

CONSIGLIO D'EUROPA

**RACCOMANDAZIONE N. R (99) 5
DEL COMITATO DEI MINISTRI AGLI STATI MEMBRI
PER LA PROTEZIONE DELLA PRIVACY SU INTERNET**

LINEE-GUIDA

**per la protezione delle persone rispetto alla raccolta e al trattamento
di dati personali sulle autostrade dell'informazione**
*(adottate dal Comitato dei Ministri il 23 febbraio 1999
nel corso della 660ma riunione dei Delegati dei Ministri)*

Preambolo

Il Comitato dei Ministri, ai sensi dell'articolo 15.b dello Statuto del Consiglio d'Europa,

Considerando che scopo del Consiglio d'Europa è quello di realizzare un'unione più stretta fra i suoi membri;

Rilevando lo sviluppo delle nuove tecnologie e dei nuovi servizi di comunicazione e di informazione on-line;

Consapevole che tale sviluppo influirà notevolmente sul funzionamento della società in genere e sui rapporti fra le persone, in particolare offrendo possibilità ulteriori di comunicazione e di scambio di informazioni sul piano nazionale e internazionale;

Consapevole dei vantaggi che gli utilizzatori delle nuove tecnologie possono ricavare da tale sviluppo;

Ritenendo, comunque, che lo sviluppo delle tecnologie e la generalizzazione della raccolta e del trattamento di dati personali sulle autostrade dell'informazione comportino rischi per la privacy delle persone fisiche;

Ritenendo che gli sviluppi tecnologici permettano anche di contribuire al rispetto dei diritti e delle libertà fondamentali, e in particolare del diritto alla privacy, all'atto del trattamento di dati personali relativi a persone fisiche;

Consapevole della necessità di mettere a punto tecniche che consentano l'anonimato degli interessati e la segretezza delle informazioni scambiate attraverso le autostrade dell'informazione, nel rispetto dei diritti e delle libertà altrui e dei valori di una società democratica;

Consapevole che le comunicazioni effettuate con l'ausilio delle nuove tecnologie dell'informazione è egualmente soggetta al rispetto dei diritti dell'uomo e delle libertà fondamentali, e in particolare del diritto al rispetto della privacy e della segretezza della corrispondenza, così come sanciti dall'articolo 8 della Convenzione europea dei diritti dell'uomo;

Riconoscendo che la raccolta, il trattamento e in particolare la comunicazione di dati personali attraverso le nuove tecnologie dell'informazione, e in particolare attraverso le autostrade dell'informazione, sono regolati dalle disposizioni della Convenzione per la protezione delle persone rispetto al trattamento automatico di dati personali (Strasburgo 1981, ETS N. 108) e da raccomandazioni settoriali in materia di protezione dei dati, e in particolare dalla Raccomandazione N. R (90) 19 sulla protezione dei dati personali utilizzati per finalità di pagamento e altre finalità correlate, dalla Raccomandazione N. R (91) 10 sulla comunicazione a terzi di dati personali detenuti da soggetti pubblici e dalla Raccomandazione N. R (95) 4 sulla protezione dei dati personali nel settore delle telecomunicazioni, con particolare riferimento ai servizi telefonici;

Ritenendo che sia opportuno sensibilizzare utilizzatori e fornitori di servizi Internet in merito alle disposizioni generali della Convenzione prima ricordata relativamente alla raccolta e al trattamento di dati personali sulle autostrade dell'informazione;

Raccomanda ai governi degli Stati membri di dare ampia diffusione alle Linee-guida contenute nell'allegato alla presente Raccomandazione, in particolare presso gli utilizzatori ed i fornitori di servizi su Internet, nonché presso tutte le autorità nazionali incaricate di verificare il rispetto delle disposizioni in materia di protezione dei dati.

Allegato

alla Raccomandazione N. R (99) 5 del Comitato dei Ministri agli Stati membri

per la protezione della privacy su Internet

Linee-guida per la protezione delle persone rispetto

alla raccolta ed al trattamento di dati personali sulle autostrade dell'informazione

eventualmente da inserire in o allegare a codici deontologici

I. INTRODUZIONE

Le presenti linee-guida enunciano i principi di una prassi corretta in materia di privacy per gli utenti ed i fornitori di servizi Internet (FSI).¹ Questi principi possono essere ripresi nell'ambito di codici deontologici.

Gli utenti dovrebbero essere a conoscenza delle responsabilità dei fornitori di servizi Internet (FSI), e viceversa. Pertanto, è opportuno che utenti e fornitori di servizi leggano il testo nella sua interezza, anche se per facilitarne l'impiego esso si presenta suddiviso in più parti. Possono risultare pertinenti le linee-guida di una sola parte ovvero di più parti.

L'uso di Internet comporta responsabilità per ciascuna delle vostre azioni ed implica inoltre rischi per la privacy. E' importante adottare comportamenti che offrano protezione a voi e favoriscano rapporti positivi con gli altri. In questo documento vengono offerti alcuni suggerimenti pratici per tutelare la privacy, ma dovrete conoscere anche i diritti e gli obblighi cui siete legalmente soggetti.

Ricordate che il rispetto per la privacy è un diritto fondamentale delle persone che può essere tutelato per legge, e in particolare attraverso norme per la protezione dei dati, per cui può essere senz'altro il caso di verificare la vostra situazione giuridica.

II. PER GLI UTENTI

1. Ricordate che Internet non è sicuro. Tuttavia, esistono e vengono continuamente messi a punto strumenti che permettono di migliorare la protezione dei vostri dati². Utilizzate dunque tutti gli strumenti disponibili per proteggere i vostri dati e le vostre comunicazioni, ad esempio le forme legalmente ammesse di cifratura per garantire la segretezza della posta elettronica e codici di accesso per il vostro personal computer³.

2. Ricordate che ogni transazione compiuta, ogni sito visitato su Internet lascia una traccia. Queste "tracce elettroniche" possono essere utilizzate, a vostra insaputa, per generare un profilo delle vostre caratteristiche e dei vostri interessi. Se non desiderate la creazione di tali profili, siete invitati ad utilizzare gli strumenti tecnici più recenti che

¹ V. Parte IV, primo paragrafo.

² Il termine "dati" è riferito ai "dati personali" e indica qualunque informazione riguardante voi o altre persone.

³ Ad esempio, utilizzate una parola-chiave e modificatela regolarmente.

prevedono la possibilità di venire informati ogniqualvolta si lascia una traccia, e di rifiutare queste tracce. Potete inoltre informarvi sulle politiche in materia di privacy dei singoli siti e programmi, preferendo quelli che registrano pochi dati o che sono accessibili in forma anonima.

3. La migliore forma di tutela della privacy è rappresentata dall'anonimato nell'accesso a e nell'utilizzazione di servizi, e dalla disponibilità di forme anonime di pagamento. Informatevi sulle possibilità tecniche per ottenere l'anonimato, laddove ciò sia opportuno⁴.

4. L'anonimato assoluto può non essere appropriato a causa di limitazioni di ordine giuridico. In tal caso, se la legge lo consente, potete utilizzare uno pseudonimo in modo che la vostra identità personale sia nota solo al vostro FSI.

5. Comunicate al vostro FSI, e ad ogni altro soggetto, solo i dati che sono necessari per una specifica finalità di cui siete stati messi al corrente. Fate particolare attenzione alle carte di credito e ai numeri di conto, che su Internet possono essere utilizzati anche in modi impropri con grande facilità.

6. Ricordate che il vostro indirizzo di posta elettronica costituisce un dato personale, e che altri potrebbero desiderare di utilizzarlo per scopi diversi - ad esempio per l'inserimento in annuari o elenchi di utenti. Non esitate a informarvi sulle finalità dell'annuario o di ogni altra utilizzazione. Potete chiedere che il vostro indirizzo sia cancellato se non desiderate figurare in un elenco.

7. Siate prudenti con i siti che chiedono dati aggiuntivi rispetto a quelli necessari per accedere al sito o compiere una determinata operazione, oppure che non vi dicono per quale motivo abbiano necessità di ottenere da voi questi dati.

8. Ricordate che siete legalmente responsabili per il trattamento dei dati, ad esempio in caso di caricamento o scaricamento illeciti, e che potete essere sempre rintracciati anche se vi servite di uno pseudonimo.

9. Non inviate messaggi di disturbo. Possono ritorcersi contro di voi ed avere conseguenze legali.

10. Il vostro FSI ha la responsabilità di compiere un utilizzo corretto dei dati. Chiedete al vostro FSI quali dati raccoglie, tratta e registra, in che modo e per quali finalità. Ripetete questa richiesta a intervalli regolari. Insistete affinché il vostro FSI modifichi i dati se non sono corretti, o li cancelli se sono eccessivi, non aggiornati o non più necessari. Chiedete al FSI di informare di queste modifiche le altre parti alle quali abbia comunicato i vostri dati.⁵

11. Se non siete soddisfatti del modo in cui il vostro attuale FSI raccoglie, utilizza, registra o comunica dati, e se il FSI rifiuta di modificare i propri comportamenti, prendete in considerazione la possibilità di rivolgervi ad un altro FSI. Se ritenete che il vostro FSI non rispetti le norme in materia di protezione dati, potete informare le autorità competenti oppure adire le vie legali.

⁴ Ad esempio, utilizzando posti pubblici Internet oppure carte d'accesso prepagate e carte di pagamento.

⁵ La legislazione in materia di protezione dei dati, conformemente all'art. 5 della Convenzione per la protezione dei dati elaborata dal Consiglio d'Europa, prevede che il soggetto che tratta i dati sia responsabile dell'esattezza e dell'aggiornamento dei dati stessi.

12. Tenetevi al corrente dei rischi per la privacy e la sicurezza su Internet e degli strumenti disponibili per ridurre tali rischi.

13. Se avete intenzione di inviare dati in un altro Paese, dovrete essere consapevoli del fatto che là essi possono godere di una protezione minore. Se si tratta di dati che vi riguardano, siete evidentemente liberi di trasmetterli in ogni caso. Tuttavia, prima di inviare in un altro Paese dati relativi ad altre persone, dovrete informarvi sulla possibilità di effettuare il trasferimento in questione⁶ - ad esempio, presso le autorità competenti nel vostro Paese. Potrebbe essere necessario chiedere al destinatario di adottare le misure⁷ necessarie a garantire la protezione dei dati.

III. PER I FORNITORI DI SERVIZI SU INTERNET

1. Utilizzate le procedure corrette e le tecnologie disponibili, preferibilmente quelle che sono oggetto di una certificazione, per tutelare la privacy degli interessati (anche se non utilizzano Internet), in particolare garantendo l'integrità e la segretezza dei dati nonché la sicurezza fisica e logica della rete e dei servizi forniti sulla rete.

2. Informate gli utenti dei rischi per la privacy associati all'utilizzo di Internet prima che essi si mettano in lista per un servizio o lo utilizzino. Può trattarsi di rischi per l'integrità dei dati, la segretezza, la sicurezza della rete oppure di altri rischi per la privacy quali la raccolta o la registrazione occulte di dati.

3. Informate gli utenti degli strumenti tecnici che possono legittimamente utilizzare per ridurre i rischi a carico della sicurezza dei dati e delle comunicazioni, quali le forme di cifratura e di firma digitale ammesse dalla legge. Offrite questi strumenti tecnici ad un prezzo definito dai costi effettivi e non dissuasivo.

4. Prima di accettare abbonamenti e di collegare utenti a Internet, informateli delle possibilità di accedere in modo anonimo ad Internet, e di utilizzarne e pagarne i servizi mantenendo l'anonimato (ad esempio, attraverso carte di accesso prepagate). Talora l'anonimato totale non è indicato a causa di limitazioni di legge. In casi del genere, se la legge lo consente, offrite la possibilità di utilizzare pseudonimi. Informate gli utenti sui programmi che permettono di effettuare ricerche e navigare sul Web in modo anonimo. Configurate il vostro sistema in modo da evitare o ridurre al minimo l'utilizzazione di dati personali.

5. Non leggete, modificate o cancellate messaggi inviati ad altri.

6. Non permettete alcuna ingerenza nel contenuto di comunicazioni, a meno che tale ingerenza sia prevista dalla legge ed attuata da una pubblica autorità.

7. Raccogliete, trattate e registrate dati personali relativi agli utenti solo se ciò è necessario per scopi espliciti, specifici e legittimi.

⁶ La legislazione di numerosi Paesi europei proibisce il trasferimento verso Paesi che non garantiscano un livello di protezione dei dati adeguato o equivalente a quello del vostro Paese. Sono comunque previste alcune eccezioni, in particolare se l'interessato ha acconsentito al trasferimento dei propri dati verso un Paese del tipo suddetto.

⁷ Può trattarsi di garanzie sviluppate e/o presentate, in particolare nell'ambito del contratto che regola il flusso transfrontaliero dei dati.

8. Non comunicate dati a terzi se non nei casi previsti dalla legge⁸.
9. Non conservate i dati per un periodo superiore a quello necessario per realizzare le finalità del trattamento⁹.
10. Utilizzate dati personali per i vostri scopi promozionali o di marketing solo se l'interessato, una volta informato, non vi si è opposto oppure, nel caso del trattamento di dati relativi al traffico o di dati sensibili, ha dato il proprio consenso esplicito.
11. Siete responsabili dell'utilizzo corretto dei dati. Indicate in modo chiaro e visibile la vostra politica in materia di privacy sulla pagina iniziale del sito. Tale indicazione dovrebbe consentire di accedere, attraverso un legame ipertestuale, ad una spiegazione dettagliata della prassi adottata in materia di privacy. Prima che l'utente inizi a utilizzare i servizi disponibili, all'atto di visitare il vostro sito e ogniqualvolta ne faccia richiesta, informatelo sulla vostra identità, sui dati che raccogliete, trattate e conservate, sulle modalità relative, le finalità e il periodo di conservazione. Se occorre, chiedete il suo consenso. Su richiesta dell'interessato, correggete senza indugio i dati inesatti, cancellateli se sono eccessivi, non più aggiornati o non più necessari, e bloccate il trattamento dei dati se l'utente vi si oppone. Informate di qualsiasi modifica i terzi ai quali avete comunicato i dati. Evitate di raccogliere dati in modi occulti.
12. Le informazioni fornite agli utenti devono essere accurate e aggiornate.
13. Pensateci due volte prima di pubblicare dati sul vostro sito! Così facendo potreste violare la privacy altrui e forse commettereste un reato.
14. Prima di inviare dati in un altro Paese, informatevi sull'ammissibilità del trasferimento - ad esempio presso le autorità competenti nel vostro Paese¹⁰. Potrebbe essere necessario chiedere al destinatario di fornire garanzie indispensabili a garantire la protezione dei dati¹¹.

IV. CHIARIMENTI E MEZZI DI TUTELA

1. Quando nel presente testo si utilizza il termine "fornitore di servizio", esso si intende riferito, se del caso, anche agli altri operatori su Internet - fornitori di accesso, di contenuti, gestori di rete, ideatori dei programmi di navigazione, moderatori di gruppi di discussione, ecc. .
2. E' importante che vi assicuriate del rispetto dei vostri diritti. I meccanismi di feedback offerti da gruppi di utenti di Internet, associazioni di fornitori di servizi Internet, autorità di protezione dati o altri soggetti sono strumenti importanti per garantire il rispetto

⁸ In genere la legislazione in materia di dati personali consente la comunicazione a terzi nel rispetto di specifiche condizioni, e in particolare

- per quanto riguarda dati sensibili e dati sul traffico, purché l'interessato abbia dato esplicitamente il proprio consenso;
- per quanto riguarda gli altri dati, se la comunicazione è necessaria per raggiungere la finalità legittima perseguita ovvero se l'interessato, dopo esserne stato informato, non vi si è opposto.

⁹ Ad esempio, non conservate dati relativi alla fatturazione se ciò non è previsto dalla legge.

¹⁰ V. nota 6.

¹¹ V. nota 7.

delle presenti linee-guida. Contattate questi soggetti se avete bisogno di chiarimenti o di mezzi di tutela.

3. Le presenti linee-guida si applicano a tutte le autostrade informatiche.