la direttiva generale 95/46/CE stabilendo disposizioni specifiche sul piano giuridico e tecnico. La direttiva 97/66/CE si applica al trattamento dei dati personali in relazione alla fornitura di servizi di telecomunicazione accessibili al pubblico nelle reti di telecomunicazione pubbliche all'interno della Comunità. I servizi Internet sono servizi di telecomunicazione. Internet, pertanto, rientra nel settore delle telecomunicazioni pubbliche.

La direttiva 95/46/CE si applica a tutte le tematiche non espressamente coperte dalla direttiva 97/66/CE, come gli obblighi a carico del responsabile del trattamento e i diritti dei singoli oppure i servizi di telecomunicazione non accessibili al pubblico[34]. I dati personali forniti volontariamente dall'utente Internet durante la connessione alla rete rientrano sempre nell'ambito di applicazione della direttiva in questione.

Nella tabella che segue, si è tentato di definire i casi in cui si applicano rispettivamente la direttiva specifica 97/66/CE e la direttiva 95/46/CE, illustrando i principi più pertinenti. Tuttavia, si dovrebbe tenere conto del fatto che, quando gli attori svolgono vari ruoli contemporaneamente, saranno inevitabili alcune sovrapposizioni.

Attore	**Funzione**	**Eventuale trattamento di dati personali**	**Disposizioni pertinenti della direttiva sulle telecomunicazioni:**
Fornitore di telecomunicazioni Es.: AT&T	- Connessione tra gli utenti Internet e i *fornitori di servizi Internet*	- Registrazione delle connessioni tra l'utente Internet e il *fornitore di servizi Internet* - Trasferimento dell'identificazione della linea chiamante dell'utente Internet al *fornitore di servizi Internet*	- Direttiva sulle telecomunicazioni, segnatamente: riservatezza delle comunicazioni, dati sul traffico e sulla fatturazione, e presentazione e restrizione della linea chiamante e identificazione della linea

[33] In questo documento, il termine "la direttiva" si riferisce alla direttiva 95/46/CE.
[34] V. il considerando 11 della direttiva 97/66/CE.

			collegata.
Fornitore di servizi Internet[35] Es.: World Online	- Fornitura del servizio Internet richiesto - Trasferimento della richiesta dall'utente Internet al *proxy* server (cache) - Trasferimento della richiesta dall'utente Internet al sito web - Trasferimento della risposta dal *proxy* server all'utente Internet - Trasferimento della risposta dal sito web all'utente Internet	- Registrazione dell'identificazione della linea chiamante - Allocazione dell'indirizzo IP ad una sessione - Possibilità di memorizzare gli elenchi delle visite effettuate nel sito web, ordinati in base all'indirizzo IP - Scambio di dati con i siti web richiesti - Registrazione delle sessioni (ora di login e logout, e quantità di dati trasferiti) - Estrazione delle informazioni da intestazioni e contenuti.	- Direttiva sulle telecomunicazioni, segnatamente: riservatezza delle comunicazioni, dati sul traffico e sulla fatturazione
Servizio di *portale* Es.: Yahoo, AOL, Macropolis	- Selezione della fornitura di informazioni - Fornitura di informazioni (fornitore di contenuti) e, a volte, beni o servizi	- Registrazione delle richieste effettuate ai siti a monte del portale - Eventuale registrazione delle visite effettuate nel sito - Registrazione delle pagine di riferimento, parole chiave inserite (chattering data) - Deposito di *cookie* sul disco fisso dell'utente Internet - Elaborazione di profili degli utenti	- Direttiva sulle telecomunicazioni (applicabile al *fornitore di servizi Internet* che ospita il *sito portale*)
Normale sito web/homepage Es.: www.coe.int	- Fornitura di informazioni (fornitore di contenuti) e, a volte, beni e servizi	- Eventuale registrazione delle visite effettuate nel sito - Registrazione delle pagine di riferimento, parole chiave inserite (chattering data) - Deposito di *cookie* sul disco fisso dell'utente Internet - Elaborazione di profili degli utenti	
Fornitori di servizi supplementari Es.: Nedstat Doubleclick Banners	- Personalizzazione di pagine web	-Elaborazione di profili degli utenti (unendo il *clickstream* di vari siti web)	- Non sempre si tratta di un servizio di telecomunicazione e pertanto la direttiva sulle telecomunicazioni si applica solo in alcuni casi.

[35] In linea di principio, l'espressione *fornitore di servizi Internet* utilizzata in questo documento comprende anche i fornitori di accesso Internet (v. la definizione riportata nel glossario). Il presente documento si riferisce ai fornitori di accesso Internet solo quando si occupa di temi che li riguardano direttamente.

Fornitori di *router* e linee di connessione (spesso di proprietà dei fornitori di telecomunicazioni)	- Connessione *fornitori di servizi Internet*	- Direzionamento dei dati dall'utente Internet al sito web IP. - Rischio di intercettazione illecita	- Direttiva sulle telecomunicazioni: in particolare, la sicurezza e la riservatezza delle comunicazioni

Per capire se le due direttive sono applicabili o meno, la questione chiave è, ovviamente, stabilire se il servizio in questione può essere considerato un "servizio di telecomunicazione" secondo la definizione di cui all'articolo 2(d) della direttiva 97/66/CE: *trasmissione e inoltro dei segnali su reti di telecomunicazione*.

Se è applicabile la direttiva specifica sulle telecomunicazioni, è necessario applicare le norme specifiche in essa contenute.

Fornitore di telecomunicazioni

Non vi è dubbio che il collegamento degli utenti Internet ad un *fornitore di servizi Internet*, la fornitura di servizi Internet agli utenti Internet, nonché l'inoltro delle richieste e delle risposte dagli utenti Internet ai server dei siti web e ritorno sono servizi di telecomunicazione. Pertanto, la direttiva 97/66/CE si applica ai fornitori di servizi di telecomunicazione, ai *fornitori di servizi Internet* e ai fornitori di *router* e linee per il traffico Internet.

Fornitori di servizi Internet (ivi compresi i fornitori di accesso)

Lo stesso dicasi per i *fornitori di servizi Internet*; non vi è alcun dubbio che la direttiva specifica sulle telecomunicazioni si applichi alle loro attività.

Un caso interessante riguarda le istituzioni o le persone che hanno accesso diretto ad Internet senza l'aiuto di un *fornitore di servizi Internet*. Tali istituzioni agiscono, di fatto, quali *fornitori di servizi Internet* che collegano la propria rete privata ad Internet.

L'articolo 3 della direttiva 97/66/CE definisce il proprio ambito di applicazione specificando che essa riguarda i servizi di telecomunicazione offerti al pubblico su reti pubbliche di telecomunicazione nella Comunità. Nel caso sopra citato, non si tratta di una rete pubblica ma privata, a disposizione di un determinato gruppo di utenti. Si può pertanto concludere che questi servizi, pur rientrando nella definizione di servizi di telecomunicazione, non possono essere considerati servizi accessibili al pubblico e, pertanto, non rientrano nell'ambito di applicazione della direttiva 97/66/CE.

E' importante chiarire che, in questi casi, le disposizioni oggetto della direttiva specifica si applicherebbero se le informazioni venissero inviate a qualcuno che si trova al di fuori della rete privata.

Ovviamente, in questi casi si applicano pienamente le disposizioni della direttiva generale sulla protezione dei dati.

Normali siti web

Di norma, un sito web è ospitato da un *fornitore di servizi Internet*. Ciò significa che la persona responsabile di un sito web (ad esempio, il sito web del Consiglio d'Europa) affitta una certa capacità di memoria da un *fornitore di servizi Internet* per memorizzare il proprio sito web e renderlo disponibile. Significa inoltre che il *fornitore di servizi Internet* risponde, per conto del Consiglio d'Europa, alle richieste degli utenti Internet relative alle pagine web.

Di conseguenza, il soggetto cui appartiene il sito web (nella fattispecie, il Consiglio d'Europa) decide solo quali informazioni saranno disponibili sul sito, ma non svolge direttamente alcun tipo di operazione che comporti *la trasmissione o l'inoltro dei segnali sulle reti di telecomunicazione.*

Laddove sia possibile ordinare beni o servizi attraverso un sito web, la persona responsabile del sito fornirà tali beni o servizi. I servizi di telecomunicazione in quanto tali non sono di solito forniti dalla persona responsabile del sito, ma dal *fornitore di servizi Internet*.

Si può affermare, pertanto, che i siti web sono abbonati ai servizi di telecomunicazione (trasmissione) del fornitore di servizi Internet che ospita il sito web, ma non svolgono direttamente alcuno di questi servizi. La direttiva 97/66/CE è applicabile ai *fornitori di servizi Internet* in quanto tali, ma non ai siti web cui si applica invece la direttiva generale.

Servizi di portale

Un *sito portale* fornisce una panoramica ordinata di collegamenti (link) web. Mediante il *portale* visitato, l'utente Internet può visitare con facilità i siti web selezionati di altri fornitori di contenuti.

Un *sito portale* è ospitato da un *fornitore di servizi Internet*. In alcuni casi, il *sito portale* appartiene al *fornitore di servizi Internet* (ad esempio, worldonline.nl); in altri, invece, il *fornitore di servizi Internet* ospita il *sito portale* per conto di un terzo che fornisce il contenuto.

In entrambi i casi, è il *fornitore di servizi Internet* che fornisce il servizio di telecomunicazione secondo la definizione di cui all'articolo 2 della direttiva 97/66/CE e a cui si applica, pertanto, la direttiva. Quest'ultima non si applica, invece, al fornitore di contenuti.

Servizi supplementari

I fornitori di servizi supplementari non rientrano, in tutti i casi, nell'ambito di applicazione della direttiva sulla vita privata e le telecomunicazioni.

Alcuni di questi fornitori di servizi (come Nedstat) trattano i dati rilevati dai siti web per poi rivenderli ai proprietari dei siti. I dati trattati provengono da Internet, ma la loro attività non comporta, in linea di principio, la *trasmissione o l'inoltro dei segnali sulle reti di telecomunicazione.* Essi, pertanto, non svolgono un ruolo essenziale nel processo di comunicazione tra l'utente Internet e il sito web. Se i dati che essi trattano consistono solo di dati aggregati non identificabili, si potrebbe persino affermare che essi non rientrano nella direttiva generale poiché non si tratta di dati personali.

Attori quali DoubleClick, Engage o Globaltrash pubblicano annunci pubblicitari nelle pagine richieste. Normalmente, esiste un accordo contrattuale che vincola tali società pubblicitarie al *fornitore di servizi Internet* che ospita le pagine web in cui vengono pubblicati i banner.

A tale scopo, dal punto di vista tecnico, ogni volta che si accede a un sito web, questo contatta la società pubblicitaria (*collegamento ipertestuale* automatico) in modo che quest'ultima possa inserire i banner pubblicitari nelle pagine richieste.

Inoltre, la società pubblicitaria può depositare *cookie*-file sul disco fisso dell'utente Internet al fine di elaborare i profili dei visitatori del sito, in modo da poter pubblicare nella pagina web banner pubblicitari personalizzati[36].

Non risulta chiaro se le attività centrali di DoubleClick, Engage e altre società pubblicitarie possono essere considerate un servizio di telecomunicazioni o meno. Sembra che esse non trasmettano e instradino segnali secondo la definizione dell'articolo 2 della direttiva sulle telecomunicazioni. Esse forniscono informazioni di contenuto da pubblicare sulle pagine web richieste, utilizzando le infrastrutture e le reti di telecomunicazioni disponibili.

Si tratta, comunque, di un buon esempio di una situazione in cui la definizione esistente di servizi di telecomunicazioni è difficile da applicare ai servizi correlati a Internet.

II. La revisione della direttiva sulle telecomunicazioni: la definizione di "servizi di comunicazione elettronica"

Nel 1999, la Commissione europea ha annunciato, in una comunicazione[37], la propria intenzione di effettuare una revisione generale del quadro normativo esistente per il settore delle telecomunicazioni a livello europeo. Nel contesto di tale revisione generale del quadro normativo del settore delle comunicazioni, verrà rivista e aggiornata anche l'attuale direttiva sul trattamento dei dati personali e la protezione della vita privata nel settore delle telecomunicazioni.

Il Gruppo di lavoro di cui all'articolo 29 ha già espresso alcuni commenti concernenti questa revisione nel parere 2/2000 presentato dall'Internet Task Force e adottato il 3 febbraio 2000[38].
Il testo della comunicazione della Commissione europea ha messo in evidenza il fatto che la revisione prevista avrebbe rivolto un'attenzione particolare alla terminologia utilizzata nella direttiva 97/66/CE al fine di chiarire quali nuovi servizi e tecnologie rientrano nella direttiva in questione, evitando eventuali ambiguità ed agevolando l'applicazione coerente dei principi in materia di protezione dei dati. Nel parere 2/2000, il Gruppo di lavoro si è compiaciuto di tale revisione terminologica per le finalità suddette.

La proposta di direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche è stata pubblicata dalla Commissione il 12 luglio 2000[39]. Il comunicato stampa[40] della Commissione europea sottolinea il fatto che uno degli obiettivi del nuovo pacchetto è garantire la tutela del diritto alla vita privata su Internet.

La proposta non parla più di "servizi di telecomunicazione" ma di "servizi di comunicazione elettronica". Il memorandum esplicativo della proposta afferma che tale cambiamento si è reso necessario per allineare la terminologia con la proposta di direttiva

[36] Il libro "Net Worth" (op cit.) recita a pag. 275: "Because *cookies* can also be used to match browsing habits and preferences, they are increasingly being used to target advertisements to specific people. Indeed, Doubleclick, Globaltrash and ADSmart are examples of companies that use *cookies* to target advertisements to consumers at their enabled websites."
[37] Documento COM (1999) 539.
[38] Parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni, presentato dall'Internet Task Force, adottato il 3 febbraio 2000, WP 29, 5009/00/IT/def.
[39] Documento COM (2000) 385.
[40] La Commissione propone la revisione delle norme relative alla comunicazione elettronica, Bruxelles, 12 luglio 2000, IP/00/749.

che stabilisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica[41].

Il termine "servizi di comunicazione elettronica" non viene definito nella proposta di direttiva sulla vita privata e le telecomunicazioni ma nell'articolo 2(b) della proposta di direttiva che stabilisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica.

La nuova definizione recita: *"servizi di comunicazione elettronica", i servizi forniti a pagamento consistenti esclusivamente o prevalentemente nella trasmissione e nell'instradamento di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti.*

La nuova definizione si basa in realtà sulla stessa idea centrale della precedente (la trasmissione e l'instradamento di segnali su servizi di comunicazioni elettroniche), ma l'inclusione di un elenco di esempi dei servizi compresi ed esclusi dalla definizione è molto utile poiché getta luce sulle discussioni illustrate nella sezione precedente.

Dall'elenco incluso nella nuova definizione si può concludere che chi fornisce contenuti trasmessi utilizzando reti e servizi di comunicazioni elettroniche non rientrerà nell'ambito di applicazione della direttiva modificata sulla vita privata e le telecomunicazioni. Ciò trova conferma nel preambolo della proposta di direttiva che stabilisce un quadro comune per le reti e i servizi di comunicazioni elettroniche (considerando 7) che recita che *è necessario separare la disciplina dei mezzi di trasmissione dalla disciplina dei contenuti.* Si afferma, tuttavia, che tale separazione non incide sul riconoscimento dei collegamenti fra i due aspetti.

La principale conseguenza di tale separazione è che i servizi supplementari come DoubleClick ovvero chi fornisce contenuti ad un *portale* o a un sito web (ma non li ospita) non rientrano in questa direttiva ma solo in quella generale. Significa inoltre che i *fornitori di servizi Internet* rientrano nella direttiva specifica nella misura in cui essi operano in quanto fornitori di accesso e forniscono la connessione a Internet, e rientrano solo nella direttiva generale quando operano in qualità di fornitori di contenuti[42].

Il vantaggio della netta separazione tra la disciplina dei contenuti e dei mezzi di trasmissione è la chiarezza che essa reca con sé. In pratica, tuttavia, sarà meno facile operare con una tale separazione; si pensi, ad esempio, al caso di un *fornitore di servizi Internet* che fornisce anche contenuti ospitando il proprio *sito portale*. Il *fornitore di servizi Internet* dovrà applicare la direttiva generale a tutte le sue attività e la direttiva specifica (che comporta obblighi specifici) alle attività in cui egli opera in qualità di fornitore di accesso.

Un altro aspetto interessante della nuova definizione di "servizi di comunicazioni elettroniche" è il riferimento al fatto che il servizio dovrà essere fornito a pagamento. Né il preambolo né il memorandum esplicativo fanno riferimento all'inclusione di tale termine o ne indicano le modalità di interpretazione. Ciò potrebbe essere interpretato come il fatto che i fornitori di accesso gratuito non rientrano nell'ambito di applicazione della direttiva modificata sulla vita privata e le telecomunicazioni poiché essi non ricevono alcun compenso (quanto meno in termini finanziari) dagli utenti Internet.

[41] COM (2000) 393.
[42] Questo aspetto non è preso in considerazione in questo documento.

Tuttavia, tale interpretazione non risulta corretta poiché nella giurisprudenza della Corte europea di giustizia è stato chiarito che, con riguardo ai servizi ai sensi dell'articolo 50 (ex articolo 60) del trattato CE[43], il compenso non deve essere necessariamente corrisposto dal fruitore del servizio ma può essere corrisposto, ad esempio, dalle società pubblicitarie.

Nel caso di un fornitore di accesso gratuito, chi pubblica annunci o banner pubblicitari nelle pagine Internet offre di fatto un compenso al fornitore in questione. Risulta evidente, pertanto, che tali servizi rientrano nella definizione di servizi di comunicazioni elettroniche e quindi nell'ambito di applicazione della direttiva.

Tuttavia, sarebbe auspicabile chiarire tale questione nel testo della direttiva poiché chi legge il testo non conosce l'interpretazione di questo termine fornita dalla Corte europea di giustizia. Ciò potrebbe avvenire, ad esempio, nel preambolo della direttiva.

III. Altre disposizioni giuridiche applicabili

Vi è inoltre una seria di altre disposizioni comunitarie che riguardano alcuni aspetti correlati ad Internet. Possono essere citati i seguenti atti: direttiva 1999/93/CE relativa ad un quadro comunitario per le *firme elettroniche*[44], direttiva 97/7/CE sulla protezione dei consumatori in materia di contratti a distanza[45] e la direttiva 2000/31/CE su taluni aspetti giuridici dei servizi della società dell'informazione (direttiva sul commercio elettronico)[46].

Tuttavia, la maggior parte di tali disposizioni non stabilisce norme specifiche complete in materia di protezione dei dati e, nella maggior parte dei casi, affidano la disciplina di tale argomento alle direttive specifiche. Ad esempio, la direttiva sul commercio elettronico stabilisce, al considerando 14, che *"la protezione dei singoli relativamente al trattamento dei dati personali è disciplinata unicamente dalla direttiva 95/46/CE e dalla direttiva 97/66/CE che sono integralmente applicabili ai servizi della società dell'informazione (…) e pertanto non è necessario includere tale aspetto nella presente direttiva"*, e nell'articolo 1.5 b) che *"la presente direttiva non si applica alle questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE"*.

Il considerando 14 della direttiva sul commercio elettronico sottolinea il fatto che *l'applicazione della presente direttiva deve essere pienamente conforme ai principi relativi alla protezione dei dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità degli intermediari. La presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet.*

Tuttavia, l'articolo 8 della direttiva sulle *firme elettroniche* contempla alcune norme specifiche sulla protezione dei dati relative ai fornitori di servizi di certificazione e agli organismi nazionali responsabili dell'accreditamento o della supervisione. L'articolo obbliga gli Stai membri a provvedere a che i fornitori di servizi di certificazione e gli organismi nazionali responsabili dell'accreditamento o della supervisione si conformino alle disposizioni della direttiva generale sulla protezione dei dati. Inoltre, tale disposizione stabilisce che i fornitori di servizi di certificazione che rilasciano certificati

[43] Causa C-109/92 Wirth [1993] ECR I-6447 , 15.
[44] Direttiva 1999/93/CE del 13 dicembre 1999 relativa ad un quadro comunitario per le *firme elettroniche*, Gazzetta ufficiale delle Comunità europee, 19 gennaio 2000, da L 13/12 a 13/20.
[45] Direttiva 1997/7/CE del 20 maggio 1997 sulla protezione dei consumatori in materia di contratti a distanza, Gazzetta ufficiale delle Comunità europee, 4 giugno 1997, L 144.
[46] Direttiva 2000/31/CE dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico), Gazzetta ufficiale delle Comunità europee, 17 luglio 2000, da L 178/1 a 178/16.

al pubblico possono raccogliere dati personali solo direttamente dalla persona cui i dati si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato. I dati non possono essere raccolti o trattati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Il terzo paragrafo dell'articolo 8 di questa direttiva è particolarmente importante. Esso prevede che, fatti salvi gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi, gli Stati membri non vietano al prestatore di servizi di certificazione di riportare sul certificato uno pseudonimo in luogo del nome del firmatario.

Il preambolo di questa direttiva (considerando 24) sottolinea l'importanza del fatto che i fornitori di servizi di certificazione osservino la legislazione in materia di protezione dei dati e la vita privata degli individui al fine di accrescere la fiducia da parte degli utenti nelle comunicazioni elettroniche e nel commercio elettronico.

IV. Applicazione della legislazione nazionale sulla protezione dei dati e relativi effetti internazionali

L'articolo 4(1)(a) e (b), della direttiva prevede l'applicazione delle disposizioni nazionali degli Stati membri laddove:

- "il trattamento venga effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;
- il responsabile non sia stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico".

La direttiva specifica che la nozione di stabilimento implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile e che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fatto determinante a questo riguardo.

Come stabilito nell'articolo 4 (1)(c) della direttiva, i dati raccolti mediante strumenti automatizzati o non automatizzati nel territorio dell'UE/SEE sono soggetti alle disposizioni della legislazione comunitaria sulla protezione dei dati.

Il considerando 20 della direttiva fornisce un'ulteriore spiegazione: "la tutela delle persone prevista dalla presente direttiva non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva".

Sebbene l'interpretazione della nozione di "strumenti" o "mezzi" abbia dato vita ad un dibattito sulla relativa portata, alcuni esempi rientrano indubbiamente nell'ambito di applicazione dell'articolo 4.

Potrà trattarsi, ad esempio, di un file di testo installato sul disco fisso di un computer che riceverà, memorizzerà e invierà informazioni ad un server situato in un altro paese. Tali file di testo, denominati *cookie*, vengono utilizzati per raccogliere dati per un paese terzo. Se il computer è ubicato in un paese dell'UE e il paese terzo si trova fuori dall'UE,

quest'ultimo dovrà applicare alla raccolta di dati effettuata mediante il *cookie* i principi della legislazione nazionale di quello Stato membro.
In tal caso, in conformità all'articolo 4(2), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento.

V. Conclusioni

- Su Internet vengono trattate grandi quantità di dati personali cui si applicano le direttive sulla protezione dei dati.
- La direttiva generale si applica in tutti i casi mentre quella specifica si applica ai servizi di telecomunicazioni. A causa della terminologia utilizzata nella direttiva 97/66/CE, è talvolta difficile stabilire quando si tratta di un servizio di telecomunicazione.
- La revisione del quadro normativo del settore delle telecomunicazioni ha consentito di chiarire l'ambito di applicazione della direttiva sulla vita privata e le telecomunicazioni. Tuttavia, alcuni aspetti potrebbero richiedere ulteriori chiarificazioni, in particolare in riferimento alla necessità di includere la nozione di pagamento nella definizione di servizi di comunicazioni elettroniche. L'interpretazione fornita a tale proposito dalla Corte europea di giustizia dovrebbe essere riportata nel preambolo della direttiva al fine di evitare qualsiasi eventuale equivoco circa l'ambito di applicazione della direttiva.
- La legislazione europea sulla protezione dei dati deve essere applicata ai dati raccolti utilizzando strumenti automatizzati o non automatizzati situati nel territorio dell'UE/SEE.

CAPITOLO 4: POSTA ELETTRONICA

I. Introduzione

Non è facile descrivere in poche parole gli elementi tecnici fondamentali della posta elettronica. Ciò dipende, principalmente, dai seguenti fattori:

- esistono alcuni *protocolli* ufficiali ma, come nel caso del *protocollo* HTTP, il livello di rischio per la vita privata dipenderà dal modo in cui tali protocolli vengono effettivamente implementati. Vi sono migliaia di diversi programmi client o server di posta elettronica e sembra molto difficile tirare conclusioni complessive, poiché non esistono dati affidabili sull'uso di tali programmi;

- i trattamenti invisibili effettuati da tali programmi non sono facili da rilevare, come indicato dal termine "invisibile", e tali programmi stanno diventando talmente ampi e complicati che è quasi impossibile riuscire ad elencarne tutte le funzionalità, anche le più nascoste.

La descrizione che segue non può pertanto essere considerata completa e non sarà sempre rappresentativa di ciò che succede ogni giorno su centinaia di milioni di personal computer connessi a Internet in tutto il mondo.

II. Attori

Nella gestione di una comunicazione di posta elettronica sono coinvolti vari attori, ognuno dei quali deve tenere conto delle questioni relative alla protezione dei dati in ogni fase di tale processo. Gli attori sono[47]:

- il mittente di un messaggio
- il destinatario di un messaggio (titolare di un indirizzo di posta elettronica)
- il fornitore di servizi di posta elettronica (il server di posta che memorizza il messaggio inviato all'utente finché l'utente non desidera scaricarlo)
- il fornitore di software del programma client di posta elettronica per il mittente
- il fornitore di software del programma client di posta elettronica per il destinatario
- il fornitore di software del programma server di posta

III. Descrizione tecnica

Fondamentalmente, un utente che desidera utilizzare la posta elettronica necessita di quanto segue:

- un "client di posta elettronica", che è un programma installato sul PC dell'utente
- un indirizzo di posta elettronica (un account di posta elettronica)
- una connessione a Internet

[47] L'operatore di telecomunicazioni non è coinvolto in modo particolare nella gestione della posta elettronica, ma svolge un ruolo fondamentale nel convogliare i segnali che rendono possibile ogni forma di comunicazione di posta elettronica. Questo attore ha obblighi di sicurezza specifici derivanti dalle direttive.

Il processo di invio di un messaggio di posta elettronica

E' disponibile una vasta gamma di "client di posta elettronica", ma tutti devono rispettare gli standard Internet. L'invio di un messaggio di posta elettronica consiste fondamentalmente delle seguenti fasi:

- l'utente crea un messaggio nel proprio "client di posta elettronica" e compila il campo dell'indirizzo del destinatario inserendo il relativo indirizzo di posta elettronica;
- premendo il pulsante di invio del client di posta elettronica, il messaggio di posta elettronica verrà trasferito al server di posta del corrispondente (di solito un'organizzazione o alla casella di posta presso l'account di posta elettronica dell'utente da parte del *fornitore di servizi Internet*;
- se il messaggio di posta elettronica viene consegnato al server di posta dell'organizzazione, il server di posta in questione trasmetterà il messaggio di posta elettronica direttamente al destinatario o ad un relay server di posta (“trasmissione esterna”);
- il messaggio di posta elettronica può passare attraverso vari relay server di posta fino a raggiungere il server di posta del destinatario;
- il destinatario è connesso direttamente al server di posta (ad esempio all'interno di una LAN) o deve stabilire una connessione per scaricare la propria posta.

Indirizzi di posta elettronica

L'indirizzo di posta elettronica consta di due parti separate dal carattere “@”, ad esempio john.smith@nowhere.com o subs34219@nowhere.org.

- La parte destra identifica l'host presso cui il destinatario possiede un account. Si tratta infatti di un nome DNS che si riferisce all'indirizzo IP del server di posta.
- La parte sinistra descrive l'identificazione esclusiva del destinatario. Si tratta del nome con cui il destinatario è noto al servizio di posta elettronica. Nessun obbligo tecnico stabilisce che l'identificativo debba corrispondere al nome reale del destinatario. Può trattarsi di uno pseudonimo scelto dal destinatario o di un codice casuale assegnato arbitrariamente dal server di posta al momento della registrazione del destinatario.

Dal punto di vista tecnico, l'identificazione non è necessaria per inviare un messaggio di posta. E' proprio come accade nel mondo reale, dove chiunque può inviare una lettera senza fornire il proprio nome. Nel caso dello *spamming*, il mittente non utilizzerà infatti un account di posta elettronica, ma accederà direttamente al *protocollo* SMTP. Ciò consentirà all'utente di eliminare o modificare il proprio indirizzo di posta elettronica.

Protocolli di posta elettronica

Oltre al *protocollo* TCP/IP, per la posta elettronica vengono usati altri due *protocolli*:

1. Il primo è denominato Simple Mail Transport Protocol (SMTP) e consente di INVIARE un messaggio di posta da un client al server di posta del destinatario. La posta non viene inviata direttamente al computer client del destinatario, poiché il computer non sarà necessariamente accesso o comunque connesso a Internet quando il mittente decide di inviare un messaggio di posta elettronica. Ciò significa che per ricevere un messaggio di posta, l'utente Internet deve possedere una casella di posta

(un account) su un server. Significa, inoltre, che il fornitore di servizi di posta deve memorizzare il messaggio e conservarlo fino a quando il destinatario non decide di scaricarlo.

2. Il secondo *protocollo* è denominato POP e consente al destinatario di stabilire una connessione con il server di posta per controllare se vi sono messaggi di posta per lui. A tale scopo, il destinatario deve fornire il nome della propria casella di posta e una password per impedire a terzi di leggere la propria posta.

Di solito, i programmi client di posta elettronica comprendono entrambi i *protocolli*, poiché un utente Internet che invia un messaggio di posta desidera anche, con tutta probabilità, ricevere una risposta.

IV. Rischi per la vita privata

Una serie di questioni comporta rischi specifici per la vita privata.

Raccolta di indirizzi di posta elettronica

Come illustrato in precedenza, l'indirizzo di posta elettronica è indispensabile per stabilire una connessione. Tuttavia, esso rappresenta anche una preziosa fonte di informazioni che comprendono dati personali sull'utente. E' utile, pertanto, capire quali sono i vari metodi di raccolta di indirizzi di posta elettronica.

Gli indirizzi di posta elettronica possono essere rilevati in vari modi:

- il fornitore del software "client di posta elettronica", che viene acquistato o ottenuto gratuitamente, potrebbe chiedere all'utente di registrarsi;
- è inoltre possibile creare un codice nel software del client che trasmetterà il proprio indirizzo di posta elettronica al fornitore del software senza che l'interessato ne sia a conoscenza (trattamento invisibile);
- in alcuni browser, sono stati individuati dei "buchi" di sicurezza che consentono ad una pagina web di conoscere gli indirizzi di posta elettronica dei visitatori. Ciò può avvenire attraverso contenuti attivi malevoli utilizzando, ad esempio, *JavaScript*;
- alcuni browser, inoltre, possono essere configurati in modo da inviare l'indirizzo di posta elettronica sotto forma di password anonima all'apertura delle connessioni FTP (solitamente, non si tratta comunque di un'impostazione predefinita);
- l'indirizzo di posta elettronica può essere richiesto da vari siti web in varie occasioni (ad esempio, sui siti commerciali in un ordine di acquisto, per la registrazione prima di accedere a una chat room, ecc.);
- gli indirizzi di posta elettronica potrebbero essere raccolti negli spazi pubblici in Internet in vari altri modi[48];
- un messaggio di posta elettronica potrebbe essere intercettato durante la trasmissione.

[48] Ulteriori indagini sull'attività di *spam* e sulla raccolta di indirizzi di posta elettronica sono state effettuate dall'autorità francese per la protezione dei dati, meglio nota come CNIL. V. in particolare la relazione della CNIL sulla posta elettronica e la protezione dei dati del 14 ottobre 1999, disponibile sul sito web della CNIL: www.cnil.fr.

Dati sul traffico

E' fondamentale distinguere tra il contenuto di un messaggio di posta elettronica e i dati sul traffico. I dati sul traffico sono i dati richiesti dai *protocolli* per effettuare una trasmissione corretta dal mittente al destinatario.

I dati sul traffico consistono, in parte, delle informazioni fornite dal mittente (ad esempio, l'indirizzo di posta elettronica del destinatario) e, in parte, delle informazioni tecniche generate automaticamente nel corso del trattamento di un messaggio di posta elettronica (ad esempio, la data e l'ora dell'invio, il tipo e la versione di "client di posta elettronica").

Tutti i dati sul traffico, o una parte di essi, vengono inseriti in un'intestazione trasmessa al destinatario unitamente al messaggio. Le parti dei dati sul traffico trasmesse vengono utilizzate dal server di posta del destinatario e dal "client di posta" per gestire in modo corretto la posta in arrivo. Il destinatario potrebbe usare i dati sul traffico trasmessi (proprietà di posta elettronica) a scopo di analisi (per verificare, ad esempio, il percorso seguito dal messaggio di posta elettronica in Internet).

La definizione di "dati sul traffico" comprende, in genere, quanto segue:

- indirizzo di posta elettronica e indirizzo IP del mittente
- tipo, versione e linguaggio dell'agente client
- indirizzo di posta elettronica del destinatario
- data e ora dell'invio di posta elettronica
- dimensione del messaggio di posta elettronica
- serie di caratteri utilizzata
- oggetto del messaggio di posta (che fornisce anche informazioni sul contenuto della comunicazione)
- nome, dimensione e tipo degli allegati
- elenco dei relay SMTP usati per la trasmissione

In pratica, i dati sul traffico vengono normalmente memorizzati dai server di posta elettronica del mittente e del destinatario. Essi potrebbero essere memorizzati anche dai relay server durante il percorso della comunicazione attraverso Internet.

Poiché la direttiva 97/66/CE non fornisce una definizione ufficiale di dati sul traffico, occorre richiamare l'attenzione sul fatto che i dati personali non necessari per effettuare la comunicazione e ai fini della fatturazione ma generati durante la trasmissione potrebbero essere erroneamente considerati dati sul traffico da alcuni attori Internet convinti di poterli memorizzare.

Nella raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei *fornitori di servizi Internet* a fini giudiziari[49], il Gruppo di lavoro istituito dall'articolo 29 si è occupato di alcuni problemi relativi alla vita privata correlati ai dati sul traffico. Il Gruppo di lavoro ritiene che il mezzo più efficace per limitare i rischi inaccettabili per la vita privata, nella salvaguardia delle esigenze delle autorità giudiziarie, consista

[49] Raccomandazione 3/99 sulla conservazione delle comunicazioni da parte dei *fornitori di servizi Internet* a fini giudiziari, adottata il 7 settembre 1999, 5085/99/IT/definitivo, WP 25.

nell'evitare che i dati sul traffico vengano conservati, in linea di principio, esclusivamente a fini giudiziari e che le leggi nazionali costringano gli operatori di telecomunicazioni, i servizi di telecomunicazione e i *fornitori di servizi Internet* a conservare i dati sul traffico per un periodo superiore a quello necessario a fini di fatturazione.

La Conferenza di primavera 2000 dei commissari europei per la protezione dei dati, tenutasi a Stoccolma, ha puntualizzato, nella relativa dichiarazione ufficiale, il fatto che "laddove, in casi specifici, i dati sul traffico devono essere conservati, vi deve essere una necessità dimostrabile, il periodo di conservazione deve essere il più breve possibile a la pratica deve essere chiaramente disciplinata dalla legge".

Contenuti di posta elettronica

La riservatezza delle comunicazioni è tutelata dall'articolo 5 della direttiva 97/66/CE. In virtù di tale disposizione, è vietata la lettura, ad opera di terzi, del contenuto di un messaggio di posta elettronica tra due soggetti. Se il contenuto del messaggio di posta elettronica viene memorizzato, durante il trasferimento, presso i relay server, esso deve essere cancellato subito dopo l'inoltro.

Se il relay server non riesce ad inviare il messaggio di posta elettronica, quest'ultimo può essere memorizzato per un periodo di tempo breve e limitato sul server in questione finché non viene rinviato al mittente unitamente ad un messaggio d'errore indicante che non è stato possibile recapitare il messaggio di posta elettronica al destinatario.

Il contenuto di un messaggio di posta elettronica rimane memorizzato presso il server di posta finché il "client di posta elettronica" dell'utente non ne richiede la consegna. In alcuni casi, l'utente può decidere di lasciare il messaggio di posta memorizzato presso il server di posta pur avendone scaricata una copia. Se l'utente non decide in tal senso, il messaggio di posta deve essere cancellato non appena il server di posta si è accertato che il destinatario lo ha debitamente ricevuto.

Se il contenuto deve essere sottoposto ad un'analisi antivirus, quest'ultima deve essere impostata, in automatico, esclusivamente per tale scopo. Il contenuto non deve essere analizzato per scopi diversi e non deve essere mostrato a terzi, nemmeno in seguito al rilevamento di un virus.

Un altro rischio per la vita privata associato alla posta elettronica riguarda l'impossibilità da parte dell'utente di eliminare, in modo semplice ed efficace, un messaggio di posta elettronica inviato o ricevuto, poiché la funzione di cancellazione non elimina necessariamente i messaggi di posta dal sistema. In questo caso, può rivelarsi relativamente facile per un altro utente della stessa macchina o per un gestore di sistema, nel caso di una macchina collegata in rete, reperire un messaggio che l'utente originario desiderava cancellare e pensa di avere eliminato dal sistema. Ovviamente, questo problema non riguarda solo la posta elettronica, ma è particolarmente importante in tale contesto. Per risolverlo, i sistemi dovrebbero essere progettati in modo che la funzione di cancellazione permetta di eliminare effettivamente le informazioni dal sistema.

Hardware e software possono essere utilizzati per sorvegliare il traffico in rete. Tale operazione è denominata *sniffing*. Il software di *sniffing* è in grado di leggere tutti i pacchetti di dati su una rete e visualizzare in chiaro tutte le comunicazioni non cifrate. Il tipo più semplice di *sniffing* può essere effettuato utilizzando un normale PC collegato ad una rete mediante un comune software.

Se l'operazione di *sniffing* viene effettuata in corrispondenza dei nodi o giunzioni centrali di Internet, essa potrebbe consentire l'intercettazione e la sorveglianza su vasta scala dei contenuti di posta elettronica e/o dei dati sul traffico mediante la selezione di alcuni

criteri, di solito la presenza di parole chiave. L'operazione di *sniffing*, in quanto attività di sorveglianza generale e a campione, anche se condotta da organismi governativi, può essere consentita solo se effettuata in base alle condizioni imposte dall'articolo 8 della Convenzione europea sui diritti umani.

In tale contesto, è interessante analizzare le attuali preoccupazioni espresse a livello internazionale circa l'eventuale sorveglianza delle comunicazioni internazionali e, in particolare, il sistema di intercettazione satellitare "Echelon". Attualmente, la sorveglianza globale rappresenta una questione scottante nell'ordine del giorno del Parlamento europeo[50]. In una relazione al direttore generale per la ricerca presso il Parlamento europeo[51] relativa allo sviluppo delle tecnologie di sorveglianza e al rischio di abuso delle informazioni economiche, si afferma che il sistema "Echelon" esiste da oltre vent'anni. Secondo tale relazione, Echelon utilizza estensivamente le reti di comunicazioni di tipo Internet globali NSA[52] e GCHQ[53] per consentire ai clienti di informazione a distanza di dialogare con i computer presso ogni luogo di raccolta e ricevere automaticamente i risultati.
Un altro controverso sistema di sorveglianza è Carnivore che, secondo le informazioni pubblicate dall'EPIC[54], sorveglia il traffico sugli impianti dei fornitori di servizi Internet al fine di intercettare le informazioni contenute nella posta elettronica di persone sospettate di crimini. L'EPIC afferma che Carnivore è presumibilmente in grado di analizzare milioni di messaggi di posta elettronica al secondo e di consentire agli organi giudiziari di intercettare tutte le comunicazioni digitali di un cliente di un *fornitore di servizi Internet*. Nel Congresso degli Stati Uniti, nei media e nella comunità della vita privata, sono stati sollevati seri dubbi circa la legalità di Carnivore e le sue potenzialità di abuso. In risposta al clamore pubblico relativo a Carnivore, il Procuratore generale Janet Reno ha annunciato il 27 luglio 2000 la divulgazione delle caratteristiche tecniche del sistema ad un "gruppo di esperti" per mitigare le preoccupazioni pubbliche.

La discussione sulla sorveglianza globale delle comunicazioni rientra, inoltre, nell'ordine del giorno del Consiglio d'Europa. Il 27 aprile 2000[55], il Comitato di esperti sulla criminalità nel cyberspazio ha pubblicato il proprio "progetto di convenzione sulla cybercriminalità". Tale convenzione agevolerà la raccolta di informazioni richiedendo alle società che forniscono servizi Internet di raccogliere e memorizzare informazioni per conto degli organi giudiziari. Essa richiederà lo scambio a livello internazionale di tali informazioni tra le autorità governative in vari settori di giurisdizione, anche con quelle che non aderiscono alla Convenzione europea dei diritti umani o ad altri atti del Consiglio d'Europa o dell'Unione europea nel campo della protezione dei dati.
Sinora non era prevista alcuna disposizione finalizzata a tutela del diritto fondamentale alla vita privata e i dati personali nei paesi terzi che ricevono dati personali dai cittadini dell'UE né è previsto alcun principio fondamentale volto al rispetto della norma dei diritti umani fondamentali, quali la necessità e la proporzionalità.
Senza voler commentare, a questo punto, il testo del progetto di convenzione, il Gruppo di lavoro desidererebbe tuttavia ribadire il punto di vista espresso dai commissari europei per la protezione dei dati in una dichiarazione formulata in occasione della conferenza di

---

[50] Per ulteriori informazioni, v. la Commissione del Parlamento europeo sulle libertà e i diritti dei cittadini, la giustizia e gli affari interni: http://www.europarl.eu.int/committees/en/default.htm. V. anche EPIC Alert 7.07, 20 aprile 2000.
[51] Relazione sui sistemi di intercettazione 2000, maggio 1999.
[52] National Security Agency, USA.
[53] Controparte britannica dell 'NSA.
[54] EPIC Alert 7.15, 3 agosto 2000.
[55] Il testo del progetto di convenzione è disponibile su:
http://conventions.coe.int/treaty/en/projets/cybercrime.htm

Stoccolma nel mese di aprile 2000. Tale dichiarazione recita: *La Conferenza di primavera del 2000 dei commissari europei per la protezione dei dati guarda con preoccupazione alle proposte relative al fatto che i fornitori di servizi Internet dovrebbero conservare abitualmente i dati sul traffico oltre le esigenze di fatturazione al fine di consentire l'eventuale accesso da parte degli organi giudiziari.*

La Conferenza sottolinea il fatto che tale conservazione sarebbe un'invasione impropria dei diritti fondamentali garantiti agli individui dall'articolo 8 della Convenzione europea sui diritti umani. Laddove, in casi specifici, i dati sul traffico devono essere conservati, vi deve essere una necessità dimostrabile, il periodo di conservazione deve essere il più breve possibile e la pratica deve essere chiaramente disciplinata dalla legge.

Il Gruppo di lavoro istituito dall'articolo 29 si è occupato degli aspetti relativi alla vita privata nel contesto dell'intercettazione delle comunicazioni nella raccomandazione 2/99[56]. In questa raccomandazione, il Gruppo di lavoro sottlinea il fatto che ogni intercettazione delle telecomunicazioni, intesa come la presa di conoscenza da parte di un terzo del contenuto e/o dei dati del traffico legati all'utilizzazione dei servizi di telecomunicazioni tra due o più corrispondenti, e in particolare dei dati del traffico concernenti l'uso dei servizi di telecomunicazioni, costituisce una violazione del diritto alla vita privata degli individui e della riservatezza della corrispondenza. Segue che le intercettazioni sono ammissibili solamente se soddisfano tre esigenze fondamentali, in conformità all'articolo 8, paragrafo 2, della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950[57], e all'interpretazione di questa disposizione da parte della Corte europea dei diritti dell'uomo: una base giuridica, la necessità della misura in una società democratica e la conformità ad uno degli obiettivi legittimi enumerati nella convenzione[58].

V. Analisi di temi particolari

Webmail

I sistemi di posta elettronica che utilizzano le pagine web come interfaccia sono denominati, nel loro insieme, "*webmail*" (ad esempio, Yahoo, HotMail, ecc.). E' possibile accedere alla *webmail* da qualsiasi parte del mondo senza che l'utente debba connettersi ad un determinato *fornitore di servizi Internet*, come quando si utilizza un normale account di posta elettronica.

La *webmail* è solitamente gratuita, ma per ottenere un account gratuito, spesso agli utenti viene chiesto di comunicare al fornitore i propri dati personali. Dalle indagini svolte dalle autorità per la protezione dei dati emerge che molti fornitori di *webmail* vendono o diffondono i dati personali a fini di invio di materiale pubblicitario.

[56] Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni, adottata il 3 maggio 1999, 5005/99/def., WP 18.

[57] Occorre sottolineare che le garanzie fondamentali riconosciute dal Consiglio d'Europa in relazione all'intercettazione delle telecomunicazioni comportano obblighi per gli Stati membri, indipendentemente dalle distinzioni fatte a livello dell'Unione europea in base alla natura comunitaria o intergovernativa dei campi interessati.

[58] La convenzione del Consiglio d'Europa N. 108 stabilisce che l'intercettazione può essere tollerata solo quando essa costituisce una misura necessaria in una società democratica per la tutela degli interessi nazionali elencati nell'articolo 9, paragrafo 2, della convenzione e quando essa è strettamente definita nei termini di tale finalità.

La *webmail* utilizza il *protocollo* HTML (invece del POP) per leggere e controllare la posta elettronica. I messaggi vengono infatti forniti nella classica pagina HTML.

Tale particolarità consente al fornitore di servizi di posta di inserire una pubblicità personalizzata (dal punto di vista grafico, al di fuori del messaggio vero e proprio) nella pagina web dove viene visualizzato il messaggio. La *webmail* è ampiamente sponsorizzata e in essa vengono visualizzati molti banner pubblicitari.

Poiché i sistemi di *webmail* si basano sul *protocollo* HTTP, essi sono esposti ai cosiddetti "Web Bugs" ("bachi web"), che rappresentano un tentativo di smascherare l'identità di posta elettronica di una persona che utilizza *cookie* e *tag* HTML.

I fornitori di *webmail* non dovrebbero inserire *collegamenti ipertestuali* invisibili nelle pagine web il cui URL comprende l'account di posta elettronica. In tal caso, infatti, essi contribuiranno a trasmettere alla società pubblicitaria l'indirizzo di posta elettronica della persona cui i dati si riferiscono. E' questa un'altra modalità di invasione della vita privata dell'utente mediante il trattamento invisibile dei dati.

Elenchi

Su Internet sono presenti vari servizi che forniscono elenchi di indirizzi di posta elettronica. Questi elenchi pubblici sono soggetti alle stesse norme di quelle applicabili agli elenchi telefonici e ad altri dati forniti al pubblico, come spiegherà il capitolo 6. Nell'ambito del quadro giuridico esistente, agli utenti deve essere concesso, quanto meno, il diritto di opporsi al trattamento dei propri dati, in base alla direttiva 95/46/CE (articolo 14) e alla direttiva 97/66/CE (articolo 11).

Occorre notare che il progetto modificato di direttiva concernente il trattamento dei dati personali e la tutela della vita privata nel settore delle telecomunicazioni armonizza gli obblighi dei responsabili del trattamento a tale riguardo e prevede l'esercizio, da parte delle persone interessate, del diritto di comparire negli elenchi. Il Gruppo di lavoro ritiene che tale fatto rappresenti un miglioramento importante.

Spam

Lo *"Spam"* può essere definito come la pratica di inviare messaggi di posta elettronica non richiesti, solitamente a carattere commerciale, in grossi quantitativi e in diverse riprese, a individui con i quali il mittente non ha alcun contatto precedente[59]. Il Gruppo di lavoro istituito dall'articolo 29 si è già occupato di tale questione nel proprio parere 1/2000 su alcuni aspetti del commercio elettronico[60].

Dal punto di vista del cittadino, il problema è triplice: in primo luogo, la raccolta dell'indirizzo di posta elettronica di un individuo senza il suo consenso o la sua conoscenza; in secondo luogo, il ricevimento di grandi quantità di messaggi pubblicitari indesiderati; e in terzo luogo, il costo del tempo di connessione.

Gli indirizzi di posta elettronica possono essere raccolti in elenchi pubblici o mediante varie tecniche. Ad esempio, l'indirizzo di posta elettronica può essere fornito dall'utente stesso in occasione dell'acquisto di beni o servizi su Internet. In altri casi, gli indirizzi di posta elettronica forniti dall'utente ad un fornitore possono essere venduti a terzi dal fornitore in questione.

[59] V. la relazione della CNIL sul mailing elettronica e la protezione dei dati, 14 ottobre 1999.
[60] Parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali presentato dall'Internet Task Force, adottato il 3 febbraio 2000, 5007/00/IT/def., WP 28.

Secondo il Gruppo di lavoro, le norme della direttiva sulla protezione dei dati costituiscono una risposta chiara ai problemi di riservatezza derivanti dallo *spam* e definiscono chiaramente i diritti e i doveri di tutti gli interessati. E' necessario distinguere due situazioni:

- se un indirizzo di posta elettronica viene raccolto da una società direttamente presso l'interessato in vista dell'effettuazione di mailing elettronici da parte della società stessa, o di terzi a cui l'indirizzo possa essere successivamente ceduto, la società in questione deve informare l'interessato al momento in cui ne trascrive l'indirizzo[61]. L'interessato, inoltre, come minimo, deve avere la possibilità, al momento della raccolta e successivamente in qualsiasi momento, di opporsi all'utilizzazione dell'indirizzo, e ciò in maniera facile ed elettronica, come ad esempio cliccando su un'apposita casella, sia per quanto riguarda le utilizzazioni effettuate dalla società originale che per quelle effettuate successivamente da altre imprese che abbiano ricevuto i dati da quella originale[62]. Alcune norme nazionali di recepimento delle direttive interessate prevedono persino l'obbligo di richiedere il consenso preventivamente. I requisiti dell'articolo del progetto di direttiva sul commercio elettronico in materia di comunicazioni commerciali non richieste permetterebbero di integrare a livello tecnico tali norme, stabilendo l'obbligo di consultare un registro presso il fornitore di servizi Internet, senza peraltro sminuire in alcun modo gli obblighi generali applicabili ai responsabili del trattamento;
- se un indirizzo di posta elettronica viene raccolto in uno spazio pubblico di Internet, il suo impiego per mailing elettronici sarebbe contrario alla pertinente legislazione comunitaria, e ciò per tre ragioni. Primo, il fatto potrebbe essere considerato come trattamento "sleale" dei dati personali ai sensi dell'articolo 6(1)(a) della direttiva generale. Secondo, sarebbe contrario al principio della finalità di cui all'articolo 6(1)(b) di tale direttiva, in quanto l'interessato aveva reso noto il suo indirizzo di posta elettronica per motivi del tutto diversi, ad esempio la partecipazione ad un newsgroup. Terzo, dato il citato squilibrio dei costi e il fastidio recato al destinatario, tali spedizioni non possono essere considerate giustificate in termini dell'equilibrio di interessi di cui all'articolo 7(f)[63].

Una caratteristica particolare dei mailing elettronici di natura commerciale è che, mentre i costi a carico del mittente sono estremamente ridotti se paragonati a quelli dei metodi tradizionali di marketing diretto, vi è un costo a carico del destinatario in termini di tempo di connessione. Tale situazione economica incentiva, chiaramente, l'uso su vasta scala di questo strumento di marketing e porta a trascurare le preoccupazioni relative alla protezione dei dati, nonché i problemi causati dal mailing elettronico.

I costi dei messaggi di posta elettronica non richiesti vengono sostenuti sia dal destinatario sia dal fornitore di posta Internet del destinatario (può trattarsi del server di *webmail* o del *fornitore di servizi Internet* del destinatario).

[61] Direttiva 95/46/CE, articolo 10
[62] Direttiva 95/46/CE, articolo 14.
[63] Questa disposizione (si tratta di uno dei vari eventuali motivi leciti di trattamento) prevede che il trattamento dei dati sia "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento …..a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata".

Il server di posta deve memorizzare, per qualche tempo, i messaggi di posta elettronica non richiesti. Il destinatario deve pagare[64] per scaricare un messaggio indesiderato e perde del tempo per ordinare i messaggi ricevuti ed eliminare quelli non richiesti, in particolare quando i messaggi di *spamming* non sono identificati come tali nell'oggetto (di solito, viene inserito il codice "ADV:" tra i primi caratteri dell'oggetto). Secondo le stime, lo *spam* (cioè posta elettronica non richiesta, "spazzatura" o "robaccia") costituisce attualmente il 10% di tutta la posta elettronica mondiale[65].

VI. Aspetti relativi alla riservatezza e alla sicurezza

La posta elettronica offre le stesse possibilità di comunicazione della posta tradizionale. Pertanto, le stesse norme si applicano alla segretezza della corrispondenza.

Chiunque ha il diritto di inviare un messaggio di posta a chi lo desidera senza che questo venga letto da terzi. L'articolo 5 della direttiva 97/66/CE, che riguarda le comunicazioni e i relativi dati sul traffico inviati, ad esempio, mediante la posta elettronica, stabilisce degli obblighi in merito alla riservatezza delle comunicazioni. Oltre a tali obblighi, l'articolo 4 della stessa direttiva impone ai fornitori dei servizi di telecomunicazioni di prendere le appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei propri servizi e, in caso di un particolare rischio di violazione della sicurezza, di informare gli abbonati indicando tutti i possibili rimedi, compresi i relativi costi.

Nel mondo non in linea (off-line), chiunque ha la possibilità di inviare una lettera in forma anonima o utilizzando uno pseudonimo. Per poter inviare un messaggio di posta elettronica anonimo, l'utente può richiedere ai vari fornitori di tale servizio un indirizzo di posta elettronica anonimo.

Dal punto di vista dell'utente, una serie di questioni è rilevante in base al tipo di posta elettronica:

- la riservatezza, cioè la protezione dei dati trasmessi per impedirne l'intercettazione. Un eventuale modo per assicurare la riservatezza è la *cifratura* del messaggio da inviare.

La *cifratura* e la decifratura si basano su programmi che integrano i normali programmi di posta elettronica (plug-in) o programmi di posta elettronica e browser che offrono tali funzioni. L'efficacia della *cifratura* dipende dagli algoritmi e dalla lunghezza della chiave utilizzata.

- l'*integrità*, che garantisce che l'informazione non venga alterata né accidentalmente né deliberatamente. L'*integrità* può essere conseguita calcolando un codice speciale sulla base del testo e trasmettendo tale codice cifrato speciale unitamente al testo. Il destinatario può quindi decifrare il codice e, ricalcolandolo, controllare se il messaggio è stato modificato.

- l'*autenticazione*, che garantisce che l'utente sia esattamente chi dichiara di essere. L'*autenticazione* può essere verificata scambiando le *firme digitali* in base a *certificati digitali*. Non è necessario che i certificati riportino il vero nome dell'utente. Essi possono indicare uno pseudonimo, secondo quanto previsto dall'articolo 8 della direttiva sulle *firme elettroniche*[66].

---

[64] L'operatore di telecomunicazioni, se l'utente utilizza un *modem*. In caso contrario, se l'utente utilizza una linea affittata, sebbene a causa di un messaggio non richiesto ('spam') i costi non insorgano immediatamente (si tratta di un canone forfettario), risulta evidente, da un punto di vista macroeconomico, che le spese generali derivanti da una massiccia attività di 'spam' vengono addebitate al fornitore di servizi Internet con ripercussioni successive sul canone delle linee affittate.

[65] V. il libro "Net Worth" (op cit), pag. 3.

[66] Direttiva 1999/93/CE del 13 dicembre 1999 relativa a un quadro comunitario per le *firme elettroniche*, Gazzetta ufficiale delle Comunità europee, 19 gennaio 2000, L 13/12 - 13/20.

VII. Misure intese al miglioramento della vita privata[67]

In questo capitolo, meritano di essere citati due tipi di strumenti: i filtri di posta elettronica e la posta elettronica anonima[68].

1) Il filtraggio della posta elettronica consente di schermare la posta elettronica in arrivo dell'utente e di lasciare passare solo i messaggi di posta elettronica che l'utente ha indicato di voler ricevere. Questi sistemi vengono utilizzati ampiamente per schermare lo *spam*.
Attualmente, varie società forniscono strumenti che gli utenti Internet possono installare sul proprio computer per schermare i messaggi di posta elettronica non desiderati. Inoltre, vari pacchetti di posta elettronica consentono agli utenti di filtrare i messaggi quando vengono ricevuti sul desktop.
I filtri più efficaci sono quelli che lasciano transitare solo alcuni messaggi di posta elettronica. Sebbene tale sistema funzioni per chi dispone di una rete immutabile di corrispondenti di posta elettronica, esso sarebbe scomodo per la maggior parte degli utenti, poiché richiederebbe l'approvazione di ogni nuovo corrispondente di posta elettronica.
Le tecnologie di filtraggio più comuni ammettono tutta la posta elettronica tranne quella proveniente da taluni nomi di dominio o indirizzi, oppure dotata di parole chiave nell'oggetto. Tuttavia, i mittenti più tenaci modificano spesso il nome di dominio o l'indirizzo di posta per raggirare i filtri, in particolare grazie al fatto che gli account di posta elettronica basati sul web sono spesso gratuiti ed è facile aderirvi o recedervi in qualsiasi momento. Infine, è difficile effettuare un filtraggio efficace utilizzando parole chiave, poiché la probabilità di errore è molto elevata.

2) La posta elettronica anonima consente agli utenti di offrire il proprio indirizzo di posta elettronica in linea senza dover rivelare la propria identità[69]. Su Internet, questo servizio è disponibile attualmente a titolo gratuito attraverso una serie di società che forniscono servizi di "ritrasmissione".

Grazie a questi servizi, il ritrasmettitore elimina l'identità dell'utente dalla posta elettronica consegnata. Le risposte al messaggio di posta elettronica anonimo pervengono al ritrasmettitore il quale confronta l'indirizzo anonimo con l'indirizzo di posta elettronica reale e consegna la risposta al cliente in modo sicuro.

VIII. Conclusioni

Dal punto di vista della protezione dei dati, occorre affrontare le seguenti questioni relative alla posta elettronica:

Trattamento invisibile eseguito dai "client di posta" e dai relay SMTP

La persona interessata deve avere la possibilità di conservare l'anonimato, in particolare quando partecipa ai gruppi di discussione. Da quanto risulta, gli indirizzi di posta elettronica dei partecipanti a tali gruppi di discussione vengono spesso spediti insieme al

[67] Per maggiori particolari, v. il capitolo 9 relativo alle misure intese al miglioramento della vita privata.
[68] V. il libro " Net Worth" (op. cit), pag. 275 e seguenti.
[69] Il presente documento fa riferimento anche a questo tipo di servizio nel capitolo 6 (Pubblicazioni e forum), nella relativa sezione V sulle misure intese al miglioramento della vita privata.

contenuto del messaggio[70]. Ciò non è conforme all'articolo 6 della direttiva 95/46/CE, che limita il trattamento dei dati allo stretto necessario per finalità legittime[71].

Conservazione dei dati sul traffico da parte di intermediari e fornitori di servizi di posta

Ai sensi dell'articolo 6 della direttiva 97/66/CE, i dati sul traffico devono essere cancellati al termine della comunicazione. La direttiva prevede un numero limitato di deroghe a tale principio, ad esempio se il trattamento successivo è necessario a fini di fatturazione[72].

Intercettazione

In conformità alla Convenzione europea dei diritti umani e alla direttiva 97/66/CE, è illecita l'intercettazione della posta elettronica (comunicazione e relativi dati sul traffico) a meno che essa non sia autorizzata per legge in casi specifici. Lo *sniffing* su vasta scala deve essere comunque vietato. Il principio di specificità, che è il corollario del divieto di qualsiasi sorveglianza generale o a campione, implica che, per quanto riguarda i dati sul traffico, le autorità pubbliche possono avere accesso a tali dati solo in casi specifici, e non in modo generale e attivo[73].

Memorizzazione e analisi dei contenuti di posta elettronica

I contenuti di posta elettronica devono essere mantenuti segreti e non devono essere letti né dagli intermediari né dai fornitori servizi di posta, neppure per le cosiddette "finalità di sicurezza della rete". Se per analizzare gli allegati si utilizza un software per l'analisi antivirus, il software installato deve offrire sufficienti garanzie di riservatezza. Se viene rilevato un virus, il fornitore di servizi dovrà essere in grado di segnalarne la presenza al mittente. Anche in questo caso, il fornitore di servizi di posta elettronica non è autorizzato a leggere il contenuto del messaggio o degli allegati.

Il Gruppo di lavoro istituito dall'articolo 29 raccomanda vivamente di cifrare i contenuti dei messaggi di posta elettronica. Ciò è particolarmente importante quando il messaggio contiene dati personali sensibili. I fornitori di servizi di posta elettronica dovrebbero mettere a disposizione, senza costi aggiuntivi, strumenti di facile uso per la cifratura del contenuto dei messaggi di posta elettronica. Al contempo, i fornitori dovrebbero offrire agli utenti la possibilità di scaricare i messaggi di posta elettronica dal server di posta del fornitore al client dell'utente, attraverso una connessione sicura. Si dovrebbe inoltre tenere conto delle esigenze di *integrità* e di *autenticazione*.

[70] Per maggiori particolari, v. il capitolo 6 in seguito.
[71] Questo principio è approfondito nella raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet effettuato da software e hardware adottata dal Gruppo di lavoro il 23 febbraio 1999, 5093/98/IT/def., WP 17.
[72] V. inoltre la raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari, adottata dal Gruppo di lavoro il 7 settembre 1999.
[73] V. a tale riguardo la raccomandazione 2/99 del Gruppo di lavoro sul rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni, adottata il 3 maggio 1999, 5005/99/def., WP 18.

Messaggi di posta elettronica non richiesti (spam)

Se un indirizzo di posta elettronica viene raccolto da una società direttamente presso l'interessato in vista dell'effettuazione di mailing elettronici da parte della società stessa, o di terzi a cui l'indirizzo possa essere successivamente ceduto, la società in questione deve informare l'interessato al momento in cui trascrive l'indirizzo. L'interessato, inoltre, deve avere la possibilità, al momento della raccolta e successivamente in qualsiasi momento, di opporsi all'utilizzazione dell'indirizzo, e ciò in maniera facile ed elettronica, come ad esempio cliccando su un'apposita casella, sia per quanto riguarda le utilizzazioni effettuate dalla società originale che per quelle effettuate successivamente da altre imprese che abbiano ricevuto i dati da quella originale.

Se un indirizzo di posta elettronica viene raccolto in uno spazio pubblico di Internet, il suo impiego per mailing elettronici sarebbe contrario alla pertinente legislazione comunitaria.

Elenchi di indirizzi di posta elettronica

Come nel caso degli elenchi telefonici, attualmente la persona interessata deve avere almeno la facoltà di recesso, in conformità ai principi di limitazione della finalità (articolo 6(1)(b) della direttiva 95/46/CE), nonché il diritto di non essere inclusa negli elenchi (articolo 11 della direttiva 97/66/CE). Inoltre, la persona interessata ha la possibilità di comparire in un elenco speciale di indirizzi di posta elettronica non utilizzabile a fini di marketing diretto.
E' importante ricordare che, nell'attuale versione della proposta di direttiva sulla tutela della vita privata nel settore delle telecomunicazioni, il diritto di recesso sarà modificato in diritto di adesione; ciò rappresenta un miglioramento sostanziale per le persone interessate.

CAPITOLO 5: NAVIGAZIONE E RICERCA

I. Introduzione

L'attività più comune degli utenti Internet è forse visitare i siti web per raccogliere informazioni. Ciò comporta la visualizzazione passiva del contenuto di una pagina web. E' anche possibile interagire con le pagine web in modo più attivo. Spesso, l'utente Internet deve cliccare un *collegamento ipertestuale*, premere su un messaggio pubblicitario sullo schermo (banner) o compilare moduli. Tutte queste attività prenderanno complessivamente il nome di 'websurfing' (navigazione nel web). In pratica, la navigazione avviene mediante un apposito web browser che connette l'utente Internet ad un web server presente da qualche parte su Internet.

Dal punto di vista della protezione dei dati, le principali domande sono tre:

- Durante la navigazione, quali informazioni relative alle attività dell'utente Internet vengono generate?
- Dove vengono memorizzate tali informazioni?
- Quali informazioni sono necessarie per i servizi forniti dai siti web?

L'ultima domanda riguarda i dati personali che un utente Internet rivela volontariamente, nonché le condizioni corrispondenti, ma essa non sarà trattata in questa sede poiché questo capitolo si incentra sui dati personali attinenti al processo (tecnico) di navigazione. Le fasi successive del processo di navigazione sono solo accennate e viene fornita un'indicazione dei dati personali generati.

II. Descrizione tecnica e attori interessati

Il processo di navigazione

· Fornitori di telecomunicazioni. Per contattare un sito web, un utente Internet accede generalmente ad Internet mediante una connessione telefonica ad un *fornitore di servizi Internet*. Il fornitore di telecomunicazioni registra la chiamata al *fornitore di servizi Internet*.

• Fornitore di accesso Internet. Il punto di ingresso al fornitore di servizi Internet è il server di accesso alla rete. Generalmente, questo server registra l'identificazione della linea chiamante della connessione. La maggior parte dei fornitori di servizi Internet registra il nome di login, l'ora di login e logout, e la quantità di dati trasferiti durante una sessione. Occorre notare che, in alcuni casi, il fornitore di telecomunicazione corrisponde al fornitore di accesso Internet.

· Allocazione dell'indirizzo IP. Dopo avere stabilito il contatto con il fornitore di accesso Internet, quest'ultimo assegna un indirizzo IP dinamico per la durata della sessione dell'utente Internet [74]. In seguito, tutte le comunicazioni effettuate durante una sessione avvengono verso e da questo indirizzo IP. Il numero IP accompagna tutti i pacchetti trasmessi in tutte le fasi successive della comunicazione. Occorre notare che il numero IP assegnato è sempre compreso in una determinata gamma di numeri assegnati al rispettivo

[74] Talvolta vengono utilizzati indirizzi IP statici per lo stesso utente e per lunghi periodi di tempo. Gli indirizzi IP statici vengono utilizzati spesso quando si ricorre a tecnologie di accesso alternative (ADSL, via cavo, mobili). Poiché queste si stanno diffondendo in misura crescente, anche l'uso relativo di indirizzi IP statici sta aumentando.

fornitore di accesso Internet. Pertanto, il fornitore di accesso da cui provengono i pacchetti IP può essere reperito con facilità da terzi[75] [76].

In seguito, il traffico Internet viene memorizzato dal *fornitore di servizi Internet* mediante il cosiddetto numero di porta, che specifica il servizio e il *protocollo* corrispondente. Presso il fornitore di servizi Internet, questo traffico viene riconosciuto da un numero di porta corrispondente. Inoltre, esso può essere trasferito direttamente a un *router* che connette l'utente Internet con i siti web esterni desiderati.

La richiesta viene trasferita spesso a un *proxy* server dedicato. Questo server registra la richiesta relativa ad un determinato sito web. Il *proxy* server contiene una copia del contenuto della maggior parte dei siti web visitati più spesso. Se il sito web richiesto dall'utente Internet si trova nel *proxy* server, quest'ultimo dovrà solo richiedere al sito web in questione un aggiornamento delle eventuali modifiche avvenute da quando la copia è stata memorizzata nel *proxy*. Tale misura riduce notevolmente la quantità di dati da scambiare tra il *fornitore di servizi Internet* e il sito web, poiché consente di comunicare solo le modifiche invece delle intere pagine. Il *proxy* server può memorizzare un elenco particolareggiato delle visite ai siti web connessi ad un indirizzo IP, in un determinato momento. Queste possono essere collegate ad un singolo utente mediante l'indirizzo IP e la registrazione dei tempi della sessione.

· *Router*. Nel percorso tra il *fornitore di servizi Internet* e il sito web visitato, il traffico attraversa generalmente vari *router* che convogliano i dati tra l'indirizzo IP dell'utente Internet e l'indirizzo IP del sito web. Per quanto riguarda la memorizzazione di dati personali, tali *router* sono considerati elementi neutrali, sebbene funzioni dedicate potrebbero consentire l'intercettazione del traffico Internet in corrispondenza di tali punti.

· Siti web normali. Dopo avere stabilito la connessione con il sito web, quest'ultimo raccoglie le informazioni sull'utente Internet che lo sta visitando. Tutte le richieste sono accompagnate dall'indirizzo IP di destinazione. Il sito web sa inoltre da quale pagina è stato trasferito l'utente Internet (è noto infatti il riferimento della pagina precedente, o URL). Queste informazioni relative alle visite dei siti web vengono generalmente memorizzate nel 'Common Log File'. Tutte le informazioni sopra descritte possono essere utilizzate per creare, mediante un apposito log analyser, informazioni cumulative sul traffico verso e da un sito web, nonché sulle attività dei visitatori.

Durante la connessione con un sito web, alcune informazioni supplementari vengono raccolte nella comunicazione tra il browser software più comune utilizzato dagli utenti Internet e i siti web visitati. Si tratta dei cosiddetti 'chattering data', che comprendono generalmente le seguenti informazioni[77]:

- Sistema operativo
- Tipo e versione del browser
- *Protocolli* usati per la navigazione
- Pagine di riferimento
- Preferenze linguistiche
- *Cookie*

[75] In alcuni casi, anche altre entità, come università, organizzazioni o società, possono agire da fornitore di servizi Internet.
[76] In qualche misura, gli indirizzi IP vengono anche assegnati su base geografica.
[77] Per maggiori particolari, v. il capitolo 2.

Il sito web dispone di un potere di raccolta supplementare inviando i cosiddetti *cookie*[78]. Si tratta di pezzi di dati che possono essere memorizzati in file di testo e depositati nel disco fisso dell'utente Internet, e che possono essere conservati in copia dal sito web. Essi costituiscono una parte standard del traffico HTTP e, in quanto tali, possono essere trasportati, senza ostacoli, insieme al traffico IP. Un *cookie* può contenere un numero esclusivo (GUI, Global Unique Identifier) che permette una personalizzazione migliore rispetto agli indirizzi IP dinamici. Tali *cookie* ampliano la capacità dei siti web di memorizzare e 'personalizzare' le informazioni relative ai propri visitatori. Il *cookie* può essere riletto regolarmente dal sito per identificare un utente Internet e riconoscerlo in occasione delle visite successive, controllare le eventuali password, analizzare un percorso durante una sessione e all'interno del sito, registrare le transazioni, come gli articoli acquistati, personalizzare un sito, ecc.

I *cookie* possono avere una natura diversa: possono essere persistenti, ma possono avere anche una durata limitata, come i cosiddetti "*cookie* di sessione". In alcuni casi, possono essere utili per fornire un determinato servizio attraverso Internet o per facilitare la navigazione da parte dell'utente Internet. Ad esempio, alcuni siti web personalizzati utilizzano i *cookie* per identificare gli utenti ad ogni visita successiva; in questo modo, gli utenti non dovranno registrarsi ogni volta nel sito web per controllare le proprie notizie.

Le implicazioni per la vita privata derivanti dall'uso dei *cookie* non devono essere sottovalutate. Questo problema sarà trattato nella sezione relativa all'analisi giuridica di questo capitolo.

- *Siti portale*

Alla luce della crescente complessità di Internet, spesso gli utenti Internet si connettono ad un sito web mediante i cosiddetti siti *portale*, che forniscono una panoramica dei collegamenti web in modo ordinato.
Spesso, tali *portali* contengono collegamenti a siti commerciali e potrebbero essere paragonati a un centro commerciale contenente molto negozi. I siti *portale* raccolgono le informazioni nello stesso modo dei siti web in generale, ma possono anche memorizzare le informazioni sulle visite effettuate in tutti i siti 'a monte' del portale.
Un *sito portale* è sempre ospitato da un *fornitore di servizi Internet* e, in alcuni casi, può appartenere al fornitore medesimo. In tal caso, il *fornitore di servizi Internet* ha la possibilità di raccogliere i dati sulle visite effettuate da un utente nei siti a monte di tale *portale* ed è pertanto in grado di creare un profilo completo dell'utente in questione.
L'autorità olandese per la protezione dei dati (Registratiekamer), in una relazione[79] su Internet e la vita privata, basata sulle indagini effettuate presso 60 *fornitori di servizi Internet* nei Paesi Bassi, ha concluso che il fornitore di contenuti (nella fattispecie, il *fornitore di servizi Internet* che possiede un *portale*) ha la possibilità di conoscere la quantità di annunci pubblicitari che sono stati presentati, la frequenza delle visite effettuate da un utente ad un negozio elettronico, i prodotti acquistati e il prezzo pagato.

- *Fornitori di servizi supplementari*

[78] Nella fattispecie, si fa riferimento ai cookie persistenti, cioè quelli che permangono per più di una sessione.
[79] V. la relazione della Registratiekamer report (ARTZ, M.J.T. e VAN EIJK, M.M.M.), *Klant in het web: Privacywaarborgen voor Internettoegang*, Achtergrondstudies en verkenningen 20 giugno 2000, disponibile su: www.registratiekamer.nl La relazione sottolinea il fatto che nei Paesi Bassi quasi tutti i fornitori di accesso dispongono di una propria pagina web utilizzata anche come *portale* per l'avvio della navigazione.

A volte, i dati raccolti dai siti web vengono trasferiti (automaticamente) a terzi rispetto alla comunicazione originaria (ad esempio, società specializzate nell'analisi delle statistiche web, come Nestat). Lo scopo può essere quello di creare dati statistici cumulativi relativi alle visite effettuate in un sito web, che vengono rivenduti ai proprietari dei rispettivi siti web. Generalmente, i banner pubblicitari raccolgono informazioni sui siti web visitati da una persona mediante i *cookie* file. I fornitori di servizi, come DoubleClick o Globaltrash, accumulano le informazioni relative alle visite effettuate in tutti i vari siti in cui essi pubblicano i propri annunci pubblicitari. Grazie a tali dati è possibile compilare un profilo delle preferenze degli utenti Internet da utilizzare, successivamente, per personalizzare le pagine web.

La navigazione dal punto di vista dell'utente Internet

Nella maggior parte dei casi, un PC dotato di un browser software, all'avvio caricherà automaticamente una determinata pagina di avvio del web. Tale pagina di avvio può contenere *collegamenti ipertestuali* che possono essere attivati per visitare altri siti web o motori di ricerca. Sfogliando, il browser dell'utente Internet invia ad un server (che può essere ubicato in qualsiasi parte del mondo) la richiesta di trasmettere una pagina web specifica (contraddistinta dal relativo URL) ospitata dal server in questione. Cliccando su un *collegamento ipertestuale*, l'utente Internet scarica di fatto la pagina web richiesta nel proprio computer.

L'utente Internet, dopo essersi connesso con il proprio *fornitore di servizi Internet*, sceglie generalmente uno dei seguenti approcci durante la navigazione:

- accede direttamente al sito web richiesto inserendo l'URL, come www.amazon.com. L'URL contiene anche il *protocollo*;
- raggiunge il sito web mediante un sito di riferimento (*portale*) contenente *collegamenti ipertestuali* verso altri siti. Tali servizi di *portale* stanno diventando sempre più popolari poiché il numero di pagine web è in aumento e gli utenti Internet necessitano di maggiori indicazioni per reperire materiale interessante;
- reperisce i siti pertinenti inserendo prima un'interrogazione in un sito web mediante un motore di ricerca. I motori di ricerca usano l'indicizzazione mediante l'inserimento di parole chiave. L'utente inserisce una o più parole chiave e inizia la ricerca. Il motore di ricerca cerca, nella propria base di dati degli indici, i titoli dei siti corrispondenti e i relativi indirizzi URL. Il motore di ricerca è in grado di assemblare i profili personali accumulando i termini di ricerca inseriti dall'utente Internet e i siti web successivamente visitati. La personalizzazione viene spesso effettuata mediante i *cookie*. Vari motori di ricerca offrono inoltre servizi più personalizzati per i quali all'utente Internet viene chiesto di fornire informazioni sulle proprie preferenze personali al fine di ricevere, ad esempio, aggiornamenti regolari dei siti web in relazione ad un determinato argomento [80];

Descrizione dei dati più rilevanti generati e memorizzati nei vari punti del processo di navigazione web

	Dati generati e/o memorizzati	Osservazioni
1.Fornitori di telecomunicazioni	Dati sul traffico della connessione al *fornitore di servizi Internet*	Può corrispondere al *fornitore di servizi Internet*

[80] In questo contesto è importante citare la posizione comune sui motori di ricerca adottata dal Gruppo di lavoro internazionale sulla protezione dei dati e le telecomunicazioni adottata il 15 aprile 1998 all'incontro di Hong Kong, disponibile su: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm

2. *Fornitore di servizi Internet*: server di accesso alla rete	*Identificazione della linea chiamante*, indirizzo IP, dati della sessione	
3. *Fornitore di servizi Internet: proxy*	Pagine web visitate dall'indirizzo IP ad una determinata ora	
4. *Router*	Indirizzo IP	
5. Siti web	Indirizzo IP URL della pagina precedente Dati della sessione (ora, tipo di transazione) Nomi e dimensioni dei file trasferiti *Cookie*	Assemblati nell' 'Extended Common Log File'
6. *Portali*	Informazioni collettive sulle visite effettuate nei siti web cui esse si riferiscono *Cookie*	Possibilità di creare profili completi degli utenti (dati sulle comunicazioni e sul comportamento dell'utente a disposizione del *fornitore di servizi Internet*)
7. Fornitori di servizi (tra cui i motori di ricerca)	Analisi dei logfile raccolti dai vari siti web Dati/profili raccolti dai siti web accumulati mediante i *cookie* Motori di ricerca: parole chiave inserite dall'utente Internet	Ad es. NedStat Ad es. DoubleClick

III. Rischi per la vita privata

Milioni di utenti Internet in tutto il mondo navigano spesso nel World Wide Web o cercano informazioni su Internet. Tuttavia, tali attività non sono esenti da rischi dal punto di vista della vita privata.

Nel contesto di Internet, molte informazioni vengono raccolte e trattate in modo invisibile per la persona interessata. A volte, l'utente Internet non è consapevole del fatto che i suoi dati personali sono stati raccolti e successivamente trattati, e che potrebbero essere utilizzati per finalità di cui l'utente non è a conoscenza. La persona interessata non è al corrente del trattamento e non è libero di decidere al riguardo[81].

Vi sono poi ulteriori rischi quando i dati raccolti durante le attività di navigazione degli utenti Internet possono essere collegati con altre informazioni esistenti sullo stesso utente. Il timore di un tale collegamento dei dati personali relativi agli utenti Internet è stato uno dei temi principali nei dibattiti relativi alla fusione della società pubblicitaria Internet DoubleClick e Abacus Direct, una società che si occupa di ricerche di mercato.

Il timore è dovuto al fatto che, qualora le due aziende dovessero fondersi, la base di dati di DoubleClick, contenente i dati sulle abitudini degli utenti Internet, potrebbe essere

[81] Il Gruppo di lavoro istituito dall'articolo 29 si è occupato di questo argomento nella raccomandazione 1/99 adottata il 23 febbraio 1999: raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet effettuato da software e hardware, adottata il 23 febbraio dal Gruppo di lavoro, 5093/98/IT/def., WP 17

confrontata con la base di dati di Abacus Direct, contenente i nomi e gli indirizzi reali, nonché informazioni particolareggiate sulle abitudini di acquisto dei clienti[82].

La fusione ha avuto luogo nel mese di novembre 1999. In base alle informazioni fornite sul sito web DoubleClick[83], i dati relativi al nome e all'indirizzo forniti volontariamente da un utente su un sito web di Abacus Alliance avrebbero dovuto essere collegati da Abacus attraverso l'uso di un codice di corrispondenza e il *cookie* di DoubleClick on altre informazioni relative all'utente in questione.
Tra i dati contenuti nella base dati Abacus Online figurano il nome dell'utente, l'indirizzo, il catalogo di vendita al dettaglio e la storia degli acquisti effettuati on-line, nonché i dati demografici. La base di dati comprende inoltre le informazioni dell'utente non personalmente identificabili raccolte dai siti web e da altre società che intrattengono rapporti commerciali con DoubleClick.
Secondo DoubleClick, non è stato creato sinora alcun collegamento tra le basi di dati della DoubleClick e dell'Abacus.

Nuovo software di sorveglianza

I fornitori di servizi Internet potranno disporre, a breve, di nuove tecnologie di sorveglianza che genereranno molte più informazioni sui modelli di traffico e sulle preferenze di contenuto rispetto a quelle esistenti nella rete PSTN (public switched telecommunications network). Tali tecnologie promettono di fornire l'equivalente Internet dei registri dettagliati delle chiamate PSTN ed oltre.

Questi tipi di programmi software sono popolarmente noti come applicazioni E.T. *" poiché dopo essersi insediati nel computer dell'utente ed avere appreso ciò che serve, essi fanno ciò che faceva l'extraterrestre di Steven Spielberg: chiamano casa*[84].

Per fare un esempio, la Narus, una società privata di software di Palo Alto, California (UA), offre ai *fornitori di servizi Internet* un software in grado di 'sorvegliare il flusso di dati e analizzare ogni pacchetto per estrarne l'intestazione e le informazioni sul carico pagante"[85]. La Narus afferma di operare in stretta collaborazione con partner chiave, come Bull, Cisco e Sun Microsystems. Questo software può essere utilizzato per l'identificazione e la misurazione della telefonia Internet e di altre applicazioni (ad esempio, web, posta elettronica o fax IP), ma si propone anche di sorvegliare il contenuto potenzialmente fatturabile all'interno del traffico IP (ad esempio, materiale coperto dal diritto d'autore che prevede una royalty o l'uso su richiesta di un'applicazione oppure gli audio clip). Il software della Narus riferisce ai fornitori di servizi Internet in tempo reale quali sono i principali siti web visitati, nonché i tipi di contenuto visualizzati e scaricati[86].
Alexa[87] è uno strumento che può essere aggiunto ad un browser per accompagnare l'utente durante la navigazione, fornendo informazioni supplementari sul sito visitato (sul proprietario del sito registrato, le stime e le revisioni del sito) e dando suggerimenti sui siti correlati. A fronte della fornitura di questo servizio agli utenti, Alexa ha creato una

[82] V. EPIC alert 6.10, 30 giugno1999. La stessa preoccupazione è stata espressa durante la causa Harriet M. Judnick contro DoubleClick presso la Corte Suprema dello Stato di California.
[83] www.doubleclick.net:8080/privacy_policy/ Tale fusione è illustrata nei particolari nel capitolo 7 relativo alle transazioni elettroniche su Internet.
[84] V. l'articolo di copertina di Time Magazine di COHEN, Adam del 31 luglio 2000: *How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.*
[85] http://www.narus.com
[86] V. PALTRIDGE, Sam, *Mining and Mapping Web Content*, in: Info, The Journal of policy, regulation and strategy for telecommunications, information and media, vol. 1, no. 4 agosto 1999, p. 327-342
[87] http://www.alexa.com

delle più grandi basi di dati sulle tipologie di uso del web. All'inizio del 1999, Amazon ha sborsato 250 milioni di dollari statunitensi in titoli per l'acquisto di Alexa. Per quanto riguarda la propria politica sulla vita privata, Alexa dichiara che le informazioni raccolte relative all'uso del web rimangono anonime grazie all'impiego dei registri d'uso del web e dei dati dei *cookie*.

Tra gli altri prodotti di Alexa figura il programma zBubbles, uno strumento di shopping on-line che raccoglie i dati di navigazione relativi all'utente allo scopo di fornire consigli sui prodotti, consulenza sullo shopping di tipo comparativo, ecc. In base alle informazioni pubblicate da Time Magazine[88], zBubbles invia informazioni ad Alexa anche quando gli utenti non effettuano acquisti. Il prodotto è studiato per essere installato sullo schermo per l'intera durata della sessione di navigazione, anche se la maggior parte degli utenti non effettua acquisti in continuazione.

Un altro esempio interessante di software di sorveglianza è Radiate, già conosciuto con il nome di Aureate. Radiate è una società pubblicitaria che collabora con i produttori di *shareware*. Si dice[89] che gli annunci pubblicitari di Radiate erano accompagnati da un software E.T. che è stato installato nei computer di 18 milioni di persone e che utilizzava la loro connessione Internet per riferire gli annunci pubblicitari da esse selezionati. La versione originale del software Radiate, che risiede tuttora in innumerevoli computer, è stato scritta in modo da continuare a 'chiamare' casa anche dopo la cancellazione del *shareware*. Gli utenti avevano bisogno di uno strumento speciale per cancellare il file, che la società ha successivamente fornito sul proprio sito web.

Attualmente, esistono centinaia di applicazioni E.T. Si ritiene che oltre 22 milioni di persone le abbiano scaricate[90]. I programmi software di sorveglianza E.T. rappresentano, di nuovo, un esempio di tecnologie in grado di trattare i dati personali degli utenti senza che essi ne siano a conoscenza (trattamento invisibile): la maggior parte degli utenti non sa che questi programmi sono stati installati sui loro computer.

Spesso, i produttori di queste applicazioni E.T. affermano che, sebbene possano raccogliere i dati degli utenti di computer, essi non li collegano alle persone. Tuttavia, ciò non offre all'utente garanzie sufficienti poiché, visto il valore commerciale dei dati personalizzati, le società che li raccolgono potrebbero modificare le loro politiche in qualsiasi momento. Il rischio potenziale di uso improprio dei dati è sempre in agguato[91].

IV. Analisi giuridica

Il punto di partenza per l'analisi giuridica dei fenomeni di navigazione e ricerca su Internet è che, in linea di principio, entrambe le direttive sulla protezione dei dati (direttiva 95/46/CE e 97/66/CE) si applicano a Internet[92].

Disposizioni principali della direttiva generale 95/46/CE: principio della finalità, trattamento leale e informazione della persona interessata

[88] Come citato nell'articolo di COHEN, A. in Time Magazine (op cit).
[89] Come citato nell'articolo di COHEN, A. in Time Magazine (op cit.).
[90] Come citato nell'articolo di COHEN, A. in Time Magazine (op cit.).
[91] Come citato nell'articolo di COHEN, A. in Time Magazine (op cit.).
[92] V. WP 16, documento di lavoro: *Trattamento dei dati personali su Internet*, adottato il 23 febbraio 1999 dal Gruppo di lavoro, 5093/98/IT/def.

Tre dei temi trattati nella direttiva generale meritano un'attenzione speciale in questo capitolo: il principio della finalità, i principi del trattamento leale e delle informazioni da fornire alla persona interessata.

Informazioni da fornire alla persona interessata

Su Internet, il flusso di dati scorre molto velocemente e le norme tradizionali concernenti le informazioni da fornire alla persona interessata circa il trattamento e la finalità vengono spesso ignorate. In alcuni casi, gli utenti Internet sono pienamente consapevoli dell'esistenza o delle capacità del software o hardware attraverso cui avviene il trattamento (ad esempio, i *cookie* o le applicazioni software E.T.).

Il Gruppo di lavoro ha trattato questi casi nella sua raccomandazione 1/99[93]. In questa raccomandazione, il Gruppo di lavoro ha sottolineato il fatto che una condizione per rendere legittimo il trattamento dei dati personali è che il soggetto interessato sia informato e sia messo al corrente del trattamento in questione. I prodotti Internet di software e hardware dovrebbero mettere a disposizione degli utenti Internet le informazioni sui dati che si intendono raccogliere, memorizzare o trasmettere, e lo scopo per cui ciò viene fatto.
I prodotti Internet software e hardware dovrebbero inoltre permettere all'utente dei dati di avere facilmente accesso, in qualsiasi momento, ai dati raccolti che lo riguardano.
La velocità dei flussi di dati su Internet non può essere addotta quale pretesto per la mancata osservanza degli obblighi che discendono dalla direttiva generale. Infatti, Internet è uno strumento che consente di fornire al soggetto interessato informazioni semplici e veloci. Ogniqualvolta vengono raccolti dati personali, all'individuo devono essere fornite informazioni essenziali[94] in modo tale da garantire una raccolta leale dei dati personali, cioè, in base alla situazione, direttamente sullo schermo o dal punto in cui avviene la raccolta, oppure attraverso una casella di dialogo (ad esempio, nel caso del deposito dei *cookie*). A chi non condivide il trattamento e desidera avere ulteriori informazioni in merito, deve essere data la possibilità di cliccare da qualche parte. Alcuni siti web contengono una clausola sulla vita privata, in cui forniscono informazioni sui dati trattati, le finalità del trattamento e il modo in cui una persona interessata può esercitare i propri diritti. Ma non è sempre così e, anche quando sono previste clausole sulla vita privata, spesso esse non contengono tutte le informazioni necessarie.

Pur essendo molto favorevole alla previsione di clausole precise e complete sulla vita privata, il Gruppo di lavoro incoraggia vivamente a fornire alle persone interessate le informazioni direttamente dallo schermo, o utilizzando apposite caselle di dialogo che compaiono sullo schermo quando i dati vengono raccolti, senza che alla persona interessata venga richiesto di agire direttamente per accedere a tali informazioni, poiché non sempre gli utenti Internet leggono le clausole sulla vita privata di tutti i siti visitati navigando da un sito all'altro.

Per avere un serio ruolo di informazione, le clausole sulla vita privata non devono essere troppo lunghe, devono avere una struttura chiara e fornire informazioni precise sulla politica del trattamento dei dati del sito, in termini chiari e comprensibili. Il lavoro dell'OCSE in questo campo (generatore di clausole sulla vita privata o 'privacy wizard') potrebbe consentire il conseguimento di tali obiettivi, sebbene l'uso del generatore non garantisce di per sé la conformità alle direttive europee.

[93] Raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet effettuato da software e hardware, adottata il 23 febbraio 1999 dal Gruppo di lavoro, 5093/98/IT/def., WP 17.
[94] Le informazioni indicate nella casella devono contenere, come minimo, i particolari sul responsabile del trattamento, le finalità del trattamento e, ove applicabile, il diritto di opporsi al trattamento.

In pratica, le clausole sulla vita privata da sole probabilmente non basteranno poiché, come spesso accade, quelle previste non consentono informazioni sufficienti dal punto di vista della protezione dei dati. Un recente studio svolto negli Stati Uniti dall'EPIC[95] relativo alle clausole sulla vita privata dei 100 maggiori siti di commercio elettronico ha mostrato che solo pochi siti web ad alto traffico offrivano una tutela adeguata della vita privata. Di fatto, nessuno di essi osservava elementi importanti della prassi di informazione leale analizzata nell'indagine[96].

Principio della finalità

Le informazioni da fornire al soggetto interessato devono, in tutti i casi, contenere spiegazioni ampie e chiare circa la finalità del trattamento. L'articolo 6 della direttiva generale vieta il trattamento successivo dei dati per usi non compatibili.

Questo principio è particolarmente importante per i siti web che raccolgono informazioni dagli utenti Internet sul loro comportamento di navigazione, per i programmi software autorizzati dall'utente per sorvegliarne il comportamento su Internet, per una finalità specifica ma non per altre finalità (sconosciute), nonché per i *fornitori di servizi Internet*. In linea di principio, i dati di navigazione relativi agli utenti Internet dovrebbero essere raccolti solo dai *fornitori di servizi Internet* nella misura in cui essi sono necessari per fornire un servizio all'utente, nella fattispecie per visitare i siti che l'utente desidera. I *fornitori di servizi Internet*, a volte, adducono la necessità di conservare questi dati per poter sorvegliare le prestazioni dei propri sistemi. Ma a tale scopo, non è necessario conservare dati identificabili, poiché è possibile misurare e sorvegliare le prestazioni di un sistema sulla base di dati aggregati.

Una recente relazione della Registratiekamer[97] ha concluso che quando i fornitori di accesso Internet conservano i dati sul traffico degli utenti a livello individuale, essi non agiscono nella loro qualità di fornitori di accesso. Questa informazione è particolarmente interessante per le loro attività in quanto fornitori di contenuto. Tuttavia, dovrebbe essere chiarito che si tratta di una finalità completamente diversa.

Sarebbe utile poter integrare nei mezzi tecnici il principio della limitazione della finalità. Inoltre, ciò dovrebbe essere considerata una forma di tecnologia intesa al miglioramento della vita privata[98].

Trattamento leale

L'articolo 6 della direttiva generale contiene una serie di principi intesi a garantire il trattamento leale dei dati personali. Uno di essi è quello della finalità o limitazione dello scopo, cui si riferivano i paragrafi precedenti.

Questo articolo specifica inoltre che i dati personali devono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati. Ciò significa che, una volta che i dati sono stati resi anonimi in modo che non sia più possibile collegarli alla persona interessata, essi possono essere utilizzati per altre finalità, ad esempio, per misurare le prestazioni del servizio offerto da un fornitore di servizi Internet o per compilare un questionario sul numero dei visitatori di un sito web.

---

[95] Indagine "Surfer Beware III: Privacy Policies Without Privacy Protection", v. EPIC alert 7.01, 12 gennaio 2000. Disponibile su www.epic.org/reports/surfer-beware.html

[96] Le American Fair Information Practices sono le linee guida fondamentali per la tutela delle informazioni personali negli Stati Uniti.

[97] *Klant in het web: Privacywaarborgen voor Internettoegang* (op cit.)

[98] V. il capitolo 9 in seguito.

I principali motori di ricerca conservano dei registri delle interrogazioni contenenti un resoconto delle interrogazioni e altre informazioni, tra cui i termini usati[99]. I termini usati interessano alle imprese che cercano di selezionare *meta-tag* per le pagine web e per stimare la domanda on-line di contenuti correlati ad un particolare prodotto, società o marca. Se non esistono collegamenti tra il registro delle interrogazioni e l'identità dell'utente Internet che ha inserito la parola chiave, non vi sono ostacoli giuridici che impediscono la conservazione di tali dati aggregati.

Se non vengono resi anonimi, i dati relativi alla ricerca e alla navigazione su Internet non devono essere conservati dopo il termine della sessione Internet. Questo aspetto sarà spiegato in modo più particolareggiato nel trattare le disposizioni della direttiva specifica sulla vita privata e le telecomunicazioni relative ai dati sul traffico.

Per quanto riguarda la lealtà della finalità del trattamento dei dati, occorre tener conto anche dell'articolo 7 della direttiva. L'articolo stabilisce una serie di condizioni che legittimano il trattamento, tra cui il consenso da parte della persona interessata e l'equilibro tra l'interesse legittimo del responsabile del trattamento e i diritti fondamentali dell'individuo. Tale equilibrio di interessi deve essere sempre tenuto in considerazione dal responsabile del trattamento nel rilevare i dati da un utente Internet.

Disposizioni principali della direttiva specifica sulla tutela della vita privata nel settore delle telecomunicazioni

Come si può vedere nella tabella riportata nel capitolo 3, alcune disposizioni della direttiva sulle telecomunicazioni sono particolarmente pertinenti per la navigazione e la ricerca su Internet.

Sebbene il titolo della direttiva 97/66/CE si riferisca al settore delle telecomunicazioni in generale, è evidente che la terminologia utilizzata nel testo è stata scelta sulla base della tecnologia ISDN. La maggior parte delle disposizioni della direttiva utilizzano termini quali "chiamate", che alludono alla telefonia tradizionale e ISDN, e ne complicano l'applicazione ai servizi Internet. Tuttavia, è di solito possibile includere i servizi Internet nell'ambito di applicazione della direttiva pur senza qualche difficoltà, come vedremo nei paragrafi che seguono.

Tuttavia, molti di questi problemi terminologici vengono risolti nel testo della proposta di direttiva modificata del 12 luglio 2000[100]. In questa proposta, viene aggiornata una serie di definizioni per garantire che siano coperti tutti i vari tipi di servizi di trasmissione per le comunicazioni elettroniche, indipendentemente dalla tecnologia usata.

I riferimenti al termine "chiamate" sono ora limitati ai casi in cui il legislatore desidera riferirsi specificamente alle chiamate telefoniche, come risulta chiaro dall'inclusione di una definizione di tale termine nell'articolo 2(e)[101]. In tutti gli altri casi, il nuovo testo parla di "comunicazioni" o "servizi di comunicazioni".

I paragrafi che seguono commenteranno le più rilevanti disposizioni della direttiva 97/66/CE. Laddove utile, il presente documento farà riferimento alle modifiche introdotte dalla nuova proposta di direttiva modificata.

---

[99] V. PALTRIGDE, S., *Search engines and content demand,* in *Mining and Mapping Web Content*, in: Info, The Journal of policy, regulation and strategy for telecommunications, information and media, vol. 1, no. 4 agosto 1999, p.330-333.

[100] COM (2000) 385.

[101] Con "chiamata" si intende una connessione stabilita mediante un servizio telefonico disponibile al pubblico, che consente una comunicazione reciproca in tempo reale.

Articolo 4: Sicurezza

I fornitori dei servizi di telecomunicazione devono prendere la appropriate misure di sicurezza che tengano conto dello stato dell'arte. Tali misure devono essere proporzionali ai rischi derivanti dalla situazione specifica.

Tale disposizione è particolarmente rilevante per i fornitori dei *router* e delle linee di connessione poiché tali strutture trasportano quantità massicce di informazioni.

Nella nuova proposta, questo articolo resta invariato tranne la sostituzione del termine "servizi di telecomunicazione" con il termine "servizi di comunicazioni elettroniche".

Articolo 5: Riservatezza

Le normative nazionali devono garantisce la riservatezza delle comunicazioni. In particolare, esse vietano l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza il consenso di questi ultimi[102].

Nelle attività di navigazione e ricerca su Internet vi sono vari attori cui si applica questo articolo: i fornitori dei *router* e delle linee di connessione, i *fornitori di servizi Internet* e, in generale, i fornitori di telecomunicazioni.

In linea di principio, questo articolo si riferisce al contenuto della comunicazione. Tuttavia, la distinzione tra i dati sul traffico e il contenuto non è facile da applicare nel contesto di Internet e, certamente, non per quanto riguarda la navigazione. I dati di navigazione potrebbero, in teoria, essere considerati dai sul traffico. Tuttavia, il Gruppo di lavoro ritiene che la navigazione attraverso vari siti deve essere considerata una forma di comunicazione e, in quanto tale, deve rientrare nell'ambito di applicazione dell'articolo 5.

Il comportamento di navigazione di un utente Internet (dati di navigazione) che visita vari siti web può di per sé rivelare molto sulla comunicazione in corso. Conoscendo i nomi dei siti web visitati, è possibile, nella maggior parte dei casi, acquisire un quadro piuttosto preciso della comunicazione effettuata. Inoltre, è possibile a chiunque sia in possesso dei dati sul traffico visitare il sito e vedere esattamente i contenuti ai quali l'utente ha avuto accesso.

Il Gruppo di lavoro ritiene, pertanto, che i dati di navigazione di un utente Internet devono essere soggetti allo stesso livello di protezione del "contenuto". Tale forma di comunicazione, pertanto, deve rimanere riservata. In questo senso, si può affermare che i *clickstream* rientrano nell'ambito di applicazione di questo articolo.

La nuova proposta di direttiva modificata definisce i "dati relativi al traffico" nell'articolo 2(1)(b): *con "dati sul traffico" è inteso ogni dato sottoposto a trattamento nel corso o ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica.* I dati di navigazione rientrerebbero pertanto in questa definizione e sarebbero considerati dati sul traffico.

La revisione della direttiva ha introdotto importanti miglioramenti ampliando l'ambito di applicazione dell'articolo 5 a coprire non solo il contenuto della comunicazione ma anche i dati sul traffico correlati. Assicurando un protezione uguale al contenuto e ai dati sul

[102] V. al riguardo la raccomandazione 2/99 del Gruppo di lavoro relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni, adottata il 3 maggio 1999, 5005/99/def., WP 18.

traffico correlati, la distinzione (a volte difficile) tra tali concetti diviene meno importante. Il Gruppo di lavoro si compiace di tale miglioramento.

Articolo 6: Dati sul traffico e sulla fatturazione

I dati sul traffico devono essere cancellati o resi anonimi al *termine della chiamata.* Per interpretare questo articolo nel contesto di Internet, è necessario definire cosa si intende per dati sul traffico e contenuto della comunicazione.

Questo articolo sembra riferirsi in particolare alle telecomunicazioni a commutazione di circuito, che collegano due o più parti comunicanti. I dati sul traffico vengono creati quando viene stabilita e mantenuta tale connessione. Ciò rende particolarmente difficile l'applicazione di questo articolo nel contesto di Internet.

Al traffico Internet si applica quanto segue: i pacchetti trasmessi vengono 'avvolti' in varie intestazioni di *protocollo* (ad esempio intestazione TCP, IP e Ethernet). Queste intestazioni di *protocollo* vengono lette in corrispondenza di ogni nodo (*router*) attraversato dal pacchetto, per decidere dove inviarlo in seguito. Tuttavia, non sembra esservi la necessità che ogni nodo intermedio, dopo avere trasmesso il pacchetto, memorizzi le informazioni di intestazione.

Il trattamento delle informazioni di intestazione (che potrebbero comprendere anche dati sul contenuto dei pacchetti) deve essere considerato alla stregua dei dati sul traffico ai sensi dell'articolo 6 della direttiva 97/66/CE e, pertanto, deve essere reso anonimo o cancellato non appena questi dati non sono più necessari per mantenere la comunicazione; in altri termini, non appena l'utente Internet accede al sito web.

Non vi sono dubbi sul fatto che dati quali quelli della sessione di login (ora di login e logout, quantità di dati trasferiti, tempo di avvio e fine della sessione, ecc.) debbano rientrare nell'ambito di applicazione dell'articolo 6.

L'elenco dei siti web visitati da un utente Internet (comportamento di navigazione) deve, in qualsiasi caso, essere considerato alla stregua dei dati sul traffico (ed, eventualmente, avere la stessa protezione del contenuto). Soprattutto, questo elenco, in linea di principio, deve essere cancellato al *termine della sessione di Internet*.

E' interessante notare che un resoconto delle attività di navigazione dell'utente viene conservato nel suo PC. Ciò può costituire un problema nel momento in cui lo stesso computer viene utilizzato da più persone.

In passato, il Gruppo di lavoro ha espresso la propria opinione sul tema della conservazione dei dati sul traffico da parte dei *fornitori di servizi Internet* a fini giudiziari[103]. Questa raccomandazione afferma che, in linea di principio, i dati sul traffico che non sono necessari per la fatturazione non dovrebbero essere considerati. Nel caso dei *fornitori di servizi Internet* gratuiti, non vi sarebbe alcuna necessità di conservare i dati sul traffico, poiché non necessari ai fini della fatturazione, per un periodo di tempo superiore di quanto non sia necessario per le normali operazioni.

La direttiva modificata sostituisce la frase "al termine della chiamata" con " al termine della trasmissione", che rende tutto molto più chiaro. Il comportamento di navigazione, pertanto, deve essere cancellato non appena termina la connessione Internet.

Il nuovo testo introduce la possibilità di trattamento successivo ai fini della fornitura di servizi a valore aggiunto o della commercializzazione dei propri servizi di comunicazione elettronica, sempre che l'abbonato abbia dato il suo consenso. Tuttavia, il

[103] Raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari, adottata il 7 settembre 1999, 5085/99/IT/def., WP 25

termine "servizio a valore aggiunto" non è definito nella proposta; il Gruppo di lavoro ritiene sia necessario chiarire cosa includere nella definizione al fine di garantire la limitazione della finalità e limitare nuovi rischi per la vita privata. Allo stesso modo, il Gruppo di lavoro raccomanda l'inclusione di una "prova di necessità" riguardante la possibilità di trattare i dati sul traffico a fini di commercializzazione propria da parte del fornitore[104].

Articolo 8: Identificazione della linea chiamante e collegata

Su Internet, non esistono linee chiamanti da identificare o meno. Non esiste un canale di instradamento distinto attraverso il quale è possibile determinare l'identità del chiamante prima che venga stabilita la connessione.

Su Internet, l'indirizzo IP non può essere separato dalla comunicazione (i pacchetti) e pertanto il concetto di *identificazione della linea chiamante* non è direttamente applicabile.

Dal punto di vista tecnico, non è possibile fornire servizi di telecomunicazione correlati ad Internet senza trasmettere e utilizzare l'indirizzo IP usato dall'utente Internet durante una sessione.

Si può pertanto concludere che l'articolo 8 della direttiva sulle telecomunicazioni non è applicabile agli indirizzi IP allo stesso modo dei numeri telefonici.

La proposta di direttiva modificata del 12 luglio 2000 segue questa linea di pensiero. L'enunciato dell'articolo resta praticamente invariato e fa riferimento alle "chiamate", un concetto che, nel nuovo testo, è riservato ai servizi telefonici.

V. Misure intese al miglioramento della vita privata

La tutela della vita privata durante la navigazione web può essere resa efficace in diversi modi. Di seguito sono illustrati alcuni metodi per migliorare la tutela della vita privata dell'utente[105].

In primo luogo, molti metodi di reperimento di dati personali si basano sull'uso dei *cookie*. Il browser software usato dall'utente Internet consente di rifiutare il deposito di *cookie* sul proprio disco fisso, caso per caso o sistematicamente. Occorre notare, tuttavia, che un numero crescente di siti web offre un servizio completo solo se la funzione dei *cookie* è abilitata.

Il 20 luglio 2000, Microsoft ha annunciato l'introduzione di una 'beta security patch' per la prossima versione di Internet Explorer che consente di migliorare la gestione dei *cookie*[106]. La versione sperimentale della patch sarà disponibile al pubblico entro la fine di agosto. Secondo le prime informazioni, la patch offrirà varie funzioni per consentire agli utenti di controllare i *cookie* in modo più efficace. Il browser riuscirà a differenziare tra cookie diretti (first-party) ed indiretti (third-party); l'impostazione predefinita segnalerà all'utente quando viene depositato un *cookie* indiretto. I *cookie* indiretti persistenti sono molto usati dalle società pubblicitarie, come DoubleClick o Engage, per tracciare le attività degli utenti di computer. Inoltre, la nuova funzionalità permetterà agli utenti Internet di cancellare tutti i *cookie* con un solo clic e consentirà un migliore accesso alle informazioni sulla sicurezza e sulla vita privata.

[104] V. il parere 7/2000 del Gruppo di lavoro, adottato il 2 novembre 2000, WP 36.
[105] Per maggiori particolari, v. il capitolo 9 relativo alle misure intese al miglioramento della vita privata.
[106] EPIC Alert 7.14, 27 luglio 2000.

Tuttavia, la security patch non aumenta il controllo del consumatore sull'uso, peraltro prevalente sui siti commerciali, dei *cookie* diretti.

Le caratteristiche di gestione dei *cookie* ricalcano quelle di altre recenti security patch prodotte da Microsoft per risolvere i problemi legati alle fughe di dati. Nel mese di maggio 2000, la società ha prodotto una patch per il famoso programma Outlook in grado di disattivare i *cookie* nei messaggi di posta elettronica. Tuttavia, è biasimevole che questa tecnologia non consenta ancora al sito da cui origina il *cookie* di indicare immediatamente la relativa finalità di utilizzo.

In secondo luogo, il fornitore di servizi Internet può contribuire significativamente alla tutela della vita privata dell'utente Internet limitando i dati personali memorizzati al minimo necessario per stabilire la comunicazione e assicurare le prestazioni tecniche. In particolare, in molti casi, il fornitore di servizi Internet può nascondere il numero IP di un utente Internet da una pagina web riferendo a quel sito da uno speciale proxy server. In tal caso, viene trasmesso solo il numero IP mascherato allocato dal proxy server, mentre l'indirizzo dell'utente Internet rimane presso il *fornitore di servizi Internet*. Tuttavia, questi servizi vengono offerti raramente su base standard.

In terzo luogo, per alcuni siti *portale* è possibile agire da *fiduciari* che tutelano i dati personali dell'utente. Tali 'infomediari' possono fungere da vigilanti fornendo ai siti web solo i dati personali che rispettano la vita privata dell'utente Internet o possono 'barattare' i dati personali sottoposti in cambio di determinati benefici, con la piena conoscenza e il consenso da parte dell'utente Internet[107]. Tuttavia, quest'ultima opzione deve essere considerata con cautela.

Il metodo più rigoroso è la scelta da parte dell'utente Internet di servizi che tengono nascosto intenzionalmente l'indirizzo IP al sito web visitato. Sono disponibili alcuni siti web 'anonimizzanti' e i corrispondenti prodotti software dedicati per nascondere l'indirizzo IP dell'utente Internet ridirezionano la comunicazione attraverso server dedicati che sostituiscono l'indirizzo IP con un altro.

Ovviamente, l'esistenza di nuovi programmi E.T. di sorveglianza solleva nuove questioni circa le eventuali modalità di tutela dai programmi in questione. Un eventuale metodo di protezione[108], anche se non facilmente praticabile, sarebbe quello di suddividere fisicamente i dischi fissi dei computer in settori pubblici e privati, in modo che le operazioni di scaricamento non influiscano sulle informazioni che si vogliono mantenere riservate. Quando si scaricano le applicazioni da Internet o dalla posta elettronica, si consiglia comunque la massima cautela.

VI. Conclusioni

- E' necessario fornire agli utenti che navigano o effettuano ricerche in rete l'accesso anonimo a Internet. Pertanto, si consiglia vivamente l'uso dei *proxy* server.
- L'uso crescente del software di sorveglianza è una tendenza di cui tenere conto e a cui prestare l'attenzione necessaria poiché può avere gravi ripercussioni sulla vita privata degli utenti Internet.

[107] Per maggiori particolari, v. il libro "Net Worth" (op cit.).
[108] Come suggerito da Cheswick, ricercatore responsabile presso Lucent technologies, nell'articolo di COHEN, A. in Time Magazine (op cit.).

- Alcuni dei concetti e delle definizioni usati nel testo attuale della direttiva sulle telecomunicazioni non sono facili da applicare nel contesto dei servizi correlati a Internet.

  - La separazione tradizionale tra contenuti e dati sul traffico non può essere applicata agevolmente alle attività Internet, in particolare nel contesto della navigazione. Da un lato, il concetto di dati sul traffico deve essere interpretato in modo più ampio ad includere i dati di intestazione, nonché tutti i dati di login. Dall'altro, ai dati sul comportamento di navigazione deve essere garantito lo stesso livello di protezione dei dati sul contenuto.

  - Nel contesto di Internet necessitano di essere riviste anche le disposizioni relative all'*identificazione della linea chiamante.*

- La revisione di questa direttiva ha migliorato notevolmente il primo di questi punti, ampliando l'ambito di applicazione dell'articolo 5 ad includere non solo il contenuto della comunicazione ma anche i dati sul traffico correlati, garantendo in tal modo una protezione uguale ad entrambi. Il Gruppo di lavoro si compiace di tale miglioramento. Anche il secondo problema è stato risolto chiarendo il fatto che tale disposizione si applica solo alle chiamate telefoniche e non a Internet.

  La revisione della direttiva ne ha accresciuto notevolmente la chiarezza, adeguando la terminologia al contesto più ampio di oggi, facilitando in tal modo l'interpretazione delle disposizioni esistenti. Tuttavia, il Gruppo di lavoro desidera sottolineare che il concetto di "servizi a valore aggiunto" necessita di essere specificato ulteriormente al fine di escluderne un'interpretazione troppo ampia.

CAPITOLO 6: PUBBLICAZIONI E FORUM

I. Introduzione

Le pubblicazioni e i forum disponibili in Internet hanno una caratteristica in comune in quanto essi rendono disponibili al pubblico dati personali con (ad esempio, forum di discussione pubblici) o senza (ad esempio, elenchi) il coinvolgimento della persona interessata. I motivi della pubblicazione di dati personali variano in base al contesto. L'utente Internet può divulgare alcune informazioni poiché gli viene chiesto di farlo per poter accedere, ad esempio, ad una chat room oppure le informazioni possono essere pubblicate da terzi, come un'amministrazione pubblica, per motivi amministrativi.
La questione fondamentale derivante da tale diffusione di informazioni è l'applicazione delle disposizioni sulla vita privata ai dati offerti al pubblico sul web. Contrariamente ad un'opinione molto diffusa, la protezione che discende dalla legislazione sulla protezione dei dati si applica anche ai dati offerti al pubblico. Questo capitolo dedicherà un'attenzione particolare alle motivazioni e alla necessità di ogni pubblicazione di dati personali, alla finalità della pubblicazione e ai rischi di uso improprio di tali dati.

II. Descrizione tecnica

Forum di discussione pubblici

Gli aspetti tecnici del trattamento dei dati nell'ambito dei forum di discussione pubblici variano in base alla natura del forum. E' possibile distinguere tra due tipi di forum: gruppi di discussione e chat room.

Gruppi di discussione

I gruppi di discussione sono forum classificati per argomento, in cui tutti i dati inviati dagli utenti vengono memorizzati per un periodo di tempo fisso, al fine di agevolare i contributi o le risposte degli utenti ad un argomento specifico.

Una domanda o un articolo comprende un "titolo" e un "corpo del testo". Il collegamento tra un articolo e la relativa risposta è detto "filo".

I messaggi vengono trasferiti ai server dei gruppi di discussione mediante *protocolli* specifici. Il tipico *protocollo* di trattamento per le notizie è l'NNTP (News Network Transfer Protocol), ma alcuni gruppi di discussione usano anche il *protocollo* HTTP. L'NNTP elabora le connessioni permanenti tra i server dei gruppi di discussione e aggiorna i messaggi automaticamente. I messaggi vengono conservati da un server del gruppo di discussione su un disco fisso e possono essere consultati da tutte le persone connesse. Le notizie vengono presentate in formato HTML.

Ogni server confronta con gli altri il proprio elenco di articoli in ogni gruppo di discussione e scambia con essi gli articoli nuovi. Tali raffronti comportano milioni di scambi di dati su Internet.

Visto il numero dei gruppi, gli utenti memorizzano solo un elenco selezionato di essi e il software di consultazione presenta solo i titoli delle notizie, lasciando scegliere agli utenti interessati se scaricare o meno il testo degli articoli.

Chat room

Vi sono tre tipi principali di chat room: Internet Relay Chat (IRC), Webpage (*Java*) Chat, e ICQ (I seek you) Chat.

1. IRC è il supporto di chat originario di Internet. Esso utilizza un protocollo che consente agli utenti di comunicare pubblicamente, in tempo reale, all'interno di un forum con un numero indefinito di persone, oppure privatamente con un solo interlocutore. Le chat room si basano sugli argomenti discussi, come i gruppi di discussione, ma differiscono da essi in quanto i canali vengono cancellati al termine di una discussione.

A causa dei ritardi nella trasmissione delle informazioni sull'IRC principale, sono state create reti indipendenti. Le reti principali sono EfNet, UnderNet e DalNet.

2. Webpage Chat consente di dialogare senza un programma distinto: l'unico strumento necessario è un recente web browser Internet. Vi sono due tipi di Webpage Chat: quella dedicata, disponibile sulla maggior parte dei portali web di ricerca e quella istituita da un singolo sulla propria homepage. La Wepage Chat, pur essendo facile da usare, dispone di capacità limitate: a differenza dell'IRC, è possibile solo scambiare testo e non è possibile modificare i colori o inviare suoni, oppure inviare o ricevere file, eseguire script o personalizzare l'interfaccia di chat.

3. ICQ è uno strumento che informa l'utente su chi è in linea in qualsiasi momento, quando persone predefinite (contenute in un elenco di contatti personali) si connettono e consente di contattarli, chiacchierare e inviare messaggi, pur continuando a navigare in rete, sempre che tutti i partecipanti stiano utilizzano ICQ. Al programma può essere comunicato di impostare l'utente come invisibile, assente o non disponibile.

Pubblicazioni ed elenchi

Su Internet, sono generalmente disponibili pubblicazioni ed elenchi sotto forma di basi di dati, che offrono criteri di ricerca al fine di ottenere informazioni su una o più persone.

La fonte di informazione per gli elenchi telefonici è, tradizionalmente, l'elenco nazionale ufficiale pubblicato, a seconda del paese, dall'operatore di telecomunicazioni principale o da una società ad hoc incaricata della relativa compilazione sulla base dell'elenco degli abbonati alla rete telefonica.

Gli elenchi di posta elettronica vengono compilati con vari mezzi, dall'iscrizione volontaria degli utenti Internet in un elenco presentato da un *fornitore di servizi Internet* alla raccolta incontrollata degli indirizzi di posta elettronica nei siti web, come i gruppi di discussione.

Altri tipi di pubblicazioni, come gli elenchi forniti dagli organismi pubblici, vengono compilati per argomento. Essi possono includere, ad esempio, la giurisprudenza di un paese, con le date delle sentenze, i tribunali, le località, forse persino i nomi delle parti, il giudice e un estratto della causa.

La maggior parte delle basi di dati prevedono vari criteri di ricerca che consentono l'accesso personalizzato alle informazioni e risultati strutturati in vari modi. In un elenco telefonico, una ricerca potrebbe iniziare da un nome o un numero di telefono, nella base di dati della giurisprudenza, il criterio potrebbe essere la data di una sentenza, il nome di una parte, ecc.

III. Rischi per la vita privata

Forum di discussione pubblici

Il rischio principale per la vita privata[109] deriva dall'accessibilità dei dati personali divulgati dall'utente Internet. L'accessibilità dei dati può tradursi in una raccolta e utilizzazione successive per finalità non sempre chiaramente previste dalla persona che partecipa al forum pubblico. Né la persona è sempre a conoscenza dei particolari solitamente pubblicati insieme al contenuto del contributo apportato al forum.

Nel caso dei gruppi di discussione, ad esempio, l'indirizzo di posta elettronica del partecipante viene solitamente pubblicato insieme al nome o allo pseudonimo della persona che invia il messaggio[110]. Alcuni forum di discussione visualizzano l'indirizzo IP del computer di un partecipante, nonché il relativo pseudonimo. Alcuni *fornitori di servizi Internet* prevedono la possibilità di partecipare a un forum senza essere identificati dagli altri partecipanti ma anche, per contro, la possibilità di partecipare ma di consentire agli altri partecipanti di leggere un profilo specifico elaborato dalla persona interessata.

Le informazioni personali disponibili on-line variano da un forum all'altro. Una regola generale è che, per poter accedere a una chat room, viene compilato un elenco di identificazione particolareggiato su richiesta del *fornitore di servizi Internet*, che solitamente comprende l'indirizzo di posta elettronica, la data di nascita, il paese, il sesso e, talvolta, talune preferenze della persona.

Da un punto di vista tecnico, la fornitura di tali informazioni particolareggiate non è, tuttavia, necessaria per il regolare funzionamento del gruppo di discussione o della chat room, ai sensi dell'articolo 6 della direttiva 95/46/CE.

Inoltre, queste informazioni di registrazione potrebbero comportare l'utilizzo successivo dei dati da parte del *fornitore di servizi Internet* ed essere combinate con altri particolari sulla persona rilevati on-line nelle chat room.

Due delle finalità principali di utilizzo dei dati rilevati e/o pubblicati sono:

1. controllare la natura della trasmissione di contenuti per garantire che non vengano resi disponibili contenuti inadeguati e/o per stabilire la responsabilità nel caso in cui tali contenuti dovessero risultare illeciti[111]. A tale scopo, per mantenere identificabile il contenuto, vengono spesso conservate le tracce dei dati in occasione di ogni contributo effettuato, senza preselezione, anche se basterebbero l'indirizzo di posta elettronica ed, eventualmente, il nome del partecipante;

2. la compilazione di elenchi di dati personali. I dati personali possono essere rilevati sul web mediante un software in grado di effettuare ricerche in rete e raccogliere tutti i dati disponibili di una determinata persona. Il Gruppo di lavoro, nella sua raccomandazione 3/97[112], ha riportato la citazione di un articolo di giornale che ha

[109] L'autorità spagnola per la protezione dei dati (Agencia de Proteccion de Datos) si è occupata di questo tema nel documento "Recomendaciones a los usuarios de Internet" (raccomandazioni agli utenti Internet), disponibile in lingua spagnola e inglese nel relativo sito Internet: www.agenciaprotecciondatos.org

[110] L'indirizzo di posta elettronica è spesso costituito dal nome dell'utente Internet, nella prima parte, specialmente quando l'indirizzo viene definito automaticamente da un fornitore di accesso Internet mediante il nome registrato dell'utente. Il più delle volte, tuttavia, l'utente può modificare il contenuto di quella parte dell'indirizzo e, ad esempio, usare uno pseudonimo. E' possibile, inoltre, richiedere un secondo indirizzo per il quale il fornitore di accesso Internet consentirà all'utente di scegliere il nome.

[111] Forse per evitare che la responsabilità ricada sul fornitore di servizi responsabile dei forum.

[112] Raccomandazione 3/97 relativa all'anonimato su Internet, adottata dal Gruppo di lavoro il 3 dicembre 1997.

spiegato *come si poteva compilare una biografia dettagliata di una persona scelta a caso, utilizzando tale software e sfruttando le informazioni provenienti da tutti i gruppi di discussione a cui la persona ha partecipato,* tra cui, ad esempio, l'indirizzo, il numero di telefono, il luogo di nascita, il posto di lavoro, i luoghi di vacanza preferiti e altri interessi personali. Questi dati possono essere rilevati e successivamente trattati per finalità diverse, quali il marketing diretto, ma anche la solvibilità o la vendita di dati a società di assicurazione o datori di lavoro. Alcuni siti Internet offrono già al pubblico strumenti di ricerca che consentono di reperire tutti i messaggi inviati da una persona ai gruppi di discussione in base al relativo nome o indirizzo di posta elettronica[113].

Pubblicazioni ed elenchi

La disponibilità in linea di informazioni personali rilevate dai registri pubblici o da altre fonti disponibili al pubblico, come gli elenchi, solleva questioni simili a quelle illustrate in precedenza. Esse riguardano l'eventuale uso successivo dei dati personali a livello internazionale per una finalità diversa da quella per cui essi sono stati inizialmente resi pubblici[114].

Come già puntualizzato in precedenza, l'automazione dei dati e la possibilità di eseguire ricerche a testo integrale consentono un numero illimitato di modi di richiedere e ordinare le informazioni, mentre la diffusione di Internet aumenta il rischio di raccolta per finalità improprie. L'automazione, inoltre, ha facilitato di gran lunga la possibilità di combinare dati disponibili al pubblico provenienti da varie fonti in modo da ottenere un profilo delle condizioni o dei comportamenti delle persone. Inoltre, dovrà essere rivolta particolare attenzione al fatto che rendere disponibili i dati personali al pubblico serve ad alimentare le nuove tecniche di *data warehousing (accaparramento di dati)* e *datamining (estrazione di dati)*[115]. Usando queste tecniche, i dati possono essere rilevati senza specificare in anticipo la finalità, e le varie finalità vengono definite solo al momento dell'uso effettivo[116].

Per illustrare questo motivo di preoccupazione, possono essere citati vari casi specifici:

- mentre le basi di dati della giurisprudenza contengono atti giuridici pubblici, la relativa pubblicazione in forma elettronica su Internet, che fornisce ampi criteri di ricerca sulle cause di tribunale, potrebbe condurre alla creazione di file di informazioni sulle persone, come nel caso in cui le basi di dati venissero consultate per ottenere un elenco delle sentenze di tribunale relative ad una determinata persona e non per avere informazioni sulla giurisprudenza.

---

[113] V., ad esempio, il sito Internet di Deja: "http://www.deja.com/home_ps.shtml?", che fornisce uno "strumento di ricerca potente" che offre vari criteri di ricerca, tra cui l'autore dei messaggi di un gruppo di discussione. Il sito dichiara di possedere la base di dati più completa di messaggi di gruppi di discussione sul web.

[114] V. sull'argomento il contributo di Marcel PINET, membro della CNIL, alla Conferenza internazionale dei commissari per la protezione dei dati tenutasi nel mese di settembre 1998 a Santiago de Compostela, Spagna, disponibile su www.cnil.fr, in Internet-Initiatives.

[115] *Data mining* e *data warehousing* comportano il vaglio di tonnellate di dati per scoprire modelli e relazioni in essi contenuti, ad esempio, l'attività commerciale e la storia di un'organizzazione; si ritiene che l'accaparramento dei dati contribuisca ai processi decisionali. Il trattamento della grande quantità di informazioni viene effettuato con l'ausilio di software in grado di agevolare il collegamento tra informazioni correlate presenti nella base di dati. V. la relazione della Registratiekamer (BORKING, J., ARTZ, M. e VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen 10, settembre 1998, disponibile su www.registratiekamer.nl

[116] Parere 3/99 sull'informazione nel settore pubblico e la protezione dei dati personali, adottato dal Gruppo di lavoro il 3 maggio 1999.

- Informazioni specifiche su una persona possono essere ottenute anche combinando i dati inseriti in basi di dati elettroniche distinte. In questo modo, si potrebbero ottenere i nomi delle persone che non hanno diritto al voto confrontando i registri anagrafici con quelli elettorali.

- Gli elenchi degli indirizzi su Internet prevedono di solito criteri di ricerca di persone non solo per nome ma anche per indirizzo e numero di telefono. Le persone che danno il proprio consenso alla pubblicazione dei propri indirizzi nell'elenco telefonico "cartaceo" non prevedono la possibilità che vengano effettuate tali ricerche derivate.

La disponibilità di dati in forma elettronica significa che essi possono essere usati per finalità diverse: ad esempio, per il marketing diretto, selezionando le categorie di persone che vivono nella stessa zona (forse per la vendita di sistemi di allarme nelle zone residenziali), o l'identificazione e il rilevamento di una persona che telefona ad un'azienda per una semplice e, a suo parere, anonima richiesta di informazioni.

Le pubblicazioni su Internet possono condurre ad altre forme di rilevamento di informazioni personali, finalizzate non solo ai dati personali contenuti in una chat room, in un registro pubblico o in un elenco, ma anche alle informazioni dirette fornite in una pagina web personale. L'indicizzazione automatica di queste pagine mediante robot di ricerca può condurre alla compilazione di file contenenti informazioni personali ricavate dalle pagine in questione e all'eventuale commercializzazione e *spamming* del relativo autore o dei partecipanti.

IV. Analisi giuridica

Forum pubblici

E' prevista l'imposizione di obblighi ai *fornitori di servizi Internet* al fine di limitare i rischi di raccolta illecita dei dati personali inviati alle chat room o ai gruppi di discussione.

La raccomandazione N. R (99) 5 del Consiglio d'Europa sulla tutela della vita privata su Internet[117] invita i *fornitori di servizi Internet* ad informare gli utenti sui rischi per la vita privata presenti nell'uso di Internet prima che essi sottoscrivano o inizino ad utilizzare i servizi. Tali rischi possono riguardare l'*integrità dei dati*, la riservatezza, la sicurezza della rete o altri rischi per la vita privata, come la raccolta o la registrazione nascoste dei dati.

Il modulo di registrazione che devono compilare le persone che desiderano accedere ad un forum pubblico deve essere conforme alle disposizioni di cui all'articolo 6 della direttiva 95/46/CE sul trattamento leale dei dati personali, il quale stabilisce che i dati devono essere rilevati per una finalità legittima, e devono essere pertinenti e non eccedenti rispetto a tale finalità.

Il carattere legittimo della finalità può essere determinato con riferimento all'articolo 7 della direttiva 95/46/CE, che prevede, in particolare, il consenso esplicito della persona interessata al trattamento dei propri dati personali, nonché l'equilibrio tra l'interesse legittimo del responsabile del trattamento e i diritti fondamentali dell'interessato (articolo 7 (a) e (f))

Gli utenti devono essere informati in modo chiaro e trasparente circa la finalità, la qualità dei dati rilevati e l'eventuale periodo di conservazione. Qualora all'utente non venga fornita alcuna indicazione chiara sulle condizioni di trattamento dei dati, l'assenza di

[117] Raccomandazione del Comitato dei ministri agli Stati membri adottata il 23 febbraio 1999. Disponibile su www.coe.int/dataprotection/

reazione non può essere considerata come un assenso implicito al trattamento successivo dei dati da parte del responsabile del trattamento (ad esempio, a fini di invio di materiale pubblicitario).

Occorre sottolineare il fatto che ai fornitori di servizi non serve necessariamente conoscere l'identità precisa dell'utente. Prima di approvare gli abbonamenti e connettere gli utenti a Internet, essi devono informarli sulla possibilità di accedere a Internet mantenendo l'anonimato o utilizzando uno pseudonimo, nonché di usare i servizi in forma anonima[118].

Questo principio è stato riconosciuto dal Gruppo di lavoro nella raccomandazione 3/97 relativa all'anonimato su Internet[119]. Mentre non vi è alcun dubbio circa la legittimità dell'anonimato in situazioni quali la condivisione di esperienze personali (vittime di violenze sessuali o persone che soffrono di dipendenza dall'alcol) o di opinioni politiche, il Gruppo di lavoro ha sottolineato il fatto che la necessità di anonimato su Internet va molto oltre questi casi specifici, *poiché i dati transazionali, identificabili per il solo fatto di esistere, possono costituire uno strumento attraverso il quale il comportamento di una persona può essere seguito e controllato in una misura che non è mai stata possibile prima.*

Il controllo dei gruppi di discussione e delle chat room per vietare contenuti impropri deve essere esercitato in conformità al principio della proporzionalità sancito dall'articolo 6 della direttiva 95/46/CE, laddove l'identificazione e la raccolta di tutti i dati personali inseriti in un forum pubblico sono considerati sproporzionati rispetto ad altri strumenti di controllo esistenti. Sono state proposte altre alternative, come soluzioni contrattuali che prevedono la "qualità del contenuto" o il coinvolgimento di un moderatore il cui compito sarebbe di sorvegliare i contributi e stabilire se i relativi contenuti sono illeciti e nocivi.

Oltre a questi principi fondamentali, va aggiunto che la conservazione dei dati sul traffico da parte dei *fornitori di servizi Internet* è disciplinata molto severamente, come nel caso degli operatori di telecomunicazioni. In generale, i dati sul traffico devono essere cancellati o resi anonimi al termine della comunicazione (articolo 6, paragrafo 1 della direttiva 97/66/CE). Gli operatori di telecomunicazioni e i *fornitori di servizi Internet* non hanno la facoltà di raccogliere e memorizzare dati esclusivamente a fini giudiziari, se non in virtù di una legge basata su motivazioni e condizioni specifiche[120].

Pubblicazioni ed elenchi

Il Gruppo di lavoro ha ribadito[121] il fatto che la legislazione europea sulla protezione dei dati si applica ai dati personali offerti al pubblico e che tali dati devono comunque essere protetti.

Il principio essenziale applicabile ai dati personali pubblici è il principio della finalità o della limitazione della finalità, in base al quale i dati personali vengono rilevati per finalità determinate, esplicite e legittime e non devono essere successivamente trattati in modo incompatibile con tali finalità (articolo 6(1)(b) della direttiva 95/46/CE).

Il Gruppo di lavoro, inoltre, ha sottolineato il fatto che i dati personali offerti al pubblico non costituiscono una categoria omogenea che può essere considerata in modo uniforme dal punto di vista della protezione dei dati: mentre può esistere l'accesso pubblico ai dati,

---

[118] S. LOUVEAUX, A. SALAÜN, Y. POULLET, *User protection in the cyberspace: some recommendations*, CRID, p. 12, disponibile su http://www.droit.fundp.ac.be/crid/.
[119] Raccomandazione adottata dal Gruppo di lavoro il 3 dicembre 1997.
[120] Raccomandazione 3/99 relativa alla conservazione dei dati sulle comunicazioni da parte dei *fornitori di servizi Internet* a fini giudiziari, adottata dal Gruppo di lavoro il 7 settembre 1999.
[121] Parere 3/99: v. sopra.

tale accesso può essere soggetto a determinate condizioni (come la prova dell'interesse legittimo) e a restrizioni alla successiva utilizzazione (come l'utilizzo a fini di invio di materiale pubblicitario).

La pubblicazione di dati personali su Internet potrebbe portare ad un trattamento successivo dei dati che il soggetto interessato potrebbe anche non prevedere. Gli articoli 10, 11 e 14 della direttiva 95/46/CE stabiliscono, a tale riguardo, che il soggetto interessato ha il diritto di essere informato circa l'uso dei propri dati personali. Il soggetto interessato, inoltre, deve essere informato del proprio diritto di opporsi, con mezzi semplici ed efficaci, al trattamento dei dati personali a fini di invio di materiale pubblicitario.

L'idea di uno "sportello unico" per opporsi al trattamento dei dati personali contenuti in un unico elenco potrebbe rappresentare una soluzione interessante alle difficoltà incontrate dalle persone nell'opporsi ad ogni trattamento, alla luce della relativa diffusione a livello nazionale e internazionale[122].

Se la finalità prevista del trattamento è incompatibile con la finalità originaria, l'equilibrio tra il diritto alla tutela della vita privata e gli interessi del responsabile del trattamento deve essere conseguito mediante l'imposizione al responsabile del trattamento di condizioni più severe. Quest'ultimo deve ottenere il consenso del soggetto interessato o essere in grado di invocare una norma giuridica o statutaria che giustifichi il trattamento.

Tuttavia, non risulta chiaro se il responsabile del trattamento è obbligato a rispettare il diritto di opposizione del soggetto interessato o ad ottenere il suo consenso per poter trattare i dati.

La disciplina in materia di elenchi Internet nei vari paesi è un esempio di tali approcci diversi. La questione è se è necessario il consenso prima che l'elenco venga reso disponibile in formato elettronico, quando esso presenta criteri di ricerca diversi da quelli originariamente previsti nell'elenco cartaceo.

Alcuni paesi (come Spagna e Belgio) ritengono che l'ampliamento dei criteri di ricerca potrebbe consentire il trattamento dei dati personali per finalità incompatibili con la finalità originaria e che, pertanto, il trattamento non dovrebbe essere consentito senza prima informarne la persona interessata e senza il suo esplicito consenso. In altri paesi (ad esempio, il Regno Unito), la conformità al diritto di opposizione previsto dalla direttiva sembra essere ritenuta sufficiente, in linea di principio, sebbene essa dipenda dalla presenza o meno di un obbligo giuridico a pubblicare le informazioni nell'elenco.

Queste interpretazioni dei testi giuridici comportano delle differenze nel livello di protezione nei paesi dell'UE e dei conflitti pratici quando, ad esempio, un elenco contenente i dati personali dei cittadini di un paese con un livello di protezione più elevato viene pubblicato in Internet da parte di un paese dotato di un livello di protezione inferiore.

Tali conflitti sono stati discussi a livello europeo ed un'interpretazione comune dei testi da parte del Gruppo di lavoro ha condotto ad una posizione ufficiale che raccomanda l'applicazione armonizzata del principio da parte degli Stati membri dell'UE[123].

---

[122] Ciò potrebbe rivelarsi particolarmente utile per quanto riguarda la diffusione degli elenchi su Internet. I reclami gestiti dalle autorità per la protezione dei dati riguardano spesso la pubblicazione di dati provenienti da un determinato paese quando la persona interessata è stata registrata in un elenco di opposizione solo nel proprio paese.

[123] Parere 5/2000 sull'uso degli elenchi pubblici per i servizi di ricerca derivata o a criteri multipli (elenchi derivati), WP 33, adottato il 13 luglio 2000.

L'articolo 12 della proposta di revisione della direttiva 97/66/EC[124] stabilisce che l'individuo ha la possibilità di decidere gratuitamente se i suoi dati debbano essere riportati negli elenchi pubblici, per quale finalità specificata e in quale misura. Ciò costituisce un passo positivo nella direzione giusta, che il Gruppo di lavoro ha pienamente appoggiato.

V. Misure intese al miglioramento della vita privata

Oltre alle disposizioni giuridiche citate in precedenza, vi sono alcune soluzioni tecniche che possono migliorare la protezione dei dati personali a vari livelli.

In generale, il Gruppo di lavoro sostiene che il browser software deve essere configurato, per default, in modo che venga trattata solo la quantità minima di informazioni necessarie per stabilire una connessione Internet[125].

Anonimato nei forum pubblici

Per quanto riguarda l'anonimato su Internet e nei forum pubblici in particolare, la nozione di "pseudoidentità" potrebbe offrire una soluzione alternativa alla questione dell'equilibrio tra il controllo legittimo degli abusi e la protezione dei dati personali. Tale identità verrebbe attribuita ad un individuo attraverso un fornitore di servizi specializzati. In linea di principio, l'anonimato verrebbe così rispettato anche se, in determinati casi, potrebbe essere ricostruito un collegamento con la vera identità dell'individuo da parte del fornitore di servizi specializzati, ad esempio in caso di sospetto di attività criminali. Per quanto riguarda la posta elettronica, i ritrasmettitori anonimi forniscono all'utente un indirizzo anonimo, a cui altre persone possono inviare i propri messaggi di posta, che vengono poi inoltrati al vero indirizzo dell'utente (a volte un server pseudonimo), oppure essi inviano o spediscono il messaggio del mittente senza indicarne il nome o l'indirizzo[126].

Indicizzazione sistematica dei dati

Esistono, inoltre, strumenti intesi a garantire che gli autori di pagine personali non siano soggetti all'indicizzazione delle proprie pagine e alla raccolta dei loro dati personali senza esserne a conoscenza. Lo scopo del *Robot exclusion protocol* (protocollo di esclusione dei robot) è impedire che tutte o alcune delle pagine di un sito web vengano indicizzate automaticamente da un motore di ricerca[127]. Questo protocollo viene identificato dalla maggior parte dei motori di ricerca sul web. Il file “robots.txt” inserito nell'indirizzo Internet contiene istruzioni destinate ai robot di ricerca, che indicano che alcuni robot non sono graditi o che solo alcune pagine identificate del sito possono essere lette e indicizzate.

Poiché solo un fornitore di servizi è in grado di inserire i cosiddetti "*protocolli* di esclusione dei robot" nell'indirizzo del sito, gli autori di pagine web personali ospitate da un fornitore di servizi, qualora non riescano a convincere il fornitore di servizi ad inserire tale protocollo, possono inserire un apposito *meta-tag* di robot in ogni pagina per evitarne

[124] Nella versione pubblica del 12 luglio 2000, COM(2000) 385.
[125] Raccomandazione 1/99 del **G**ruppo di lavoro sul trattamento invisibile e automatico dei dati personali su Internet effettuato da software e hardware, adottata il 23 febbraio 1999.
[126] Questi ritrasmettitori sono denominati Cypherpunk (per la prima generazione) o Mixmaster (per la seconda generazione che utilizza tecniche più avanzate). Server anonimi molto conosciuti sul web erano “anon.penet.fi” o “alpha.c2.org”. Pare, tuttavia, che entrambi abbiano chiuso. Un server nuovo è “Nym.alias.net”. Messaggi anonimi possono essere inviati anche attraverso un documento HTML. In tal caso, il messaggio e il destinatario finale vengono inviati al server WWW in forma non cifrata.
[127] Parere 3/99, v. sopra.

l'indicizzazione. Lo svantaggio dei *meta-tag* di robot è che essi non vengono ancora riconosciuti da tutti i motori di ricerca presenti su Internet.

Accesso on-line alle informazioni pubbliche

L'ultimo argomento trattato in questo capitolo riguarda l'accesso on-line alle informazioni pubbliche, il quale tuttavia è comunque soggetto alle norme sulla tutela della vita privata.

Le soluzioni tecniche applicate a tali basi di dati possono contribuire a limitare l'uso illecito delle informazioni in esse contenute:

- i criteri di ricerca devono essere definiti in modo che i dati possano essere utilizzati solo in conformità alla finalità originaria. Il Gruppo di lavoro ha ribadito, nella sua raccomandazione del 13 luglio 2000 sugli elenchi derivati, che "il responsabile del trattamento (…) deve attuare misure tecniche ed organizzative appropriate ai rischi che il trattamento comporta e alla natura dei dati tutelati (cfr. articolo 17 della direttiva 95/46/CE). Ciò significa, ad esempio, che il database dovrà essere progettato al fine di impedirne, per quanto possibile, usi fraudolenti quali modifiche illecite dei criteri di ricerca oppure la copia o l'accesso all'intero database per ulteriori elaborazioni. I criteri di ricerca, ad esempio, dovranno essere abbastanza precisi da consentire solo la visualizzazione di un numero limitato di risultati per pagina. Il risultato dovrà esser quello di garantire, anche senza mezzi tecnici, le finalità di ricerca alle quali l'abbonato ha dato il proprio consenso"[128]

- la consultazione on-line di basi di dati può essere limitata, ad esempio, restringendo il campo dell'interrogazione o i criteri di interrogazione. Deve essere possibile raccogliere una grande quantità di dati usando un'interrogazione ampia, come le prime lettere di un nome. Inoltre, si potrebbe rendere tecnicamente impossibile la richiesta di sentenze giudiziarie in base, ad esempio, al nome di una persona o la richiesta del nome di una persona in base al relativo numero telefonico.

A tale scopo, gli strumenti tecnici dovrebbero essere configurati e usati in base ai principi giuridici descritti in questo capitolo.

VI. Conclusioni

In teoria, le disposizioni giuridiche e gli strumenti tecnici disponibili offrono un livello notevole di protezione della persona interessata per quanto riguarda la disponibilità al pubblico di alcuni dei suoi dati personali su Internet. Il principio della finalità, in base al quale i dati personali non possono essere soggetti a trattamento per una finalità incompatibile con la finalità originariamente specificata, è di importanza fondamentale per quanto riguarda i dati resi pubblici in determinate circostanze.

Un'attenzione particolare deve esser rivolta, inoltre, al principio della limitazione del periodo di conservazione dei dati personali. Tali dati devono essere cancellati dopo un

[128] Il Gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni ha adottato una raccomandazione simile sugli elenchi derivati in occasione dell'incontro di Hong Kong il 15 aprile 1998: *if the reverse directories are not forbidden by law, they are services which require the express consent given voluntarily. At least the right to object and the right of access generally recognized by existing national and international rules on the protection of personal data shall be guaranteed; It is in any case necessary to endow the persons with the right to be informed by their provider of telephone or e-mail service, at the time of the collection of data concerning them, or if they have already subscribed , by a specific means of information, of the existence of services of reverse search and - if express consent is not required - of their right to object, free of charge, to such a search.* Il testo integrale di questa raccomandazione è disponibile su: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm

periodo ragionevole, per evitare l'elaborazione di profili che raccolgano, ad esempio, i messaggi inviati da una persona ad un gruppo di discussione nel corso degli anni.

Tali persone devono essere informate del tempo di conservazione previsto e della disponibilità on-line di tali dati pubblici.

Attualmente, i problemi riguardano principalmente la mancanza di informazione sia nei confronti delle persone interessate sia dei responsabili del trattamento circa le disposizioni giuridiche da osservare.

Per migliorare la situazione, l'obiettivo principale è di accelerare gli sforzi intesi a conseguire una maggiore trasparenza su Internet ed armonizzare l'interpretazione dei principi fondamentali concernenti il controllo dei dati della persona interessata.

La direttiva 97/66/CE, nella versione modificata del 12 luglio 2000, offre un'ottima opportunità di armonizzare alcuni di questi temi.

CAPITOLO 7: TRANSAZIONI ELETTRONICHE SU INTERNET

I. Introduzione

Il commercio elettrico può essere definito come "qualsiasi forma di transazione in cui gli attori interagiscono elettronicamente e non mediante scambi fisici o il contatto fisico diretto".[129] Questa definizione comprende le transazioni riguardanti l'acquisto di beni o servizi come pure quelle utilizzate per migliorare la qualità dei servizi, oppure la fornitura di nuovi servizi da parte di organizzazioni pubbliche o private.

Alla luce della definizione suddetta e in considerazione del fatto che la finalità principale del presente capitolo è studiare le tematiche correlate a Internet, esso si incentrerà sulle transazioni che avvengono su Internet, tralasciando qualsiasi altra forma di interazione effettuata mediante reti pubbliche o private.

Si prevede che l'impatto delle transazioni elettroniche sarà di portata internazionale, poiché il commercio elettronico è, per definizione, globale e consente ad ogni società (indipendentemente dalle dimensioni o dal fatturato) di offrire e vendere i propri prodotti in tutto il mondo.

Le transazioni elettroniche consentono alle organizzazioni di essere più efficienti e flessibili, di lavorare a più stretto contatto con i fornitori e di rispondere alle esigenze e alle aspettative dei propri clienti in base a modalità impossibili da immaginare in passato.

Tuttavia, per conseguire tali obiettivi è necessaria una grande quantità di informazioni e ciò potrebbe determinare l'invasione di settori fondamentali della vita privata delle persone.

II. Attori

I principali attori delle transazioni elettroniche sono:

- l'utente, nell'ambito della direttiva 95/46/CE, la persona fisica che desidera acquistare un prodotto o richiedere un servizio[130];
- l'operatore di telecomunicazioni, che non è direttamente coinvolto nelle transazioni di commercio elettronico ma svolge un ruolo chiave nell'inoltro dei segnali che rendono possibile qualsiasi forma di trasmissione elettronica. Questo attore ha obblighi di sicurezza specifici, che derivano dalle direttive;
- il *fornitore di servizi Internet*, che fornisce l'accesso a Internet;
- il commerciante elettronico, il soggetto che offre prodotti o servizi attraverso Internet;
- la piattaforma finanziaria, che è necessaria nella maggior parte dei casi e che coinvolge sia la banca del commerciante sia la banca del cliente, nonché un gateway di pagamento che si occupa degli aspetti tecnici necessari per autorizzare l'operazione finanziaria e il pagamento. Il gateway si occupa di tutte le connessioni tra gli istituti finanziari, per consentire lo scambio di denaro elettronico garantendo che tutti gli attori soddisfino ai requisiti necessari per effettuare la transazione.
    - *Terzi fiduciari*. Nei casi più complessi e sicuri, essi sono indispensabili per autenticare le parti e fornire una *cifratura* abbastanza efficace per garantire la riservatezza della transazione.

[129] Ufficio dei progetti della società dell'informazione, *Electronic Commerce - An Introduction* (http://www.ispo.cec.be/ecommerce/answers/introduction.html)

[130] Attualmente, la maggior parte delle transazioni elettroniche (circa il 90%) si svolge tra aziende, cioè tra persone giuridiche, che non rientrano nella direttiva 95/46/CE (v. articoli 2 (a) e 3(1)).

In base alle forme di commercio e agli attori od operatori interessati, possono essere identificati tre modelli diversi di transazioni elettroniche[131].

1) Fornitura on-line di beni e servizi immateriali. Utilizzata, per lo più, dalle case di software e dalle imprese di comunicazioni per le quali l'infrastruttura Internet è ottimale per la distribuzione e la vendita a distanza in tempo reale dei propri prodotti. Tali prodotti vanno dal software, i video film, i giochi e la musica on-line agli abbonamenti a bollettini on-line, riviste o programmi di sostegno tecnico.

In questo caso, oltre agli ovvi risparmi derivanti dall'accesso diretto ai clienti, che evitano in tal modo qualsiasi dipendenza da eventuali intermediari, vi è un altro grande vantaggio per le società dedite a questo tipo di commercio. Esse possono acquisire una conoscenza precisa e accurata del consumatore finale, dei suoi hobby, interessi e abitudini di acquisto.

Questa categoria comprende, inoltre, la maggior parte dei servizi offerti dalle organizzazioni del settore pubblico, come i pagamenti o i rimborsi on-line delle imposte dirette, le applicazioni elettroniche o le richieste di pagamenti integrativi e le azioni di follow-up.

2) Ordinazione elettronica di beni materiali. Questa categoria coinvolge molti tipi diversi di società. In primo luogo, le grandi imprese che utilizzano Internet per accedere direttamente al consumatore. I produttori o rivenditori di hardware TI sono stati i primi ad utilizzare questo canale commerciale, il che è facile da comprendere vista la natura dell'utente Internet. Attualmente, un numero crescente di imprese vende abbigliamento, profumi, libri, CD e biglietti aerei, ecc.

Internet offre inoltre la possibilità alla piccole e medie imprese di sviluppare nuove attività commerciali ad una portata che sarebbe impossibile utilizzando le loro risorse tradizionali. Infatti, come hanno notato alcuni osservatori, vi è una bella differenza tra l'investimento iniziale necessario per offrire al pubblico qualche centinaia di migliaia di CD musicali attraverso un negozio elettronico su Internet e tentare di fare lo stesso aprendo un negozio nel centro di una città.

Inoltre, tutti i siti di commercio elettronico che forniscono beni materiali dipendono, in ultima analisi, da un'organizzazione logistica per la consegna a domicilio degli articoli al consumatore. Attualmente, queste organizzazioni logistiche stanno investendo in tecnologie Internet al fine di sostenere gli ordini elettronici e la localizzazione delle spedizioni tra le società partner, e tra la società logistica e il consumatore finale, in modo che tutti i partecipanti possano sapere, in tempo reale, dove si trovano i beni ordinati e quando ne è previsto il recapito. In tale contesto, è sicuramente possibile che taluni distributori ed esperti logistici decideranno di fondersi, nel prossimo futuro, per sfruttare le informazioni chiave relative al processo di distribuzione detenute dalle società logistiche (prevalentemente gli indirizzi per il ritiro e la consegna).

3) Reti e centri commerciali. Il commercio on-line non esclude i distributori tradizionali privi di un'effettiva conoscenza delle nuove tecnologie. Essi hanno la possibilità di partecipare ai cosiddetti centri commerciali Internet, una struttura che consente loro di inserire i propri prodotti nella vetrina di un centro commerciale elettronico. Nei centri commerciali, i negozi sono classificati per categoria e i visitatori utilizzano un sistema di ricerca interno per reperire l'elenco dei siti che offrono il prodotto desiderato. I banner pubblicitari possono essere finalizzati in base alle parole chiave inserite o ai negozi

[131] La seguente classificazione è stata tratta dallo studio della Commissione delle Comunità europee *"On-line services and data protection and the protection of privacy"*, disponibile su http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf

visitati, e il centro commerciale Internet offre ai propri membri un'infrastruttura di pagamento sicura.

I centri commerciali Internet, in funzione del proprio ruolo, raccolgono spesso informazioni molto particolareggiate e accurate sui visitatori e gli acquirenti (negozi visitati, interessi, abitudini di acquisto, indirizzi, particolari personali e informazioni sui pagamenti), che possono rivelarsi molto utili per elaborare i profili dei clienti ai fini delle strategie pubblicitarie o di marketing[132].

Il ruolo di questi centri commerciali potrà cambiare in futuro con la relativa integrazione in siti più ampi, i cosiddetti *portali*, "supersiti" web che offrono una serie di servizi tra cui ricerche web, notiziari, elenchi di pagine bianche e gialle, posta elettronica gratuita, gruppi di discussione, shopping on-line e collegamenti con altri siti.

I portali moderni offrono opportunità di shopping sempre maggiori su scala internazionale, sia attraverso annunci pubblicitari classificati sia attraverso i motori di ricerca. E nulla impedirà a tali portali di offrire, nel prossimo futuro, le proprie piattaforme di pagamento sicuro ed agenti intelligenti per l'utente in grado di effettuare ricerche sul web, trattare i prezzi (tra cui, persino, le condizioni relative alla vita privata di un contratto commerciale)[133] e concludere contratti per conto del cliente.

III. Pagamenti sicuri

L'importanza crescente del commercio elettronico comporta la necessità, per la vendita di beni e servizi, di sistemi di pagamento. Le preoccupazioni circa i rischi di sicurezza relativi all'inserimento dei dati delle carte di credito in Internet e la possibilità di divulgazione a terzi non autorizzati di informazioni personali riservate sono due dei fattori che limitano l'espansione del commercio elettronico.

Per risolvere questi problemi sono stati elaborati, e sono tuttora allo studio, vari metodi. Attualmente, il più comune è il Secure Sockets Layer (SSL)[134], che è implementato nei browser più popolari e stabilisce una canale sicuro tra i computer del consumatore e del commerciante, mediante la *cifratura* e *i certificati digitali.*

La procedura fondamentale di funzionamento dell'SSL è la seguente. Prima che il computer del commerciante (server) possa stabilire una connessione sicura con il computer del consumatore (client), quest'ultimo deve avere la certezza di essere connesso con un server sicuro. Per verificare l'identità del server, viene utilizzato il relativo *certificato digitale*. Dopo che il server è stato autenticato, il client e il server possono cifrare i reciproci dati e garantirne l'*integrità*, come il numero della carta di credito utilizzata per la transazione e qualsiasi altro particolare personale.

---

[132] Le modalità di raccolta di queste informazioni sono spiegate in modo più particolareggiato nel capitolo 5 relativo alla navigazione e alla ricerca

[133] Parere 1/98: Piattaforma per le preferenze in materia di protezione della vita privata (P3P) e la norma aperta per i profili (OPS), adottato dal Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali il 16 giugno 1998 (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm). V. inoltre il libro di HAGEL III, J. e SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information*, Harvard Business School Press, 1999 e la relazione *Intelligent software agents and privacy*, di J. BORKING, B.M.A. VAN ECK e P. SIEPEL, Registratiekamer in collaborazione con l'Ontario Information and Privacy Commissioner, Achtergrondstudies and verkenningen, gennaio 1999, disponibile su www.registratieakamer.nl

[134] La descrizione completa del sistema SSL è disponibile su http://developer.netscape.com/tech/security/ssl/howitworks.html e http://home.netscape.com/eng/server/console/4.0/help/app_ssl.htm

Occorre notare che l'SSL non consente al cliente di avere il controllo sull'uso o il trattamento successivo dei propri dati personali da parte del commerciante e che l'*autenticazione* del client non è obbligatoria, rendendo così possibili le frodi attraverso l'uso improprio dell'identità di un'altra persona.

Per far fronte a tali problemi e fornire un quadro completamente affidabile per le transazioni di commercio elettronico, alcune società di carte di credito hanno elaborato, congiuntamente e con il sostegno dei principali sviluppatori di software, un nuovo protocollo. Il protocollo si chiama Secure Electronic Transactions (SET) e prevede trasmissioni riservate (mediante la *cifratura*), l'*autenticazione* delle parti (titolare della carta, ente emittente, commerciante, beneficiario e gateway di pagamento mediante certificati digitali), nonché l'*integrità* e l'impossibilità di revoca delle istruzioni di pagamento relative a beni e servizi (attraverso le *firme digitali*)[135].

Poiché il sistema suddetto non è particolarmente adatto quando è prevista una grande quantità di transazioni di esiguo valore, è in fase di sviluppo un metodo alternativo denominato denaro elettronico o e-cash. Il principio generale è scaricare denaro sul disco fisso di un computer (oppure, in futuro, sul chip di una carta intelligente). Ogniqualvolta viene eseguito un pagamento on-line, l'utente trasferisce unità di denaro (monete) dal computer o dalla carta intelligente al conto del commerciante o del fornitore di servizi. In questo settore, esistono molte tecnologie concorrenti. La più interessante, dal punto di vista della protezione delle informazioni personali, è rappresentata dai sistemi di pagamento completamente anonimi basati su un meccanismo di firme cieche[136]. Questi meccanismi potrebbero impedire il tracciamento delle transazioni, poiché la banca che "firma" il denaro elettronico non collega il consumatore ad una determinata transazione.

IV. Rischi per la vita privata

Indipendentemente dal tipo di transazione effettuata o dal sistema di pagamento usato, la differenza sostanziale tra il mondo fisico e quello elettronico è che, nel primo, vi è una serie di attività che possono rimanere anonime (come guardare le vetrine, entrare in vari negozi, esaminare prodotti diversi e, se si paga in contanti, effettuare acquisti), mentre nel secondo, tutto può essere registrato, aggiunto ad informazioni precedenti o appena acquisite, e trattato quasi senza costi al fine di produrre informazioni più complete su ogni persona. E tutto ciò può avvenire non solo senza il consenso del cittadino interessato, ma anche senza che egli ne sia a conoscenza. Inoltre, mediante le tecnologie

[135] Usando il protocollo SET durante una transazione, le parti coinvolte comunicano attraverso due paia di chiavi di cifratura simmetriche e uniche; le chiavi di cifratura pubbliche per la firma dei documenti relativi ad una transazione, cioè l'offerta di acquisto, e le chiavi private comprendenti una firma digitale per la transazione effettiva, cioè le istruzioni di pagamento, che garantiscono l'integrità della trasmissione e il fatto che l'ordine non verrà revocato. Esso funziona come una doppia firma: le due chiavi interagiscono in modo tale che un pagamento non può essere considerato valido a meno che l'offerta di acquisto non venga accettata dal commerciante, mentre l'ordine effettivo non viene onorato a meno che il pagamento non venga approvato dall'istituto finanziario. Il commerciante non conosce le istruzioni di pagamento mentre la banca non ha accesso ai contenuti dell'ordine. Per una descrizione particolareggiata del funzionamento del complesso protocollo SET, v. SET Secure Electronic Transaction Specification Book 1: Business Description disponibile su http://www.setco.org/download.html. V. inoltre GARFINKEL, S., *Web security and commerce*, Oreilly associates, giugno 1997, capitolo 12: Understanding SSL and TLS.

[136] Per una dissertazione teorica sulle modalità di funzionamento di questi sistemi, v. CHAUM, David "A Cryptographic Invention Known as a Blind Signature Permits Numbers to Serve as Electronic Cash or to Replace Conventional Identification. The Author Hopes It May Return Control of Personal Information to the Individual" http://www.eff.org/pub/Privacy/chaum_privacy_id_Article, apparso su *Scientific American*, agosto 1992

di *data warehouse* (*accaparramento di dati)* e *data mining (estrazione di dati)*[137] è possibile trattare una quantità enorme di informazioni, non solo per selezionare le persone che rispondono a determinati requisiti o criteri, ma anche per rivelare relazioni nascoste tra dati apparentemente non correlati, esplicitando in tal modo alcuni modelli comportamentali che potrebbero essere usati per adottare decisioni commerciali o amministrative in merito a determinati cittadini.

Nella maggior parte dei casi, quando una persona effettua un acquisto o sottoscrive un servizio, come un abbonamento, egli deve obbligatoriamente fornire i propri dati personali al commerciante o al fornitore di servizi per autenticare l'acquirente, fornire garanzie di pagamento o fornire un indirizzo fisico o elettronico per la consegna dei beni o dei servizi. Pertanto, a meno che il pagamento non venga effettuato con denaro elettronico o non si utilizzino tecnologie intese al miglioramento della vita privata per nascondere il proprio indirizzo IP e acquistare un bene immateriale, raramente l'anonimato rappresenta oggi una possibilità sul web.

Questo capitolo si concentrerà, pertanto, sui rischi associati all'uso non autorizzato di tipo secondario dei dati personali e su quelli correlati alla violazione della riservatezza o alla falsa identità.

1.Uno degli usi secondari più diffusi dei dati personali è la *pubblicità.* Dopo avere identificato la persona, mediante le informazioni fornite registrandosi nel server o altri dispositivi tecnologici come i *cookie*, le relative informazioni vengono usate per personalizzare annunci pubblicitari in funzione delle sue abitudini, interessi, *clickstream* o modelli di acquisto. E non solo annunci che si riferiscono al titolare del sito web dei servizi o delle offerte, ma anche quelli pubblicati da terzi che hanno concordato di sostenere i costi finanziari del funzionamento del server effettuandone la pubblicità.

I paradigmi della pubblicità Internet sono le tecniche usate dalle società pubblicitarie, come DoubleClick. Le attività di DoubleClick si propongono di fornire spazio pubblicitario in rete e di facilitare agli inserzionisti la scelta dello spazio che fornirà una base idonea per le attività di comunicazione. L'altro elemento chiave del successo di DoubleClick sono le tecnologie TI, che consentono di isolare i criteri di identificazione e offrire agli inserzionisti strumenti per comunicare con gli utenti in modo mirato. Questa tecnologia utilizza una base di dati contenente dati relativi a vari milioni di utenti Internet, garantendo in tal modo che vengano contattati, mediante le campagne pubblicitarie, solo gli utenti 'target' desiderati.

A tale scopo, DoubleClick raccoglie ed effettua il trattamento di dati personali che consentono di identificare gli utenti, descriverne le abitudini e determinare, in tempo reale, quegli elementi della popolazione che è probabile che soddisfino i criteri di finalizzazione delle campagne pubblicitarie in corso. DoubleClick assegna un numero di identificazione esclusivo ad ogni utente che visita uno dei siti web della rete DoubleClick e deposita un *cookie*, che verrà usato in seguito per identificare l'utente quando accederà ad un altro sito DoubleClick e, in base ai relativi dati, per personalizzare l'annuncio più adatto all'utente in questione. Anche se il visitatore non accetta il *cookie*, è comunque possibile elaborarne il profilo, in particolare se il suo indirizzo IP è di tipo statico.

[137] V. la relazione della Registratiekamer (BORKING, J., ARTZ, M. and VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen 10, settembre 1998, disponibile su www.registratiekamer.nl

I dati personali registrati nella base di dati di DoubleClick sono: la parte permanente dell'indirizzo IP, cioè l'indirizzo della rete, il dominio, il paese, lo stato federale (USA), il codice postale, il codice SIC (Standard Industrial Classification System, USA), le dimensioni e il fatturato della società (in via opzionale), il sistema operativo, la versione, il fornitore di servizi, il numero di identificazione (assegnato da DoubleClick), il riferimento alle attività di browsing (rilevamento e analisi dei siti visitati dall'utente)[138].

Il 23 novembre 1999, è avvenuta la fusione tra DoubleClick e Abacus Direct Corporation. Abacus, che è oggi una divisione di DoubleClick, continuerà a gestire Abacus Direct, la componente di posta diretta di Abacus Alliance. Inoltre, è stato annunciato che Abacus ha dato il via alla creazione di Abacus Online, la componente Internet di Abacus Alliance.
Secondo le informazioni riportate nel sito web di DoubleClick, la componente Abacus Online di Abacus Alliance consentirà ai consumatori statunitensi di Internet di ricevere messaggi pubblicitari personalizzati in base ai propri interessi individuali[139].
Per quanto riguarda la fusione suddetta, un cittadino californiano ha depositato una querela presso la Corte suprema dello Stato della California chiedendo di procedere contro DoubleClick a causa dell'esercizio su Internet di pratiche illecite, fuorvianti e ingannevoli che violano i diritti di riservatezza dell'opinione pubblica.

Nella querela si afferma inoltre che DoubleClick induce e ha indotto l'opinione pubblica *(...) ad una falsa idea di tutela della vita privata e di sicurezza riguardo all'uso di Internet, acquisendo in modo ingannevole, memorizzando e vendendo milioni delle informazioni più private e personali degli utenti Internet a scopo di lucro. (…) Quando un utente Internet visita un sito web pubblico, viene depositato sul suo computer un cookie identificato in modo esclusivo. In seguito, quando l'utente in questione visita un sito web che dispone di informazioni sull'identità dell'utente in questione (…), quest'ultimo viene collegata al cookie di identificazione. I convenuti, mediante l'uso della base di dati di Abacus , sono in grado di ottenere una quantità potenzialmente enorme di dati personali relativi all'utente. Vengono inoltre individuati e registrati le abitudini di acquisto, le risposte alla pubblicità e i siti web visitati dall'utente Internet*[140].

DoubleClick afferma che, in seguito alle reazioni dell'opinione pubblica relative al progetto di collegare la propria base di dati con quella di Abacus, sinora non sono stati ancora fatti passi concreti in questa direzione.

Un altro esempio di come i dati personali possono essere sottoposti a trattamento secondo modalità inaccettabili da parte dell'utente Internet comune è l'attività svolta da SurfAid, una piccola società che fa parte della divisione IBM Global Services di Somers (New York)[141]. Questa società riceve quotidianamente i logfile di accesso dei propri clienti e ne effettua il pretrattamento per scoprire il percorso seguito dai visitatori per raggiungere il sito web del client. Vengono quindi usati potenti strumenti di *datamining (estrazione di dati)* per esplorare il file del client, che in alcuni casi contiene oltre 150 milioni di voci, e produrre una relazione giornaliera accessibile al client. In seguito, i client possono usare i programmi *OLAP* per scomporre e analizzare le informazioni.

2. Un altro rischio in cui incorrono le persone durante le transazioni elettroniche è la violazione della riservatezza delle informazioni trasmesse. Poiché Internet è una rete

[138] Secondo quanto riportato nello studio *On-line services and data protection and privacy*, di GAUTHRONET, S. e NATHAN, F., pubblicato dalla Commissione della Comunità europea. Disponibile su http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf
[139] www.doubleclick.net:8080/privacy_policy/
[140] Harriet M. Judnick v.s. DoubleClick, Inc.
[141] WATTERSON, Karen, *La minería de datos ya es una tendencia dominante*; DATAMATION (edizione spagnola), febbraio 2000

pubblica aperta dotata di *protocolli* noti, incentrata più sulla condivisione di informazioni che sulla protezione della relativa riservatezza o sicurezza, non è molto difficile per chiunque sia in possesso di qualche conoscenza tecnica dotarsi di una serie di strumenti software per intercettare e divulgare i dati trasmessi su Internet. E' inoltre possibile assumere in mala fede l'identità di una società o un'istituzione per ottenere informazioni che potrebbero essere usate in seguito per commettere frodi o crimini.

3. E' in fase di sviluppo una nuova forma di commercio: il commercio elettronico mobile, che si basa sulla terza generazione di telefoni cellulari e altri dispositivi palmari in grado di accedere in modo sicuro alla posta elettronica e alle pagine web usando un protocollo nuovo[142]. Ne consegue che ai dati transazionali e di browsing potrebbero essere aggiunti i dati sull'ubicazione e sul traffico, nonché le abitudini di viaggio, al fine di elaborare un profilo ancora più accurato del consumatore. E, se si prendono in considerazione le fusioni e le concentrazioni tra le società di telecomunicazioni, i fornitori di servizi, i *portali* e le società di contenuti, la possibilità di aggregazione, integrazione e trattamento comune aumenta in modo esponenziale.

Un semplice esempio di ciò che potrà accadere in futuro è il fatto che, prevedibilmente, gli annunci pubblicitari seguiranno le persone ovunque attraverso i loro telefoni cellulari o gli assistenti digitali personali. "E' un tipo di finalizzazione basato sul posizionamento globale e non è poi così lontano," ha annunciato un portavoce di DoubleClick[143].
Un altro esempio è il progetto comune tra Yahoo! e CellPoint Systems AB inteso alla commercializzazione congiunta di un localizzatore persona-persona che utilizza i telefoni cellulari. Il sistema Yahoo! Find-A-Friend può essere utilizzato per ottenere informazioni come: "John si trova nei pressi di Picadilly Circus, a circa 3,2 km a nord-ovest da te", usando le risorse di rete dei telefoni cellulari GSM. Sebbene per partecipare a questo programma occorra il consenso, l'esempio indica le potenzialità delle nuove tecnologie delle telecomunicazioni, che consentono la localizzazione delle persone attraverso i dispositivi mobili[144].

V. Analisi giuridica

In primo luogo, occorre ricordare che, come spiegato nei particolari nel capitolo 3, le norme sulla protezione dei dati oggetto della direttiva 95/46/CE e della direttiva 97/66/CE si applicano a Internet e ai dati personali soggetti a trattamento nelle transazioni elettroniche[145]. I paragrafi che seguono si incentreranno sugli aspetti di questi testi giuridici che riguardano, in modo particolare, le transazioni elettroniche.

Legittimazione del trattamento dei dati: principio della finalità (articoli 5 - 7 della direttiva 95/46/CE)

Il primo aspetto da considerare è la raccolta e il trattamento leali e leciti dei dati, compresi i principi della finalità e proporzionalità. Nel contesto delle transazioni elettroniche, è importante considerare il fatto che i dati personali potrebbero essere rilevati in modo che la persona interessata non se ne accorga. Il Gruppo di lavoro ha dichiarato più volte la propria preoccupazione riguardo a tutti i tipi di trattamenti

[142] Wireless Application Protocol (WAP).
[143] Jane Weaver, MS NBC, 16/04/2000
[144] Per ulteriori informazioni, v. http://www.cellpt.com/v2/000504.htm
[145] Il trattamento dei dati personali su Internet. Documento di lavoro adottato dal Gruppo di lavoro sulla protezione delle persone con riguardo al trattamento dei dati personali il 23 febbraio 1999. (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm)

attualmente effettuati su Internet da software e hardware senza che la persona interessata ne sia a conoscenza e che sono pertanto "invisibili" alla persona in questione[146].
Quando vengono raccolti i dati personali di un utente Internet, la persona deve essere informata in modo chiaro sulla finalità del trattamento e sui destinatari o le categorie di destinatari di tali informazioni, in modo da poter decidere se effettuare o meno le transazioni alle condizioni suddette.

Inoltre, dovrebbero essere resi espliciti anche gli usi secondari dei dati personali e deve essere ottenuto il consenso qualora gli usi secondari non siano considerati compatibili con la finalità principale. Tra gli esempi di usi secondari incompatibili figurano la comunicazione di dati transazionali a terzi per consentire l'elaborazione di profili degli acquirenti ai fini delle proprie campagne pubblicitarie[147], oppure l'uso di strumenti di *datamining (estrazione di dati)* per estrarre modelli comportamentali dall'elenco dei nomi dei siti web visitati da un utente Internet.

Occorre notare, inoltre, che il consenso, da parte della persona interessata, al trattamento dei propri dati personali nel quadro di una transazione elettronica commerciale non è richiesto per la raccolta dei dati necessari allo svolgimento della transazione. Si tratta, di per sé, di un motivo legittimo di trattamento dei dati personali dell'utente necessario per tale finalità, secondo quanto stabilito nell'articolo 7(b) della direttiva. Qualsiasi altro dato correlato, tra cui i dati invisibili che non sono in alcun modo necessari per lo svolgimento della transazione, possono essere soggetti a trattamento solo sulla base degli altri motivi legittimi indicati nell'articolo 7 della direttiva, ad esempio il consenso inequivocabile, l'adempimento di un obbligo legale, l'interesse vitale della persona interessata o gli interessi legittimi dei responsabili del trattamento a condizione che non prevalgano i diritti e libertà fondamentali della persona interessata. Ciò vale anche per le transazioni di pubblica amministrazione, poiché la legittimità della raccolta e del trattamento dei dati personali da parte degli organismi pubblici si basa sulle norme giuridiche[148].

Un uso secondario, citato di frequente dai responsabili del trattamento dei siti web personali, è la manutenzione tecnica e il dimensionamento dell'apparecchiatura TI. Si tratta, ovviamente, di una preoccupazione legittima al fine di offrire un buon servizio ai clienti, ma che può essere risolta completamente utilizzando dati non identificabili, poiché per dimensionare i computer e le linee di telecomunicazione sono necessari solo dati aggregati. I responsabili del trattamento possono conservare i dati personali per motivi tecnici solo se ciò è strettamente necessario rispetto alla finalità e se una delle motivazioni legittime del trattamento dei dati è applicabile in questo caso.

Informazione della persona interessata (articolo 10 della direttiva 95/46/CE)

Il responsabile del trattamento, inoltre, deve fornire alla persona interessata informazioni chiare, tra cui l'identità del responsabile del trattamento, le finalità del trattamento, i destinatari dei dati, se rispondere alle domande è obbligatorio o volontario, nonché le eventuali conseguenze di una mancata risposta, e l'esistenza del diritto di accesso ai dati e di rettifica in merito ai dati che riguardano la persona interessata. La persona interessata deve essere informata del proprio diritto di opporsi al trattamento.

---

[146] Raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet effettuato da software e hardware, adottata dal Gruppo di lavoro sulla protezione delle persone con riguardo al trattamento dei dati personali il 23 febbraio 1999.
(http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm)

[147] Direttiva 95/46/CE, articolo 14 (b)

[148] V. il capitolo 6 per una dissertazione sul principio di specificazione della finalità applicato ai dati disponibili al pubblico.

Le informazioni devono essere fornite alla persona interessata direttamente sullo schermo da cui vengono raccolti i dati o attraverso un'apposita casella di dialogo, come spiegato nel capitolo 5.

Per i siti web è molto semplice fornire le informazioni alla persona interessata e accertarsi che quest'ultima abbia avuto almeno la possibilità di leggerle visualizzandole come componente obbligatoria del processo di transazione, prima di prendere qualsiasi decisione. Per essere completamente certi che le clausole visualizzate non siano state successivamente modificate, esse possono includere una firma elettronica creata con la chiave privata del commerciante. In questo modo, l'utente ha la prova delle condizioni che ha concordato. Tale idea sembra attuare l'articolo 10, paragrafo 3, della direttiva sul commercio elettronico che stabilisce che *le clausole e le condizioni generali del contratto proposte al destinatario devono essere messe a sua disposizione in un modo che gli permetta di memorizzarle e riprodurle*[149].

Conservazione dei dati personali e dei dati sul traffico (articolo 6 della direttiva 95/46/CE e articolo 6 della direttiva 97/66/CE)

L'articolo 6(1)(e) della direttiva sancisce l'obbligo di non conservare dati identificabili per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati.

Per quanto riguarda i dati sul traffico, devono essere osservate le severe restrizioni imposte dall'articolo 6 della direttiva 97/66/CE: i dati sul traffico devono essere cancellati o resi anonimi al termine della comunicazione (nella fattispecie, della transazione elettronica).

Il Gruppo di lavoro ha affrontato il tema specifico della conservazione dei dati sul traffico da parte dei *fornitori di servizi Internet* a fini giudiziari nella raccomandazione 3/99[150]. Questa raccomandazione sottolinea il fatto che, in linea di principio, i dati sul traffico non devono essere conservati esclusivamente a fini giudiziari e che le leggi nazionali devono costringere gli operatori delle telecomunicazioni, i servizi di telecomunicazione e i *fornitori di servizi Internet* a mantenere dati sul traffico per un periodo di tempo superiore a quello necessario ai fini di fatturazione[151].

Decisioni individuali automatizzate (articolo 15 della direttiva 95/46/CE)

Come citato in precedenza, i dati correlati alle transazioni non possono essere conservati a tempo indeterminato. Ciò vale, in particolar modo, quando si prevede di usare i dati nell'ambito di decisioni individuali automatizzate (come il rifiuto di una richiesta o il recesso da un acquisto) basate su dati precedentemente memorizzati.

In tal caso, devono essere fornite alla persona interessata garanzie adeguate[152]. Tra tali garanzie figurano il diritto per qualsiasi persona di non essere sottoposta ad una decisione che abbia effetti significativi nei suoi confronti e che sia fondata esclusivamente su un trattamento automatizzato dei dati che la riguardano.

---

[149] Direttiva 2000/31/CE dell'8 giugno 2000.

[150] V. http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

[151] V. inoltre a tale riguardo la dichiarazione ufficiale dei commissari europei per la protezione dei dati effettuata a Stoccolma secondo cui "*laddove, in casi specifici, i dati sul traffico devono essere conservati, vi deve essere una necessità dimostrabile, il periodo di conservazione deve essere il più breve possibile e la pratica deve essere chiaramente disciplinata dalla legge*".

[152] V. l'articolo 12(1)(a), paragrafo 3, della direttiva 95/49/CE.

Diritti della persona interessata (articolo 12 della direttiva 95/46/CE)

E' obbligatorio, inoltre, stabilire procedure chiare ed efficaci per consentire alla persona interessata di esercitare i propri diritti di accesso, rettifica, cancellazione o congelamento dei dati. Quando le persone interessate esercitano i propri diritti, il responsabile del trattamento deve fornire loro informazioni trasparenti sull'esistenza o meno di dati personali registrati negli archivi del responsabile del trattamento e, in tal caso, quali sono i dati soggetti al trattamento, la relativa fonte, le finalità del trattamento, le categorie di dati trattati e i destinatari o le categorie di destinatari cui sono comunicati i dati. Queste informazioni devono essere fornite in forma intelleggibile e, nell'ambito delle transazioni elettroniche, si raccomanda di fornire le informazioni attraverso la connessione in linea stabilita, a meno che la persona interessata non abbia richiesto di riceverle in un altro modo standard.

Una questione molto importante riguardante l'accesso ai dati correlati alle transazioni elettroniche, o rilevati attraverso di esse, è il diritto della persona interessata ad ottenere informazioni non solo sui dati fondamentali o primari, ma anche sulle informazioni derivate o consolidate. Ciò significa che, qualora sia stato effettuato qualsiasi tipo di elaborazione di profili, classificazione o suddivisione in categorie, ovvero se sono stati aggiunti dati ottenuti da terzi, devono essere comunicati all'interessato anche questi trattamenti, secondo quanto specificato nell'articolo 12(a) della direttiva.

Obblighi del responsabile del trattamento: riservatezza e sicurezza dei trattamenti (articoli 16 e 17 della direttiva 95/46/CE e 4 e 5 della direttiva 97/66/CE)

In tema di riservatezza e sicurezza, i responsabili del trattamento devono adottare misure appropriate per proteggere le informazioni fornite dai relativi clienti dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, come nel caso delle transazioni elettroniche su Internet. Tali misure devono tenere conto dei rischi per la sicurezza e la riservatezza, della natura dei dati e delle tecnologie d'avanguardia.

Diritto applicabile (articolo 4 della direttiva 95/46/CE)

Un'altra questione che solleva preoccupazioni in merito al commercio elettronico su Internet è il diritto applicabile al trattamento dei dati personali rilevati dai siti web fuori dall'UE/SEE. Ciò comporta una serie di problemi che richiedono di essere analizzati caso per caso. Tuttavia, tale analisi deve tenere conto del fatto che le disposizioni di cui alla direttiva 95/46/CE si applicano chiaramente ai trattamenti effettuati usando strumenti situati, interamente o in parte, nel territorio dell'UE anche quando i responsabili del trattamento sono stabiliti fuori dalla Comunità[153].

VI. Conclusioni

- Alla persona interessata devono essere fornite informazioni chiare e comprensibili in piena conformità al principio dell'informazione. Più specificamente, le informazioni sulla protezione dei dati, che sono strettamente correlate allo svolgimento della transazione elettronica, devono essere visualizzate, in via obbligatoria, nel corso della transazione elettronica in questione al fine di garantire che tali informazioni siano state comunicate alla persona interessata. Ciò deve risultare chiaro, indipendentemente dalle informazioni fornite ai visitatori di siti web che non effettuano acquisti. Come misura supplementare, deve essere messa a disposizione

[153] Per maggiori particolari, v. il capitolo 3.

della persona interessata una firma digitale delle condizioni di trattamento dei dati personali in modo che la persona in questione possa sincerarsi, successivamente, che le clausole non sono state modificate.

- Deve essere rispettato interamente il principio della proporzionalità. Devono essere raccolti solo i dati necessari alla transazione elettronica. Inoltre, il trattamento di qualsiasi dato (in particolare, effettuato in modo invisibile per la persona interessata) deve essere giustificato in base a uno dei motivi di legittimazione di cui all'articolo 7 della direttiva.
- Se la persona interessata decide di non fornire altri dati personali oltre a quelli necessari allo svolgimento della transazione, la persona in questione non deve essere soggetta a discriminazioni per quanto riguarda le condizioni della transazione.
- Non deve essere effettuato alcun trattamento secondario senza che la persona interessata ne sia a conoscenza. Alla persona interessata devono essere fornite, al momento dell'accesso, tutte le informazioni sulla logica riguardante tali trattamenti. Inoltre, per legittimare il trattamento, devono sussistere il consenso inequivocabile oppure altri criteri di legittimazione secondo quanto previsto dalla direttiva 95/46/CE.
- In virtù delle disposizioni giuridiche esistenti, devono essere utilizzate le tecnologie di *cifratura* per tutelare, il più possibile, la riservatezza delle transazioni elettroniche e per garantire l'*integrità* dei messaggi mediante una *firma elettronica*.
- Laddove necessario, al fine di salvaguardare le transazioni, potrebbe essere raccomandabile utilizzare la tecnologia dei *certificati digitali* e, in particolare, qualora sia necessario un livello di sicurezza più elevato, i *certificati digitali* potrebbero essere memorizzati su carte intelligenti.
- Dal punto di vista della protezione dei dati, la possibilità di usare metodi di pagamento sicuri e anonimi rappresenta un elemento chiave per la tutela della vita privata su Internet.
- La raccolta e il trattamento di dati personali mediante sistemi automatizzati o simili, ubicati nel territorio dell'UE/SEE, sono soggetti alle disposizioni della legislazione comunitaria sulla protezione dei dati.
- Per quanto riguarda i dati sul traffico, devono essere osservate le severe restrizioni imposte dall'articolo 6 della direttiva 97/66/CE e deve essere presa in considerazione la raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei *fornitori di servizi Internet* a fini giudiziari.

CAPITOLO 8: CYBERMARKETING

I. Introduzione

Internet non è solo una piattaforma di informazione di portata mondiale, ma anche un mercato internazionale in cui imprese concorrenti tentano di attrarre potenziali clienti. Il successo dipende dalla conquista del maggior numero possibile di clienti e, in particolare, di quelli realmente interessati al prodotto o al servizio offerto dall'impresa. A tale scopo, esse utilizzano profili e annunci pubblicitari mirati, basati sui predetti profili e presentati mediante la pubblicazione di banner nei siti web.
Un altro modo per raggiungere i clienti è l'invio di posta elettronica, e spesso il modo più efficace è l'inoltro, a più riprese, di grandi quantità di messaggi di posta elettronica non richiesti agli indirizzi di posta elettronica (cioè alle persone) reperiti negli spazi pubblici di Internet. Questo genere impopolare di invio di posta elettronica è denominato "spamming"[154].
In entrambi i casi, è necessario disporre dei dati personali dei clienti. Questi dati vengono spesso rilevati con facilità da Internet. Molti utenti Internet non sanno che, durante la navigazione, essi lasciano dietro di sé una grande quantità di dati che possono essere utilizzati per fare ipotesi sui loro settori di interesse, preferenze e comportamenti[155].

La pubblicità mirata può essere accettabile in una certa misura, quando è nell'interesse del cliente. Ma se l'utente non sa quali dati vengono rilevati e da chi, e per quale finalità essi saranno utilizzati, egli perderà il controllo dei propri dati personali. E' pertanto sbagliato rilevare questi dati senza il consenso dell'utente e persino senza che quest'ultimo ne sia a conoscenza.

II. Descrizione tecnica

Elaborazione di profili e pubblicità on-line[156]

L'elaborazione di profili on-line può essere effettuata in vari modi:
- Un sito web crea i profili rilevando i dati dei propri clienti dalle interazioni tra il sito web e il cliente. Ciò avviene mediante l'uso dei *cookie*, che seguono le mosse dell'utente sul web. In base alle modalità di configurazione del browser dell'utente, è possibile che egli sia a conoscenza del fatto che il sito web stia depositando un *cookie* sul suo disco fisso. Usando il profilo del cliente, il sito web offrirà al cliente prodotti (ad esempio, libri) o riferimenti ad altri siti web che possano interessarlo.
- Nel campo del "cybermarketing ad incentivi", le persone possono partecipare ad un gioco o a una gara se forniscono i propri dati personali per l'elaborazione di profili. In tal caso, la raccolta di dati avviene normalmente con la conoscenza della persona e ed è quindi soggetta alla sua autorizzazione[157].

---

[154] V. il capitolo 4: Posta elettronica, sezione V: Analisi di temi specifici, spam.
[155] V. il capitolo 5: Navigazione e ricerca, per maggiori particolari sui dati generati nel corso del processo di navigazione.
[156] In questo contesto è importante citare la posizione comune riguardante i profili on-line su Internet, adottata dal Gruppo di lavoro internazionale per la protezione dei dati nel settore delle telecomunicazioni in occasione del 27° incontro del Gruppo di lavoro tenutosi il 4-5 maggio a Rethymnon (Creta). Il testo di questa raccomandazione è disponibili su: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm
[157] Tuttavia, ciò riguarderà esclusivamente il caso in cui il sito web offra all'utente informazioni sufficienti riguardanti i dati trattati, la finalità del trattamento, l'identità del responsabile del trattamento, ecc. V. l'articolo 10 della direttiva.

- Le società pubblicitarie in rete (ad esempio, DoubleClick, Engage[158]) gestiscono e inviano *banner* pubblicitari[159] (in seguito denominati *banner*) su base contrattuale per conto di vari siti web. I *banner* vengono inseriti nel sito web richiesto mediante un *collegamento ipertestuale* invisibile con una società pubblicitaria.

  Per fornire al cliente il *banner* più "appropriato", le società pubblicitarie in rete elaborano dei profili usando una serie di *cookie* attraverso il *collegamento ipertestuale*. In base alla configurazione del browser, l'utente può essere a conoscenza del deposito del *cookie* e può dare o meno il proprio consenso. Il profilo del cliente viene collegato al numero di identificazione del *cookie* della società pubblicitaria in modo da poter essere ampliato ogniqualvolta il cliente visita un sito web che detiene un contratto con la società pubblicitaria.

I dati rilevati, dopo essere stati analizzati, possono essere integrati con dati demografici (età, genere, ecc.) e combinati con altri dati che caratterizzano il gruppo cui l'utente ovviamente appartiene in base al proprio comportamento on-line (ad esempio, interessi, comportamenti). Questo lavoro di analisi ed integrazione può essere effettuato da programmi speciali (in particolare, gli strumenti di *datamining*) disponibili sul mercato.
Il risultato di tali procedure è l'elaborazione di profili molto particolareggiati, che consentono all'impresa web o alla società pubblicitaria in rete di prevedere i gusti, le esigenze e le abitudini di acquisto di un consumatore e, in base a tali ipotesi, di fornire un *banner* che corrisponda il più possibile agli interessi del cliente.
Quando i dati rilevati, raccolti attraverso il numero di identificazione del *cookie* della società pubblicitaria, non vengono collegati con i dati identificabili[160] di una determinata persona, essi possono essere considerati anonimi. Ma spesso, ad esempio quando il cliente compila un modulo d'ordine sul sito web dove la società pubblicitaria ha inserito il proprio *banner*, i dati identificabili potrebbero essere collegati o combinati con i dati esistenti già inseriti in un *cookie*, e fornire un profilo identificabile della persona interessata[161].

Invio di posta elettronica

Per una campagna di posta commerciale, una società deve disporre di un elenco completo e appropriato di indirizzi di posta elettronica dei potenziali utenti. Come citato in precedenza, spesso è molto facile usare le risorse disponibili su Internet.
Vi sono tre modi diversi di rilevare gli indirizzi di posta elettronica da Internet[162]: la raccolta diretta presso i clienti o visitatori dei siti web, l'acquisto o il noleggio di elenchi forniti da terzi[163] e la raccolta presso gli spazi pubblici[164], come gli elenchi pubblici di

---

[158] Per maggiori particolari in merito alle tecniche utilizzate da tali società pubblicitarie, v.: *Rischi per la vita privata* nel capitolo 5, Navigazione e ricerca, e il capitolo 7, Transazioni elettroniche su Internet.
[159] I banner pubblicitari sono piccole caselle grafiche che compaiono sopra il contenuto del sito web o che sono integrate in esso.
[160] Occorre tenere presente che la definizione di dati identificabili di cui all'articolo 2 (a) della direttiva 95/46/CE è molto ampia: "si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".
[161] V. il capitolo 3: Applicazione della legislazione sulla protezione dei dati; sezione I, Considerazioni giuridiche di carattere generale: dati personali su Internet.
[162] V. il capitolo 4 sulla posta elettronica per maggiori particolari sulla raccolta di indirizzi di posta elettronica.
[163] Questi elenchi possono contenere anche indirizzi di posta elettronica rilevati presso gli spazi pubblici di Internet.

posta elettronica o le liste di indirizzi di posta elettronica, i gruppi di discussione o le chat room.

Su Internet, sono disponibili alcuni strumenti che agevolano la raccolta di indirizzi di posta elettronica. Questi programmi consentono di effettuare ricerche nei siti web o in parti della Usenet specificati in precedenza, mediante un elenco di URL o parole chiave correlate ad un campo di interesse predefinito (ad esempio, sport, viaggi) e quindi forniscono tutti gli indirizzi di posta elettronica reperiti nei siti/nelle pagine o nei forum.
Vi è una serie di servizi che fungono da intermediari nella raccolta degli indirizzi di posta elettronica e nella vendita o il noleggio di liste di indirizzi di posta elettronica a prezzi molto bassi.
Vi sono inoltre altri strumenti, specializzati nell'invio di messaggi di posta elettronica, che fungono da "fornitori di servizi di posta elettronica", cioè senza l'uso di un fornitore di servizi Internet o di altri fornitori che offrono servizi di posta elettronica. Questi programmi consentono, da un lato, di raggirare tutti i filtri per i messaggi di posta elettronica non richiesti (spamming), installati da quei fornitori e, dall'altro, garantiscono un funzionamento rapido e automatico. Il mittente, se lo desidera, può usare il servizio di host-spamming, anch'esso offerto a basso prezzo, che prevede che lo spamming venga effettuato da terzi.

III. Analisi giuridica

In materia di elaborazione di profili on-line e posta elettronica possono trovare applicazione varie direttive.

La direttiva sulla protezione dei dati

La direttiva generale stabilisce che i dati personali devono essere rilevati lealmente, per finalità determinate, esplicite e legittime, e trattati lealmente e lecitamente in conformità alle finalità dichiarate[165].
Il trattamento deve essere effettuato sulla base di motivazioni legittime, quali il consenso, l'esecuzione di un contratto, un obbligo legale o un equilibrio di interessi.[166] Inoltre, la persona deve essere informata della finalità del trattamento, ivi compresa la trasmissione dei dati a terzi prima che tale trasmissione venga effettuata[167], e deve avere il diritto di opporsi al trattamento dei propri dati personali a fini di invio di materiale pubblicitario[168].
La persona interessata, inoltre, deve avere il diritto di accedere ai dati che la riguardano e rettificarli, cancellarli o congelarli[169].

La direttiva sulle vendite a distanza

La direttiva sulle vendite a distanza[170] stabilisce che, come minimo, i consumatori devono avere il diritto di opporsi alle comunicazioni a distanza effettuate mediante la posta elettronica[171].

---

[164] V. il capitolo 6 sulle pubblicazioni e i forum.
[165] Direttiva 95/46/CE, articolo 6.
[166] Direttiva 95/46/CE, articolo 7.
[167] Direttiva 95/46/CE, articolo 10.
[168] Direttiva 95/46/CE, articolo 14.
[169] Direttiva 95/46/CE, articolo 12.
[170] Direttiva 97/7/CE del Parlamento europeo e del Consiglio del 20 maggio 1997 sulla protezione dei consumatori in materia di contratti a distanza
[171] Direttiva 97/7/CE, articolo 10.

La direttiva specifica sulla tutela della vita privata e le telecomunicazioni

La direttiva 97/66/CE offre la possibilità ai legislatori nazionali di attuare la possibilità di adesione o di recesso per quanto riguarda le comunicazioni commerciali non richieste[172]. I casi in cui vengono usati sistemi automatizzati di chiamata o telefax a fini di invio di materiale pubblicitario sono soggetti al preventivo consenso del consumatore[173]. La definizione di sistemi automatizzati di chiamata, che è molto ampia, potrebbe essere applicata agevolmente anche alla posta elettronica.

Nel mese di luglio 2000, la Commissione europea ha presentato una proposta relativa ad una nuova direttiva concernente il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, in sostituzione della direttiva 97/66/CE.
In questa proposta, l'articolo riguardante le comunicazioni commerciali non richieste comprende esplicitamente la posta elettronica, che è consentita solo nel caso in cui gli abbonati abbiano dato preventivamente il loro consenso.

La direttiva sul commercio elettronico

La direttiva sul commercio elettronico[174] stabilisce che le comunicazioni commerciali di posta elettronica devono essere identificabili some tali[175] e che devono essere consultati regolarmente e rispettati i registri in cui possono iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni[176].
Sebbene né la direttiva generale né quella sulle telecomunicazioni si riferiscano esplicitamente al commercio elettronico, esse devono essere applicate in questo settore: i considerando e l'articolo 1, paragrafo 5 b), della direttiva sul commercio elettronico chiariscono che questa direttiva non si propone in alcun modo di modificare i principi giuridici e le disposizioni oggetto del quadro normativo esistente. Ne segue che l'attuazione della direttiva sul commercio elettronico deve essere completamente in linea con i principi sulla protezione dei dati sanciti dalla legislazione pertinente. Pertanto, la legislazione nazionale sulla protezione dei dati continuerà ad applicarsi alle società responsabili del trattamento dei dati personali[177]. Inoltre, gli Stati membri possono attuare le norme che sono previste dalla direttiva sulle telecomunicazioni e che superano le disposizioni della direttiva sul commercio elettronico, cioè che le comunicazioni commerciali possono essere soggette al preventivo consenso da parte del destinatario[178].

IV. Conclusioni

Le norme stabilite dalla direttiva generale, la direttiva sul commercio elettronico, la direttiva sulle vendite a distanza e la direttiva sulle telecomunicazioni sono applicabili all'uso della posta elettronica a fini di 'cybermarkting'.

---

[172] Direttiva 97/66/CE, articolo 12 (2).
[173] Direttiva 97/66/CE, articolo 12 (1).
[174] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.
[175] Direttiva 2000/31/CE, articolo 7.
[176] Direttiva 2000/31/CE, articolo 7.
[177] Direttiva 95/46/CE, articolo 4.
[178] Direttiva 97/66/CE, articolo 12. Proposta di direttiva relativa al trattamento dei dati prsonali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, articolo 13 relativo alle comunicazioni commerciali indesiderate.

All'elaborazione di profili on-line si applica solo la direttiva generale. Sebbene l'elaborazione di profili on-line rientri nel commercio elettronico, tale argomento non viene trattato nella direttiva sul commercio elettronico. Inoltre, neppure la pubblicità in rete rientra nella direttiva modificata sulle telecomunicazioni in quanto i fornitori che effettuano questo servizio sono esclusi esplicitamente dall'ambito di applicazione di tale direttiva.
E' pertanto possibile concludere quanto segue:

Elaborazione di profili e pubblicità on-line[179]

- I fornitori di servizi Internet devono informare gli utenti sulla finalità del trattamento dei dati che li riguardano prima della raccolta[180]. Ciò comprende il tipo, l'ambito di applicazione e il periodo di memorizzazione, nonché le finalità del trattamento, ad esempio l'uso per l'elaborazione di profili[181]. Deve essere inoltre indicato espressamente se i dati verranno comunicati a terzi.
  Queste informazioni devono essere fornite anche nei casi in cui i dati vengano rilevati usando pseudonimi o numeri di identificazione non personalizzati. In particolare, gli utenti devono essere informati in anticipo del deposito di eventuali *cookie* per l'elaborazione di profili. Ciò deve avvenire mediante un'apposita casella (prompt) che viene attivata anche se il browser non notifica all'utente il deposito del *cookie*.
- Agli utenti, in qualsiasi momento e come minimo, deve essere riconosciuto il diritto di opporsi al trattamento dei dati che li riguardano[182]. Di conseguenza, i dati rilevati durante l'uso futuro di Internet non potranno essere usati per ampliare un profilo esistente. Ciò riguarda anche i casi in cui il trattamento è soggetto al preventivo consenso dell'utente.
- La personalizzazione dei profili deve essere soggetta al preventivo consenso informato delle persone interessate, le quali devono avere il diritto di revocare il proprio consenso in qualsiasi momento e con effetto futuro.
- Agli utenti deve essere data, in qualsiasi momento, la possibilità di accedere ai propri profili a fini di controllo. Essi devono inoltre avere il diritto di rettificare e cancellare i dati memorizzati[183].

Posta elettronica

- L'impresa che rileva un indirizzo di posta elettronica *direttamente presso l'utente* a fini di invio di posta elettronica da parte dell'impresa in questione o di terzi cui l'indirizzo di posta elettronica sarà comunicato, deve informare l'utente, mediante strumenti tecnici adeguati, di tali finalità al momento della raccolta[184].
- Poiché gli Stati membri possono scegliere tra l'attuazione della possibilità di adesione e quella di recesso, le imprese che inviano comunicazioni commerciali di posta elettronica devono garantire, mediante strumenti tecnici adeguati, che tali comunicazioni di posta elettronica siano identificabili da parte del destinatario[185].

[179] Queste conclusioni di basano sulla decisione formulata dalle autorità tedesche per la protezione dei dati riguardanti una specifica società pubblicitaria in rete. Anche il *Gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni* ha adottato una *posizione comune* che riflette tale decisione. V http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm
[180] Direttiva 95/46/CE, articolo 10.
[181] Direttiva 95/46/CE, articolo 6.
[182] Direttiva 95/46/CE, articolo 14.
[183] Direttiva 95/46/CE, articolo 12.
[184] Direttiva 95/46/CE, articolo 10.
[185] Direttiva 2000/31/CE, articolo 7.

- Poiché gli Stati membri possono scegliere tra l'attuazione della possibilità di adesione o di recesso, prima di inviare comunicazioni commerciali di posta elettronica, l'impresa deve consultare i registri negativi in cui possono iscriversi le personale fisiche che non desiderano ricevere tali comunicazioni commerciali. Tali registri devono essere rispettati in ogni caso[186]. Sarebbe molto utile l'esistenza di registri negativi internazionali.
- La raccolta di indirizzi di posta elettronica *presso gli spazi pubblici su Internet* e il relativo uso per l'invio di comunicazioni commerciali sono contrari alla legislazione comunitaria in materia, cioè alla direttiva generale[187]. In primo luogo, questa prassi costituisce un trattamento sleale dei dati personali[188]. In secondo luogo, essa è contraria al principio della finalità,[189] poiché le persone pubblicano il proprio indirizzo di posta elettronica per una finalità specifica, ad esempio, la partecipazione ad un gruppo di discussione, e tale finalità è molto diversa da quella dell'invio di comunicazioni commerciali per posta elettronica. In terzo luogo, non si può ritenere che essa superi la prova dell'equilibrio di interessi[190], alla luce del fatto che il mittente viene penalizzato in termini di tempo, costi e fastidio irragionevole.
- Cinque Stati membri (Germania, Austria, Italia, Finlandia e Danimarca) hanno adottato misure intese e vietare le comunicazioni commerciali non sollecitate. In altri Stati membri, esiste o un sistema di possibilità di recesso oppure la situazione non è del tutto chiara. Le società dei paesi in cui è prevista la possibilità di recesso possono finalizzare i propri indirizzi di posta elettronica non solo nel proprio paese ma anche verso i consumatori degli Stati membri dotati di un sistema che prevede la possibilità di adesione. Inoltre, poiché molto spesso gli indirizzi di posta elettronica non forniscono l'indicazione del paese di residenza dei destinatari, un sistema di regimi divergenti nel mercato interno non consente una soluzione comune per quanto riguarda la vita privata del consumatore. La possibilità di adesione è quindi una soluzione ben equilibrata ed efficace per eliminare gli ostacoli alla fornitura di comunicazioni commerciali pur proteggendo il diritto fondamentale dei consumatori alla vita privata. Il Gruppo di lavoro, pertanto, si compiace e sostiene la proposta di far fronte agli invii di posta elettronica indesiderati come per i sistemi automatizzati di chiamata e ai telefax. In tutte queste situazioni, l'abbonato non ha un'interfaccia umana e sostiene, interamente o in parte, i costi della comunicazione. Il grado di invasione nella vita privata e l'onere economico sono comparabili.[191]

[186] Direttiva 2000/31/CE, articolo 7.
[187] V. il *parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali* presentato dall'Internet Task Force (WP 28).
[188] Direttiva 95/46/CE, articolo 6 (1) (a).
[189] Direttiva 95/46/CE, articolo 6 (1) (b).
[190] Direttiva 95/46/CE, articolo 7 (f).
[191] V. il parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 COM (2000) 385, adottato il 2 novembre 2000, WP 36.

CAPITOLO 9: MISURE INTESE AL MIGLIORAMENTO DELLA VITA PRIVATA

I. Introduzione

La direttiva comunitaria sulla protezione dei dati contiene due principi che hanno conseguenze dirette per la progettazione e l'uso di nuove tecnologie:
- il principio della "finalità" o dello "scopo" prevede che i dati personali possono essere usati solo se necessario per una determinata finalità legittima; in altre parole, i dati personali non possono essere usati senza un motivo legittimo e la persona conserva l'anonimato (articolo 6(1) e 7).
- il principio della "sicurezza dei dati" prevede che i responsabili del trattamento attuino misure di sicurezza appropriate rispetto ai rischi per i dati personali presentati dalla memorizzazione o trasmissione, allo scopo di proteggere i dati personali dalla distruzione accidentale o illecita e dalla perdita accidentale, dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta la trasmissione di dati all'interno di una rete, nonché da qualsiasi altra forma illecita di trattamento (articolo 17).

Il suddetto principio della "finalità" o dello "scopo" è l'idea che soggiace al concetto di tecnologia intese al miglioramento della vita privata. Tale concetto si riferisce ad una serie di tecnologie che salvaguardano la vita privata, in particolare minimizzando o eliminando la raccolta o il trattamento successivo di dati identificabili [192].
Le tecnologie intese al miglioramento della vita privata mirano ad impedire qualsiasi forma illecita di trattamento, ad esempio rendendo tecnicamente impossibile l'accesso ai dati personali da parte di persone non autorizzate, in modo da evitarne l'eventuale distruzione, alterazione o diffusione.
L'attuazione pratica di tale concetto richiede soluzione organizzative e tecniche.

Queste tecnologie si basano spesso sull'uso di un protettore dell'identità[193]. Il protettore dell'identità può essere considerato un elemento del sistema che controlla il rilascio della vera identità della persona ai vari processi all'interno del sistema di informazione. Il suo compito è delimitare alcune zone del sistema, che richiedono l'accesso alla vera identità. Una delle funzioni più importanti del protettore dell'identità è convertire la vera identità di un utente in uno pseudonimo, un'identità alternativa (digitale) che l'utente può adottare utilizzando il sistema.
Possono essere usate varie tecniche per inserire un protettore di identità in un sistema di informazione, tra cui le tecniche di *cifratura* che prevedono le *firme digitali*, le firme cieche, gli pseudonimi digitali e i *terzi fiduciari*.

II. Tecnologie intese al miglioramento della vita privata

Questa sezione descrive e analizza una serie di tecnologie intese al miglioramento della vita privata[194].

---

[192] V. la relazione di HES, R. e BORKING, J. (editori), *Privacy-enhancing technologies: the path to anonymity (revised edition)*, Registratiekamer, in collaborazione con l'Ontario Information and Privacy Commissioner, Achtergrondstudies en Verkenningen 11, L'Aia, novembre 1998. Disponibile su www.registratiekamer.nl
[193] Per maggiori particolari, v. la relazione in materia della Registratiekamer (op cit.) - in particolare, la pagina 7 e seguenti .
[194] V. la guida on-line EPIC agli strumenti pratiche per la vita privata, disponibile su www.epic.org/privacy/tools.html

Cookie killer

Vengono analizzati in seguito due tipi di risposte alla risoluzione dei problemi per la vita privata derivanti dai cookie. La prima ha avuto origine dalla stessa industria Internet ed è stata inserita nei principali browser disponibili sul mercato. La seconda è pervenuta dai vari attivisti in materia di vita privata o dalle case di software. Essa consiste di strumenti che consentono di cancellare tutti i *cookie* o una parte di essi.

Il meccanismo di opposizione ai cookie usato dall'industria

L'unico tentativo visibile per risolvere il problema dei *cookie* è rappresentato dal meccanismo di opposizione ai *cookie* utilizzato nei comuni browser sin dalla versione 3. Un utente Internet informato può parametrare il browser scegliendo uno delle tre opzioni che seguono:

– accettare ogni *cookie*
– rifiutare *cookie* o *cookie* non rinviato al server di origine (Netscape)
– decidere caso per caso

I meccanismi di opposizione ai cookie restano insufficienti per i seguenti motivi:

1. Normalmente, l'impostazione predefinita è la più invasiva per la vita privata (l'accettazione di tutti i *cookie*) e l'utente Internet medio non sa che il *cookie* viene usato ampiamente, ad esempio dalle società di cybermarketing per tracciare le parole chiave inserite nei motori di ricerca usando strumenti di trattamento invisibili..
2. Il meccanismo di bloccaggio dei *cookie* inibisce il ricevimento di nuovi *cookie* ma non impedisce l'invio sistematico e invisibile dei *cookie* già ricevuti.
3. La natura dei *cookie* può essere molto diversa: alcuni sono utili e non hanno carattere identificativo (ad esempio, la lingua preferita). Altri sono di tipo identificativo ma possono essere usati in conformità alle disposizioni sulla vita privata. In generale, si può affermare che i *cookie* di sessione[195] sono molto meno invasivi per la vita privata di quelli persistenti. Il rifiuto di tutti i *cookie* potrebbe non essere nell'interesse dell'utente Internet.
4. Molti siti web rifiutano l'accesso agli utenti che non intendono accettare i *cookie*.
5. Molti siti web (o quelli collegati in modo ipertestuale invisibile) inviano serie di *cookie* e un approccio di tipo caso per caso obbligherà l'utente a rifiutarne uno dopo l'altro, causando il cosiddetto "affaticamento da mouse", che condurrà l'utente ad accettare il cookie una volta per tutte per non essere più disturbato.
6. In alcuni casi, la formulazione dell'avviso relativo al *cookie* [196] sembra incompleta e può essere fuorviante.
7. Quando si installa un nuovo browser, il primo sito da visitare (per default, il sito web del produttore del browser) può inviare un *cookie* prima che l'utente abbia la possibilità di disattivare la relativa funzione.

Nel mese di luglio 2000, Microsoft ha annunciato l'uscita di una 'beta security patch' per la prossima versione di Internet Explorer che consentirà di migliorare la gestione dei *cookie* web.[197] Secondo le prime informazioni, la patch offrirà varie funzioni per consentire agli utenti di controllare i *cookie* in modo più efficace. Il browser riuscirà a

[195] I cookie senza durata fissa non verranno memorizzati sul disco fisso ma solo nella memoria RAM.
[196] In MSIE 4.O UK, la formulazione dell'avviso relativo ai cookie è la seguente:" *Per consentire un'esperienza di browsing più personalizzata, consentite a questo sito web di depositare informazioni sul vostro computer? Cliccando Sì, il sito web salverà un file sul vostro computer. Cliccando No, è possibile che questa pagina web non venga visualizzata correttamente*." L'utente Internet deve poi cliccare su un pulsante per conoscere il dominio (e non il mittente!) dei cookie e la relativa durata.
[197] EPIC Alert 7.14, 27 luglio 2000.

differenziare tra cookie diretti (first-party) ed indiretti (third-party); l'impostazione predefinita segnalerà all'utente quando viene depositato un *cookie* indiretto. I *cookie* indiretti persistenti sono molto usati dalle società pubblicitarie, come DoubleClick o Engage, per tracciare le attività degli utenti di computer. Inoltre, la nuova funzionalità permetterà agli utenti Internet di cancellare tutti i *cookie* con un solo clic e consentirà un migliore accesso alle informazioni sulla sicurezza e sulla vita privata. Tuttavia, la security patch non aumenta il controllo del consumatore sull'uso, peraltro prevalente sui siti commerciali, dei *cookie* diretti.

Programmi indipendenti

Cookie washer, *cookie* cutter, *cookie* master o *cookie* cruncher sono solo alcuni dei programmi freeware o *shareware* che ogni utente Internet può scaricare e usare sulla rete[198]. Anche in questo caso, si possono fare osservazioni simili alle precedenti:

1. l'utente Internet deve trattare i propri *cookie* file quotidianamente e caso per caso, a causa della natura diversa dei vari *cookie*;
2. nel caso dei programmi *shareware*, talvolta l'utente Internet deve pagare per tutelarsi;
3. il meccanismo di gestione dei *cookie* non è sempre facile da usare o da comprendere da part di un utente Internet medio.

Proxy server

Un *proxy* server è un server intermedio tra l'utente Internet e la rete. Funge da *web cache*, migliorando sensibilmente il tasso di visualizzazione delle informazioni (ad esempio, la visualizzazione di pagine web). Molte grandi organizzazioni o fornitori di accesso Internet hanno già adottato questa soluzione. Le pagine, le immagini o i logo scaricati dall'esterno da parte di un membro di un'organizzazione vengono memorizzati in una memoria cache nel *proxy* e verranno messi immediatamente a disposizione anche degli altri membri dell'organizzazione.

In questo caso, non è necessario che ogni membro dell'organizzazione sia ubicato prima del proxy server per disporre di un proprio indirizzo IP, poiché non accede direttamente ad Internet. Inoltre, il *proxy* server non trasmetterà, di norma[199], l'indirizzo IP dell'utente Internet al sito web e potrà filtrare il browser chattering. Poiché i *proxy* server gestiscono il protocollo HTTP, essi possono eliminare, modificare o memorizzare con facilità i *cookie* memorizzati nell'intestazione HTTP.

Software anonimizzante

Il software anonimizzante consente agli utenti di interagire in modo anonimo durante la visita dei siti web, passando prima da un sito web anonimizzante che ne maschera l'identità[200].

Passando da un sito web anonimizzante prima di accedere a qualsiasi altro sito Internet, l'utente può consentire al sito web destinatario di trattenere i dati personali, come l'indirizzo IP dell'utente. I siti anonimizzanti impediscono, inoltre, l'invio ai siti web dei dati di sistema (come il sistema operativo e il browser utilizzati), il deposito di *cookie* nei browser e bloccano *Java* e *JavaScript*, che possono accedere ai dati personali contenuti nei browser.

---

[198] Alcuni di questi programmi sono disponibili su http://tucows.belgium.eu.net/cookie95.html .

[199] Purtroppo, alcuni proxy aggiungono all'intestazione HTTP l'indirizzo TCP/IP del PC per cui stanno lavorando.

[200] V. il libro " Net Worth" (op. cit), pag. 273 e seguenti.

Anonymiser[201] o Zero-Knowledge Systems[202] ne costituiscono due ottimi esempi.

Anonymiser sostiene di:

- fungere da intermediario tra l'utente e i siti visitati, mascherando l'identità dell'utente in questione da misure di tracciamento invasive
- bloccare i programmi Internet contenuti nella pagine web (*Java* e *JavaScript*) che possono danneggiare il computer dell'utente o che sono in grado di rilevare dati personali sensibili.

Anonymiser offre due servizi: la navigazione anonima e la posta elettronica anonima, e un prodotto, il server anonimizzante. Il server anonimizzante consente a chiunque di creare un proprio sito anonimizzante.

A volte, l'utente Internet deve pagare per poter sfruttare appieno i vantaggi dei servizi anonimi e deve sempre contattare il sito web di Anonymiser per usare i servizi anonimizzanti. Ciò significa che questo servizio rimane vulnerabile alla sorveglianza di terzi. Anonymiser è in grado di fornire servizi anonimi, come la navigazione, la posta o il trasferimento di file.

Dal punto di vista tecnico, Anonymiser fune da *proxy* server e nasconde il browser chattering HTTP nonché l'indirizzo IP del navigatore.

Il problema principale legato all'uso di questo servizio è che l'utente Internet deve affidarsi ad una determinata società la quale conoscerà tutte le attività svolte dall'utente sul web.

Zero-Knowledge Systems propone un software denominato "Freedom". Questa soluzione si basa su almeno tre relay TCP/IP combinati con una pesante *cifratura* (almeno 128 bit). Poiché il TCP/IP viene usato da tutti i servizi in rete, ogni servizio viene in tal modo cifrato e anonimizzato. Ognuna della tre stazioni intermedie TCP/IP conosce solo l'indirizzo TCP di quella precedente. Non tengono registri in modo che nemmeno due relay insieme sono in grado di tracciare le informazioni richieste o reperite. Naturalmente, l'instrdamento delle informazioni è dinamico e cambierà, probabilmente, anche durante una comunicazione molto breve. Sembra che Freedom integri anche un sistema di gestioe dei *cookie*.

Un altro esempio di questo tipo di servizi è offerto da **privada.com.** Questa società offre servizi che sostengono tutti i tipi di transazioni in rete, tra cui il browsing, la posta elettronica, l'invio di messaggi e, a breve, il commercio elettronico. L'infrastruttura di Privada si basa su un sistema di compartimentazione e cifratura.
L'utente riceve un CD-ROM o scarica un'applicazione client, PrivadaControl, dal proprio *fornitore di servizi Internet*. PrivadaControl comunica con i server della rete Privada che risiedono presso il fornitore di servizi Internet e funge da parete tagliafuoco (firewall) per la vita privata dell'utente. PrivadaControl mira a proteggere tutte le informazioni e i dati dal punto della transazione fino alla rete, garantendo la tutela della vita privata da parte di tutti gli attori, inclusi Privada e il *fornitore di servizi Internet*.
Usando PrivadaControl, l'utente crea un account digitale privato che rappresenta le sue attività on-line, dissociando completamente tutte le informazioni personali dall'utente dalle sue attività on-line. Sembra che PrivadaControl consenta all'utente di creare o cancellare identità digitali, scegliere tra di esse durante l'interazione on-line e impostare attributi e caratteristiche ad esse relativi.

[201] http://www.anonymizer.com/3.0/index.shtml
[202] http://www.zeroknowledge.com

Questo sistema non consente di bloccare tutti gli applet Java o i comandi Active-X ma permette all'utente di decidere il livello al quale possono funzionare la personalizzazione e i servizi web. I cookie vengono depositati sui server centralizzati della rete Privata e non sul personal computer dell'utente. Qualsiasi logfile o tentativo di datamining da parte di un sito web viene associato all'identità on-line dell'utente e non alla sua vera identità. Privada sostiene che gli utenti possono eliminare con facilità tutti i cookie depositati.

Il sistema proposto da **iPrivacy** viene presentato come un sistema in grado di permettere il commercio elettronico anonimo, dalla navigazione allo shopping e la spedizione. Esso consente al consumatore di navigare, effettuare ricerche in rete e fare acquisti on-line in modo anonimo senza rivelare l'identità del destinatario. Secondo la società, nemmeno loro conoscerebbero la vera identità dei consumatori che usano questi servizi. Per quanto riguarda la transazione, solo il consumatore e l'utente della carta di credito sarebbero a conoscenza delle informazioni personali per quanto riguarda l'acquisto effettuato on-line[203].

Filtri di posta elettronica e posta elettronica anonima[204]

Questi sistemi sono già stato descritti nel capitolo relativo alla posta elettronica. Ciò che segue è un riassunto delle caratteristiche principali.

- Il filtraggio della posta elettronica scherma la posta elettronica in arrivo dell'utente e lascia passare solo i messaggi di posta elettronica che l'utente ha indicato di voler ricevere. Questi sistemi vengono utilizzati ampiamento per filtrare gli spam.

- La posta elettronica anonima consente agli utenti di offrire il proprio indirizo di posta elettronica on-line senza dover rivelare la propria identità[205]. Su Internet, questo servizio è disponibile attualmente a titolo gratuito attraverso una serie di società che forniscono servizi di "ritrasmissione". Grazie a questi servizi, il ritrasmettitore elimina l'identità dell'utente dalla posta elettronica consegnata.

Infomediari

Una persona può decidere, inoltre, di avvalersi di un cosiddetto infomediario[206]. L'infomediario è una persona fidata o un'organizzazione abilitata web specializzata nei servizi di informazione e conoscenza relativi a, o per conto di, una comunità virtuale. L'infomediario agevola ed incentiva la comunicazione intelligente e l'interazione tra i membri della comunità virtuale. Esso amministra e coltiva un patrimonio di conoscenze proprietario costituito da contenuti e collegamenti ipertestuali di interesse specifico per la comunità. In conformità ai vincoli di riservatezza imposti dalla comunità virtuale, l'infomediario raccoglie, organizza e rilascia, selettivamente, informazioni sulla comunità e i relativi membri per soddisfare alle esigenze della comunità virtuale in questione…".

[203] http://www.iprivacy.com
[204] V. il libro " Net Worth" (op. cit), pag. 275 e seguenti.
[205] Questo documento fa riferimento a questo tipo di servizio anche nel capitolo 6 (Pubblicazioni e forum), nella sezione relativa alle misure intese al miglioramento della vita privata.
[206] http://www.fourthwavegroup.com/Publicx/1635w.htm

L'infomediario è un nuovo tipo di intermediario commerciale che aiutare i clienti a catturare, gestire e massimizzare il valore dei propri dati personali[207]. I consumatori hanno mostrato di essere disposti a fornire i propri dati personali se essi possono trarne dei vantaggi, ma essi riconoscono, in misura crescente, di vendere la propria vita privata a poco prezzo a società che utilizzano i loro dati per promuovere i propri interessi. La remunerazione sulle informazioni che essi diffondono è, in parole povere, insoddisfacente[208].

Gli infodmediari possono aiutare i client a fare ottimi affari con i venditori, aggregando le loro informazioni con quelle di altri client e usando il loro potere di mercato combinato per contrattare con i venditori per loro conto. Essi fungono da custodi, agenti e intermediari delle informazioni dei client, la commercializzazione presso le imprese (e ne consentono l'accesso) per conto del client tutelando, al contempo, i relativi dati personali da eventuali abusi.

L'aspetto positivo di un infomediario è che, in molti casi, esso può acquistare i beni o i servizi desiderati e fornirli al consumatore finale, conservandone l'anonimato. La società di infomediazione può inoltre fornire agenti intelligenti per aiutare gli abbonati a svolgere i propri compiti.

I client degli infomediari avranno teoricamente la possibilità di rimanere anonimi per sempre, navigando sul web e facendo acquisti on-line. Tuttavia, essi saranno incoraggiati a non farlo poiché riceveranno un piccolo compenso dai venditori ogniqualvolta decideranno di diffondere la propria identità o il proprio indirizzo di posta elettronica. Tale compenso potrà assumere la forma di un pagamento in denaro o uno sconto sul prezzo del prodotto venduto.

I client riceveranno inoltre pagamenti in contati a fronte della fornitura ai venditori selezionati dell'accesso ai loro profili. L'importo del pagamento in contati dipenderà dalle preferenze dei singoli client per quanto riguarda la vita privata. I client che scelgono di rimanere completamente anonimi rinunceranno ai pagamenti in contanti in cambio di garanzie relative alla loro vita privata. I client che sono tranquilli dei controlli imposti dall'infomediario sull'accesso alle loro informazioni e che capiscono il valore della diffusione selettiva al venditore possono generare pagamenti in contanti per se stessi.

In conclusione, si può affermare che sebbene gli infomediari possano svolgere un ruolo positivo per quanto riguarda la tutela dei dati personali degli utenti con cui essi intrattengono un rapporto di fiducia, la base di questa attività sta nella possibilità di guadagno derivante dalla diffusione o dall'accesso ai dati personali del cliente.

A seconda delle circostanze e della natura dell'infomediario, ciò può rappresentare sia un miglioramento sia un'invasione della vita privata.

III. Altre misure intese al miglioramento della vita privata

Per migliorare la trasparenza del trattamento o facilitare l'esercizio dei diritti delle persone interessate, possono essere utilizzate anche altre tecniche, tra cui:

[207] Uno degli studi più completi relativi a questo nuovo organismo è il libro"Net Worth: the emerging role of the infomediary in the race for customer information"; HAGEL III, J. e SINGER, M., Harvard Business School Press.
[208] HAGEL III, J. e SINGER, M, op. cit.

P3P

P3P significa Platform for Privacy Preferences (Piattaforma per le preferenze in materia di protezione della vita privata)[209]. L'obiettivo della P3P è consentire ai siti web di esprimere le proprie preferenze in materia di vita privata e agli utenti di esercitare le proprie preferenze rispetto a tali prassi, in modo che essi possano prendere decisioni informate sulle proprie esperienze web e controllare l'uso delle proprie informazioni. L'intera comunità della protezione dei dati ha seguito lo sviluppo della P3P con grande interesse.

Nel mese di aprile 1998, il Gruppo di lavoro internazionale per la protezione dei dati nel settore delle telecomunicazioni ha emanato una posizione comune sugli elementi essenziali delle tecnologie intese al miglioramento della vita privata (ad esempio, la P3P) sul World Wide Web[210]. Il documento stabilisce le condizioni essenziali che qualsiasi piattaforma tecnica deve rispettare con riguardo alla tutela della vita privata sul World Wide Web, con l'obiettivo di evitare la raccolta sistematica di dati personali:

1. La tecnologia non può, di per sé, salvaguardare la vita privata sul web. Essa deve esse applicata in base a un quadro normativo.
2. Qualsiasi utente deve avere la possibilità di navigare nel web in modo anonimo. Ciò si applica anche allo scaricamento delle informazioni di dominio pubblico.
3. Prima che i dati personali, in particolare quelli diffusi dall'utente, vengano trattati dal fornitore di un sito web, deve essere ottenuto il consenso informato dell'utente. Inoltre, nella configurazione predefiniti della piattaforma tecnica devono essere inserire talune norme basilari inderogabili.

Due mesi più tardi, nel mese di giugno 1998, anche il Gruppo di lavoro ha emanato un parere[211]. Il parere sottolineava il fatto che una piattaforma tecnica per la protezione della vita privata non sarà di per sé sufficiente a garantire tale protezione sul web. Occorre che essa sia applicata in un quadro di regole esecutive sulla tutela dei dati, in grado di fornire a tutti un livello minimo e non negoziabile di protezione della vita privata. Il parere citava inoltre una serie di questioni specifiche che sarebbero state sollevate dall'attuazione di un tale sistema nell'Unione europea.

Per esaminare l'applicazione della piattaforma P3P nell'ambito della direttiva europea sulla protezione dei dati e promuovere la comunicazione tra la comunità dell'UE sulla protezione dei dati e gli sviluppatori di software, è stato organizzato un seminario nel mese di settembre 1999, a cui hanno partecipato una delegazione di alto livello del World Wide Web Consortium e i membri dell'Internet Task Force. Il seminario ha evidenziato che un buona numero di questioni deve ancora essere affrontato.

Una volta risolte tali questioni, la piattaforma P3P potrà svolgere un ruolo positivo se applicato nell'ambito di un contesto adeguato. I principali aspetti positivo della piattaforma P3P sono i seguenti[212]:

---

[209] L'ultimo progetto di lavoro del protocollo P3P è disponibile sul sito web W3C: http://www.w3.org/TR/1999/WD-P3P

[210] Questo testo è disponibile su: http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm

[211] Parere 1/98 sulla piattaforma per le preferenze in materia di protezione della vita privata (P3P) e la norma aperta per i profili (OPS), adottato il 16 giugno 1998, WP 11, XV D/5032/98.

[212] V. l'articolo di CAVOUKIAN, A. e GURSKI, M. (Information and Privacy Commissioner Ontario) e MULLIGAN, D. e SCHWARTZ, A. (Center for Democracy Technology), *P3P and privacy: an update for the Privacy Community*, disponibile su: wysiwyg://16/http://www.cdt.org/privacy/pet/p3pprivacy.

- la piattaforma P3P può contribuire alla standardizzazione delle clausole sulla vita privata. Tale fatto, se attuato, pur non offrendo di per sé alcuna protezione per la vita privata, potrebbe promuovere notevolmente la trasparenza ed essere utilizzato per sostenere gli sforzi intesi a migliorare la tutela della vita privata.
- La piattaforma P3P può sostenere la crescita delle scelte relative alla vita privata, come l'anonimato e gli pseudonimi.

Occorre tuttavia tenere conto dei limiti[213] della piattaforma P3P:

- la piattaforma P3P non può proteggere la vita privata degli utenti in paesi dotati di una legislazione insufficiente sulla vita privata: non ha la capacità di creare una clausola pubblica o di richiedere che le proprie specifiche vengano rispettate sul mercato;
- la piattaforma P3P non può garantire che le società rispettino le clausole relative alla vita privata. Infatti, la piattaforma P3P non può garantire che il sito si comporti come esso stesso sostiene. Le sanzioni per il mancato rispetto di una dichiarazione di intento possono essere stabilite solo per legge o attraverso l'adesione ad un ente di autoregolamentazione.

La certificazione relativa alla vita privata

La certificazione consiste in un marchio di qualità apposto da un sito web. Negli anni, sono apparse vari sistemi di certificazione relativi alla vita privata, tra cui TRUSTe[214], Privaseek[215], Better Business Bureau[216] e WebTrust[217]. Queste organizzazioni americane mirano ad operare a livello internazionale, anche in Europa, come già accade per alcune di esse. Contemporaneamente, vengono intraprese iniziative con finalità internazionali anche a livello europeo, come L@belsite in Francia.

La certificazione relativa alla vita privata viene concessa alle società che rispondono ad una serie di requisiti specificati dall'ente di certificazione. Questo ente può esercitare una qualche forma di controllo sulla conformità alle clausole di riservatezza pubblicate dalle società titolari della certificazione, svolgendo controlli periodici sulle attività di tali aziende. In alcuni casi, l'ente di certificazione si occupa anche dei reclami presentati dalle persone interessate nei confronti delle società che riportano tale certificazione nei propri siti web.

La certificazione della vita privata solleva una serie di questioni:

1. la prima riguarda il contenuto della certificazione. Il diritto di informazione, accesso, il principio della minimizzazione dei dati, il diritto di opposizione, il principio della legittimità e proporzionalità e l'obbligo di notifica all'autorità nazionale per la protezione dei dati sono alcuni dei capisaldi dei principi europei sulla protezione dei dati. Il principale rischio sociale sarebbe rappresentato dall'ampia diffusione di certificazione sulla vita privata a livello europeo, che potrebbe essere ingannevole sia per gli utenti che per i responsabili del trattamento. Seppure l'impressione possa essere un'altra, non tutte le certificazioni garantiscono seriamente la conformità ai principi sulla protezione dei dati sopra citati;

2. il secondo problema risiede nel controllo delle prassi del sito web in materia di vita privata. Sono previsti molti tipi di controllo. Alcune delle maggiori preoccupazioni in proposito sono:

[213] V. la nota precedente.
[214] http://www.truste.org
[215] http://www.privaseek.com
[216] http://www.bbbonline.org/businesses/privacy/index.html
[217] http://www.cpawebtrust.org/consumer/index.html

- chi esercita il controllo, secondo quali modalità e con che tipo di mandato da parte della società controllata? Nel peggiore dei casi, sembra che il responsabile del controllo sarà principalmente la persona interessata, con tutti i problemi che ciò comporta nell'identificare il mancato rispetto delle prassi sulla vita privata pubblicate, nel dimostrarlo e riferirlo al responsabile della certificazione. Inoltre, non tutti gli enti di certificazione sono in grado di assicurare che tutte le società agiscono in base alle politiche dichiarate;
- chi pagherà? Poiché la certificazione è un'iniziativa privata che non beneficia spesso di un sostegno finanziario da parte dello Stato, alcuni enti di certificazione saranno messi sotto pressione dalle società che essi dovrebbero controllare;
- quali eventuali sanzioni saranno applicate?

I possibili effetti di miglioramento della vita privata delle certificazioni in materia non devono, tuttavia, essere sottovalutati poiché essi possono contribuire alla sensibilizzazione degli utenti Internet con riguardo alla vita privata.

Possono essere fatte alcune proposte per risolvere i problemi suddetti:

1. contenuto della certificazione: per garantire che le certificazioni sulla vita privata siano conformi alla legislazione europea sulla protezione dei dati, potrebbe essere accordata dal Gruppo di lavoro una norma europea relativa alle certificazioni sulla vita privata. Questa norma dovrà specificare i requisiti cui una certificazione dovrà soddisfare[218].

Potrebbero coesistere certificazioni diverse finché agli utenti Internet non risulterà chiaro quali sono le certificazioni che rispondono alle norme europee.

2. Controllo delle prassi dei siti web in materia di vita privata: l'affidabilità delle prassi dei siti web in materia di vita privata potrebbe essere notevolmente migliorata obbligando i siti web dotati di marchio di qualità a sottoporsi a controlli periodici. La norma europea relativa alle certificazioni sulla vita privata potrebbe prevedere tale requisito e determinare le eventuali modalità di svolgimento di tali controlli obbligatori, ad esempio l'autocontrollo mediante un elenco di spunta standard, un controllo effettuato da terzi, ecc.

IV. Conclusioni

- Dovrebbero essere elaborate raccomandazioni relative alla produzione di browser conformi alla vita privata e dotati di impostazioni predefinite rispettose della vita privata;
- i proxy server anonimi possono nascondere l'indirizzo IP e potrebbero essere offerti gratuitamente in seguito alla sottoscrizione di un abbonamento Internet presso qualsiasi *fornitore di servizi Internet*;
- i siti web non dovrebbero negare l'accesso agli utenti che non intendono accettare i *cookie* a meno che tali *cookie* di sessione non siano indispensabili ai fini del collegamento tra l'utente e i suoi vari acquisti on-line, e consentire un'adeguata fatturazione;
- deve essere incoraggiato l'uso delle tecnologie intese al miglioramento della vita privata, in particolare se installate dai *fornitori di servizi Internet* o da altri attori;
- sembra che alle persone devono essere fornite maggiori informazioni sull'esistenza delle tecnologie intese al miglioramento della vita privata. Il settore pubblico

[218] L'autorità francese per la protezione dei dati (CNIL) ha svolto delle attività interessanti in questo campo, che potrebbero servire come base per la norma europea. V. www.cnil.fr

dovrebbe intraprendere i passi necessari per sensibilizzare e sostenere lo sviluppo di tali soluzioni, nonché per utilizzarle e sostenerle[219];

- una norma europea per le certificazioni sulla vita privata dovrebbe essere concordata dal Gruppo di lavoro. Tale norma dovrebbe prevedere l'obbligo che i siti web si sottopongano a controlli periodici.

[219] Nei Paesi Bassi, durante la discussione parlamentare della nuova legge sulla protezione dei dati al Senato è stata approvata una mozione in cui si invitava il governo ad incoraggiare lo sviluppo e l'uso delle tecnologie intese al miglioramento della vita privata e ad incoraggiare il settore pubblico a fungere da promotore di tali tecnologie per i propri trattamenti di dati personali.
Mozione N. 31 di NICOLAÏ C.S., presentata il 18 novembre 1999 riguardante il progetto di legge 25 892 (Regels inzake de bescherming van persoonsgegevens, Wet bescherming persoonsgegevens), L'Aia, Tweede Kamer, vergaderjaar 1999–2000, 25 892, N. 31.

CAPITOLO 10 : CONCLUSIONI

Il presente documento si è occupato di una serie di argomenti illustrati in vari capitoli, ognuno dei quali riporta le osservazioni conclusive su questioni specifiche. Questo documento descrive, tuttavia, temi comuni correlati a tutti i servizi Internet, i quali meritano di essere trattati in termini più generali.
Dopo un riassunto delle tendenze e dei rischi per la vita privata osservati in tutti i vari ambiti dell'uso di Internet, il documento tenta di fornire alcune linee guida e raccomandazioni, considerando le iniziative che potrebbero essere intraprese a vari livelli.

1. Tendenze e rischi

Lo sviluppo di Internet è esponenziale. L'utente Internet ha a sua disposizione una quantità crescente di servizi, dallo shopping on-line alla partecipazione a forum insieme a persone di tutto il mondo. A causa di questa complessità, diventa sempre più difficile avere un'idea adeguata di tutte le possibilità offerte all'utente. Le società cercano modi per attirare l'utente e distinguersi dalle altre offrendo servizi personalizzati e/o gratuiti.
La personalizzazione dei servizi si basa sull'uso dei dati personali degli utenti, che le società tentano di ottenere usando varie risorse, come incoraggiando la fornitura di tali dati da parte degli utenti stessi nell'ambito di programmi di fedeltà, omaggi o servizi gratuiti, raccolta presso le fonti disponibili al pubblico, ecc.
I profili elaborati non sono solo preziosi per le società che desiderano finalizzare un cliente, ma hanno un valore economico intrinseco poiché vengono spesso venduti o affittati a terzi.

Attualmente, lo sviluppo di nuove tecnologie consente di seguire un utente Internet con maggiore facilità. Ad esempio, quando un cliente utilizza un telefono mobile per connettersi ad Internet, è possibile generare i dati che ne indicano l'ubicazione.
Quando l'utente stabilisce una connessione Internet attraverso strumenti nuovi, ad esempio via ADSL o cavo, gli viene assegnato un indirizzo IP statico che ne agevola l'inseguimento di sessione in sessione. Le nuove generazioni di software e hardware offrono nuove funzioni che accrescono la capacità di sorvegliare le attività dell'utente in tempo reale, spesso senza che egli lo sappia. In questo documento sono stati forniti numerosi esempi di trattamento invisibile e software E.T.
In questo contesto, diventa difficile per l'utente medio conservare l'anonimato mentre è connesso a Internet.

La combinazione di queste capacità in evoluzione comporta nuovi rischi per la vita privata dell'utente Internet, in particolare quando i dati si concentrano nella mani di un unico o di un numero limitato di responsabili del trattamento.
Quando, ad esempio, i responsabili del trattamento utilizzano tecnologie di estrazione dei dati, essi hanno la possibilità tecnica non solo di trattare e riorganizzare i dati, ma anche di scoprire nuovi collegamenti e caratteristiche correlati alla persona interessata, che di solito è all'oscuro di tale possibilità e non è in grado di prevede un simile trattamento.
Tali rischi derivano anche dal fatto che alcuni dati vengono conservati on-line per un arco di tempo molto lungo; ad esempio, i messaggi inviati ai gruppi di discussione e alle mailing list vengono conservati, spesso, per diversi anni e possono essere consultati usando strumenti di ricerca derivata.

Tale disponibilità di dati personali ne consente un uso secondario imprevisto, che è spesso incompatibile con la finalità per cui i dati sono stati originariamente raccolti.

2. Linee guida e raccomandazioni

2.1. Sensibilizzazione dell'utente Internet

Alla luce dei rischi crescenti per la vita privata dell'utente Internet, secondo quanto descritto in precedenza, è particolarmente rilevante garantire che vengano messi in atto strumenti adeguati per assicurare che l'utente riceva tutte le informazioni necessarie per fare una scelta informata. Vari attori devono occuparsi della fornitura di queste informazioni all'utente.

In primo luogo, i responsabili della raccolta di dati personali on-line devono fornire alla persona interessata tutte le informazioni necessarie. Tali informazioni, citate nell'articolo 10 della direttiva 95/46/CE, devono essere fornite in qualsiasi caso, al momento della raccolta dei dati. Sebbene la pubblicazione nel sito web di una clausola sulla vita privata rappresenti un modo adeguato per fornire al pubblico informazioni generali, è necessario che le informazioni vengano fornite alla persona interessata presso cui vengono raccolti i dati in modo semplice a accessibile ogniqualvolta che tali dati vengono raccolti, ad esempio sullo stesso schermo in cui la persona in questione deve inserire i propri dati o mediante un'apposita casella di dialogo (prompt).

Se il responsabile del trattamento è una società privata, la conformità a tali norme non è importante solo in termini giuridici ma anche per il proprio interesse commerciale, poiché la fiducia e la sicurezza delle persone aumenteranno e potrebbero influire sui loro rapporti con la società. Per quanto riguarda lo sviluppo del commercio elettronico, ad esempio, si osserva che gli utenti sono riluttanti ad effettuare transazioni elettroniche se temono che i loro dati personali non saranno protetti e tutelati in modo corretto.

Se il responsabile del trattamento è un'autorità pubblica, la conformità alle norme sulla protezione dei dati è un elemento chiave, poiché il comportamento di tale autorità dovrebbe essere d'esempio per l'opinione pubblica generale. Ad esempio, le autorità pubbliche che intraprendono attività di governo elettronico dovrebbero considerare la vita privata tra i pilastri del sistema di scambio di dati. Inoltre, anche quando esse non operano in qualità di responsabili del trattamento, la loro responsabilità riguarda comunque il settore dell'educazione generale e dell'informazione al pubblico.
In particolare, alle autorità per la protezione dei dati è affidato il compito di sensibilizzare il pubblico sui rischi collegati all'uso di Internet, ma anche sui diritti e gli obblighi previsti dalla legislazione. Ciò può avvenire in vari modi, come la pubblicazione di depliant, relazioni, comunicati stampa, l'inserimento di raccomandazioni pratiche nei moduli delle notifiche, l'organizzazione o partecipazione a conferenze o seminari su tali temi, dedicati ai vari attori e settori della società.

Tradizionalmente, sono le associazioni e i tutori della vita privata a svolgere attività di sensibilizzazione del pubblico, secondo modalità che, talvolta, hanno condotto a miglioramenti importanti per quanto riguarda la conformità dei prodotti Internet alla vita privata.
In vari paesi dell'Unione europea, si è osservato che anche le associazioni dei consumatori si stanno occupando ed interessando, in misura crescente, degli aspetti delle attività dei consumatori per quanto riguarda la vita privata. Tale ruolo può rivelarsi particolarmente positivo, poiché non si limita alla fornitura di informazioni, ma si estende anche alla rappresentanza dei consumatori nei loro rapporti con le società o le autorità pubbliche. Queste associazioni, ad esempio, possono sorvegliare l'osservanza

delle leggi da parte dei fornitori di servizi Internet, o informare le autorità pubbliche sui reclami ricevuti in relazione ad un determinato sito web o società Internet.

Anche le associazioni professionali possono esercitare un'influenza positiva, informando i nuovi attori dei loro obblighi giuridici.

Tutte le parti sopra citate svolgono un ruolo importante nel fornire al consumatore le informazioni necessarie per consentirgli di operare una scelta responsabile. Dipende poi dalla persona utilizzare gli strumenti a sua disposizione per garantire il rispetto dei propri diritti ed, eventualmente, per chiarire che non accetterà servizi o prodotti che non sono conformi al quadro normativo esistente.

2.2. Applicazione della legislazione esistente in modo coerente e coordinato

La protezione dei dati on-line può essere garantita, in modo sufficiente, solo nel rispetto del quadro normativo esistente. In considerazione del carattere internazionale della rete, è essenziale che i responsabili del trattamento possano contare su un'interpretazione coerente e coordinata, e sull'applicazione delle norme europee sulla protezione dei dati. Ciò è importante non solo per le persone interessate e i responsabili del trattamento all'interno dell'UE, ma anche per quanti risiedono fuori dall'Unione, i quali devono tenere comunque conto del quadro normativo in essere, in particolare quando raccolgono dati personali utilizzando strumenti ubicati all'interno dell'Unione. In questo contesto, il Gruppo di lavoro ha un ruolo importante da svolgere.

In varie occasioni, il Gruppo di lavoro ha evidenziato la presenza di lacune o temi controversi nella legislazione esistente e ha emanato documenti che forniscono un'interpretazione comune ed eventuali soluzioni in proposito. Un'attenzione particolare è stata rivolta alla revisione della direttiva 97/66/CE, che ha apportato alcuni miglioramenti importanti alla terminologia utilizzata. Sebbene il Gruppo di lavoro si compiaccia del fatto che nel progetto di direttiva sono stati presi in considerazione temi nuovi, sono state presentante alcune proposte relative a punti specifici che potrebbero essere chiariti ancor meglio.

Il Gruppo di lavoro è preoccupato del fatto che le modifiche della legislazione esistente si tradurranno, in alcuni casi, in disposizioni giuridiche più severe per quanto riguarda, in particolare, le possibilità di sorveglianza sul web e la generalizzazione delle esigenze di identificazione dell'utente. Il Gruppo di lavoro ha ricordato il fatto che, sebbene potrebbero essere in gioco altri interessi legittimi, occorre sempre trovare un equilibrio tra gli interessi in questione e la protezione dei dati personali della persona interessata.

Occorre sottolineare il fatto che l'interpretazione e l'applicazione della legislazione non sono compito delle sole autorità pubbliche, ma che il settore privato può fornire un contributo proficuo in tal senso investendo nello sviluppo dell'autoregolamentazione o di codici di condotta riguardanti temi più specifici che interessano un determinato settore.

2.3. Sviluppo e uso di tecnologie che migliorano, rispettano e sono conformi alla vita privata

Come affermato in precedenza, il trattamento dei dati personali su Internet dipende, in gran parte, dalla configurazione tecnica di hardware e software, nonché dai protocolli e dalle norme tecniche usati per la trasmissione delle informazioni.
Pertanto, è particolarmente importante tenere conto delle disposizioni sulla vita privata sin dalle fase più precoce dello sviluppo di tutti questi strumenti; ad esempio, un browser non dovrebbe trasmettere più informazioni di quante non siano necessarie per stabilire una connessione con un sito web. Si incoraggia chi si occupa della progettazione e lo sviluppo di questi strumenti tecnici a consultare le autorità nazionali per la protezione dei dati in merito alle disposizioni giuridiche esistenti in materia.
Inoltre, per chiarire all'opinione pubblica quali sono i prodotti conformi alla vita privata, sarebbe utile mettere in atto un sistema di marchi di certificazione che consentirebbe di riconoscere con facilità i prodotti conformi alle disposizioni sulla protezione dei dati.

Poiché, tradizionalmente, le nuove tecnologie sono considerate una minaccia per la vita privata, dovrebbe essere puntualizzato, altresì, che esse rappresentano anche uno strumento utile in termini di tutela della vita privata.

In primo luogo, alcune tecnologie esistenti possono essere utilizzate per migliorare la trasparenza e la semplicità delle informazioni fornite alla persona interessata, ad esempio fornendo agli utenti informazioni semplici e accessibili al momento della raccolta dei dati personali.
In secondo luogo, esse possono rivelarsi uno strumento utile per semplificare l'esercizio dei diritti delle persone interessate, consentendo, ad esempio, l'accesso diretto on-line ai dati personali od offrendo la possibilità di opporsi al trattamento.

Tenendo conto del fatto che l'utente medio non è necessariamente a conoscenza degli aspetti tecnici dell'uso di Internet, e che non sempre è in grado di prendere autonomamente decisioni in merito o addirittura di modificare la configurazione dell'hardware e del software utilizzati, è determinante che le impostazioni predefinite dei prodotti offrano il massimo livello di protezione della vita privata.

E' stata sviluppata una serie di strumenti supplementari, meglio conosciuti come "tecnologie intese al miglioramento della vita privata" al fine di aiutare gli utenti a tutelare la loro vita privata, in particolare minimizzando o eliminando la raccolta o il trattamento successivo di dati identificabili e impedendo tecnicamente qualsiasi forma illecita di trattamento. Tra gli esempi di tali strumenti figurano i proxy server, i cookie killer, il software anonimizzante, gli strumenti di pseudonimizzazione (particolarmente preziosi per l'elaborazione di profili), i filtri per la posta elettronica, ecc. Tra gli eventuali nuovi prodotti potrebbero figurare carte intelligenti contenenti un protettore di identità portatile (portable identity protector - PIP), che la persona potrà inserire in qualsiasi macchina da cui stabilisce una connessione on-line.

Di tutti gli attori già citati nel paragrafo 2.1, l'industria e il settore pubblico sono quelli che dovrebbero investire e incoraggiare per primi lo sviluppo e l'attuazione di tecnologie che proteggono la vita privata. L'utente dovrebbe essere informato dell'esistenza di tali strumenti, che dovrebbero essere resi disponibili a costi ragionevoli.

2.4. Creazione di meccanismi sicuri di controllo e riscontro

La protezione dei dati on-line può essere efficace solo mettendo in atto strumenti adeguati per sorvegliare e valutare la conformità al quadro normativo e alle disposizioni tecniche illustrati in precedenza.
A tale scopo, anche se le autorità per la protezione dei dati hanno il compito di controllare, in primo luogo, l'esecuzione, altri attori si stanno adoperando nella direzione dell'autosorveglianza, avendo compreso l'impatto che la loro politica sulla vita privata può avere sul comportamento dei consumatori nei loro confronti.

Le autorità per la protezione dei dati possono contribuire allo sviluppo e al buon funzionamento di tali sistemi di autosorveglianza fornendo indicazioni, ad esempio sotto forma di elenchi di spunta per l'autovalutazione concordati a livello europeo.

Inoltre, potrebbero essere concesse delle certificazioni allo scopo di aiutare il consumatore ad avere un'indicazione affidabile della conformità di un trattamento di dati alla legislazione sulla protezione dei dati dell'UE. Il Gruppo di lavoro intende assumere iniziative in questo campo al fine di garantire, in particolare, che vengano concesse certificazioni sulla vita privata ai siti web che sono conformi alla legislazione europea sulla protezione dei dati.

Il Gruppo di lavoro invita tutti gli attori coinvolti nelle attività Internet a tenere conto di questo documento di lavoro e ad intraprendere le iniziative necessarie per mettere in pratica le raccomandazioni in esso contenute.

Il Gruppo di lavoro auspica che il presente documento di lavoro possa contribuire alla sensibilizzazione e promuovere il dibattito pubblico su questo tema, che richiederà sicuramente un'ulteriore analisi ed approfondimento in futuro.

GLOSSARIO DI TERMINI TECNICI[220]

ADSL

ADSL (Asynchronous Digital Subscriber Line) è un protocollo di telecomunicazione che può essere utilizzato sulle classiche linee con doppino incrociato in rame. Permette di raggiungere velocemente sino a un MB al secondo, mantenendo simultaneamente la linea libera per le normali conversazioni telefoniche. L'ADSL richiede modem dedicati ADSL da installare ad entrambe le estremità della linea locale.

Autenticazione

Accertamento dell'identità di un utente che si connette ad un computer o accertamento dell'*integrità* di un messaggio trasmesso.

Banner

I *banner* pubblicitari sono piccole caselle grafiche che appaiono alla sommità o all'interno di un sito web.

Identificazione della linea chiamante

Quando viene effettuata una chiamata, questa funzione consente all'utente chiamato di identificare il chiamante presentando il numero della linea chiamante.

Clickstream

Informazioni derivate dal comportamento di una persona, il percorso o le scelte effettuate visitando i siti web. Queste informazioni contengono i collegamenti seguiti dall'utente e registrati nel web server (i computer dei *fornitori di servizi Internet* per coloro che non dispongono di un proprio web server).

Cookie

I *cookie* sono pezzi di dati creati da un web server, che possono essere memorizzati come file di testo e depositati sul disco fisso dell'utente, mentre una copia può essere conservata dal sito web. Essi rappresentano una parte standard del traffico HTTP e, in quanto tali, possono essere trasportati, senza ostacoli, con il traffico IP. Un *cookie* può contenere un numero esclusivo (GUI, Global Unique Identifier) che permette una migliore personalizzazione rispetto agli indirizzi IP dinamici. I cookie permettono al sito web di tenere traccia dei modelli e preferenze dell'utente.
I *cookie* contengono una serie di URL (indirizzi) per cui che essi sono validi. Il browser, quando incontra questi URL di nuovo, invia quei determinati cookie al web server.

[220] Parte di queste definizioni è stata tratta dalle seguenti fonti:
- http://www.techweb.com/encyclopedia
- http://webopedia.Internet.com
- Personal Data Privacy and the Internet: a guide for data users, Office of the Privacy Commissioner for Personal Data, Hong Kong, 1998.

La natura dei cookie può essere diversa: possono essere persistenti o avere una durata limitata, i cosiddetti *cookies* di sessione.
E' possibile disabilitare i cookie nel proprio browser o visualizzare un apposito avviso prima di accettarli.

Integrità dei dati

Il processo inteso ad impedire la cancellazione o contraffazione accidentale dei dati di una banca dati.

Datamining (estrazione di dati)

Comporta il vaglio di tonnellate di dati per scoprire modelli e relazioni contenuti nell'attività commerciale e nella storia. Viene normalmente effettuato utilizzando programmi che analizzano i dati in automatico.

Data warehouse (magazzino di dati)

Una base dati progettata per sostenere il processo decisionale di un'organizzazione. Può contenere quantità enormi di dati. Per esempio, grandi organizzazioni di vendita al dettaglio possono avere 100GB o più di storia transazionale. Quando la base di dati è organizzata per un dipartimento o una funzione, viene spesso chiamata 'datamart' piuttosto che *data warehouse*.

Certificato digitale

Un *certificato digitale* è un documento elettronico che contiene due gruppi di informazioni e che si propone come prova di identità nel mondo elettronico. Il primo gruppo di informazioni è rappresentato dalle varie e proprie informazioni del certificato, come il nome o lo pseudonimo della persona giuridica o fisica che ha richiesto il certificato, la relativa chiave pubblica, la validità del certificato e il nome dell'ente di certificazione. Il secondo gruppo di informazioni è rappresentato dalla *firma elettronica* dell'ente di certificazione. L'intero messaggio è firmato in modo digitale da un ente di certificazione che viene incaricato dai vari server (gli enti di certificazione sono una sorta di terzi fiduciari) e può verificare il rapporto tra la persona giuridica o fisica e la relativa chiave pubblica.

Firma digitale

Una *firma digitale* è una stringa di dati aggiunta ad un messaggio e la sua integrità è garantita dalla crifratura (o riassunto di un messaggio) ottenuta con la chiave privata del firmatario. Chiunque riceva il messaggio firmato potrà controllare se è stata modificata semplicemente decifrando la firma con la chiave pubblica del mittente e confrontando la stringa decifrata con il messaggio originale o il relativo riassunto.

Servizio dei nomi di dominio (Domain Name Service - DNS)

Il DNS (*Domain Name Service*) è un meccanismo di assegnazione dei nome ai computer identificati da un indirizzo IP. Questi nomi si presentano sotto forma di <nomi>.dominio di primo livello, dove <nomi> è una stringa costituita da una o più stringhe secondarie separate da un punto.

Dynamic Host Configuration Protocol (DHCP)

Il *Dynamic Host Configuration Protocol* (DHCP) è un protocollo Internet che consente di automatizzare la configurazione dei computer che utilizzano il TCP/IP. Il DHCP può essere usato per assegnare gli indirizzi IP automaticamente. (http://www.dhcp.org)

Firma elettronica

Dati in formato elettronico collegati o logicamente associati ad altri dati elettronici e che servono come metodo di autenticazione (Articolo 2(1) della direttiva sulle *firme elettroniche*).

Cifratura

Informazioni e messaggi codificati in modo da non potere essere letti, in linea di principio, da una persona diversa dal destinatario desiderato il quale può accedere ad una chiave o una password. Esistono due tipi principali di sistemi di *cifratura*.
- Il sistema a chiave simmetrica o privata, che utilizza una chiave segreta condivisa tra il mittente ed il destinatario di un messaggio. Il vantaggio principale è rappresentato dalla velocità di elaborazione e lo svantaggio più grosso è dato dalla difficoltà di condividere in modo sicuro le chiavi tra molti utenti.
- Il sistema a chiave asimmetrica o pubblica, che utilizza un paio di chiavi generate in maniera tale che anche conoscendone una è quasi impossibile indovinare l'altra. Il messaggio cifrato usando una delle due chiavi può essere decifrato utilizzando l'altra. Una delle chiavi è resa pubblica ed utilizzata per cifrare il messaggio che viene decifrato da ogni utente con la propria chiave privata segreta. La chiave privata segreta è anche utilizzata per firmare i messaggi in forma digitale.

Parete tagliafuoco

Si tratta di un metodo per proteggere una rete. Può essere implementato in un unico *router* che filtra i pacchetti indesiderati oppure potrebbe utilizzare, nei router e negli host, una combinazione di tecnologie. Le *pareti tagliafuoco* sono ampiamente utilizzate per consentire agli utenti l'accesso sicuro ad Internet e per separare il server web pubblico di un'azienda dalla sua rete interna. Sono anche utilizzate per garantire la sicurezza di segmenti di rete interni. Per esempio, una rete secondaria di ricerca o contabilità potrebbe essere vulnerabile alle intrusioni dall'interno.

Collegamenti ipertestuali

Collegamento predefinito tra due oggetti. Il collegamento è rappresentato da un testo o da un'icona. Sulle pagine del World Wide Web, un *collegamento ipertestuale* è rappresentato da un testo sottolineato, solitamente in blu, mentre un collegamento ipertestuale grafico è rappresentato da una piccola immagine grafica.

Fornitore di servizi Internet

Società che fornisce l'accesso e la connessione ad Internet ai privati o alle aziende.
I piccoli *fornitori di servizi Internet* forniscono il servizio via *modem* e ISDN, mentre quelli più grandi offrono anche allacciamenti privati. Ai clienti viene generalmente fatturato un canone fisso mensile ma potrebbero essere addebitati altri costi. Pagando una tariffa, è possibile creare e mantenere un sito web personale sul server del *fornitore di servizi Internet*, permettendo così, anche ad una piccola organizzazione, di essere presente in rete con un proprio nome di dominio.

I fornitori più grossi, oltre all'accesso Internet, forniscono anche basi di dati proprietarie, forum e servizi.
In questo documento, il termine *fornitore di servizi Internet* comprende i genere anche i fornitori di accesso Internet. Il termine fornitore di accesso Internet viene utilizzato solo quando risulta chiaro che si fa riferimento esclusivamente all'accesso a Internet; in tutti gli altri casi, viene utilizzato il termine generico di *fornitore di servizi Internet*.

Java e JavaScript

Java è un vero e proprio linguaggio di programmazione non destinato ai programmatori improvvisati e sicuramente non agli utenti finali. *JavaScript* è un linguaggio di scrittura che usa una sintassi simile a *Java,* ma non viene compilato nel codice byte. Esso rimane nel codice di origine inserito in un documento HTML e deve essere tradotto una riga alla volta in codice macchina dall'interprete *JavaScript*. *JavaScript* è molto famoso ed è supportato da tutti i browser web. *JavaScript* ha un ambito di applicazione più limitato di *Java* e si occupa prevalentemente di elementi presenti sulla pagina web in sé.

Meta-tag

I *meta-tags* sono tag HTML che forniscono informazioni su una pagina web. A differenza dei normali tag HTML, i *meta-tag* non influiscono sulle modalità di presentazione della pagina. Essi forniscono invece informazioni, come l'autore della pagina, la frequenza di aggiornamento, il contenuto della pagina e le parole chiave che rappresentano tale contenuto. Molti motori di ricerca usano queste informazioni per creare i propri indici.

Modem

(**MO**dulatore-**DEM**odulatore) Dispositivo che adatta un terminale o un computer ad una linea telefonica analogica, convertendo gli impulsi digitali in frequenze audio e vice versa. Il termine di solito si riferisce a modem con velocità di 56 KB al secondo (V.90), l'attuale velocità massima, o ai precedenti modem con velocità di 28,8 KB al secondo (V.34). Il termine può anche essere riferito a modem con cavo ad alta velocità o modem DSL, oppure ad adattatori di terminale ISDN, i quali sono completamente digitali e non sono tecnicamente dei modem. Un modem è un convertitore analogico-digitale e viceversa. Un *modem* inoltre chiama la linea, risponde alla chiamata e controlla la velocità di trasmissione. La velocità dei modem è passata da 300, 1200, 2400, 9600, 14400, 28800, 33300 sino a 56000 bps. Qualunque sia la velocità massima, alcune velocità inferiori sono tuttora supportate in modo che il *modem* possa accettare anche modem precedenti o negoziare verso il basso su linee più rumorose.

OLAP

On**L**ine **A**nalytical **P**rocessing. Software di supporto decisionale che permette all'utente di analizzare velocemente informazioni che sono state riepilogate in visualizzazioni e gerarchie multidimensionali. Per esempio, strumenti OLAP vengono utilizzati per l'analisi delle tendenze relative alle vendite e alle informazioni finanziarie. Essi permettono agli utenti di scavare all'interno di masse di statistiche sulle vendite per isolare i prodotti più volatili. Prodotti OLAP tradizionali, conosciuti anche come OLAP multidimensionali o MOLAP, riassumono anticipatamente le transazioni in visioni multidimensionali. Le interrogazioni degli utenti in questi tipi di basi di dati sono molto veloci perché il consolidamento è già stato effettuato. OLAP deposita i dati in una

struttura a cubo che può essere ruotata dall'utente, rendendola particolarmente adatta ai riepiloghi finanziari.

Sito portale

Un *sito portale* fornisce una panoramica di collegamenti web in modo ordinato. Attraverso il *portale* visitato, l'utente Internet può visitare con facilità i siti web selezionati di altri fornitori di contenuti.
I portali moderni sono "supersiti" che forniscono una serie di servizi, tra cui la ricerca web, notiziari, elenchi di pagine bianche e gialle, posta elettronica gratuita, gruppi di discussione, shopping on-line e collegamenti ad altri siti.

PPP

Il PPP (Point to Point Protocol) è un protocollo di telecomunicazione ampiamente utilizzato per connettere due computer utilizzando la relativa porta seriale o un modem ad essi collegato. Si tratta di un protocollo di secondo livello usato principalmente tra il personal computer di un utente privato e il server di accesso Internet di un fornitore di servizi Internet quando si stabilisce una connessione TCP/IP su una classica linea telefonica.

Proxy server

Il *proxy server* è un server intermedio posto tra l'utente Internet e la rete. Il proxy server funge da web cache, migliorando notevolmente le prestazioni di Internet. Molte grandi organizzazioni o fornitori di accesso Internet hanno già adottato questa soluzione. Ogni pagina, immagine o logo, ricevuti esternamente da un membro di un'organizzazione, vengono memorizzati su una cache e verranno messi istantaneamente a disposizione di qualunque membro di questa organizzazione. Non sarà più necessario che ogni membro dell'organizzazione situato a monte del proxy server abbia un proprio indirizzo IP, poiché non accedono direttamente a Internet.

Protocollo

In questo contesto, un *protocollo* è una serie di regole tecniche che devono essere osservate da due partner per scambiarsi le informazioni. I protocolli sono organizzati in una gerarchia di strati. Ogni strato è responsabile della gestione di un particolare aspetto del processo di telecomunicazione e provvede a funzioni basilari che devono essere utilizzate dagli strati superiori. Tradizionalmente, in Internet, il protocollo TCP/IP è sempre utilizzato come strato intermedio. Ethernet (utilizzato nelle reti LAN), ADSL (utilizzato nelle linee telefoniche), ATM (utilizzato dagli operatori di telecomunicazioni), X-75 (utilizzato sulle linee ISDN), PPP (utilizzato sulle linee telefoniche standard) sono alcuni esempi di protocolli di secondo livello. Dall'altro lato, HTTP (per la navigazione), SMTP e POP (per la posta elettronica), FTP (per il trasferimento di file) sono protocolli di primo livello. Ciò significa che ogni potenziale minaccia per la vita privata presente nel protocollo TCP/IP sarà una delle debolezze dei protocolli superiori. In pratica, gli strati sono una serie di sottoprogrammi che funzionano su un computer collegato ad Internet.

Router

Un *router* è un importante dispositivo che fornisce i percorsi per le *reti TCP/IP*. Ciò significa che il percorso TCP/IP è dinamico, in funzione dei guasti o dei sovraccarichi di

alcuni router o collegamenti. Esso può anche essere utilizzato come *parete tagliafuoco* tra un'organizzazione e Internet, e garantisce che da un determinato *fornitore di servizi Internet* possano derivare solo indirizzi IP autorizzati.

Shareware

Software che può essere scaricato da Internet. In genere, può essere scaricato gratuitamente a fini di prova ma, per poterlo usare legalmente, è necessario pagare un importo esiguo agli sviluppatori di software. Il software che può essere scaricato e utilizzato a titolo completamente gratuito è detto *freeware.*

Sniffing

Il software di *sniffing* consente di sorvegliare il traffico e leggere tutti i pacchetti di dati sulla rete in modo da presentare in chiaro tutte le comunicazioni che non sono cifrate. La forma più semplice di *sniffing* può essere eseguita utilizzando un comune PC connesso ad una rete utilizzando un software comunemente disponibile.

Spamming (o spam)

Invio di grandi quantità di materiale pubblicitario non richiesto attraverso la posta elettronica.

Rete TCP/IP

Una *rete TCP/IP* (Transport Control Protocol/Internet Protocol) è basata sulla trasmissione di piccoli pacchetti di informazione. Ogni pacchetto comprende l'indirizzo IP del mittente e del destinatario. Questa rete è priva di connessione. Questo significa che a differenza, ad esempio, della rete telefonica, non è necessaria alcuna connessione preliminare tra due dispositivi prima che la comunicazione possa iniziare. Significa anche che sono possibili, contemporaneamente, comunicazioni con più interlocutori.

Terzi fiduciari[221]

Un *terzo fiduciario* può essere descritto come un'entità incaricata da altre entità con riguardo ai servizi e alle attività relativi alla sicurezza.

Un *terzo fiduciario* viene usato per offrire servizi a valore aggiunto agli utenti che desiderano migliorare la fiducia e la sicurezza commerciale dei servizi che essi ricevono e per agevolare le comunicazioni sicure tra i partner commerciali. I *terzi fiduciari* devono offrire valore per quanto riguarda l'*integrità*, la riservatezza e le prestazioni positive dei servizi e delle informazioni coinvolte nelle comunicazioni tra le applicazioni commerciali. Inoltre, gli utenti richiedono che i servizi dei *terzi fiduciari* siano disponibili all'occorrenza, entro i termini del contratto di servizio concordato.

In genere, un *terzo fiduciario* è un'organizzazione che è stata autorizzata o accreditata da un'autorità di regolamentazione e fornisce servizi di sicurezza, su base commerciale, ad una vasta gamma di organismi, tra cui quelli del settore delle telecomunicazioni, finanziario e delle vendite al dettaglio.

Ad esempio, un *terzo fiduciario* potrebbe essere usato per sostenere la fornitura di firme digitali per garantire l'*integrità* di documenti. Inoltre, essi potrebbero fornire servizi di cifratura end-to-end agli utenti e inserire, ad esempio, una funzione di recupero o backup per consentire il recupero di una chiave qualora andasse perduta (di solito, per i documenti e i file che sono stati cifrati dai dipendenti) oppure per sostenere una richiesta di intercettazione lecita.

[221] Definizione tratta da ETSI "Requirements for *TTP* services".

L'uso dei *terzi fiduciari* è soggetto al requisito fondamentale che il *terzo fiduciario* in questione sia incaricato dalle entità che esso sostiene per eseguire talune funzioni.

UMTS

UMTS (Universal Mobile Telecommunications System) è un protocollo di trasmissione senza fili e basato su pacchetti, a banda larga e di terza generazione, in grado di offrire velocità di trasmissione superiori a 2 Mbps. Questo nuovo protocollo a banda larga permetterà la trasmissione di video digitali di qualità televisiva verso dispositivi mobili. Attualmente, la rete GSM permette velocità di circa 11 Kbps, sufficienti per la trasmissione di suoni ma non di immagini in movimento[222].

WAP

Il WAP (Wireless Application Protocol) è un protocollo di telecomunicazione studiato da molti produttori di telefoni mobili. Esso consente l'accesso ai servizi Internet, come posta, chat, navigazione web, da un telefono mobile dedicato.[223]

Web cache

Un computer di una rete che conserva, in memoria o su disco, copie delle pagine web richieste più di recente al fine di accelerarne il reperimento. Se la pagina successiva richiesta è già stata memorizzata nella cache, essa viene reperita localmente e non da Internet. I server di web cache risiedono all'interno della parete *tagliafuoco* della società e consentono l'immediata disponibilità di tutte le pagine popolari reperite dagli utenti. Poiché il contenuto delle pagine web può cambiare, il software di caching controlla sempre le versioni più recenti della pagina e le scarica. Le pagine verranno cancellate dalla cache dopo un certo periodo di inattività.

Webmail

Sistemi di posta elettronica che utilizzano pagine web come interfaccia (ad esempio, Yahoo, HotMail ecc.). Chiunque può accedere alla *webmail* e l'utente non deve connettersi ad un determinato *fornitore di servizi Internet* come quando utilizza invece un normale account di posta elettronica.

Fatto a Bruxelles, il 21 novembre 2000

Per il Gruppo di lavoro

Il Presidente

Stefano RODOTA

[222] See http://www.umts-forum.org/

[223] Per maggiori informazioni v.: http://www.wapforum.org