70 Parere relativo ad una maggiore armonizzazione delle informative (Allegato n. 1) (*)



Euro-Company

Short Privacy Notice

A complete privacy notice is available on request

Dated: October 2004

• We keep the personal information you give us to help provide you with the products and services you require

• We may also pass on your details to other companies who may contact you about their products. You can opt out of this byticking the box below

For the full privacy notice or for access or correction, contact:

• Privacy Department
Euro Company ******

•Call 00 ******

•Or go to the Privacy notice on our website at euro.com

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100appendix1_en.pdf

71 Dichiarazione del Gruppo di lavoro *ex* art. 29 sulle attività di *enforcement* (*)

ARTICLE 29 Data Protection Working Party

12067/04/EN
WP 101

DECLARATION OF THE ARTICLE 29 WORKING PARTY ON ENFORCEMENT

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp101_en.pdf

Adopted on 25th November 2004

72 Lista di controllo Istanza di approvazione di norme aziendali vincolanti (*Binding Corporate Rules*)(*)

ARTICLE 29 Data Protection Working Party

12110/04/EN
WP 102

MODEL CHECKLIST
APPLICATION FOR APPROVAL OF BINDING CORPORATE RULES

Adopted on 25th November 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp102_en.pdf

Consiglio d'Europa

73 Principi guida per la protezione dei dati personali in relazione alle "carte intelligenti" (*smart card*) (*)

INTRODUZIONE

I comitati del Consiglio d'Europa che si occupano di questioni attinenti la protezione dei dati desideravano richiamare l'attenzione su alcuni aspetti specifici della tutela dei dati personali in relazione all'impiego di "carte intelligenti" (smart cards). Il Gruppo di progetto sulla protezione dei dati (CJ-PD) del Consiglio d'Europa ha, pertanto, chiesto ad un consulente, il dr. Karel Neuwirt (Presidente dell'Autorità ceca per la protezione dei dati), di redigere una Relazione sulla protezione dei dati in rapporto all'impiego di smart cards. Nella Relazione si riconosceva che qualunque studio in materia sarebbe stato necessariamente connesso agli sviluppi tecnologici e, pertanto, avrebbe dovuto essere collocato nel rispettivo contesto storico. Si esprimeva dunque l'auspicio di redigere un elenco di principi-guida specifici dei quali tenere conto in riferimento all'impiego di smart cards.

Dopo avere esaminato la Relazione del dr. Neuwirt ed i principi-guida ad essi allegati, il CJ-PD ha accettato di rivedere e specificare meglio alcuni di essi ed ha predisposto il documento di seguito riportato.

Ai fini dei presenti principi-guida, per "smart card" si intende un vettore mobile di dati personali dotato di funzioni automatiche di elaborazione, il quale viene rilasciato ad un interessato ed è in grado di trattare dati personali secondo le finalità e le specifiche del soggetto che lo rilascia in rapporto ad un sistema informativo cui tale vettore è collegato. La carta può essere utilizzata, ad esempio, al fine di identificare l'interessato, di svolgere operazioni che non possono essere effettuate in forma anonima, o di consentire l'accesso a luoghi o database specifici. È necessario distinguere la *smart card* dalle carte a banda magnetica o di memorizzazione, le quali non possono essere utilizzate per effettuare autonome operazioni sui dati secondo criteri logici ed aritmetici.

Le *smart card* trovano impiego crescente per una vasta gamma di applicazioni. Le caratteristiche e le potenzialità delle smart card sollevano numerosi interrogativi in termini di protezione dati, ai quali è necessario fornire risposta. Ad esempio, chi ha la titolarità dei dati personali utilizzati dal sistema? Chi è responsabile dell'accuratezza e della sicurezza dei dati qualora il sistema sia accessibile ad una pluralità di soggetti diversi? Come evitare il moltiplicarsi dei rischi di possibili violazioni della privacy dei cittadini a causa dell'impiego di tecnologie legate alle smart card? Chi deve accedere ai dati personali dell'interessato, ed a quali condizioni? ecc.

I sistemi d'informazione che utilizzino smart card associate al trattamento di dati personali ricadono nell'ambito di applicazione della Convenzione del Consiglio d'Europa per la protezione delle persone con riguardo al trattamento automatizzato di dati personali [ETS 108] (nel prosieguo, "Convenzione 108"). Tale Convenzione è stata elaborata quando ci si è resi conto che, al fine di garantire un'efficace tutela giuridica dei dati personali, sarebbe stato necessario sviluppare in modo più specifico ed organico il riferimento generico al rispetto per la vita privata contenuto nell'Articolo 8 della Convenzione per la tutela dei diritti umani e delle libertà fondamentali (nel prosieguo, "CEDU").

Diritti e garanzie ulteriori sono previsti in varie Raccomandazioni del Consiglio d'Europa, fra cui in particolare:

(*) Adottati dal CDCJ [Gruppo di progetto sulla cooperazione giuridica] in occasione della sua 79ma riunione plenaria (11-14 maggio 2004).

a) la Raccomandazione N. R(2002)9 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi,
b) la Raccomandazione N. R(99)14 sul servizio universale, relativa ai nuovi servizi di comunicazione ed informazione,
c) la Raccomandazione N. R(99)5, per la tutela della privacy su Internet,
d) la Raccomandazione N. R(97)5, sulla protezione dei dati sanitari,
e) la Raccomandazione N. R(95)4, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici,
f) la Raccomandazione N. R(90)19, sulla protezione dei dati personali utilizzati per operazioni di pagamento e per altre operazioni connesse,
g) la Raccomandazione N. R(89)2, sulla protezione dei dati personali utilizzati nel rapporto di lavoro,
h) la Raccomandazione N. R(86)1, sulla protezione dei dati personali utilizzati per scopi di previdenza sociale,
i) la Raccomandazione N. R(85)20, sulla protezione dei dati personali utilizzati per scopi di marketing diretto.

Numerosi sono i documenti e le attività del Consiglio d'Europa, in particolare attraverso i gruppi di esperti che si occupano di protezione dei dati personali, connessi indirettamente alle questioni sollevate dall'utilizzazione di smart card. In particolare, poiché le smart card possono essere utilizzate per la memorizzazione di dati biometrici, si richiama l'attenzione sui principi-guida relativi alla protezione dei dati personali sotto forma di dati biometrici attualmente in via di definizione da parte del T-PD. Le tecnologie moderne arrecano molteplici vantaggi alla vita quotidiana dei cittadini, ma comportano anche alcuni rischi legati alla possibilità di ingerenze nella privacy delle persone. Pertanto, il presente documento non si propone di descrivere i vantaggi dell'utilizzazione di smart card, bensì di specificare l'approccio da seguire per migliorare la tutela dei dati personali qualora si utilizzino tecnologie connesse alle smart card.

La raccolta ed il trattamento di dati personali in sistemi che utilizzino smart card devono rispettare tutti i principi fissati dalla normativa nazionale in materia di protezione dei dati personali.

I principi-guida che seguono non intendono fornire una risposta esauriente a tutti gli interrogativi concernenti la protezione dei dati che nascono dall'utilizzazione di smart card. Una smart card viene sempre utilizzata nell'ambito di un sistema d'informazione più ampio, e l'effettività della protezione complessiva dei dati personali utilizzati in un sistema del genere dipende da fattori e circostanze numerosi e di natura diversa. Anche la sicurezza del sistema dipende in larga parte dal comportamento di coloro che vi hanno a che fare. La tecnologia legata alle smart card sta attraversando una fase di rapidissimo sviluppo. I principi-guida in questione vogliono fissare alcuni principi fondamentali che non subiranno modifiche significative in rapporto alle innovazioni introdotte in campo tecnologico. Ciononostante, può essere opportuno integrare tali principi alla luce degli incessanti sviluppi in questo settore.

È necessario ricordare che, nella misura in cui i presenti principi-guida contengano garanzie per i diritti e le libertà fondamentali di ognuno, ed in particolare per il diritto al rispetto della vita privata, sanciti negli Articoli 5, 6 ed 8 della Convenzione 108 e nell'Articolo 8 della CEDU, è possibile derogare a tali diritti, ai sensi dell'Articolo 9 della Convenzione 108, elaborato sulla base dell'Articolo 8 della CEDU, se ciò è previsto da norme di legge e costituisce una misura necessaria in una società democratica nell'interesse
a. della tutela della sicurezza dello Stato, della sicurezza pubblica, degli interessi economici dello Stato, o della repressione dei reati;
b. della tutela dell'interessato o dei diritti e delle libertà altrui.

Per quanto concerne tali deroghe, è opportuno sottolineare che esse vanno interpretate in maniera restrittiva e devono essere applicate solo in casi eccezionali, secondo le indicazioni fornite dalla giurisprudenza della Corte europea dei diritti umani relativa al comma 2 dell'Articolo 8 della CEDU.

I principi-guida sono rivolti precipuamente ai soggetti che rilasciano la carta, i quali hanno la responsabilità primaria della protezione dei dati personali in essa contenuti. I prin-

cipi si rivolgono, inoltre, a tutti gli altri soggetti che partecipano ai sistemi d'informazione: progettisti, gestori, operatori, e gli stessi interessati. Tutti i soggetti in questione dovrebbero tenere presenti i principi enunciati nel prosieguo. I principi elaborati dovrebbero essere applicati con la massima coerenza possibile; solo in tal modo sarà possibile contribuire alla diffusione di applicazioni basate su smart card che consentano la massima interoperabilità a livello internazionale e gli standard più elevati di sicurezza.

PRINCIPI GUIDA

1. La raccolta ed il trattamento di dati personali attraverso smart card devono avvenire in modo lecito e leale. Si deve prevedere di raccogliere e memorizzare sulla carta soltanto i dati personali necessari a raggiungere gli scopi per i quali la carta stessa è utilizzata. I sistemi che utilizzano smart card devono essere trasparenti[1] per gli interessati i cui dati personali siano oggetto di trattamento.

2. I dati personali devono essere raccolti e memorizzati su una smart card soltanto per scopi legittimi, specifici ed espliciti. Non devono essere utilizzati successivamente secondo modalità che siano incompatibili con tali scopi.

3. Gli obblighi attinenti la protezione dei dati personali pertengono al soggetto che determina gli scopi del sistema e gli strumenti utilizzati per raggiungere tali scopi. Ciò comporta, nel caso di carte multifunzionali, che titolari diversi siano responsabili ciascuno per la parte che gli compete.

4. Qualora una smart card sia utilizzata per scopi di tipo diverso, il trattamento deve essere organizzato in modo da non utilizzare i dati per scopi diversi da quelli per cui sono stati raccolti. Qualora gli stessi dati siano utilizzati per scopi di tipo diverso, essi devono limitarsi a quelli strettamente necessari.[2]

5. La raccolta di dati personali sensibili[3] da registrare nella memoria della carta deve essere effettuata soltanto se prevista da norme di legge oppure se l'interessato vi ha acconsentito esplicitamente.[4] Tali dati devono essere trattati soltanto nel rispetto di opportune garanzie previste per legge.[5] Qualora la raccolta ed il trattamento dei dati in questione si fondino sul consenso esplicito, l'interessato deve avere il diritto di ritirare tale consenso in qualsiasi momento. Il rifiuto o il ritiro del consenso non devono comportare conseguenze negative per l'interessato.[6]

6. I dati registrati su una smart card devono essere tutelati da accessi, alterazioni e/o cancellazioni non autorizzati o accidentali. La carta deve assicurare un livello adeguato di sicurezza alla luce delle conoscenze tecnologiche, della natura sensibile o non sensibile dei dati registrati, del numero e della tipologia delle applicazioni, e della valutazione dei possibili rischi.[7] È necessario stabilire in anticipo, relativamente a ciascuno dei diversi scopi per i quali la carta viene utilizzata, a quali condizioni sia consentito a soggetti terzi di accedere ai dati registrati sulla carta stessa.[8]

7. Qualora si raccolgano e memorizzino dati personali su una smart card, l'interessato deve essere informato delle finalità del trattamento, dell'identità del titolare, delle categorie di dati in oggetto e dei destinatari, o delle categorie di destinatari, dei dati memorizzati. L'interessato deve ricevere ulteriori informazioni[9] se ciò è necessario per garantire la lealtà del trattamento di dati personali.

8. All'atto del rilascio della carta, il titolare deve essere informato adeguatamente delle modalità di utilizzazione e dei passi da compiere in caso di frode o comunicazione non autorizzata.[10]

9. Ogniqualvolta si realizzi uno scambio di dati personali fra una smart card ed il sistema, l'interessato deve esserne informato, a meno che sia già in possesso di tale informazione. Ciò riveste particolare importanza con riguardo alle carte contactless, ossia qualora l'interessato non debba provvedere direttamente all'inserimento o alla presentazione della carta al sistema.

(1) Il concetto di trasparenza implica che l'interessato sia informato dei dati memorizzati e della loro utilizzazione.

(2) Ad esempio, nel caso di una smart card utilizzata da un'istituzione scolastica sia per i servizi di mensa sia per quelli di biblioteca, devono essere memorizzati soltanto i dati comuni alle due funzionalità, come il nome dell'alunno e la rispettiva classe di appartenenza.

(3) Ai sensi dell'Articolo 6 della Convenzione 108, per dati sensibili si intendono "i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale [...] [e] i dati a carattere personale relativi a condanne penali". Si considerano dati sensibili anche gli altri dati definiti come tali dal diritto nazionale.

(4) Tuttavia, in taluni casi il diritto nazionale può prevedere che il consenso non è sufficiente a conferire liceità alla raccolta e/o al trattamento dei dati.

(5) Tali opportune garanzie atte a tutelare ulteriormente i dati possono trovare applicazione, ad esempio, attraverso la cifratura dei dati stessi, che attualmente rappresenta l'approccio più sofisticato. Tuttavia, è necessario tenere conto dei possibili sviluppi futuri in campo tecnologico.

(6) Se la memorizzazione di dati sensibili è necessaria per fornire un servizio all'interessato, e quest'ultimo rifiuta il proprio consenso esplicito ovvero ritira tale consenso, non sarà ovviamente più

segue nota 6, 7, 8, 9, 10

10. Gli interessati devono avere il diritto di accedere ai dati personali che li riguardano contenuti nella carta, e devono avere il diritto di farli correggere o, se necessario, aggiornare.[11]

11. I dati derivanti dall'utilizzazione di una smart card[12] devono essere cancellati se non sono più necessari per lo scopo specifico in relazione al quale la carta è stata utilizzata.

segue nota 6
possibile continuare la prestazione del servizio a favore dell'interessato.
(7) Ad esempio, se si utilizzano carte con un chip di memoria, è ammessa, in linea di principio, soltanto la registrazione di dati identificativi. Vi possono essere anche altri criteri da tenere presenti, come la quantità dei dati, il numero di potenziali lettori, le finalità del trattamento, ecc.
(8) Il rischio di utilizzazioni improprie dei dati registrati nella carta aumenta se quest'ultima è dotata di funzioni di pagamento. Si sconsiglia l'associazione fra funzioni di pagamento ed applicazioni che comportino la registrazione sulla carta di dati sensibili relativi al titolare della carta stessa.
(9) Le informazioni da fornire all'interessato possono comprendere anche le specifiche tecniche relative al sistema utilizzato.
(10) In particolare, è necessario richiamare l'attenzione del titolare della carta sulle possibili conseguenze in caso di utilizzazione impropria, comunicazione delle modalità di accesso ai dati (ad esempio, il codice) o comunicazione dei dati, nonché sulla circostanza che, in taluni casi, egli può essere chiamato a rispondere personalmente.
(11) Una possibilità per garantire l'accesso consiste nell'installazione di lettori di smart card.
(12) Ad esempio, le informazioni relative alla data ed al luogo di utilizzazione della carta.

26ª Conferenza internazionale sulla protezione dei dati Wroclaw (Polonia) 13-16 settembre 2004

74 Risoluzione della Conferenza europea per la protezione dei dati relativa all'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia (protezione dei dati nel Terzo Pilastro)

Risoluzione della Conferenza europea per la protezione dei dati relativa all'istituzione di un forum comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia (protezione dei dati nel Terzo Pilastro)

Il Trattato dell'Unione Europea (TUE), nella versione adottata il 2 ottobre 1997 (Trattato di Amsterdam) contiene, nel Titolo VI, ampie disposizioni relative alla cooperazione giudiziaria e di polizia in materia penale. Il Trattato di Nizza prevede che le autorità giudiziarie e di polizia degli Stati membri dell'UE intensifichino ulteriormente tale cooperazione. Si tratta di una delle priorità dell'Unione.

Le Autorità di protezione dei dati degli Stati Membri dell'Unione europea hanno piena coscienza della necessità di una cooperazione più stretta fra le autorità responsabili dell'azione penale negli Stati Membri, al fine di garantire ai cittadini dell'Unione un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia. Tuttavia, occorre garantire un equo bilanciamento fra tale esigenza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea.

Uno dei compiti più importanti delle Autorità di protezione dei dati è rappresentato dall'attività consultiva in materia di protezione dei dati svolta per gli enti che si occupano di legiferazione; in tale ambito, le Autorità devono sottolineare i rischi che determinate iniziative di legge possono comportare per le libertà sopra ricordate, e proporre soluzioni più vicine ai cittadini. La Commissione, il Consiglio ed il Parlamento europeo usufruiscono di tale attività consultiva con sempre maggiore frequenza.

Naturalmente le Autorità di protezione dei dati sono liete di rispondere a tali richieste nella maniera migliore possibile. Tuttavia, è bene chiarire che, al momento, sono insuffi-

cienti o assenti le strutture organizzative necessarie all'adempimento di questa importante missione, e che pertanto le Autorità non possono garantire un intervento consultivo in fase precoce, sulla base di un'analisi condotta a livello paneuropeo e secondo i dovuti standard di qualità. Ciò dipende dall'inesistenza, all'interno del Terzo Pilastro, di un forum comune e della necessaria struttura organizzativa.

Questa situazione contrasta con quella rinvenibile nel Primo Pilastro, dove è stato costituito il Gruppo di lavoro "Articolo 29" che garantisce un'idonea struttura organizzativa alle Autorità di protezione dei dati. Tale struttura comprende un segretariato permanente (messo a disposizione dalla Commissione) e le risorse utili a consentire l'organizzazione di incontri periodici a Bruxelles con i necessari servizi di traduzione. Le autorità di controllo comuni all'interno del Terzo Pilastro (ad esempio per quanto riguarda Europol, Schengen, Eurojust) hanno un mandato specifico, ed occorre un approccio più ampio per garantire l'uniformità delle garanzie concernenti la protezione dei dati nell'intero settore della cooperazione giudiziaria e di polizia.

I partecipanti alla Conferenza attualmente stanno intensificando la propria collaborazione nelle materie giudiziarie e di polizia. A tal fine, un gruppo di lavoro "Polizia", costituito sotto l'egida della Conferenza delle Autorità europee di protezione dei dati, funge da forum strategico, analizzando tematiche che esulano dal mandato degli organismi attualmente esistenti a livello UE in materia di protezione dei dati. È stato inoltre costituito un altro sottogruppo della Conferenza. Tale gruppo di progetto, formato, fra gli altri, dai presidenti delle autorità comuni di controllo (Europol, Schengen, Dogane ed Eurojust), dal presidente del Gruppo di lavoro "Articolo 29", e dal Garante europeo per la protezione dei dati, ha il compito di sviluppare approcci strategici rispetto a nuove iniziative che riguardino l'utilizzazione di dati personali per scopi giudiziari e di polizia in una prospettiva europea.

Cionondimeno, sono necessarie ulteriori misure strutturali. In concomitanza con il rafforzamento e l'avanzamento dell'architettura europea di sicurezza nel Terzo Pilastro, è essenziale incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea. Per tale motivo, la Conferenza delle Autorità europee di protezione dei dati invita il Consiglio e la Commissione ad attuare senza indugi le misure necessarie, in termini di risorse umane ed organizzative, onde consentire all'ente incaricato della protezione dei dati di iniziare l'importante attività di tutela degli interessi dei cittadini prima della fine dell'anno in corso. Il Garante europeo per la protezione dei dati, nominato ai sensi dell'Articolo 286(2) del Trattato delle Comunità europee, dovrebbe partecipare all'ente istituendo con un ruolo attivo.

La Conferenza, inoltre, invita il Consiglio e la Commissione a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro, in stretta cooperazione con i soggetti competenti.

La Presidenza è invitata a trasmettere la presente Risoluzione al Consiglio, alla Commissione ed al Parlamento.

Wroclaw, 14 settembre 2004

75 Risoluzione relativa alla proposta di uno standard-quadro ISO in materia di *privacy*

Sulla base di una proposta formulata dall'Autorità di Berlino per la protezione dei dati e l'accesso alle informazioni, l'Autorità per la protezione dei dati e l'accesso alle informazioni dello Stato di Brandeburgo, l'Autorità belga per la protezione dei dati, l'Information Commissioner del Regno Unito, l'Autorità federale tedesca per la protezione dei dati, il Centro indipendente per la protezione dei dati dello Schleswig-Holstein, l'Autorità per le informazioni e la *privacy* dello Stato di Ontario, l'Ispettore generale per la protezione dei dati personali della Polonia, l'Autorità per la protezione dei dati personali di Hong Kong, l'Autorità spagnola per la protezione dei dati, l'Ispettorato statale per la protezione dei dati della Repubblica di Lituania, e l'Autorità svizzera per la protezione dei dati propongono che la Conferenza internazionale adotti la seguente risoluzione:

Considerato che l'Organizzazione internazionale per la standardizzazione (ISO) ha istituito un Gruppo di studio sulle tecnologie della *privacy* (PTSG) nell'ambito del Comitato tecnico congiunto 1 (JTC1) con il compito di valutare la necessità di mettere a punto uno standard tecnologico in materia di *privacy* e, in caso affermativo, le modalità procedurali e la relativa portata, e quindi presentare una relazione entro il mese di novembre 2004;

Considerato che il Comitato tecnico congiunto 1 (JTC1) dell'ISO trasmette al Sottocomitato 27 (Sicurezza nelle tecnologie dell'informazione) le richieste di decisione su schemi attinenti alla *privacy* secondo una procedura accelerata;

Considerato che l'International Security, Trust, and Privacy Alliance (ISTPA, Alleanza internazionale per la sicurezza, la fiducia e la *privacy*) è un'alleanza mondiale di imprese, istituzioni e fornitori di tecnologie operanti congiuntamente allo scopo di chiarire e definire questioni attuali o in via di evoluzione connesse a sicurezza, fiducia e *privacy*;

Considerato che l'ISO ha ricevuto una proposta di standard internazionale (ISO/IEC (PAS) DIS 20886) relativa ad Quadro di riferimento per la *privacy*, presentata dall'ISTPA[1] nell'ambito di una procedura accelerata, sulla quale è aperto il voto per corrispondenza con scadenza all'11 dicembre 2004;

Considerato che il Privacy Enhancing Technology Testing and Evaluation Project (PETTEP[2], Progetto per la verifica e valutazione delle tecnologie di potenziamento della *privacy*) è una coalizione mondiale di autorità per la *privacy* e la protezione dei dati, esponenti del mondo universitario, autorità governative e organismi del settore privato, ed esperti in materia di *privacy*, la cui missione consiste nella definizione di criteri di verifica e valutazione riconosciuti a livello internazionale rispetto alle caratteristiche dichiarate da sistemi e tecnologie dell'informazione relativamente alla *privacy*;

Considerato che l'International Working Group on Data Protection in Telecommunications (Gruppo di lavoro internazionale sulla protezione dei dati nelle telecomunicazioni), in occasione del suo 35mo incontro tenutosi a Buenos Aires il 14 e 15 aprile 2004, ha adottato un Documento di lavoro su un futuro standard ISO in materia di *privacy*;[3]

Considerato che la Conferenza internazionale delle Autorità di protezione dati e della *privacy* (in appresso, la "Conferenza") desidera sostenere la definizione di uno standard internazionale delle tecnologie in materia di *privacy* efficace e riconosciuto su base globale, e mettere a disposizione dell'ISO le proprie competenze ai fini della definizione di tale standard;

Considerato che la Conferenza riconosce che la conformità a standard ISO attuali o futuri non comporta né surroga necessariamente la conformità a disposizioni di legge. La

(1) V. http://www.istpa.org
(2) Il PETTEP è un progetto condotto sotto la guida dell'Autorità per la privacy e le informazioni dello stato di Ontario, che ha svolto ricerche ed analisi finalizzate alla definizione di criteri di verifica e valutazione degli aspetti connessi alla privacy nei sistemi e nelle tecnologie dell'informazione.
(3) www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm

Conferenza in realtà considera la definizione degli standard IT in oggetto uno strumento che può essere d'ausilio onde rispettare le norme di legge in materia di protezione dati e *privacy*. La Conferenza riconosce senza alcun dubbio che, da un lato, i propri membri, ciascuno per il rispettivo ambito di giurisdizione, hanno e continueranno a mantenere in vigore norme di legge in materia di *privacy*, le quali in realtà si differenziano per alcuni profili, e che, d'altro canto, esiste complessivamente un grado elevato di concordanza fra le norme di legge in questione, il quale troverebbe il riconoscimento ottimale divenendo parte integrante di meccanismi basati sulle tecnologie dell'informazione attraverso la messa a punto di uno standard internazionale, o di più standard internazionali;

La conferenza adotta le seguenti Risoluzioni:

1. La Conferenza raccomanda rispettosamente che l'ISO metta a punto uno o più standard globali in materia di *privacy*, ed in particolare uno standard delle tecnologie in materia di *privacy*, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite.
2. La Conferenza ritiene che la definizione di uno standard internazionale in materia di *privacy* debba fondarsi sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati. Per essere efficace, uno standard relativo alle tecnologie dell'informazione deve
   - offrire criteri di valutazione e verifica riferiti alle funzionalità connesse alla *privacy* di qualsiasi sistema o tecnologia, onde facilitare il rispetto da parte dei titolari degli strumenti giuridici nazionali e internazionali in materia di protezione dei dati,
   - offrire assicurazioni sulle caratteristiche dichiarate di rispetto della *privacy* relativamente a tecnologie e sistemi utilizzati per la gestione di dati personali,
   - essere in grado di supportare le specifiche concernenti la *privacy* riferite ai dati personali relativi a una determinata persona, indipendentemente dalle combinazioni e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali.
3. La Conferenza appoggia la recente istituzione di un Gruppo di studio temporaneo sulle tecnologie della *privacy* (PTSG) con il compito di valutare l'esigenza di uno standard nonché gli ambiti e le metodologie di sviluppo di tale standard nel quadro dell'ISO.
4. La Conferenza sostiene con forza l'accelerazione, e non già il procrastinamento, dell'istituzione di un nuovo Sottocomitato permanente dell'ISO per la definizione di standard delle tecnologie dell'informazione riferiti alla *privacy*. Tale nuovo Sottocomitato dovrebbe tenere presente l'attività svolta attualmente nei Sottocomitati esistenti in rapporto a specifici temi connessi alla *privacy*.
5. La Conferenza sostiene con forza l'inserimento del *Privacy Enhancing Technology* Testing and Evaluation Project (PETTEP) quale organismo ufficiale di collegamento con il PTSG del JTC1 dell'ISO. In tal modo le Autorità di protezione dati potranno disporre di uno strumento per operare direttamente all'interno del PTSG dell'ISO, e si conferisce ai membri del PETTEP un ruolo ufficiale che consentirà loro di presentare, analizzare e contribuire all'attività del PTSG.
6. La Conferenza promuove e sostiene l'adesione al PETTEP delle Autorità di protezione dati interessate, il che consentirà loro, in quanto membri del PETTEP, di far sentire immediatamente la propria voce nel dibattito relativo alla definizione di uno standard ISO delle tecnologie della *privacy*.
7. La Conferenza riconosce che il PETTEP gode già di uno status ufficiale all'interno del PTSG, e chiede rispettosamente al PETTEP di adottare le risoluzioni della Conferenza e di presentarle quanto prima al PTSG.
8. La Conferenza, pur riconoscendo l'impegno e la determinazione dell'ISTPA nel settore della *privacy*, chiede rispettosamente il ritiro dello schema ISTPA quale specifica pubblica (PAS) fintanto che non siano state affrontate le questioni di seguito delineate:
   - Il concetto di *privacy* su cui si fonda la Proposta di standard-quadro in materia di *privacy*, ed il fatto che tale quadro deve tenere conto dell'esistenza di limiti alla raccolta di dati. Nella Proposta si definisce *privacy* "la

gestione ed utilizzazione corrette di dati personali per l'intero ciclo di vita di tali dati, conformemente a principi di protezione dati ed alle preferenze espresse dal soggetto".[4] Gli Autori della Proposta giudicano che la raccolta ed il trattamento di dati personali siano fondamentali ai fini del funzionamento corretto della società e delle relazioni commerciali moderne.[5] Tale considerazione si fonda sul presupposto che non ci siano limiti alla raccolta di dati personali. Possono sussistere circostanze in cui la raccolta ed il trattamento di dati personali sono fondamentali nel senso indicato; tuttavia, non si deve supporre che ciò costituisca la regola.

9. La Conferenza chiede rispettosamente all'ISO di sospendere eventuali richieste già avanzate per il riconoscimento di specifiche pubbliche tramite procedura accelerata di adozione nel settore della *privacy* e della protezione dei dati (ovvero di sospendere la presentazione di nuove richieste per il riconoscimento di specifiche pubbliche nel settore della *privacy* e della protezione dei dati), in quanto la definizione di uno standard in materia di *privacy* necessita di un approfondito dibattito.
10. La Conferenza chiede rispettosamente all'ISO di considerare le richieste di riconoscimento di specifiche pubbliche ed ogni altra richiesta concernente la protezione dei dati e la *privacy* come indicazioni e contributi utili alla definizione di un quadro generale nonché di potenziali standard futuri all'interno del quadro suddetto.

(4) Ibid., pag. 13.
(5) Ibid., pag. 10.

76 Versione emendata della Risoluzione della Conferenza internazionale del 2003 relativa agli aggiornamenti automatici di *software*

L'ufficio dell'Autorità australiana federale per la *privacy*, l'Autorità per l'informazione e la *privacy* dello stato di Ontario, l'Autorità per i dati personali di Hong Kong, e l'Autorità per la protezione dei dati e l'accesso alle informazioni dello stato di Brandeburgo propongono che la Conferenza Internazionale adotti la seguente risoluzione:

1. La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti.

Così facendo, esse
- sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che questi abbiano la possibilità di accorgersene, intervenire o impedirlo,
- possono assumere il controllo, almeno parziale, del *computer* terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento,
- modificano il *software* installato sul *computer*, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuarne la causa nell'aggiornamento.

Tutto ciò può comportare particolari problemi per la pubblica amministrazione e le aziende private, nella misura in cui sussistano specifici obblighi di legge a loro carico relativamente alle modalità di trattamento dei dati personali.

2. La Conferenza, pertanto, invita le società produttrici di *software*
a. ad offrire procedure per l'aggiornamento online del *software* soltanto in associazione ad un'informativa, e ad effettuare l'aggiornamento una volta ottenuto il consenso dell'utente, senza travalicare o abusare di tale consenso, secondo modalità trasparenti e senza consentire accessi non controllati al computer dell'utente;
b. a chiedere la comunicazione di dati personali soltanto con il consenso informato dell'utente e nella misura in cui ciò risulti necessario per effettuare l'aggiornamento online. Gli utenti non dovrebbero essere obbligati a fornire le proprie credenziali di identificazione –anziché di autenticazione– per dare inizio alla procedura di caricamento remoto;
c. a prevedere servizi di aggiornamento che consentano di effettuare verifiche preventive su server separati prima di procedere all'installazione.

3. La Conferenza promuove la definizione e l'applicazione di tecnologie per l'aggiornamento del software che siano rispettose della *privacy* e dell'autonomia degli utenti.