4. Lo scambio di informazioni nel quadro della cooperazione di polizia, basato sulle informazioni contenute negli archivi nazionali, è disciplinato dalla legislazione del paese interessato e, in particolare, dalla legge sulla protezione dei dati.

5.9.5 Parere n 98/4 - Registrazione delle consultazioni di cui all'art. 103 della Convenzione [109)]

BPh/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 70 riv.
Traduzione: orig.\DE

Parere n. 98/4 dell'Autorità di controllo comune destinato al Comitato esecutivo

OGGETTO: Registrazione delle consultazioni di cui all'articolo 103 della Convenzione

L'Autorità di controllo comune,

Visto l'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen;

Consapevole del fatto che il Sistema d'Informazione Schengen (SIS) è un sistema di ricerca automatizzato che richiede un'efficace protezione contro l'accesso non autorizzato da parte di terzi,

che la registrazione di una media rappresentativa delle consultazioni del sistema effettuate costituisce un mezzo di protezione adeguato contro l'accesso non autorizzato,

che l'articolo 103 CSCH impone a ciascuna Parte contraente di provvedere affinché una trasmissione in media su dieci di dati personali sia registrata nella sezione nazionale del Sistema d'Informazione Schengen dall'organo di gestione dell'archivio, ai fini del controllo dell'ammissibilità dell'interrogazione,

ritiene necessarie le seguenti esigenze minime per quanto concerne una regolare registrazione ai sensi dell'art. 103 CSCH:

1. Deve essere registrata una media sufficientemente rappresentativa di tutte le consultazioni, a prescindere dal fatto che alla relativa interrogazione venga data una risposta positiva o negativa. L'esigenza minima della registrazione del 10% può essere rispettata anche mediante una registrazione ad intervalli regolari.

2. Fanno parte degli elementi essenziali di un'adeguata registrazione:

a) generalità trasmesse della persona oggetto della consultazione,

b) identificazione del terminale utilizzato o dell'autorità che ha proceduto all'interrogazione, badando a che siano adottate tutte le misure utili per consentire l'identificazione dell'utente,

c) luogo, data e ora della consultazione,

d) motivo della consultazione, per es. indicazione del fondamento giuridico di una segnalazione.

[109)] Documento anticipato nella *Relazione per l'anno 1997*.

3. Ai fini di un controllo, in singoli casi, dell'ammissibilità della consultazione sarebbe inoltre auspicabile indicare il riferimento del dossier o il numero di base, se disponibile.

4. I dati sono utilizzati esclusivamente ai fini previsti dall'art. 103.

5. I dati registrati vanno cancellati entro 6 mesi.

L'ACC insiste affinché si tenga conto dell'obbligo previsto dall'art. 103 in conformità del presente parere.

5.9.6 Relazione sulla sicurezza degli uffici SIRENE

/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 11 dicembre 1998
SCH/Aut-cont (98) 47, 2ª rev.
Traduzione: orig./FR-PT

Progetto
Relazione dell'ACC sulla sicureza degli uffici SIRENE

In occasione della riunione del 12 dicembre 1997, l'Autorità di controllo comune ha deciso di procedere alla verifica delle misure di sicurezza messe in atto dagli Uffici SIRENE. Tale decisione è stata adottata in seguito alla fuga di documenti avvenuta tempo addietro in un Ufficio SIRENE.

Tutti i membri dell'ACC dei paesi che applicano la Convenzione hanno quindi effettuato controlli nei rispettivi uffici SIRENE e hanno trasmesso la loro relazione al Segretariato dell'ACC, i cui membri hanno annunciato che avrebbero presentato una relazione complementare.

Le relazioni delle autorità nazionali descrivono la situazione nei settori della sicurezza fisica e delle comunicazioni tra l'ufficio SIRENE e l'N.SIS; descrivono inoltre le funzioni di tracciatura, che consentono, non solo di rintracciare l'ufficio e il terminale, ma anche di identificare l'operatore che ha utilizzato un applicativo (ad esempio per un aggiornamento), nonché le condizioni di accesso ai dati del SIS e agli archivi manuali [110].

Alla luce delle precedenti constatazioni, l'ACC conclude che sono stati prodigati sforzi al fine di migliorare la sicurezza del sistema ma che questi devono proseguire.

L'ACC richiama infatti i seguenti principi:

– gli uffici SIRENE devono soddisfare tutte le condizioni contemplate all'articolo 118 della Convenzione di applicazione di Schengen;

– il livello di sicurezza degli uffici SIRENE nazionali non può essere inferiore a quello del SIS.

Premesso ciò, l'ACC propone che negli Stati dove tali principi non sono ancora applicati vadano prese le seguenti disposizioni:

1. mantenimento della sicurezza fisica al massimo livello aggiornando le tecniche impiegate. Negli Stati in cui sono state constatate lacune, vanno apportate le modifiche necessarie quanto prima e va informata l'autorita di controllo nazionale;

---

[110] Trattasi delle relazioni SCH/Aut-cont (98) 9 della Francia, 13 e 40 del Belgio, 15 dell'Italia, 21 della Germania, 28 della Grecia, 31 del Portogallo, 33 dei Paesi Bassi, 35 della Spagna e 36 dell'Austria. La relazione sulla sicurezza dell'ufficio SIRENE lussemburghese figura nella relazione annuale dell'autorità di controllo lussemburghese e sarà completata prossimamente da una nuova relazione. Anche i Paesi Bassi comunicheranno fra breve una nuova relazione di controllo.

2. cifratura delle cornunicazioni tra il SIRENE e l'N.SIS e controllo della cifratura da parte dei membri delle autorità;

3. *a)* realizzazione di un sistema di tracciatura di tutte le operazioni possibili riguardanti la base di dati N.SIS e dell'ufficio SIRENE (numero di interrogazioni, orario, tipi di dati consultati, ecc.);

b) analisi regolare degli archivi di tracciatura al fine di individuare eventuali anomalie riguardo, in particolare, al numero di interrogazioni;

4. limitazione e controllo dell'accesso agli archivi manuali dei dossier;

5. cifratura delle informazioni contenute su supporto informatico;

6. *a)* intensificazione delle misure di sicurezza al fine di garantire che l'accesso sia effettivamente limitato ai dati per i quali gli operatori hanno un'autorizzazione, in particolare verificando regolarmente le loro autorizzazioni di accesso e modificando regolarmente le password;

b) verifica regolare dei motivi di una interrogazione del SIS;

7. designazione di un funzionario responsabile della sicurezza e definizione delle norme di sicurezza comuni ai vari uffici SIRENE, applicabili al loro personale;

8. organizzazione della gestione delle informazioni stampate in modo da limitare l'ottenimento di stampe dello schermo contenenti informazioni della base di dati SIRENE e di segnalazioni SIS;

9. *inserimento* dell'organizzazione di corsi di formazione incentrati sulla sicurezza dei dati per gli utenti degli uffici SIRENE;

10. raccomandazione dell'elaborazione da parte degli N.SIS e degli uffici SIRENE di relazioni sulla sicurezza, a intervalli regolari, per esempio ogni anno.

L'evoluzione futura del sistema di comunicazione dei dati tra gli Stati, per quanto riguarda in particolare lo sviluppo del SIS, dovrà obbligatoriamente tenere conto delle condizioni di sicurezza, qualunque sia il modello, centralizzato o non centralizzato, prescelto.

Infine, l'ACC sottolinea la cooperazione di tutte le autorità nazionali interessate ed esprime la sua soddisfazione per il fatto che questa operazione di verifica condotta in modo coordinato in tutti gli Stati ha contribuito a migliorare sensibilmente la sicurezza delle informazioni. Ciò è fondamentale per la fiducia dei cittadini e delle istituzioni democratiche nel funzionamento del Sistema Schengen.

5.9.7 Dichiarazione in occasione del 50° Anniversario della dichiarazione universale dei diritti dell'uomo

BPH/BG SCHENGEN IT

Autorità di controllo comune

Bruxelles, 11 dicembre 1998
SCH/Aut-cont (98) 66
Traduzione: orig./FR

b;Dichiarazione dell'Autorità di controllo comune di Schengen in occasione del 50° anniversario della Dichiarazione universale dei diritti dell'uomo

«In occasione del 50° anniversario della Dichiarazione universale dei diritti dell'Uomo, commemorata il 10 dicembre 1998, l'Autorità di controllo comune di Schengen riunitasi a Bruxelles l'11 dicembre esprime il suo impegno nella difesa dei diritti dei cittadini rispetto al sistema d'informazione Schengen, affermando così concretamente i grandi valori della libertà e dei diritti dell'Uomo sanciti dalla Dichiarazione universale».

5.10 Consiglio d'Europa

5.10.1 Raccomandazione n. 99 (5) - Linee guida per la protezione della *privacy* su Internet

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 sono egualmente soggette 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 e 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 E 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 e i fornitori di servizi Internet (FSI) [111]. 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*. È 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 dovreste 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.

---

[111] *V. Parte IV, primo paragrafo.*

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 dati [112]. 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 computer [113]

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 a utilizzare gli strumenti tecnici più recenti che 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 e nell'utilizzazione di servizi, e dalla disponibilità di forme anonime di pagamento. Informatevi sulle possibilità tecniche per ottenere l'anonimato, laddove ciò sia opportuno [114].

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 e 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

---

[112] Il termine «dati» è riferito ai «dati personali» e indica qualsiasi informazione riguardante voi o altre persone.

[113] Ad esempio, utilizzate una parola-chiave e modificatela regolarmente.

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

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 [115].

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 a 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.

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, dovreste 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, dovreste informarvi sulla possibilità di effettuare il trasferimento in questione [116] - ad esempio, presso le autorità competenti nel vostro Paese. Potrebbe essere necessario chiedere al destinatario di adottare le misure [117] 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 a 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 a 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 utiliz-

---

[115] 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.

[116] 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.

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

zare 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.

8. Non comunicate dati a terzi se non nei casi previsti dalla legge [118].

9. Non conservate i dati per un periodo superiore a quello necessario per realizzare le finalità del trattamento [119].

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, a 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 Paese. Potrebbe essere necessario chiedere al destinatario di fornire garanzie indispensabili a garantire la protezione dei dati.

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.

---

[118] *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.

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

2. È importante che vi assicuriate del rispetto dei vostri diritti. I meccanismi di *feed-back* 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 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.

5.10.2 Schema di raccomandazione - Protezione dei dati personali raccolti e trattati per scopi assicurativi

Schema di raccomandazione sulla protezione dei dati personali raccolti e trattati per scopi assicurativi

In previsione della 18ma riunione del Bureau del CJ-PD - 19/21 gennaio 1999

Preambolo

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

1. Considerando che lo scopo del Consiglio di Europa è quello di realizzare una unione più stretta fra i suoi membri;

2. Richiamandosi ai principi generali relativi alla protezione dei dati contenuti nella Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati personali, e in particolare all'articolo 6 di tale Convenzione, in cui si afferma che i dati personali classificati come sensibili non possono essere sottoposti a trattamento se il diritto interno non prevede garanzie appropriate;

3. Consapevole del fatto che il trattamento automatizzato di dati personali per scopi assicurativi trova crescente diffusione, non solo per la preparazione, la stipula, l'esecuzione e la risoluzione di contratti assicurativi, ma anche per facilitare la gestione razionale ed economica delle assicurazioni e per la lotta alle frodi;

4. Consapevole del fatto che le assicurazioni sono fornite da vari soggetti economici, in particolare da compagnie assicurative;

5. Convinto dell'importanza che la qualità, l'integrità e la disponibilità dei dati personali rivestono per gli assicurati;

6. Rilevando che in pratica l'intera popolazione degli Stati membri è interessata da uno o più contratti assicurativi, e che per tale motivo i professionisti nel campo delle assicurazioni sono in possesso di una grande quantità di dati personali, alcuni dei quali sensibili;

7. Convinto dell'opportunità di regolamentare la raccolta e il trattamento di dati personali per scopi assicurativi, di garantire segretezza e sicurezza di tali dati personali e di verificare che ne venga compiuto un uso rispettoso dei diritti e delle libertà fondamentali dell'individuo, e in particolare del diritto alla riservatezza;

8. Tenendo conto del fatto che la mobilità dei singoli e la globalizzazione dei mercati e delle attività commerciali impongono lo scambio transfrontaliero di informazioni anche nel settore assicurativo, e richiedono una protezione dei dati equivalente in tutti gli Stati membri del Consiglio d'Europa,

RACCOMANDA AI GOVERNI DEGLI STATI MEMBRI:

1. di prendere provvedimenti affinché i principi contenuti nell'allegato alla presente Raccomandazione siano rispecchiati dal diritto interno e dalle prassi rispettive;

2. di assicurare un'ampia diffusione dei principi contenuti nell'allegato alla presente Raccomandazione presso tutte le persone, le pubbliche autorità e tutti gli enti pubblici o privati che raccolgono e trattano dati personali per scopi assicurativi, nonché presso gli enti competenti in materia di protezione dei dati;

3. di promuovere l'accettazione e l'attuazione dei principi contenuti nell'allegato alla presente Raccomandazione, in particolare attraverso l'adozione di disposizioni di legge o favorendo la definizione di un codice deontologico.

Decide che la Raccomandazione N. 86(1), sulla protezione di dati personali utilizzati per scopi di previdenza sociale, si applica alla raccolta ed al trattamento di dati per scopi di previdenza sociale nella misura in cui essi non siano regolamentati dalla presente Raccomandazione.

ALLEGATO

1. DEFINIZIONI

Ai fini della presente Raccomandazione:

a) per «dati personali» si intendono tutte le informazioni riguardanti una persona fisica identificata o identificabile («interessato»). Una persona fisica non si considera identificabile se tale identificazione richiede tempi e attività non ragionevoli.

b) per «dati sensibili» si intendono dati personali che rivelino l'origine razziale, le opinioni politiche, le fedi religiose o di altra natura, nonché i dati personali relativi alla salute, alla vita sessuale o alle condanne penali, e ogni altro dato definito sensibile ai sensi del diritto interno.

c) per «dati genetici» si intendono tutti i dati, indipendentemente dalla tipologia, che riguardano i caratteri ereditari di un individuo o le modalità di trasmissione di tali caratteri nell'ambito di un gruppo di individui legati da vincoli di parentela.

d) per «dati assicurativi» si intendono tutti i dati personali raccolti e trattati a scopi assicurativi.

e) l'espressione «per scopi assicurativi» comprende tutte le operazioni che comportano la raccolta e il trattamento di dati personali relativi alla preparazione, all'esecuzione e alla risoluzione di un contratto assicurativo.

f) per «trattamento» si intende ogni operazione o insieme di operazioni effettuate in tutto o in parte con l'ausilio di procedure automatizzate e applicate a dati personali, quali la registrazione, la conservazione o alterazione, l'estrazione, la consultazione, l'utilizzazione, la comunicazione, la comparazione o interconnessione e la cancellazione o la distruzione.

g) per «comunicazione» si intende l'atto di rendere dati personali accessibili a terzi, indipendentemente dagli strumenti o dai supporti utilizzati.

h) per «titolare dei dati assicurativi» si intende la persona fisica o giuridica, la pubblica autorità, l'organismo od ogni altro ente che, da solo o congiuntamente con altri, definisce le finalità e i metodi della raccolta e del trattamento di dati assicurativi.

2. CAMPO DI APPLICAZIONE

2.1 La presente Raccomandazione si applica alla raccolta e al trattamento di dati assicurativi.

2.2 Gli Stati membri sono invitati ad estendere l'applicazione della presente Raccomandazione al trattamento non automatizzato di dati personali per scopi assicurativi.

2.3 Non si devono sottoporre dati personali a trattamenti non automatizzati per evitare l'applicazione dei principi stabiliti nella presente Raccomandazione.

2.4 Gli Stati membri possono estendere i principi sanciti nella presente Raccomandazione alla raccolta e al trattamento di dati relativi a gruppi di persone, associazioni, fondazioni, società, società per azioni e ogni altro ente costituito direttamente o indirettamente da persone fisiche, indipendentemente dal fatto che tali enti siano dotati di personalità giuridica.

2.5 Gli Stati membri possono estendere i principi sanciti nella presente Raccomandazione alla protezione dei dati personali utilizzati per scopi di previdenza sociale.

3. Rispetto per la vita privata

3.1. Durante la raccolta ed il trattamento di dati personali occorre garantire il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata.

3.2. Le persone che, nel corso di un'attività assicurativa, hanno accesso a dati personali devono, conformemente al diritto e alla prassi interni, sottostare a norme di segretezza. In particolare, la raccolta ed il trattamento di dati sanitari devono essere effettuati unicamente da professionisti in campo sanitario, ovvero in conformità a norme di segretezza paragonabili a quelle applicabili ai professionisti in campo sanitario o in conformità a garanzie di pari efficacia previste dal diritto interno.

4. Raccolta e trattamento di dati assicurativi

4.1 La raccolta e il trattamento (compresa la comunicazione) di dati assicurativi sono effettuati in modo corretto e legittimo ed esclusivamente per specifici scopi assicurativi, tranne nei casi previsti ai principi 4.10 e 8.1. I dati assicurativi devono essere adeguati, esatti, pertinenti e non eccessivi in rapporto agli scopi per i quali sono raccolti o successivamente trattati.

4.2. In linea di principio, i dati assicurativi sono raccolti presso l'interessato o il suo rappresentante legale.

Legittimità

4.3 La raccolta ed il trattamento di dati assicurativi sono consentiti:

a) se ciò è previsto da norme di legge, in particolare ai fini dell'assicurazione obbligatoria;

b) per la conclusione, l'esecuzione e la risoluzione di un contratto assicurativo stipulato con l'interessato, e per la preparazione di tale contratto su richiesta dell'interessato;

c) se l'interessato o il suo rappresentante legale o un'autorità od ogni altra persona o ente indicati per legge hanno dato il consenso per uno o più scopi assicurativi, e nella misura in cui ciò non contrasti con le norme di diritto interno; ovvero

d) se i dati sono necessari per il perseguimento degli interessi legittimi del titolare dei dati assicurativi, nella misura in cui non prevalgano gli interessi dell'interessato.

Scopi

4.4. Salvo quanto disposto ai punti da 4.6 a 4.11, la raccolta ed il trattamento di dati assicurativi sono consentiti esclusivamente per i seguenti scopi:

a) preparazione ed emissione di un contratto assicurativo;

b) raccolta di premi e altre forme di fatturazione;

c) regolamento crediti o pagamento di altri benefici/indennità;

d) riassicurazioni;

e) assicurazioni congiunte;

f) prevenzione, accertamento e/o perseguimento di frodi;

g) affermazione, esercizio o difesa di un diritto in sede giudiziaria;

h) adempimento di un altro specifico obbligo giuridico o contrattuale; ovvero

i) gestione interna di un'impresa di assicurazioni;

[*j)* attività attuariali].

Nascituri

4.5. I dati assicurativi relativi a nascituri dovrebbero essere considerati dati personali e godere di una protezione paragonabile a quella riservata ai dati assicurativi di minori.

Dati sensibili

4.6. La raccolta e il trattamento di dati sensibili dovrebbero essere vietati, a meno che, per uno degli scopi indicati al punto 4.4.:

a) l'interessato abbia dato esplicitamente il consenso, nella misura in cui ciò non contrasti con le disposizioni del diritto interno; ovvero

b) ciò sia consentito dalla legge e

i) il trattamento sia necessario per l'adempimento di obblighi specifici del titolare; ovvero

ii) il trattamento sia necessario per l'affermazione, l'esercizio o la difesa di un diritto in sede giudiziaria;

c) ciò sia previsto dalla legge, o un'autorità ai sensi del punto 15.1. lo consenta per motivi di rilevante interesse pubblico.

4.7. [Salvo quanto previsto al punto 4.9, i dati genetici non possono essere sottoposti a trattamento per scopi assicurativi]

4.8. [Se il diritto interno lo prevede e offre garanzie adeguate, un assicuratore può, prima di concludere un'assicurazione non obbligatoria, chiedere all'interessato di comunicare i risultati di un'analisi genetica cui si sia già sottoposto, qualora:

a) i risultati si riferiscano ad una specifica analisi genetica;

b) siano stati definiti l'affidabilità ed il valore attuariale dei risultati;

c) la copertura assicurativa sia elevata; e

d) la conoscenza dei risultati possa limitare la copertura assicurativa offerta].

[La raccolta ed il trattamento di dati genetici sono effettuati da consulenti sanitari, i quali si limitano a trasmettere all'assicuratore le conclusioni raggiunte].

4.9. La raccolta ed il trattamento di dati personali relativi a procedimenti penali o condanne penali è consentita unicamente se i dati sono necessari e strettamente connessi a casi di frode, alla concessione di assicurazioni o al pagamento di risarcimenti o altre indennità [e nella misura in cui il trattamento sia conforme a garanzie adeguate previste dal diritto interno].