

- le autorità autorizzate a consentire l'intercettazione legale delle telecomunicazioni, i servizi autorizzati a procedere alle intercettazioni e la base giuridica del loro intervento,
- gli scopi per cui tali intercettazioni possono esser effettuate, per poter valutare se la misura è adeguata tenuto conto degli interessi nazionali in gioco,
- il divieto di qualsiasi sorveglianza per campione o generale delle telecomunicazioni su vasta scala,
- le circostanze e le condizioni precise (ad esempio, gli elementi che giustificano la misura, la durata della misura) che si applicano alle intercettazioni, nel rispetto del principio di specificità che deve rispettare qualsiasi ingerenza nella vita privata altrui³⁵,
- il rispetto di questo principio di specificità, corollario del divieto di qualsiasi sorveglianza per campione o generale, implica, in particolare per quanto riguarda i dati sul traffico, che le pubbliche autorità possono avere accesso a tali dati solo in casi specifici, e non in modo generale e attivo.
- le misure di sicurezza per quanto riguarda il trattamento e la memorizzazione dei dati, nonché la durata della loro conservazione,
- per quanto riguarda le persone coinvolte indirettamente o aleatoriamente³⁶ nelle intercettazioni, le garanzie particolari che si applicano al trattamento di dati personali: in particolare, i criteri che giustificano la conservazione dei dati, e le condizioni della comunicazione di tali dati a terzi,
- l'informazione della persona sotto sorveglianza, appena questa è possibile³⁷,
- i tipi di ricorso cui possono ricorrere le persone sotto sorveglianza³⁸,
- le modalità di sorveglianza di questi servizi da parte di un'autorità di controllo indipendente³⁹,
- la pubblicità - ad esempio sotto forma di relazioni statistiche regolari - della politica d'intercettazione delle telecomunicazioni effettivamente attuata⁴⁰,
- le condizioni precise per la comunicazione dei dati a terzi nel quadro di accordi bi- o multilaterali.

Fatto a Bruxelles, addì 3 maggio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

³⁵ Cfr. la precedente nota 13.

³⁶ I dati in questione si riferiscono a persone che non formano l'oggetto di misure di sorveglianza, ma il cui corrispondente è oggetto di tali misure; ad esempio: numero di telefono composto dalla persona sorvegliata e relativo ad un parente di quest'ultimo; localizzazione geografica di talune persone in contatto tramite telefonia mobile con la persona sotto sorveglianza.

³⁷ La persona sotto sorveglianza dovrebbe infatti essere informata a partire dal momento in cui l'informazione non danneggia o non danneggia più l'indagine.

³⁸ La summenzionata sentenza nella causa Leander fa presente che l'istituzione dinanzi alla quale può essere presentato il ricorso "non deve essere necessariamente un'istituzione giudiziaria stricto sensu, ma che si deve tener conto dei suoi poteri e delle sue garanzie procedurali nella valutazione dell'efficacia del ricorso". Questo ricorso "deve essere possibilmente efficace, tenuto conto delle limitazioni inerenti ad ogni sistema di sorveglianza segreta volta a proteggere la sicurezza nazionale" (paragrafi 83 e 84).

³⁹ La sentenza nella causa Leander prevede il controllo democratico delle intercettazioni specificando che "è compito del Parlamento e delle istituzioni indipendenti [del governo] vigilare sul corretto funzionamento del sistema" (paragrafo 64).

⁴⁰ Questa esigenza di pubblicità, come anche la necessità di un controllo delle intercettazioni da parte di un'autorità indipendente, sono menzionate nella "Common position on public accountability in relation to interception of private communications" adottata a Hong Kong il 15 aprile 1998 dal gruppo internazionale di lavoro sulla tutela dei dati nel settore delle telecomunicazioni.

Raccomandazione 3/99: La conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari5085/99/IT/definitivo
WP 25

Gruppo di lavoro per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 3/99: La conservazione dei dati sulle comunicazioni da parte dei fornitori di
servizi Internet a fini giudiziari

Approvata il 7 settembre 1999

Introduzione

La lotta alla criminalità elettronica costituisce un problema che sta richiamando crescente attenzione internazionale.¹ I paesi G8² hanno approvato un piano d'azione³ articolato su dieci punti, attualmente in fase di realizzazione grazie a un sottogruppo specializzato in materia di criminalità elettronica costituito dai rappresentanti delle autorità di polizia dei paesi G8. Uno dei problemi più controversi è costituito dalla conservazione dei dati sul "traffico" (comunicazioni) passato e futuro da parte dei fornitori di servizi Internet a fini giudiziari e di polizia, con trasmissione dei dati stessi alle autorità competenti. Il sottogruppo G8 sulla criminalità elettronica intende formulare raccomandazioni per garantire la possibilità di conservare ed esaminare tali dati. I ministri della Giustizia e degli Interni dei paesi G8 potranno discutere tali raccomandazioni nella riunione di Mosca del 19 - 20 ottobre 1999.

Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali⁴ è consapevole del ruolo importante che può essere svolto dai dati di traffico nel contesto delle indagini su reati commessi via Internet, ma desidera peraltro richiamare l'attenzione dei governi nazionali sui principi relativi alla protezione dei diritti e delle libertà fondamentali dei cittadini, con particolare riferimento alla riservatezza e al segreto postale, principi di cui è necessario tenere conto in questo contesto.

Il gruppo di lavoro è dell'opinione che i ministri della Giustizia e degli Interni G8 potrebbero richiedere un'interpretazione equilibrata delle due direttive UE sulla protezione dei dati⁵ a livello di attuazione onde tenere conto delle esigenze di controllo unitamente a quelle attinenti alla riservatezza.

¹ Vedi ad esempio "COMCRIME Study" "Legal Aspects of computer-related Crime in the Information Society-COMCRIME Study, January 1997 - Presentato nell'ambito del piano d'azione UE contro la criminalità organizzata - Disponibile sul sito web del Comitato consultivo giuridico: <http://www2.echo.lu/legal/en/comcrime/sieber.html>. Il Consiglio d'Europa sta lavorando su un progetto di convenzione in materia di criminalità cibernetica. Il Consiglio dell'UE ha manifestato il proprio sostegno a tale iniziativa il 27 maggio 1999. Per criminalità elettronica si intendono tutti i reati commessi su reti elettroniche, come ad esempio attacchi mediante computer, pubblicazione di materiale illecito su siti web, e attività commesse dalla criminalità transnazionale organizzata (ad es. traffico di narcotici, pornografia infantile).

² Canada, Francia, Germania, Italia, Giappone, Regno Unito, Stati Uniti d'America e Russia.

³ "Meeting of Justice and Interior Ministers of the Eight, December 9-10, 1997, Communiqué, Washington D.C. December 10, Communiqué Annex : Principles and Action Plan to Combat High-tech Crime"

⁴ Istituito in virtù dell'art. 29 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, p. 31. Disponibile su: <http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm>

⁵ Direttiva 95/46/CE, e Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, GU L 24, 30 gennaio 1998, p. 1. Indirizzo Internet: vedi nota 4.

Il gruppo di lavoro è altresì consapevole del potenziale onere per operatori di telecomunicazioni e fornitori di servizi Internet.

L'obiettivo della presente Raccomandazione, pertanto, è di contribuire ad una applicazione uniforme delle Direttive 95/46/CE e 97/66/CE, grazie alla definizione di condizioni chiare e prevedibili per gli operatori di telecomunicazioni e fornitori di servizi Internet, come pure per le autorità di controllo, nel rispetto del diritto alla riservatezza.

Situazione giuridica

Nell'ambito dell'Unione europea, la Direttiva 95/46/CE ha permesso di armonizzare la protezione della riservatezza assicurata dai sistemi giuridici degli Stati membri. La direttiva concretizza e amplifica i principi della Convenzione europea per la Protezione dei Diritti umani del 4 novembre 1950 e della Convenzione No. 108 del Consiglio d'Europa del 28 gennaio 1981 per la tutela delle persone con riguardo al trattamento automatico dei dati personali. La Direttiva 97/66/CE precisa le norme di cui sopra nel settore delle telecomunicazioni. Ambedue le direttive si applicano al trattamento dei dati personali, ivi compresi i dati Internet relativi ad abbonati e utenti.⁴

In particolare, gli artt. 6, 7, 13, 17 (1) e (2) della Direttiva 95/46/CE, e gli artt. 4, 5, 6 e 14 della Direttiva 97/66/CE vertono sulla legalità di tali trattamenti da parte di operatori di telecomunicazioni e fornitori di servizi.

Tali norme consentono ai citati operatori e fornitori di effettuare il trattamento dei dati in determinate condizioni espressamente specificate.

L'art. 6 (1) lettera b) dispone che i dati possano essere raccolti unicamente per finalità determinate, esplicite e legittime, e che non possano essere ulteriormente trattati in modo incompatibile con le finalità originali. L'art. 6 (1) lettera e) dispone che i dati personali non possano essere conservati per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti o successivamente trattati. L'art. 13 consente agli Stati membri di limitare fra l'altro la portata dell'art. 6 (1) qualora tale restrizione costituisca una misura necessaria alla salvaguardia della sicurezza dello Stato o della pubblica sicurezza, o alla prevenzione, ricerca, accertamento e perseguimento di fenomeni a carattere penale.

L'applicazione dei principi in questione è ulteriormente specificata dagli artt. 5 e 6, paragrafi 2-5, della Direttiva 97/66/CE. L'art. 5 garantisce la riservatezza delle comunicazioni effettuate attraverso le reti pubbliche di telecomunicazione e i servizi di telecomunicazione offerti al pubblico. Gli Stati membri sono tenuti a vietare l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti senza il consenso di questi ultimi, eccetto quando tali attività siano autorizzate a norma di legge in virtù dell'art. 14, paragrafo 1.

Come regola generale, i dati sul traffico devono essere cancellati o resi anonimi al termine della comunicazione (Art. 6, paragrafo 1, della Direttiva 97/66/CE). Ciò si deve alla delicatezza di tali dati, che possono consentire l'elaborazione di profili individuali di comunicazione, ivi comprese le fonti delle informazioni e la località geografica dell'utente di telefoni fissi o mobili, e ai pericoli per la riservatezza che derivano dalla raccolta, trasmissione o ulteriore utilizzazione di tali dati. L'art. 6 (2) prevede un'eccezione concernente il trattamento di taluni dati ai fini delle attività di fatturazione agli abbonati e della riscossione dei canoni di interconnessione, ma solo entro il termine del periodo durante il quale le bollette possono essere legalmente impugnate, o possono essere riscossi i pagamenti.

L'art. 14 (1) consente agli Stati membri di adottare disposizioni volte a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'art. 6, qualora tali limitazioni costituiscono una misura necessaria alla salvaguardia della sicurezza dello Stato, ed alla prevenzione, ricerca, accertamento e perseguimento di attività a carattere penale, come previsto dall'art. 13 (1) della Direttiva 95/46/CE.

Ne deriva che gli operatori e fornitori di servizi Internet non hanno facoltà di raccogliere e

⁴ Vedi "Working document: Processing of Personal Data on the Internet", approvato il 23 febbraio 1999, disponibile all'indirizzo di cui alla nota 1.

memorizzare dati esclusivamente a fini giudiziari, se non in virtù delle eccezioni ed alle condizioni di cui sopra. Ciò coincide con la prassi tradizionale di molti Stati membri, nei quali l'applicazione dei principi nazionali per la protezione dei dati si è tradotta nel divieto al settore privato di mantenere dati personali unicamente in ragione di possibili esigenze di polizia o sicurezza.

In questo contesto, merita rilevare che, ai fini delle esigenze di polizia ed alle condizioni di cui agli artt. 13 della Direttiva 95/46/CE e 14 della Direttiva 97/66/CE, la legislazione di molti Stati membri definisce le precise condizioni alle quali le forze di polizia e di sicurezza possono avere accesso ai dati memorizzati dagli operatori privati di telecomunicazioni e dai fornitori di servizi Internet per proprie finalità a carattere civile.

Come già rilevato dal Gruppo di lavoro nella Raccomandazione 2/99 sulla tutela della riservatezza nel contesto dell'intercettazione di telecomunicazioni, adottata il 3 maggio 1999⁹⁷, il fatto che una terza parte acquisisca conoscenze concernenti i dati sul traffico relativo all'utilizzazione dei servizi di telecomunicazione è stato generalmente considerato una forma di intercettazione delle telecomunicazioni, e costituisce pertanto una violazione del diritto degli individui alla riservatezza e del segreto epistolare, così come tali diritti sono garantiti dall'art. 5 della Direttiva 97/66/CE⁹⁸. Inoltre, l'accesso a tali dati è incompatibile con l'art. 6 della direttiva citata.

Qualsiasi violazione di questi diritti e obblighi è inaccettabile se non soddisfa tre criteri fondamentali, in conformità all'art. 8 (2) della Convenzione europea per la Protezione dei Diritti umani e delle Libertà fondamentali del 4 novembre 1950 ed in virtù dell'interpretazione della Corte europea dei Diritti dell'uomo: l'esistenza di una idonea base giuridica, la necessità dell'intervento in una società democratica, e la conformità ad uno dei legittimi obiettivi elencati dalla Convenzione. La base giuridica deve definire con precisione i limiti e le modalità di applicazione del provvedimento: i fini ai quali i dati possono essere trattati, il periodo di tempo durante il quale i dati possono essere (eventualmente) mantenuti, e le caratteristiche dell'accesso devono essere strettamente limitati. Le attività generali di esplorazione o sorveglianza su vasta scala devono essere vietate⁹⁹. Ne consegue che le autorità pubbliche possono avere accesso ai dati soltanto caso per caso, e mai proattivamente, o in via generale.

Questi criteri coincidono con i citati disposti dell'art. 13 della Direttiva 95/46/CE e dell'art. 14 della Direttiva 97/66/CE.

Divergenza delle norme nazionali¹⁰⁰

Per quanto riguarda il periodo durante il quale i dati sul traffico possono essere memoriz-

⁹⁷ Disponibile all'indirizzo di cui alla nota 1.

⁹⁸ Le autorità giudiziarie richiedono inoltre l'accesso alle informazioni sui collegamenti in tempo reale, e ai dati concernenti i collegamenti attivi (cosiddetti "futuro traffico dati").

⁹⁹ Vedi in particolare la sentenza Klass del 6 settembre 1978, serie A N°28, pp. 23 e seguenti, e la sentenza Malone del 2 agosto 1984, serie A N°82, pp. 30 e seguenti.

La sentenza Klass, in base a quella Leander del 25 febbraio 1987, insiste sulla necessità di "efficaci garanzie contro gli abusi" "in vista del rischio che un sistema di sorveglianza segreta per la tutela della sicurezza nazionale possa minare o persino distruggere la democrazia, col pretesto di difenderla". (Sentenza Leander, serie A N°116, pp. 14 e seguenti).

La Corte rileva, nella sentenza Klass (par. 50 e seguenti) che la valutazione dell'esistenza di garanzie adeguate ed effettive contro gli abusi dipende da tutte le circostanze del caso. Nella fattispecie, la Corte ritiene che i provvedimenti di sorveglianza previsti dalla legislazione tedesca non permettano una sorveglianza generale o esplorativa e non siano incompatibili con l'art. 8 della Convenzione europea per la Protezione dei Diritti umani. La legislazione tedesca fornisce le seguenti garanzie: la sorveglianza è limitata ai casi in cui vi sono indicazioni tali da legittimare il sospetto che un individuo stia preparando, commettendo o abbia commesso taluni gravi atti criminosi; i provvedimenti possono essere ordinati soltanto se l'accertamento dei fatti con altri metodi sia privo di prospettive di successo, o molto più difficile; ed anche in tal caso, le attività di sorveglianza possono interessare soltanto la persona dell'indagato, o i suoi presunti "contatti".

¹⁰⁰ La Commissione sta attualmente analizzando la legislazione degli Stati membri che hanno notificato provvedimenti nazionali di recepimento della Direttiva 97/66/CE e della Direttiva 95/46/CE. Vedi la tabella di recepimento per quanto riguarda la Direttiva 95/46/CE, disponibile all'indirizzo di cui alla nota 4.

zati, la Direttiva 97/66/CE ne consente la conservazione unicamente a fini di fatturazione³¹ e soltanto fino alla fine del periodo durante il quale è legalmente possibile impugnare la fattura. Questo periodo, tuttavia, varia considerevolmente negli Stati membri. In Germania, ad esempio, gli operatori delle telecomunicazioni e i fornitori di servizi di telecomunicazione hanno facoltà di memorizzare i dati necessari per la fatturazione fino a un massimo di 80 giorni, al fine di giustificare la correttezza delle fatture³². In Francia, dipende dallo status dell'operatore: gli operatori "tradizionali" di telecomunicazioni hanno facoltà di memorizzare i dati di traffico fino a un massimo di un anno, in base alla legge che definisce il periodo durante il quale possono essere contestate le fatture. Questo periodo è fissato a 10 anni per altri operatori. In Austria, la legge sulle telecomunicazioni non fissa un periodo preciso durante il quale i dati sul traffico possono essere memorizzati a fini di fatturazione, ma limita tale periodo a quello durante il quale le fatture possono essere contestate, o i pagamenti possono essere riscossi. Nel Regno Unito, secondo la legge, le fatture possono essere impugnate per un periodo di 6 anni, ma gli operatori e fornitori di servizi conservano i relativi dati per circa 18 mesi. In Belgio, la legge non definisce il periodo in questione, ma il principale fornitore di servizi di telecomunicazione lo ha fissato a 3 mesi nelle proprie condizioni generali. In Portogallo la prassi è ancora diversa, poiché, dato che il periodo non è fissato per legge, l'autorità nazionale per la protezione dei dati decide caso per caso. È interessante notare che in Norvegia il periodo è di 14 giorni.

Anche la pratica attuale dei fornitori di servizi Internet non è omogenea: sembrerebbe che i fornitori più piccoli mantengano i dati sul traffico per periodi brevissimi (poche ore) per mancanza di capacità di memoria. I fornitori più grandi, con maggiori capacità, possono mantenere i dati per qualche mese (ma la durata può dipendere dalle rispettive politiche di fatturazione: in base al tempo di collegamento, o a quota fissa).

A fini giudiziari, la legge olandese sulle telecomunicazioni obbliga gli operatori e i fornitori di servizi a raccogliere e memorizzare i dati sul traffico per tre mesi.

Ostacoli al funzionamento del Mercato interno

Queste variazioni sollevano potenziali ostacoli in seno al Mercato interno dal punto di vista della prestazione transnazionale di servizi Internet e di telecomunicazione, ma anche l'efficacia delle attività giudiziarie può essere ridotta per lo stesso motivo. Si potrebbe sostenere che un fornitore di servizi Internet con sede in uno Stato membro non ha facoltà di memorizzare i dati per un periodo superiore a quello previsto dallo Stato membro in cui l'utente risiede e utilizza il servizio. Alternativamente, un fornitore potrebbe essere obbligato a mantenere i dati per un periodo superiore a quello consentito dal proprio Stato membro in ragione della legislazione del paese di residenza degli utenti. Nel caso di fatture per comunicazioni transnazionali tramite telefoni cellulari, l'incasso non viene effettuato dall'operatore estero, ma dall'operatore nazionale degli abbonati in questione. La diversa durata dei periodi di memorizzazione può quindi comportare gli stessi problemi illustrati per i fornitori di servizi Internet. Il disposto sulla legge applicabile di cui all'art. 4 della Direttiva 95/46/CE risolve il problema soltanto nella misura in cui il fornitore di servizi Internet esercita direttamente il controllo, ed ha sede soltanto in uno Stato membro, ma non nei casi in cui è insediato in Stati membri diversi, che applicano periodi diversi, o laddove effettua il trattamento dei dati sul traffico per conto di autorità di controllo.

Raccomandazione

Alla luce di quanto precede, il Gruppo di lavoro ritiene che il mezzo più efficace per limitare inaccettabili pericoli alla riservatezza nella salvaguardia delle esigenze delle autorità giudiziarie consista nell'evitare che i dati sul traffico siano mantenuti esclusivamente a fini giudiziari, e che le leggi nazionali costringano gli operatori delle telecomunicazioni, i servizi di telecomunicazione e

³¹ E, ove necessario, per il pagamento delle tariffe di intercollegamento fra operatori delle telecomunicazioni, vedi art. 6, paragrafo 2, della Direttiva 97/66/CE.

³² Se una fattura viene contestata durante tale periodo, i relativi dati, naturalmente, possono essere mantenuti fino al termine della vertenza.

i fornitori di servizi Internet a mantenere dati sul traffico per un periodo di tempo superiore a quello necessario ai fini di fatturazione.

Il Gruppo di lavoro raccomanda che la Commissione europea proponga opportuni provvedimenti per un'ulteriore armonizzazione del periodo durante il quale gli operatori delle telecomunicazioni, i servizi di telecomunicazione e i fornitori di servizi Internet hanno facoltà di mantenere i dati sul traffico ai fini di fatturazione e di riscossione dei canoni di intercollegamento⁹³. Il Gruppo di lavoro è del parere che tale periodo debba essere sufficiente per consentire ai consumatori di contestare le fatture, ma che debba essere più breve possibile per non creare un carico eccessivo per gli operatori e i fornitori di servizi e per rispettare i principi di proporzionalità e specificità nell'ambito del diritto alla riservatezza. Il periodo in questione dovrebbe essere allineato sulla base dello standard di tutela più elevato che si riscontri negli Stati membri. Il Gruppo richiama l'attenzione sul fatto che, in diversi Stati membri, sono stati felicemente applicati periodi non superiori a tre mesi.

Il Gruppo di lavoro raccomanda altresì che i governi nazionali tengano conto delle presenti considerazioni.

Fatto a Bruxelles, addì 7 settembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁹³ In vista di questo obiettivo, non vi è motivo di effettuare distinzioni fra operatori pubblici o privati.

Documento di lavoro: Trattamento dei dati personali su Internet

5013/99/IT/final

WP 16

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Documento di lavoro: Trattamento dei dati personali su Internet

Adottato dal gruppo di lavoro il 23 febbraio 1999

Introduzione

Ogni nuova fase nel processo di sviluppo tecnologico pone problemi per la tutela dei dati personali e il diritto alla vita privata, come dimostra l'esperienza del passato per quanto riguarda ad esempio la distribuzione di personal computer, le prime applicazioni della telematica ecc. Internet rientra in tale contesto almeno per le seguenti ragioni:

- L'impiego delle infrastrutture si basa spesso direttamente sull'elaborazione di dati personali, come alcuni indirizzi del protocollo Internet.
- I servizi forniti per mezzo di queste infrastrutture offrono nuove possibilità, in particolare per quanto riguarda la distribuzione d'informazioni contenenti dati personali (ad es. indirizzari, gruppi di discussione, accesso alle basi dati ecc.).
- Gli strumenti tecnici sono nuovi, come nel caso dei programmi informatici di *browsing*, ed evolvono rapidamente.
- Molti operatori si trovano ad affrontare per la prima volta le nuove attività commerciali in linea che comportano il trattamento di dati personali ed anche i confini tradizionali tra le diverse professioni sono in rapida fase di ridefinizione.
- Uno degli usi più stimolanti di Internet è lo svolgimento di un'attività commerciale in linea: il commercio elettronico consiste in particolar modo nella vendita diretta dall'impresa ai consumatori senza alcuna intermediazione, grazie a nuovi metodi d'individuazione degli obiettivi commerciali e nuovi mezzi di pagamento.
- La dimensione globale si presenta fin dagli inizi.

In questo contesto complesso e, sotto il profilo della protezione dei dati, controverso lavorano concretamente da circa tre anni le autorità nazionali incaricate della tutela dei dati, la cui esperienza si è gradualmente consolidata (vedi ad es. i loro rapporti annuali).

Analogamente il gruppo⁴ ha iniziato ad occuparsi in modo pragmatico e in base all'urgenza dell'argomento discusso a livello europeo o internazionale delle questioni riguardanti l'applicazione al trattamento dei dati personali su Internet dei principi che reggono la tutela dei dati.

Alcuni esempi:

⁴ Istituito dall'articolo 29 della Direttiva 95/46/EC del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23 novembre 1995, p. 31. Disponibile all'indirizzo: <http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

- l'anonimato su Internet⁴⁵;
- il sostegno al "Memorandum di Berlino e Budapest" del gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni⁴⁶;
- un primo parere sul progetto P3P del Consorzio World Wide Web⁴⁷;
- la Raccomandazione 1/99 sul "Trattamento invisibile e automatico dei dati personali su Internet mediante software e hardware", adottata il 23 febbraio 1999⁴⁸.

La questione della protezione dei dati e della vita privata su Internet viene discussa anche in organismi internazionali quali il Consiglio d'Europa⁴⁹ e l'OCSE⁵⁰. In merito alla proposta dell'Unione europea di giungere a soluzioni globali nel quadro dell'OMC, tale organizzazione ha accettato d'includere la tutela dei dati nel suo programma di lavoro relativo ad aspetti del commercio elettronico attinenti alla compravendita. Il tema verrà discusso dal Consiglio per gli scambi di servizi, che si riunisce regolarmente per poter arrivare a presentare una relazione entro il giugno 1999. L'obiettivo è quello di concludere un accordo su principi fondamentali e vincolanti che consentano la libera circolazione dei dati personali nell'ambito del commercio elettronico mondiale, rispettando nel contempo il diritto dei singoli alla vita privata e che assicurino quindi l'affidabilità del commercio elettronico.

La conferenza europea dei commissari responsabili per la protezione dei dati, tenutasi a Dublino il 23 e il 24 aprile 1998, ha auspicato che il gruppo potesse sviluppare il tema in modo più sistematico al fine di chiarire quali fossero le questioni in causa e fornire soluzioni volte a contribuire a uno sviluppo d'Internet e dei servizi ad esso attinenti che rispetti il diritto dell'utente alla vita privata e garantisca l'affidabilità sia per le applicazioni commerciali che per quelle private. I commissari hanno ricordato che quanto disposto dalla legislazione dell'UE in tema di tutela dei dati si applica pienamente, secondo le modalità del caso, al trattamento dei dati personali su Internet, a prescindere dagli strumenti tecnici utilizzati.

La pertinenza delle direttive sulla protezione dei dati

Il gruppo condivide il parere espresso in occasione della conferenza europea dei commissari responsabili per la protezione dei dati. Sotto il profilo giuridico Internet non opera nel vuoto: il trattamento dei dati personali su Internet deve pertanto rispettare i principi della tutela dei dati così come avviene al di fuori della rete⁵¹. Ciò non limita assolutamente il ricorso ad Internet, ma al contrario fa parte degli elementi fondamentali volti ad assicurare la fiducia degli utenti nel funzionamento di Internet e dei servizi forniti da esso. La tutela dei dati su Internet è quindi una condizione indispensabile per l'accettazione del commercio elettronico.

La direttiva generale relativa alla protezione dei dati 95/46/EC si applica a qualsiasi trattamento di dati personali che rientri nel suo ambito a prescindere dai mezzi tecnici utilizzati. Per questo motivo il trattamento dei dati personali su Internet rientra nel campo d'applicazione della direttiva.

⁴⁵ Si veda la Raccomandazione del gruppo 3/97 "L'anonimato su Internet", adottata il 3 dicembre 1997, disponibile all'indirizzo: vedi nota 1.

⁴⁶ Si veda la Raccomandazione del gruppo 2/97 "Rapporto e orientamenti del gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni ("Memorandum di Berlino e Budapest sulla protezione dei dati e della vita privata su Internet"), adottata il 3 dicembre 1997, disponibile all'indirizzo: vedi nota 1.

⁴⁷ Si veda il Parere del gruppo 1/98 "Piattaforma in materia di rispetto della vita privata (P3P) e lo Standard di definizione di profili aperti (OPS)", adottato il 16 giugno 1998, disponibile all'indirizzo: vedi nota 1.

⁴⁸ Disponibile all'indirizzo: vedi nota 1.

⁴⁹ Il Consiglio d'Europa è in procinto di adottare linee guida in materia di protezione della vita privata sulle autostrade dell'informazione.

⁵⁰ Si vedano i risultati della conferenza di Ottawa dell'ottobre 1998: disponibile all'indirizzo <http://www.oecd.org>.

⁵¹ Si veda anche la dichiarazione ministeriale del Convegno sulle reti globali d'informazione, tenutosi a Bonn nel luglio del 1997, disponibile all'indirizzo: <http://www2.echo.lu/bonn/conference.html>.

La direttiva specifica 97/66/EC relativa alla tutela della vita privata e dei dati personali nel settore delle telecomunicazioni⁴² integra la direttiva generale 95/46/EC introducendovi norme specifiche in ambito tecnico e giuridico.⁴³

Internet è una rete di computer aperta a tutti e forma dunque parte del settore pubblico delle telecomunicazioni. Le disposizioni della direttiva 97/66/EC si applicano perciò al trattamento dei dati personali con riferimento alla fornitura di servizi di telecomunicazione disponibili al pubblico mediante reti pubbliche di telecomunicazioni all'interno della Comunità⁴⁴.

La task force Internet

Il gruppo è consapevole del fatto che l'applicazione omogenea delle direttive relative alla protezione dei dati nell'ambito del trattamento dei dati personali su Internet richiede un'analisi che tenga in considerazione soprattutto gli aspetti tecnici e giuridici. Il gruppo intende inoltre contribuire a dar risposta ai molteplici e dettagliati quesiti che potranno essere posti a questo riguardo.

Al fine di assicurare un approccio coerente e omogeneo al trattamento dei dati su Internet il gruppo ha istituito una task force interdisciplinare il cui compito è quello d'identificare le problematiche relative a Internet da discutere ed elaborare i pareri del gruppo a questo riguardo.

La task force di Internet ha già preparato la Raccomandazione 1/99 del gruppo relativa al trattamento invisibile e automatico dei dati personali su Internet mediante software e hardware⁴⁵.

La task force Internet continuerà a lavorare più generalmente sull'applicazione delle due direttive al trattamento dei dati personali su Internet e presenterà proposte riguardanti le modalità per attuarne in modo omogeneo le prescrizioni per quanto riguarda, ad esempio, i servizi di posta elettronica (e-mail) e i dati relativi al traffico su Internet.

Fatto a Bruxelles, addì 23 febbraio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁴² A norma dell'articolo 14 paragrafo 3 della Direttiva 97/66/EC, il gruppo Istituito dalla Direttiva 95/46/EC deve svolgere le sue funzioni anche per quanto concerne la tutela dei diritti e delle libertà fondamentali nonché dei legittimi interessi nel settore delle telecomunicazioni, che sono oggetto della Direttiva 97/66/EC.

⁴³ Per quanto riguarda tutti gli aspetti non specificamente regolati dalla Direttiva 97/66/EC, quali gli obblighi del controllore e i diritti delle persone fisiche o i servizi di telecomunicazione non offerti al pubblico, si applica la Direttiva 95/46/EC (si veda il punto 11 del preambolo della Direttiva 97/66/EC).

⁴⁴ Si veda l'articolo 3 paragrafo 1 della Direttiva 97/66/EC.

⁴⁵ Adottata il 23 febbraio 1999. Disponibile all'indirizzo: vedi nota 1.

6.3.4. Informazione nel settore pubblico**Parere 3/99 relativo a: L'informazione del settore pubblico e la protezione dei dati personali**

WP 20

Gruppo di protezione delle persone
rispetto al trattamento dei dati personali

Parere 3/99 relativo a: L'informazione del settore pubblico e la protezione dei dati personali

Contributo alla consultazione iniziata con il libro verde della Commissione europea intitolato
"L'informazione del settore pubblico: una risorsa fondamentale per l'Europa", COM (1998) 585

Adottato il 3 maggio 1999

Introduzione e osservazioni preliminari:

La Commissione europea ha sottoposto alla consultazione pubblica un libro verde su "informazione del settore pubblico: una risorsa fondamentale per l'Europa". L'oggetto principale del libro consiste nel promuovere una discussione sul modo di agevolare l'accesso delle informazioni detenute dal settore pubblico ai cittadini ed alle imprese nonché sulla necessità o no di armonizzare le norme nazionali in questo settore. Sembra che il documento si sia ampiamente ispirato alla rivendicazione degli operatori privati che desiderano accedere al minimo costo alle informazioni pubbliche e contestano il mantenimento dei monopoli pubblici nel campo in questione.

Una delle poste in gioco del libro verde riguarda dunque la messa a disposizione dell'informazione del settore pubblico, vale a dire di una categoria particolare di dati detti "pubblici", quelli che, essendo detenuti da organismi del settore pubblico, verrebbero resi pubblici in virtù di norme o di un uso⁶⁷ il cui fondamento implicito ed esplicito può trovarsi in una volontà di trasparenza dello stato nei confronti dei cittadini⁶⁸.

La protezione dei dati personali non è affatto ignorata da questo documento sebbene non ne rappresenti a prima vista la problematica più importante.

Il punto 111 (II. 7, pag. 17) menziona in modo esplicito che la direttiva 95/46/CE relativa alla protezione dei dati personali⁶⁹ "stabilisce norme obbligatorie per i settori pubblico e privato e [...] si applica pienamente nel caso in cui dati personali siano detenuti dal settore pubblico".

Il punto 114 sottolinea che "l'emergere della società dell'informazione potrebbe comportare nuovi rischi per la vita privata degli individui se alcuni registri pubblici diventassero accessibili sotto forma elettronica (in particolare online, su Internet, e in grandi quantità)".

Il libro verde, nel complesso, porta alla luce, tuttavia, diverse ambiguità sulla forza di tale convinzione.

⁶⁷ Com 1998 – 585, disponibile al seguente indirizzo: <http://www.echo.lu/legal/en/access.htm>.

⁶⁸ Sembra che una distinzione possa essere fatta fra la pubblicazione derivante da disposizioni di legge, l'accesso all'informazione autorizzato dalla legge, e situazioni nelle quali la questione della pubblicità o dell'accesso si pone in seguito a una domanda formulata da privati o imprese senza che entrino in gioco particolari disposizioni di legge.

⁶⁹ Il presente parere non tratta pertanto dell'altra accezione - più ampia - del concetto di dati "pubblici": l'insieme dei dati gestiti dal settore pubblico.

⁷⁰ Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla protezione delle persone fisiche in relazione all'elaborazione dei dati a carattere personale e alla libera circolazione di tali dati, GU L 281, 23 novembre 1995, p. 31. Disponibile all'indirizzo seguente: <http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm>.

In primo luogo l'impiego (nella versione inglese) del termine "publicly available" (disponibile pubblicamente) è propizio al concetto secondo il quale i dati resi pubblici sarebbero di conseguenza disponibili per qualsiasi uso. Si noterà che il principio di finalità, pilastro delle nostre legislazioni sulla protezione dei dati, s'adatta male all'aggettivo "disponibile". Il principio della lealtà della raccolta, inoltre, garantito soprattutto dall'esigenza di sicurezza dei trattamenti, potrebbe essere danneggiato per il fatto che un dato venga reso pubblico senza riflessioni né precauzioni. Per questo motivo l'espressione "publicly available" andrebbe allontanata a vantaggio di un'altra formulazione più adeguata e scevra di ambiguità (ad esempio « publicly accessible »).

In secondo luogo la domanda n 7 ("le considerazioni relative al rispetto della vita privata meritano un'attenzione particolare per quanto riguarda lo sfruttamento dell'informazione del settore pubblico?", pagina 17) potrebbe far pensare che il richiamo delle disposizioni dettate dalla direttiva 95/46/CE non porta a precise e salde conclusioni al riguardo, allorché si precisa (punto 111) che la direttiva 95/46/CE "realizza l'equilibrio necessario tra il principio dell'accesso all'informazione del settore pubblico e la protezione dei dati personali". Occorre eliminare tali ambiguità.

In tale contesto il presente parere ha per obiettivo nutrire la riflessione sulla dimensione della protezione dei dati personali, che è essenziale quando ci s'impegna ad agevolare l'accesso ai dati del settore pubblico dal momento che questi riguardano le persone fisiche. Non ha tuttavia la pretesa di fornire tutte le risposte alle domande sollevate dalla conciliazione tra l'obiettivo di agevolare l'accesso ai dati del settore pubblico, fondata sulla volontà di rafforzare la trasparenza degli Stati nei riguardi del cittadino, e la protezione dei dati personali così com'è definita dalla direttiva europea 95/46/CE.

Tale parere non tratterà quindi interrogativi sollevati dal libro verde che sembrano superare la messa a disposizione di terzi dell'informazione del settore pubblico, come ad esempio il punto di vista espresso al punto 56 (II ; 2, pagina 10) secondo cui « l'impiego delle nuove tecnologie può accrescere in modo considerevole l'efficacia della raccolta d'informazione. Esso offre agli organismi pubblici la possibilità di condividere l'informazione disponibile, quando conforme alle norme sulla protezione dei dati ».

Lo scopo è di fornire, sulla base della direttiva 95/46/CE e di esperienze concrete a fini pedagogici nel campo dei registri più conosciuti dei dati a carattere personale resi pubblici, un primo insieme di punti di riferimento che occorre prendere in considerazione all'atto di adozione di decisioni concrete. Questi punti di riferimento e esempi concreti provenienti da diversi Stati membri sono destinati ad illustrare come, nella società dell'informazione, devono essere prese in considerazione le norme di protezione dei dati in relazione a quelli derivati da registri pubblici, nonché alcune misure d'ordine tecnico o organizzativo che possono contribuire (senza tuttavia pretendere di garantire una tutela senza difetti) a conciliare la pubblicità di questi dati e il rispetto delle disposizioni di protezione dei dati a carattere personale e in particolare quelle relative al principio fondamentale in materia, ossia il principio della finalità per la quale i dati vengono, nel nostro caso, resi pubblici.

(I) Le norme di protezione dei dati si applicano ai dati a carattere personale resi pubblici

L'accessibilità delle informazioni che dipendono dal settore pubblico, in particolare mediante informatizzazione, raccomandata dal libro verde, pone il problema di sapere in quali modi verranno utilizzate le informazioni. Il loro utilizzo non può essere vietato, perché ciò è in contrasto con l'evoluzione delle nostre società. Non è quello il senso delle nostre legislazioni di protezione dei dati, che si fanno garanti della tutela dell'informatizzazione della società, e non del suo divieto.

D'altra parte, l'applicabilità delle nostre leggi di protezione dei dati ai dati personali resi pubblici, è soltanto l'espressione di un elemento che deriva dai testi stessi sulla protezione dei dati: un dato a carattere personale, anche reso pubblico, resta un dato a carattere personale e merita, di conseguenza, la dovuta protezione.

Questa dichiarazione implica necessariamente una definizione della protezione che viene offerta al dato a carattere personale reso pubblico. A tale riguardo, la direttiva 95/46/CE fornisce fin d'ora alcune risposte.

A. La direttiva 95/46/CE relativa alla protezione delle persone fisiche in relazione all'elaborazione dei dati a carattere personale e alla libera circolazione di questi dati

La direttiva permette di prendere in considerazione, nell'attuazione delle norme previste, il principio del diritto d'accesso del pubblico ai documenti amministrativi⁷⁰ ed anche altri elementi pertinenti⁷¹.

In tal modo, il principio della finalità esige che i dati a carattere personale siano raccolti per finalità determinate, esplicite e legittime, e non possono essere successivamente trattati in modo incompatibile con tali finalità⁷². Questo principio svolge un ruolo fondamentale per l'accesso dei dati a carattere personale detenuti dal settore pubblico.

Occorre in particolare determinare caso per caso in quale misura una legge esige o autorizza la pubblicazione o l'accesso da parte del pubblico a dati a carattere personale: si tratta forse di un'accessibilità integrale e illimitata nel tempo, di un utilizzo dei questi dati a qualsiasi fine, indipendentemente dalla finalità iniziale, o, al contrario, di un'accessibilità soltanto parziale e/o di un utilizzo vincolato alle finalità per le quali i dati sono stati resi pubblici? Di conseguenza, non esiste un'unica categoria di dati a carattere personale destinati a essere resi pubblici, e che dovrebbero essere trattati uniformemente dal punto di vista della protezione, ma occorre piuttosto procedere ad una analisi per gradi dei diritti dell'individuo interessato e, rispettivamente, dei diritti di accesso del pubblico. Benché l'accesso ai dati possa essere pubblico, esso può essere sottoposto ad una serie di condizioni (come la dimostrazione di un interesse legittimo) mentre lo sfruttamento dei dati, ad esempio a fini commerciali o da parte dei mass media, può essere limitato. Gli esempi che seguono illustrano questi interrogativi.

È poi utile ricordare che, indipendentemente dalla pubblicazione o meno dei dati a carattere personale, l'interessato ha sempre il diritto di accedere ai dati che lo riguardano, e il diritto di esigere, se necessario, la correzione o cancellazione di dati la cui gestione non è conforme alla direttiva, in particolare a causa di un loro possibile carattere incompleto o inesatto⁷³.

Indubbiamente, diverse disposizioni della direttiva fanno esplicitamente riferimento al carattere pubblico dei dati. Due di queste disposizioni meritano di essere citate con tutte le sfumature.

L'articolo 18.3, che impone un obbligo di notificazione all'autorità di controllo per quanto riguarda i trattamenti a cui vengono sottoposti i dati, permette di fare eccezione a quest'obbligo per la compilazione di registri "i quali, in forza di disposizioni legislative o regolamentari (... siano) predisposti per l'informazione del pubblico e siano aperti alla consultazione del pubblico". Ma i considerando 50 e 51 della direttiva precisano che queste deroghe o semplificazioni si applicano soltanto ai trattamenti il cui scopo (prima condizione) è di mantenere un registro destinato, nel rispetto del diritto nazionale, all'informazione del pubblico (2a condizione) e che sia aperto alla consulta-

⁷⁰ Vedi considerando 72. Occorre notare che la direttiva non contiene definizioni del termine "documenti amministrativi", ma che tale termine può essere inteso in senso ampio che permette di coprire almeno le "informazioni amministrative" previste dal libro verde nella proposta di classificazione (punto 73 e seguente, pagina 12).

⁷¹ Vedi l'articolo 10 e il considerando 37 della direttiva 95/46/CE sulla conciliazione del diritto alla vita privata con le norme che disciplinano la libertà d'espressione. Vedi anche la raccomandazione 1/97 del Gruppo su "Legislazione sulla protezione dei dati e mass media", adottata il 25.2.1997 (documento 5012/9, disponibile nelle 11 lingue ufficiali all'indirizzo indicato in nota alla pagina 2).

⁷² Vedi in particolare l'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/EC.

⁷³ Vedi articolo 12 della direttiva 95/46/EC.

zione del pubblico o di chiunque possa dimostrare un interesse legittimo (3a condizione), per cui tali deroghe non dispensano il responsabile del trattamento da alcuno degli altri obblighi che derivano dalla direttiva.

Infine, l'articolo 26.1. f consente una deroga all'esigenza di un livello adeguato di protezione per i dati che sono oggetto di un trasferimento verso paesi terzi quando il trasferimento dei dati stessi verso un paese che non offre lo stesso livello di garanzia è realizzato "a partire da un registro aperto alla consultazione del pubblico". Tuttavia, il considerando 58 della direttiva limita la portata del trasferimento precisando che non deve riguardare la totalità dei dati né intere categorie di dati contenuti nel registro, e che, eventualmente, il trasferimento deve essere effettuato soltanto su richiesta di persone che hanno un interesse legittimo in proposito.

Ma deriva chiaramente da queste disposizioni e precisazioni che se la protezione dei dati a carattere personale non deve ostacolare il diritto dei cittadini di avere accesso ai documenti amministrativi alle condizioni previste da ogni legislazione nazionale, la direttiva non ha inteso privare i dati accessibili al pubblico di qualsiasi protezione.

La discussione sul problema di sapere se c'è bisogno di armonizzare le norme nazionali sull'accesso all'informazione del settore pubblico deve comunque tenere conto delle norme armonizzate sulla protezione dei dati a carattere nazionale, come pure delle misure nazionali che le recepiscono.

Oltre alla missione della Commissione di vigilare sull'applicazione della direttiva, spetta inoltre al Gruppo Istituito dall'articolo 29 della direttiva di apprezzare concretamente la portata delle disposizioni nazionali adottate in applicazione della direttiva stessa nei casi precisi in cui potrebbero risultare divergenze sul piano nazionale.⁷¹

B. Esempi di conciliazione delle norme sulla protezione dei dati personali e sull'accesso alle informazioni del settore pubblico

Alcune legislazioni subordinano la diffusione di informazioni detenute dal settore pubblico a talune finalità che possono comportare un divieto d'accesso ad alcuni dati, il divieto di alcune utilizzazioni, o comunque particolari condizioni di accesso.

Ma la digitalizzazione delle informazioni e le possibilità di ricerca a testo integrale possono moltiplicare all'infinito le possibilità d'interrogazione e di selezione, mentre la diffusione di Internet aumenta i rischi di cattura e deviazione dei dati. Inoltre, la combinazione di dati del settore pubblico di provenienza diversa, una volta pubblicati, è grandemente facilitata dalla digitalizzazione dei dati stessi, e permette, in particolare, la creazione di profili sulle condizioni di vita o il comportamento degli individui⁷². Inoltre, occorre prestare un'attenzione particolare al fatto che, mettendo i dati a carattere personale a disposizione del pubblico, si alimentano in vasta misura le nuove tecniche di "data warehousing" e di "data mining". Questi metodi permettono di raccogliere dati senza alcuna indicazione preliminare delle relative finalità, che vengono definite soltanto alla fase di sfruttamento. Di conseguenza, occorre tenere attentamente conto di tutto ciò che è tecnicamente possibile fare con i dati⁷³.

È per questo che occorre verificare, caso per caso, quali potrebbero essere le ripercussioni negative sull'individuo prima di qualsiasi decisione di diffusione su supporto numerico. A seconda dei casi, occorre o decidere di non diffondere taluni dati a carattere personale, oppure sottoporre la diffusione alla decisione dell'interessato, o ad altre condizioni.

⁷¹ Vedi gli articoli 29 e 30 della direttiva 95/46/CE.

⁷² Si noti che l'utilizzazione di queste tecnologie permette anche allo Stato di elaborare siffatti profili.

⁷³ Altro esempio: grazie al controllo elettronico di due banche dati, si possono ottenere più facilmente informazioni negative su questa o quella persona, ad esempio: il vaglio del registro della popolazione (quando esiste) e degli elenchi elettorali permette di identificare le persone che non hanno diritto di voto.

Le basi dati derivanti da decisioni dell'autorità giudiziaria:

Il punto 74 del libro verde (pagina 11) che fa riferimento alle sentenze dei tribunali, per illustrare il concetto d'informazione fondamentale al funzionamento della democrazia, solleva un interrogativo di fondo. Infatti, è lecito ritenere che tutte le sentenze di tutte le giurisdizioni possano essere disponibili su Internet senza recare pregiudizio alle persone.

Strumento di documentazione giuridica, le basi dati sulla giurisprudenza possono diventare, in mancanza di precauzioni particolari, schedari informativi sui cittadini se vengono consultate non per conoscere la giurisprudenza ma ad esempio per identificare tutte le procedure giudiziarie che si riferiscono ad una stessa persona.

La Commissione per la Protezione della Vita Privata (Belgio), in un parere del 23 dicembre 1997, lo ha sottolineato con forza: "l'evoluzione tecnologica deve accompagnarsi ad una maggiore prudenza quando si tratta di identificare le parti nelle cronache giudiziarie". Essa propone che, in mancanza di una completa anonimità, le decisioni giudiziarie accessibili al pubblico non siano indicizzate in base al nome delle parti, per impedire eventuali ricerche sulla base di questo criterio.

La Commissione per la protezione dei dati personali italiana⁷⁷ ha intenzione di proporre a livello nazionale che le parti dispongano di un diritto d'opposizione alla pubblicazione del loro nome nelle basi dati della giurisprudenza. Questo diritto dovrebbe essere esercitabile in qualsiasi momento, e dovrebbe essere tenuto presente in occasione dell'aggiornamento delle basi dati diffuse su supporto magnetico. L'esercizio di questo diritto non avrebbe effetto retroattivo sulle pubblicazioni su carta.

In Francia, il ministero della giustizia, che desidera diffondere le basi dati della giurisprudenza su Internet, ha imposto, nel relativo capitolato d'oneri, l'anonimità delle decisioni.

Alcuni testi ufficiali:

La diffusione di informazioni su Internet implica una massa enorme di informazioni su scala mondiale, ed una moltiplicazione delle relative fonti. Questo cambiamento di scala geografica può comportare un rischio particolare. Infatti, è possibile che la diffusione di un'informazione legittimamente pubblica in un determinato paese possa causare, a livello mondiale, danni gravi alla vita privata o all'integrità fisica delle persone. Ciò avviene quando, ad esempio, le decisioni in materia di naturalizzazione (cittadinanza) sono oggetto di pubblicazione ufficiale obbligatoria. Tale è il caso della Francia, dove, secondo il parere della Commissione Nazionale dell'Informatica e delle Libertà (CNIL), il Governo francese, in occasione della pubblicazione su Internet della Gazzetta Ufficiale, ha escluso questo tipo di testi per evitare ad alcuni cittadini che hanno abbandonato la nazionalità d'origine il rischio di incorrere in eventuali rappresaglie.

Così, in alcuni casi, la volontà di trasparenza di uno Stato, ed in particolare dei suoi cittadini, può adattarsi male alla diffusione planetaria delle informazioni.

Altri esempi di diffusione di dati personali resi pubblici e sottoposti a condizioni miranti a proteggere gli interessati:

Le condizioni d'accesso ai dati a carattere personale contenuti nei registri possono essere molto varie, a seconda della regolamentazione: ad esempio, accesso parziale ai dati del registro, necessità di dimostrare un interesse legittimo, o divieto di impieghi commerciali.

Così, in Germania, gli elenchi dei candidati alle elezioni federali devono comportare cognome, nome, professione, giorno e luogo di nascita e indirizzo. Tuttavia, sugli elenchi resi pubblici prima dello voto dal responsabile locale o del Land incaricato dello svolgimento delle elezioni federali, il giorno di nascita è sostituito dall'anno di nascita.

In Italia, la legislazione relativa al registro della popolazione, tenuto da ogni municipio, prevede il divieto della comunicazione dei dati agli enti privi e l'obbligo di qualsiasi amministrazione che chiede la comunicazione dei dati stessi di dimostrare un congruo interesse pubblico.

⁷⁷ Garante per la protezione dei dati personali

In Francia, le liste elettorali sono pubbliche a fini del controllo della regolarità. La legge ne permette l'utilizzazione a fini politici da parte di tutti i candidati e tutti i partiti, ma ne proibisce l'impiego commerciale. Non sarebbe concepibile, in queste condizioni, che gli elenchi elettorali possano essere diffusi su Internet.

Inoltre in Francia, i dati a carattere personale contenuti nel catasto sono pubblici, ma è vietato farne un impiego commerciale.

In Grecia, il presente sistema del catasto organizzato in base ad un registro alfabetico dei proprietari di beni immobiliari sarà sostituito da un registro basato sull'identificazione dei beni immobili per impedire che le ricerche riguardino l'insieme dei beni immobiliari che appartengono ad una stessa persona. L'accesso al catasto è sottoposto alla dimostrazione di un interesse legittimo.

(II) Le nuove tecnologie possono contribuire a conciliare la protezione dei dati personali e la loro pubblicazione

Le nuove tecnologie, e talune misure amministrative di accompagnamento, pur favorendo l'accesso ai dati pubblici, in particolare con la "messa on-line", sono anche in grado di facilitare il rispetto dei principi principali di protezione dei dati, come il principio della finalità, quello dell'informazione e del diritto di opposizione, e quello della sicurezza. Tuttavia, l'utilizzazione di queste tecnologie non presenta una garanzia assoluta contro il rischio di abusi e di deviazioni dai principi di protezione dei dati personali che abbiamo descritto.

A Le condizioni tecniche d'accesso alle informazioni provenienti dal settore pubblico devono contribuire al rispetto del principio di finalità

Tenuto conto delle condizioni d'accessibilità numerica del pubblico, è certamente molto difficile garantire nella pratica la specificazione della finalità, ma un ricorso ragionato e determinato alla tecnica deve contribuire a raggiungere quest'obiettivo. Occorre per ciò verificare e definire in ogni caso le condizioni di interrogazione. A tale riguardo, si dovrebbe applicare il principio seguente: "chiunque può leggere qualsiasi dato, preso singolarmente, nella misura autorizzata, ma non tutti i dati nel loro insieme". La scelta dei criteri di ricerca deve escludere ogni possibilità di abuso in situazioni normali. Occorre inoltre verificare se non è possibile aggirare l'ostacolo ottenendo informazioni complementari presso altre fonti.

È per questo che la consultazione on-line di banche dati può essere oggetto di restrizioni tali da impedire la deviazione dalle finalità per le quali i dati vengono resi pubblici. Queste misure, da definire caso per caso, possono consistere, ad esempio, nel limitare il campo o i criteri d'interrogazione.

Così, in Francia, gli estratti dell'atto di nascita sono accessibili a chiunque dispone dell'identità, della data e del luogo di nascita di una persona. La CNIL ha subordinato la consultazione on-line di questi estratti alla condizione che la relativa richiesta elettronica comporti tutte queste informazioni. In tal modo, utilizzando gli opportuni criteri restrittivi per l'interrogazione delle basi dati, la raccolta su vasta scala di queste informazioni a scopi di utilizzo commerciale può essere evitata, e la finalità dell'accesso rispettata.

In Francia, allo stesso modo, l'elenco telefonico pubblicato su supporto telematico poteva essere interrogato a partire dalle prime lettere del cognome, il che ne rendeva più facile la teletrasmissione e l'utilizzo commerciale contro la volontà di alcuni abbonati che si erano opposti a tale impiego. Ma il blocco su Minitel e Internet di questo tipo d'interrogazione ha permesso di evitare eventuali deviazioni di finalità con questo mezzo.

Nei Paesi Bassi, i CD-Rom destinati alla diffusione dell'elenco del telefono sono stati concepiti in modo da impedire il reperimento del nome e dell'indirizzo di una persona a partire dal relativo numero di telefono (non è possibile l'interrogazione della base dati esclusivamente sul campo costituito dal numero di telefono).

Inoltre le basi dati relative ai registri delle imprese non possono essere interrogate in base al nome di una persona, il che potrebbe permettere una ricerca del complesso di imprese nelle quali una stessa persona è presente.

B Promuovere il ricorso ai mezzi tecnici che tendono ad impedire la cattura automatizzata dei dati accessibili on-line

Si può citare il protocollo di esclusione dei motori di ricerca (Robots Exclusion Protocol) che permette di evitare l'indicizzazione automatica totale o parziale delle pagine di un sito. In ogni caso, questi metodi possono essere efficaci soltanto se i progettisti dei siti e i navigatori internet sono informati della loro esistenza, e se i motori di ricerca li rispettano. Alcune società che producono motori di ricerca dichiarano di rispettare questo protocollo.

(III) Utilizzazione commerciale

I dati a carattere personale detenuti dal settore pubblico sono stati inizialmente raccolti ed elaborati con finalità precise, e, normalmente, in base ad una regolamentazione. A volte la raccolta era obbligatoria, a volte una condizione per accedere ad un servizio pubblico. Il cittadino, pertanto, non si aspetta che i dati che lo riguardano siano resi pubblici e utilizzati a fini commerciali. È per questo che, fra l'altro, alcune legislazioni nazionali permettono l'accesso pur proibendo l'utilizzo commerciale delle informazioni del settore pubblico, compresi i dati a carattere personale⁷⁸.

Dal punto di vista della direttiva 95/46/CE⁷⁹, si pone il problema di sapere se l'utilizzo commerciale deve essere considerato come finalità incompatibile con quella per cui i dati sono stati raccolti inizialmente, e, in caso affermativo, a quali condizioni potrebbe essere consentito un tale utilizzo.

Se la pubblicazione e la commercializzazione delle informazioni derivanti dal settore pubblico sono ammesse⁸⁰, occorre rispettare alcune regole, e quindi porsi il problema, caso per caso, di come conciliare effettivamente il rispetto della vita privata con gli interessi commerciali degli operatori.

La direttiva 95/46/CE riconosce il diritto degli interessati di essere informati sul trattamento dei relativi dati, ed anche un diritto di opporsi a trattamenti sia pure legittimi. Le persone devono dunque essere informate della finalità di commercializzazione, e potere opporsi a tale utilizzo con mezzi semplici e efficaci⁸¹.

Su questo punto, c'è ancora molto da fare. La molteplicità delle fonti di diffusione dei dati, il grande numero di operatori, la possibilità di teletrasmissione, tutto ciò concorre a sostenere l'idea di uno sportello unico per la protezione dei dati, affinché i cittadini non siano costretti a molteplici azioni presso tutti gli operatori. È il caso, in molti paesi, degli elenchi degli abbonati al telefono.

Per la stessa ragione, la CNIL⁸² ha raccomandato agli editori di guide di identificare su tutti i relativi supporti (carta, CD-ROM, Minitel o Internet) gli abbonati che hanno esercitato il diritto di opporsi all'utilizzazione dei loro dati a fini commerciali.

Questa idea dello sportello unico sembra essenziale, tanto per il rispetto dei diritti delle persone che per gli operatori commerciali che desiderano utilizzare dati a carattere personale.

La conciliazione del diritto alla vita privata e degli interessi commerciali degli operatori potrebbe anche portare al fatto che il consenso dell'interessato⁸³, e persino provvedimenti legislativi o normativi, siano necessari, come illustrato dall'esempio seguente:

In un parere relativo alla commercializzazione dei dati derivanti dalle licenze edilizie, la Commissione belga per la protezione della vita privata ha ritenuto che una diversa finalità (cioè la

⁷⁸ Vedi allegato 1 del libro verde: Situazione attuale negli Stati membri per quanto riguarda la legislazione e le politiche relative all'accesso all'informazione proveniente dal settore pubblico, p. 21 e seguenti.

⁷⁹ Vedi articolo 6 paragrafo 1 b della direttiva 95/46/CE.

⁸⁰ Merita sottolineare che, secondo alcuni, siccome la riunione di dati diversi permette di elaborare profili personali, si deve proibire l'utilizzazione commerciale dei dati a carattere personale, o almeno limitarla, con opportune penali in caso di infrazioni. Per quanto riguarda i dati a carattere personale ricavati da fonti ufficiali, non dovrebbero sussistere eccezioni all'obbligo di informare l'interessato (articolo 11 della direttiva).

⁸¹ Vedi articoli 10, 11 e 14 della direttiva 95/46/CE.

⁸² Commissione Nazionale dell'Informatica e delle Libertà, Francia.

⁸³ Vedi i articoli 2 h), 7a e 8 della direttiva 95/46/CE concernenti la definizione di "consenso" nonché l'esigenza di forme specifiche del consenso a seconda dei casi.