



Privacy e comunicazioni elettroniche: le principali novità della Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio

L'ambito

Porta la data del 12 luglio 2002 la Direttiva n. 2002/58/CE del Parlamento Europeo e del Consiglio, pubblicata sulla Gazzetta Ufficiale delle Comunità europee il 31 luglio u.s (data della sua entrata in vigore), relativa al trattamento dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Entro il 31 ottobre 2003 gli Stati membri della Comunità Europea dovranno adeguarsi a tale Direttiva che sostituirà, da tale data, la n. 97/66/CE (Direttiva sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni), alla quale l'Italia, in particolar modo, si era adeguata con il d.lgs. n. 171/98.

Il testo della Direttiva, in formato pdf, è liberamente consultabile al seguente indirizzo internet: http://europa.eu.int/eur-lex/it/dat/2002/l_201/l_20120020731it00370047.pdf

Le argomentazioni

La prima grossa differenza, tra le due Direttive, la si coglie già nell'intestazione: non si parla più, infatti, di settore delle telecomunicazioni ma del più ampio ed onnicomprensivo settore delle comunicazioni elettroniche.

La nuova Direttiva, di fatto, dunque, abroga e sostituisce la precedente Direttiva n. 97/66/CE (elaborata nel rispetto della Direttiva n. 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali; nel rispetto dei principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione Europea e nel rispetto della Convenzione Europea per la protezione dei diritti dell'uomo e delle libertà fondamentali).

Tale sostituzione è motivata, dal Parlamento Europeo, dalla necessità di adeguare la precedente Direttiva (che viene in gran parte replicata nella nuova) *"agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate"*.



Si legge all'art. 3 della Direttiva (Servizi interessati): *"la presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità"*.

Spiega il Parlamento: *"l'introduzione di nuove tecnologie digitali avanzate" pone "esigenze specifiche con riguardo alla tutela dei dati personali e della vita privata degli utenti"; "i servizi di comunicazione elettronica...aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata"; " occorre armonizzare le disposizioni legislative, regolamentari e tecniche adottate dagli Stati membri" con l' "obiettivo di ridurre al minimo il trattamento dei dati personali e di utilizzare dati anonimi o pseudonimi nella misura del possibile"*.

Si afferma che la Direttiva *"lascia...inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti...necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale"; "non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi"; "tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie"*.

Interessante la marcata sottolineatura del concetto di una limitata conservazione nel tempo delle comunicazioni registrate e, comunque, per un periodo non superiore a quanto necessario:

"il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione";

"la riservatezza delle comunicazioni dovrebbe essere assicurata anche nel quadro di legittime prassi commerciali. Ove necessario e legalmente autorizzato, le comunicazioni possono essere registrate allo scopo di fornire la prova di una transazione commerciale"; "le parti in comunicazione dovrebbero



essere informate sulla registrazione, il suo scopo e la durata della sua memorizzazione preventivamente alla stessa. La comunicazione registrata dovrebbe essere cancellata non appena possibile ed in ogni caso non oltre la fine del periodo durante il quale la transazione può essere impugnata legittimamente”.

Compaiono, per la prima volta rispetto alla precedente Direttiva, i riferimenti a spyware (software spia), web bugs e cookies:

“i cosiddetti software spia, bachi invisibili (“web bugs”), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza”;

“i cosiddetti marcatori (“cookies”), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni “on-line”. Allorché tali dispositivi...sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise...sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale...Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili”.

Non mancano anche le previsioni relative alle reti mobili digitali:

“le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Il trattamento di dati siffatti ai fini della fornitura di servizi a valore aggiunto dovrebbe essere autorizzato soltanto previo esplicito consenso dell'abbonato”; “...gli abbonati dovrebbero disporre, gratuitamente, di un mezzo semplice per bloccare temporaneamente il trattamento dei dati relativi alla loro ubicazione”;

“gli Stati membri possono limitare il diritto alla vita privata degli utenti e degli



abbonati riguardo all'identificazione della linea chiamante allorché ciò sia necessario per identificare le chiamate importune, e riguardo all'identificazione della linea chiamante e ai dati relativi all'ubicazione allorché ciò sia necessario per consentire ai servizi di emergenza di svolgere il loro compito nel modo più efficace possibile. A tale scopo gli Stati membri possono adottare disposizioni specifiche per autorizzare i fornitori di servizi di comunicazione elettronica a fornire l'accesso all'identificazione della linea chiamante e ai dati relativi all'ubicazione senza il previo consenso degli utenti o abbonati interessati”.

Le indicazioni relative a corrette ed auspicabili prassi di direct marketing, nel rispetto della vita privata degli utenti, riflettono le pronunce emesse, a tal riguardo, dal nostro Garante sulla Privacy, con uno spiccato accento posto sulla necessità di ottenere sempre il consenso informato da parte dell'utente:

“occorre prevedere misure per tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta, in particolare mediante dispositivi automatici di chiamata, telefax o posta elettronica, compresi i messaggi SMS”; “...per tali forme di comunicazioni indesiderate a scopo di commercializzazione diretta è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi. Il mercato unico prevede un approccio armonizzato per garantire norme semplici a livello comunitario per le aziende e gli utenti”;

“al fine di facilitare l'attuazione efficace delle norme comunitarie in materia di messaggi indesiderati a scopi di commercializzazione diretta, occorre proibire l'uso di false identità o falsi indirizzi o numeri di risposta allorché sono inviati messaggi indesiderati a scopi di commercializzazione diretta”

Vengono, inoltre, richiamati i concetti dell'opt-out e delle black list :

“allorquando gli Stati membri costituiscono un registro “opt-out” per le comunicazioni indesiderate “a persone giuridiche, principalmente imprese, sono pienamente applicabili le disposizioni dell'articolo 7 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio ... relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico)”.

Alcuni articoli in dettaglio

Dettaglio di alcuni concetti enucleati negli articoli della Direttiva:

Sicurezza (Art.4)



"Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete"

"Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili".

Riservatezza delle comunicazioni (Art.5)

Sono vietati "l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza".

"Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale"

Il citato art. 15 della Direttiva prevede (al paragrafo 1), da parte degli Stati membri, limitazioni e restrizioni di diritti ed obblighi nella "misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica" e per la "prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo".

Dati sul traffico (Art.6)

"I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi..." i seguenti casi:



-
- *i dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento”;*

 - *“ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati... nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia dato il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento”;*

 - *“il trattamento dei dati relativi al traffico... deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività”.*

Comunicazioni indesiderate (Art.13)

E' stringente il divieto, in questo articolo, della possibilità di inviare comunicazioni commerciali a chi non ne abbia fatto esplicita richiesta manifestando il proprio consenso a tal proposito, cosicché l'uso di dispositivi automatici di chiamata, del telefax e della posta elettronica "è *consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso*".

Comunque, a coloro che hanno prestato il loro consenso alla ricezione delle comunicazioni commerciali, fornendo le proprie coordinate elettroniche, deve sempre essere garantita *"la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche"*.



Si legge, a chiare lettere, nel paragrafo 4: *"in ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni"*.

Riesame (Art.18)

Singolare quanto enunciato, quasi in sordina, in questo articolo dove, dopo la normale previsione, a tre anni dalla data del 31 ottobre 2003, che la Commissione Europea presenti al Parlamento ed al Consiglio *"una relazione sull'applicazione della presente direttiva"* e sul *"relativo impatto sugli operatori economici e sui consumatori"*, si prevede che tale relazione indaghi *"in particolare"* l'impatto delle *"disposizioni sulle comunicazioni indesiderate"* : un'ennesima conferma, se mai ce ne fosse stato bisogno, della sempre delicata diatriba attinente al trattamento dei dati personali ed alle comunicazioni commerciali non sollecitate.

di Pietro Morelli

ICT Business Analyst

Autore del sito "Strategia sul Web" (www.strategiaweb.info)