

92

Livello di tutela dei dati in Australia (*)

AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

Parere dell'ACC in merito al livello di protezione dei dati in Australia

All'attenzione de:

il presidente del

Consiglio di amministrazione dell'Europol

Sig. Rob Wainwright

L'Aia

Paesi Bassi

DOCUMENTO 05/35

AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

A. Osservazioni introduttive

1. L'ACC è stata incaricata di elaborare un parere in merito alle leggi e alla prassi amministrativa dell'Australia nel settore della protezione dei dati, sulla base della relazione fascic. n. 2644-01 datata del 12 settembre 2005.
2. Detta relazione è stata sottoposta all'esame dell'ACC dal consiglio di amministrazione dell'Europol, in conformità dell'articolo 1, paragrafo 5, della decisione del Consiglio che autorizza il direttore dell'Europol ad avviare negoziati per la conclusione di accordi con Stati terzi ed organismi non connessi all'Unione europea.
3. Ai sensi dell'articolo 3, paragrafo 3, seconda parte, delle norme per la trasmissione di dati di carattere personale a Stati ed organismi terzi, l'ACC è altresì chiamata a formulare un parere durante la procedura in cui il Consiglio dell'Unione europea deve decidere se approvare o meno un accordo tra l'Europol e l'Australia. L'ACC fa notare che il presente parere riguarda unicamente l'eventuale esistenza di ostacoli all'avvio dei negoziati tra l'Europol e l'Australia suscettibili di condurre al raggiungimento di un accordo sulla trasmissione di dati di carattere personale all'Australia da parte dell'Europol.

(*) [doc. web n. 1296464]

27^{ma} Conferenza dei Garanti privacy

93 Dichiarazione di Montreux (*)

DICHIARAZIONE DI MONTREUX

**“La protezione dei dati personali e della privacy in un mondo globalizzato:
un diritto universale che rispetta le diversità”**

L'Autorità federale svizzera per la protezione dei dati, con il sostegno dell'Incaricato federale tedesco per la protezione dei dati, dell'Agenzia spagnola per la protezione dei dati, dell'Ispettore generale per la protezione dei dati personali della Polonia, del Commissario per la privacy della Nuova Zelanda, del Commissario per la privacy del Canada, del Garante europeo per la protezione dei dati, del Commissario per la privacy di Hong Kong, dell'Ispettorato statale per la protezione dei dati della Lituania, dell'Autorità olandese per la protezione dei dati, dell'Ufficio per la protezione dei dati della Repubblica Ceca, dell'Autorità italiana per la protezione dei dati personali, del Commissario per la privacy di Guernsey, del Commissario per la privacy di Victoria (Australia), dell'Incaricato per la protezione dei dati e la libertà di informazione della città di Berlino, del Commissario per la protezione dei dati del Cantone di Zug (Svizzera), propone l'adozione della seguente Dichiarazione:

Le Autorità per la protezione dei dati e della privacy riunite a Montreux in occasione della 27^{ma} Conferenza internazionale (14-16 settembre 2005) hanno stabilito di comune accordo di promuovere il riconoscimento della natura universale dei principi di protezione dei dati, ed hanno adottato la seguente Dichiarazione finale:

1. Facendo seguito alla dichiarazione adottata in occasione della 22^{ma} Conferenza internazionale delle Autorità per la protezione dei dati e della privacy, tenutasi a Venezia;
2. Richiamandosi alla Risoluzione sulla protezione dei dati e gli organismi internazionali adottata in occasione della 25^{ma} Conferenza internazionale delle Autorità per la protezione dei dati e della privacy, tenutasi a Sydney;
3. Riconoscendo che lo sviluppo della società dell'informazione è dominato dalla globalizzazione degli scambi di informazioni, dall'impiego di tecnologie per l'elaborazione dei dati di crescente invasività, e da un incremento delle misure di sicurezza;
4. Preoccupate per i rischi crescenti di sorveglianza pervasiva delle persone a livello mondiale;
5. Rilevando i benefici ed i rischi potenziali inerenti alle nuove tecnologie dell'informazione;
6. Preoccupate per le attuali disuguaglianze fra i sistemi giuridici nelle diverse parti del mondo, in particolare per l'assenza di misure a salvaguardia della protezione dei dati in alcune zone che compromette l'efficacia della protezione dei dati a livello globale;
7. Consapevoli che la rapida espansione delle conoscenze nel settore della genetica può fare del DNA umano il dato personale più sensibile in assoluto; consapevoli, inoltre, che questa accelerazione della conoscenza accresce l'importanza di un'adeguata tutela giuridica dei dati in oggetto;

(*) Montreux, 14-16
settembre 2005
[doc. web n. 1170512
vers. EN n. 1171231]

8. Ricordando che la raccolta ed il successivo trattamento di dati personali devono avvenire tenendo presenti i requisiti della protezione dei dati e della privacy;
9. Riconoscendo l'esigenza, in una società democratica, di combattere efficacemente il terrorismo e la criminalità organizzata, ma ricordando che questi obiettivi possono essere raggiunti nel migliore dei modi quando si rispettano i diritti umani, ed in particolare la dignità umana;
10. Convinte che il diritto alla protezione dei dati e della privacy rappresenti una condizione essenziale, in una società democratica, per garantire il rispetto dei diritti delle persone, la libera circolazione delle informazioni, ed un'economia di mercato aperta;
11. Convinte che il diritto alla protezione dei dati e della privacy rappresenti un diritto umano fondamentale;
12. Convinte dell'esigenza di rafforzare la natura universale di tale diritto al fine di ottenere il riconoscimento universale dei principi che disciplinano il trattamento di dati personali rispettando, al contempo, le diversità giuridiche, politiche, economiche e culturali;
13. Convinte dell'esigenza di garantire i diritti della persona a tutti i cittadini del mondo senza discriminazioni di sorta, indipendentemente dal luogo e dal momento in cui i dati personali che li riguardano sono sottoposti a trattamento;
14. Ricordando che il Vertice Mondiale sulla Società dell'Informazione tenutosi a Ginevra nel 2003 ha sottolineato, nella Dichiarazione sui principi ed il programma d'intervento, l'importanza della protezione dei dati e della privacy ai fini dello sviluppo della società dell'informazione;
15. Ricordando la Raccomandazione formulata dall'International Working Group on Data Protection in Telecommunications di tenere presente il Decalogo elaborato nel 2000, al fine di tutelare la privacy nell'ambito di accordi multilaterali in materia di privacy;
16. Riconoscendo che i principi di protezione dei dati discendono da strumenti giuridici internazionali a carattere sia vincolante sia non vincolante, quali le Linee-Guida dell'OCSE in materia di protezione della privacy e dei flussi transfrontalieri di dati personali, la Convenzione del Consiglio d'Europa per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali, le Linee-Guida ONU relative agli archivi di dati personali informatizzati, la Direttiva dell'Unione Europea 95/46 sulla protezione delle persone fisiche con riguardo al trattamento di dati personali ed alla libera circolazione di tali dati, e l'Accordo-quadro in materia di privacy nell'ambito della cooperazione economica Asia-Pacifico;
17. Ricordando che i principi in questione sono, in particolare, quelli di seguito indicati:
 - principio di liceità e correttezza nella raccolta e nel trattamento dei dati;
 - principio di accuratezza;
 - principio di finalità;
 - principio di proporzionalità;
 - principio di trasparenza;
 - principio di partecipazione individuale, in particolare la garanzia del diritto di accesso da parte della persona interessata;
 - principio di non discriminazione;
 - principio di sicurezza dei dati;
 - principio di responsabilità;
 - principio del controllo indipendente e dell'esistenza di sanzioni previste per legge;
 - principio del livello adeguato di protezione in caso di flussi transfrontalieri di dati personali.

Alla luce di quanto precede,

Le Autorità per la protezione dei dati e della privacy esprimono l'intenzione di potenziare il riconoscimento internazionale della natura universale di tali principi. Stabiliscono di comune accordo di collaborare, in particolare, con i governi e gli organismi internazionali e sovranazionali al fine di mettere a punto una convenzione universale per la protezione delle persone fisiche rispetto al trattamento di dati personali.

A tal fine, le Autorità fanno appello:

- a. alle Nazioni Unite affinché preparino uno strumento giuridico vincolante che stabilisca in modo chiaro e specifico i diritti alla protezione dei dati e della privacy come diritti umani sanzionabili;
- b. a tutti i governi del mondo affinché promuovano l'adozione di strumenti giuridici in materia di protezione dei dati e della privacy conformi ai principi fondamentali della protezione dei dati, ed inoltre estendano tali principi ai rapporti reciproci;
- c. al Consiglio d'Europa perché, a norma dell'Articolo 23 della Convenzione per la protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali, inviti gli Stati che non sono membri del Consiglio d'Europa e già dispongono di normativa in materia di protezione dei dati ad aderire alla Convenzione ed al suo protocollo addizionale.

Inoltre, le Autorità invitano:

I Capi di Stato e di governo che converranno a Tunisi in occasione del Vertice mondiale sulla società dell'informazione (16-18 novembre 2005) ad inserire nella dichiarazione finale l'impegno a sviluppare o potenziare un quadro giuridico di riferimento che garantisca il diritto alla privacy ed alla protezione dei dati a tutti i cittadini nella società dell'informazione, coerentemente con l'impegno assunto dai Capi iberoamericani di Stato e di governo in occasione del Vertice di Santa Cruz (Bolivia) (novembre 2003) nonché dai Capi di Stato e di governo dei Paesi francofoni in occasione del Vertice di Ougadougou (novembre 2004).

Le Autorità fanno appello altresì:

- a. agli organismi internazionali e sovranazionali affinché si impegnino a rispettare principi che siano compatibili con i maggiori strumenti internazionali in materia di protezione dei dati e della privacy, ed in particolare ad istituire autorità di vigilanza indipendenti dotate di poteri di controllo;
- b. alle organizzazioni non governative internazionali, quali le associazioni di imprese e di consumatori, affinché mettano a punto standard basati sui principi fondamentali della protezione dei dati ovvero compatibili con tali principi;
- c. ai produttori di hardware e software affinché sviluppino prodotti e sistemi che incorporino tecnologie per il potenziamento della privacy.

Inoltre, le Autorità stabiliscono di comune accordo:

- a. di intensificare, in particolare, gli scambi di informazioni, il coordinamento delle rispettive attività di vigilanza, la definizione di standard comuni, la promozione delle informazioni relative alle attività ed alle risoluzioni di questa Conferenza;
- b. di promuovere la cooperazione con i Paesi che ancora non dispongono di autorità di vigilanza indipendenti in materia di protezione dei dati personali;
- c. di promuovere lo scambio di informazioni con organizzazioni non governative internazionali che si occupano di protezione dei dati e privacy;
- d. di collaborare con gli incaricati per la protezione dei dati nei vari enti;
- e. di creare un sito web permanente che funga, in particolare, da base comune per la gestione delle informazioni e delle risorse.

Le Autorità per la protezione dei dati e della privacy stabiliscono di valutare periodicamente la realizzazione degli obiettivi della presente Dichiarazione, ad iniziare dalla 28^{ma} Conferenza Internazionale nel 2006.

94

Risoluzione sull'utilizzo della biometria per passaporti, carte di identità e titoli di viaggio (*)

RISOLUZIONE SULL'UTILIZZO DELLA BIOMETRIA IN PASSAPORTI, CARTE DI IDENTITÀ E TITOLI DI VIAGGIO

L'Incaricato federale tedesco per la protezione dei dati e l'Incaricato per la protezione dei dati e la libertà di informazione della città di Berlino, con il sostegno della Direzione nazionale per la protezione dei dati dell'Argentina, dell'Autorità austriaca per la protezione dei dati, e dell'Autorità italiana per la protezione dei dati, propongono l'adozione della seguente Risoluzione:

La 27^{ma} Conferenza internazionale delle Autorità di protezione dei dati e della privacy adotta la presente Risoluzione:

Rilevando che governi e organismi internazionali, ed in particolare l'Organizzazione internazionale dell'aviazione civile (ICAO), stanno attualmente completando la definizione di norme e standard tecnici volti ad integrare dati biometrici (impronte digitali, riconoscimento del volto) in passaporti e titoli di viaggio ai fini della lotta al terrorismo e della velocizzazione dei controlli alle frontiere e delle procedure di imbarco;

Consapevole che anche il settore privato ricorre in misura crescente al trattamento di dati biometrici, prevalentemente su base volontaria;

Considerando che i dati biometrici possono essere raccolti all'insaputa dell'interessato, poiché quest'ultimo può lasciare tracce biometriche in modo inconsapevole;

Ricordando che la biometria consentirà la "lettura automatica" del corpo umano, e che i dati biometrici potrebbero essere utilizzati come identificatori univoci a livello globale;

Sottolineando che l'utilizzo diffuso della biometria avrà un effetto di lunga portata sulla società a livello globale e, pertanto, dovrebbe essere oggetto di un dibattito aperto a tutte le istanze globali;

La Conferenza chiede:

1. che si dia attuazione in fase precoce ad efficaci garanzie onde limitare i rischi inerenti alla natura della biometria;
2. che si tengano rigidamente distinti i dati biometrici raccolti e memorizzati per finalità di natura pubblica (ad esempio, i controlli alle frontiere) in base ad obblighi di legge, e quelli raccolti e memorizzati per finalità contrattuali sulla base del consenso;
3. che si limiti tecnicamente l'impiego della biometria in passaporti e carte di identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso.

(*) Montreux, 14-16
settembre 2005
[doc. web n. 1170552
vers. EN n. 1170622]

95

Risoluzione sull'utilizzo di dati personali per la comunicazione politica (*)

RISOLUZIONE SULL'UTILIZZO DI DATI PERSONALI PER LA COMUNICAZIONE POLITICA

**Presentata dall'Autorità italiana per la protezione dei dati
con il sostegno dell'Autorità federale svizzera per la protezione dei dati,
l'Autorità federale tedesca per la protezione dei dati,
l'Ispettore Generale per la protezione dei dati della Polonia,
il Commissario per la protezione dei dati della città di Berlino**

La Conferenza

Considerando che la comunicazione politica costituisce uno strumento fondamentale per la partecipazione di cittadini, forze politiche e candidati alla vita democratica, e riconoscendo l'importanza di una libera comunicazione politica quale diritto fondamentale;

Considerando che la condizione di cittadino presuppone il diritto di ottenere informazioni e di essere informati adeguatamente durante campagne elettorali politiche e amministrative; che tale diritto trova applicazione anche in riferimento ad altre materie, altri eventi e posizioni politiche utili al fine di compiere scelte informate su altri temi della vita politica: referendum, elezione di candidati, accesso alle informazioni detenute da organismi politici o provenienti da rappresentanti eletti;

Considerando che le forze politiche e, in generale, gli organismi politici ed i rappresentanti eletti ricorrono a vari strumenti di comunicazione e di finanziamento, a molteplici fonti di informazione, ed alle nuove tecnologie, per stabilire contatti diretti e personalizzati con le più diverse categorie di interessati;

Considerando che in un numero crescente di Paesi vi è la tendenza ad un'espansione della comunicazione istituzionale operata da candidati e soggetti eletti, anche a livello locale o attraverso forme di e-government; che queste attività, che talora necessitano il trattamento di dati personali, riflettono il diritto dei cittadini di essere informati sull'attività degli eletti di cui sopra;

Considerando che, in tale contesto, una mole considerevole di dati personali viene continuamente raccolta da organismi politici, ed è talora sottoposta a trattamento con modalità aggressive attraverso le più diverse tecniche quali sondaggi, raccolta di indirizzi di posta elettronica attraverso programmi o motori di ricerca, sollecitazioni di voto a livello di intere città, ovvero forme di decisione politica raggiunte attraverso la TV interattiva, o forme di profilazione degli elettori; che i dati in oggetto talora comprendono illecitamente (oltre a indirizzi postali, numeri di telefono, indirizzi di posta elettronica, informazioni sulle attività professionali ed il contesto familiare) dati sensibili relativi alle opinioni o attività morali e politiche, reali o ipotizzate, ovvero alle attività di voto;

Considerando l'esistenza di forme invasive di profilazione rispetto a persone che vengono classificate –talora in modo impreciso, o sulla base di contatti superficiali– come simpatizzanti, sostenitori, aderenti o iscritti al fine di potenziare la comunicazione personalizzata rivolta a singoli gruppi di cittadini;

Considerando che tali attività devono aver luogo secondo modalità lecite e corrette;

Considerando che è necessario tutelare i diritti e le libertà fondamentali degli interessati

(*) Montreux, 14-16
settembre 2005
[doc. web n. 1170546
vers. EN n. 1170616]

evitando, attraverso opportuni provvedimenti, indebite intrusioni, danni e costi a carico degli interessati stessi, in particolare effetti negativi e discriminazioni a livello della loro sfera personale ovvero la rinuncia ad alcune forme di partecipazione alla vita politica;

Considerando che tale tutela potrebbe essere conseguita tenendo conto del pertinente interesse pubblico connesso ad alcune attività di comunicazione politica, nonché di adeguate modalità e garanzie in rapporto alle comunicazioni interne rivolte a iscritti a partiti ovvero a semplici cittadini;

Considerando che, in tale contesto, è possibile promuovere attività responsabili di marketing senza limitare la circolazione di idee e proposte politiche, e che nonostante la comunicazione politica condivida talora molte delle caratteristiche delle attività promozionali, essa presenta alcuni tratti che la distinguono dal marketing per finalità commerciali;

Considerando l'esigenza di garantire il rispetto dei principi di protezione dei dati mettendo a punto uno standard minimo a livello globale che possa contribuire ad armonizzare i livelli di tutela degli interessati, anche sulla base di codici deontologici nazionali ed internazionali e tenendo conto delle soluzioni e delle norme specificamente individuate in vari Paesi;

Considerando che le autorità per la protezione dei dati possono svolgere un ruolo crescente nel pianificare interventi coordinati, anche in collaborazione con altre autorità di controllo competenti per i settori delle telecomunicazioni, dell'informatica, dei sondaggi elettorali, e delle attività elettorali;

**adotta
la seguente Risoluzione:**

Ogni attività di comunicazione politica che comporti il trattamento di dati personali, sia essa legata o meno a campagne elettorali, dovrebbe rispettare i diritti e le libertà fondamentali degli interessati, fra cui il diritto alla protezione dei dati personali, nell'osservanza di principi consolidati in materia, ed in particolare:

Principio di necessità

I dati personali dovrebbero essere oggetto di trattamento esclusivamente se ciò risulta necessario per il raggiungimento delle finalità per cui sono specificamente raccolti.

Liceità e correttezza della raccolta

La raccolta di dati personali dovrebbe avvenire attraverso fonti accessibili lecitamente, ed il trattamento dei dati dovrebbe essere effettuato in modo corretto. Si dovrebbe verificare che, ai sensi di legge, le fonti siano pubbliche ovvero siano utilizzabili esclusivamente per scopi specifici o secondo determinate modalità o per periodi limitati o in particolari occasioni.

È necessaria particolare attenzione qualora gli interessati siano contattati attraverso modalità aggressive.

Qualità dei dati

Nel corso del trattamento è necessario rispettare gli altri principi concernenti la qualità dei dati. In particolare, i dati dovrebbero essere accurati, pertinenti, non eccedenti e aggiornati in rapporto alle specifiche finalità per cui sono raccolti, soprattutto qualora le informazioni siano relative alle opinioni sociali o politiche, o alle convinzioni etiche, dell'interessato.

Principio di finalità

I dati personali ricavati da fonti, istituzioni o associazioni pubbliche o private possono essere utilizzati per scopi di comunicazione politica se il loro trattamento ulteriore è compatibile con le finalità per cui sono stati raccolti e di cui gli interessati sono già stati informati, in particolare qualora si tratti di dati sensibili. I rappresentanti eletti devono rispettare tali principi qualora utilizzino per scopi di comunicazione politica dati personali raccolti nell'esercizio delle rispettive funzioni istituzionali.

I dati personali raccolti originariamente per attività di marketing sulla base di un consenso informato possono essere utilizzati se le finalità di comunicazione politica sono menzionate specificamente nella dichiarazione di prestazione del consenso.

Proporzionalità

Il trattamento di dati personali dovrebbe avvenire esclusivamente attraverso modalità ed operazioni pertinenti agli scopi, particolarmente nel caso di dati relativi ad elettori potenziali o del confronto fra dati ricavati da archivi o banche dati di tipo diverso.

Il trattamento ulteriore di dati personali, soprattutto quelli conservati successivamente alla circostanza in rapporto alla quale sono stati raccolti, è ammissibile se le finalità perseguite dalla comunicazione politica sono in via di raggiungimento.

Informativa agli interessati

Prima di raccogliere il dato presso l'interessato, i destinatari devono ricevere un'informativa adeguata ai mezzi di comunicazione prescelti, in cui siano specificate l'identità del titolare (singoli candidati, responsabile esterno della campagna elettorale, associazione locale di sostenitori, o associazioni locali o di altro tipo; il partito politico nel suo insieme, ecc.) e le tipologie di flussi attese fra tali soggetti.

L'informativa dovrebbe essere fornita anche quando i dati non sono raccolti presso l'interessato, almeno nel caso in cui i dati non siano destinati ad essere conservati solo in via temporanea.

Consenso

Occorre verificare che il trattamento di dati personali si fondi sul consenso dell'interessato o su un altro presupposto legittimo previsto dalla legge. Il trattamento dovrebbe rispettare le norme specifiche in vigore nei singoli Paesi in rapporto alle fonti o ai mezzi di comunicazione utilizzati, in particolare per quanto riguarda gli indirizzi di posta elettronica, i numeri di fax, i messaggi SMS e/o altri messaggi di natura testuale o visiva ed i messaggi telefonici preregistrati.

Conservazione dei dati e misure di sicurezza

Ogni titolare, sia esso una forza politica o un singolo candidato, deve adottare tutte le misure di sicurezza di natura tecnica ed organizzativa necessarie a tutelare l'integrità delle informazioni raccolte ed a prevenire la perdita e/o l'utilizzo abusivo dei dati.

Diritti degli interessati

Agli interessati dovrebbero essere riconosciuti i diritti di accesso, rettifica, blocco e/o cancellazione nonché il diritto di opporsi alle comunicazioni indesiderate, e il diritto di chiedere, gratuitamente e con modalità semplici, di non ricevere ulteriori messaggi. L'esistenza di tali diritti dovrebbe essere menzionata nelle informative fornite agli interessati.

Dovrebbero essere previsti adeguati rimedi giuridici e sanzioni in caso di violazione dei diritti di cui sopra.

Conferenza di primavera 2005

96

Dichiarazione sulla lotta al terrorismo internazionale (*)

Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005

DECLARATION

Various initiatives at EU level aim to establish the European Union's objective of an area of freedom, security and justice. In its new multi annual programme - The Hague Programme - the Union reiterates the need to fight organised cross-border crime and to repress the threat of terrorism.

The 2005 Spring Conference of European Data Protection Authorities is well aware of the need for closer co-operation between law enforcement authorities, within the EU and with third States. At the same time it is evident that the 1981 Council of Europe Convention on data protection (Convention 108) applicable in the Union and in Member States is too general to effectively safeguard data protection in the area of law enforcement. Given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection.

The Conference noted with satisfaction that The Hague Programme subjects the availability principle to strict conditions of respect for data protection principles.

The Conference also welcomes the approach of the Commission in advocating a core set of guiding principles for the treatment of personal data under the Third Pillar, to be developed in close co-operation with data protection authorities. Furthermore, the Conference is encouraged by the steps taken by the Commission towards developing a new legal framework for data protection in the Third Pillar which, it is hoped, will provide an appropriate set of rules applicable to law enforcement activities consistent with the current level of data protection in the First Pillar. When developing these detailed data protection rules, the standard of data protection found in Directive 95/46/EC should serve as a basis.

(*) Cracovia
25-26 aprile 2005
[doc. web n. 1296471]