5085/99/IT/DEFINITIVO
WP 25

GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Raccommandazione 3/99

La conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari

Approvata il 7 settembre 1999

Raccomandazione 3/99

La conservazione del dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari

Introduzione

La lotta alla criminalità elettronica costituisce un problema che sta richiamando crescente attenzione internazionale.[1] I paesi G8[2] hanno approvato un piano d'azione[3] 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 personali[4] 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

---

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 della 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: at: http:// europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

protezione dei dati[5] a livello di attuazione onde tenere conto delle esigenze di controllo unitamente a quelle attinenti alla riservatezza.

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.[6]

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

[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.

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

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 costituiscano 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 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 1999[7], 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/CE[8]. 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

---

[7] Disponibile all'indirizzo di cui alla nota 1.

[8] 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").

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 vietate[9]. 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 nazionali[10]

Per quanto riguarda il periodo durante il quale i dati sul traffico possono essere memorizzati, la Direttiva 97/66/CE ne consente la conservazione unicamente a fini di fatturazione[11] 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

---

[9] 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".

[10] 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.

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

delle fatture[12]. 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. E' 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.

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

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 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 intercollegamento[13]. 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, il 7 settembre 1999

Per il Gruppo di lavoro

Il Presidente

Peter HUSTINX

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