ARTICOLO 29 - Gruppo per la tutela dei dati personali

01611/06/IT
WP 126

Parere 8/2006 sulla revisione del quadro normativo per le reti ed i servizi di comunicazione elettronica, con particolare attenzione alla direttiva relativa alla vita privata e alle comunicazioni elettroniche

Adottato il

26 settembre 2006

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti l'articolo 29, l'articolo 30, paragrafo 1, lettera a), l'articolo 30, paragrafo 3, della richiamata direttiva e l'articolo 15, paragrafo 3, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il seguente parere:

1. Contesto

Il 29 giugno 2006 la Commissione europea ha adottato una comunicazione sulla revisione del quadro normativo comunitario per le reti ed i servizi di comunicazione elettronica {SEC (2006) 816} {SEC (206) 817}. Tale comunicazione contiene le relazioni sul funzionamento delle cinque direttive che costituiscono il quadro normativo per le reti ed i servizi di comunicazione elettronica[1], illustra in quale modo il quadro normativo ha conseguito i suoi obiettivi e individua i settori nei quali potranno essere apportati cambiamenti.

La comunicazione è integrata da un documento di lavoro dei servizi della Commissione {COM (2006) 334 definitivo} in cui sono precisate le modifiche proposte. Prima di giungere alle conclusioni illustrate nella comunicazione, la valutazione d'impatto passa in rassegna una vasta gamma di opzioni prese in considerazione. I suddetti documenti hanno dato l'avvio a una consultazione pubblica sul futuro del quadro normativo per le comunicazioni elettroniche. Le osservazioni in proposito devono essere fatte pervenire entro il 27 ottobre 2006.

In una fase successiva, tenuto conto delle osservazioni che avrà ricevuto, la Commissione formulerà proposte legislative per la modifica del quadro normativo, che saranno presentate al Parlamento europeo e al Consiglio.

La revisione riguarda inoltre la direttiva relativa alla vita privata e alle comunicazioni elettroniche (di seguito "direttiva sull'ePrivacy"), che fa parte del pacchetto sulle comunicazioni elettroniche. Il Gruppo di lavoro Articolo 29 auspica di contribuire con le osservazioni qui di seguito riportate alla consultazione pubblica, concentrandosi soprattutto sulla direttiva sull'ePrivacy.

2. Osservazioni generali

Le principali preoccupazioni del Gruppo di lavoro Articolo 29 riguardano il trattamento dei dati personali nelle comunicazioni elettroniche e attraverso le comunicazioni elettroniche, nonché la sua sicurezza, dato che esso solleva una serie di problemi in materia di protezione dei dati che il Gruppo di lavoro Articolo 29 desidera affrontare nel presente parere.

[1] Direttive 19/2002/CE (GU L 108 del 24.4.2002, pag.7), 20/2002/CE (GU L 108 del 24.4.2002 pag. 21), 21/2002/CE (GU L 108 del 24.4.2002, pag. 33), 22/2002/CE (GU L 108 del 24.4.2002, pag. 51) e 58/2002/CE (GU L 201 del 31.7.2002, pag. 37).

Nel valutare la Comunicazione, in particolare la direttiva sull'ePrivacy e le possibili modifiche da apportarvi, il Gruppo di lavoro Articolo 29 intende fare riferimento al suo parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[2]. Poiché varie proposte di detto parere non sono state prese in considerazione, il gruppo di lavoro desidera esporle nuovamente:

(1) Nel citato parere il Gruppo di lavoro Articolo 29 ha sottolineato il fatto che le disposizioni della direttiva sull'ePrivacy riguardano solo la fornitura di servizi di comunicazione elettronica accessibili al pubblico sulle reti pubbliche di comunicazioni, cosa deplorevole poiché le reti private stanno acquisendo un'importanza crescente nella vita quotidiana, con un conseguente aumento dei rischi, in particolare perché tali reti stanno diventando più specifiche (ad esempio, la sorveglianza del comportamento dei dipendenti mediante i dati sul traffico). Un altro fattore che induce a rivedere l'ambito di applicazione della direttiva è la tendenza sempre più marcata dei servizi a diventare una commistione di servizi pubblici e privati.

(2) Il gruppo di lavoro osserva che le definizioni di "servizi di comunicazioni elettroniche" e di "fornitura di una rete di comunicazioni elettroniche" non sono ancora sufficientemente chiare e che tali espressioni dovrebbero essere spiegate con più precisione affinché i responsabili del trattamento e gli utenti possano disporre di un'interpretazione chiara e univoca. Le definizioni ambigue danno adito a vari interrogativi, quali ad esempio: "un cyber café può essere considerato un fornitore di rete di comunicazioni elettroniche?". Sebbene a volte sia facile rispondere, non è sempre così.

(3) Nel precedente parere 7/2000, inoltre, il Gruppo di lavoro Articolo 29 faceva riferimento al considerando 25 della direttiva sull'ePrivacy relativamente all'uso di marcatori ("cookies"). Secondo tale considerando gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore sia installato sui loro personal computer. Il Gruppo di lavoro Articolo 29 condivide pienamente tale punto di vista. L'ultimo comma del considerando 25, tuttavia, prevedendo che l'accesso al contenuto specifico di un sito Internet possa essere subordinato all'accettazione di un marcatore, potrebbe risultare in contrasto con il principio secondo cui l'utente dovrebbe avere la possibilità di rifiutare l'installazione di un marcatore sul suo personal computer e quindi dovrebbe essere chiarito o rivisto.

3. Osservazioni specifiche su vari punti

Documento di lavoro dei servizi della Commissione, sezione 5.8 - Migliorare i meccanismi di applicazione previsti nel quadro normativo

Questa sezione prende in esame l'esigenza di adeguare i meccanismi di applicazione e i poteri di cui dispongono le autorità che attuano la direttiva sull'ePrivacy.

Il documento rileva che le ammende per inosservanza delle disposizioni normative si sono rivelate inadeguate: *"le ammende per violazioni della direttiva sull'ePrivacy sono troppo lievi e l'applicazione diseguale"*.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf

È possibile che le differenze percepibili a livello di applicazione non dipendano dalle disposizioni della direttiva sull'ePrivacy, bensì dalle differenze di recepimento a livello nazionale. Gli Stati membri, ad esempio, hanno adottato interpretazioni diverse dell'articolo 13, paragrafo 2, e sanzioni massime diverse per le violazioni di questa direttiva.

Al riguardo, sebbene sanzioni più elevate e armonizzate possano avere un maggior effetto deterrente, da sole non possono risolvere il problema della percepibile disparità di applicazione. Inoltre non sono necessariamente le sanzioni disponibili a determinare la frequenza con cui si esercitano i poteri per garantire l'applicazione delle norme. La natura di tali poteri e i meccanismi per il loro esercizio possono giocare un ruolo più importante.

In alcuni Stati membri le autorità di controllo della protezione dei dati hanno poteri d'indagine limitati, che ad esempio non conferiscono loro il diritto di accedere ai dati di comunicazioni necessari per provare violazioni della direttiva.

Se in vari Stati membri gli attuali poteri di applicazione non consentono alle autorità di regolamentazione di agire rapidamente, occorre affrontare questo problema. Un altro aspetto che rende difficile l'applicazione è il fatto che molti *spammer* sfuggono alla competenza delle autorità dell'Unione europea. Questo problema dovrebbe essere risolto attraverso una stretta cooperazione con le autorità di regolamentazione di altri paesi.

Per quanto concerne l'esplicito diritto di azione nei confronti degli spammer indicato nel documento di lavoro, non è chiaro in cosa differisca dalla situazione attuale, in cui le autorità competenti possono adottare misure nei confronti di coloro che violano la direttiva in vigore.

Documento di lavoro dei servizi della Commissione, sezione 7 - Sicurezza

Questa sezione contiene una proposta fondamentale per estendere e rafforzare le disposizioni in materia di sicurezza. Le disposizioni della direttiva sull'ePrivacy e quelle della direttiva sul servizio universale saranno incorporate in un unico capo della direttiva quadro dedicato alle disposizioni in materia di sicurezza.

Sebbene il rafforzamento delle disposizioni in materia di sicurezza possa essere vantaggioso per la tutela della privacy dei consumatori, non è chiaro quale beneficio deriverebbe dal formulare un capo ibrido specifico. Si potrebbe in effetti sostenere che la soppressione delle disposizioni in materia di sicurezza dalla direttiva sull'ePrivacy, piuttosto che sottolineare l'importanza del soggetto, come afferma il documento di lavoro, trasmetterebbe il messaggio che la sicurezza riguarda solamente le reti, la concorrenza e i fornitori di reti, mentre invece concerne anche la tutela del diritto fondamentale alla vita privata, come espresso nella direttiva sull'ePrivacy.

Il Gruppo di lavoro Articolo 29 desidera aggiungere che anziché trattare la "sicurezza" nel senso più ampio, si dovrebbe porre l'attenzione su aspetti specifici della sicurezza – non solo sulla "continuità" e sulla "riservatezza", ma anche sull'"integrità" dei dati e, in particolare, sulle questioni relative al rapporto autenticazione/anonimato. Poiché la mancanza di adeguate procedure di autenticazione può contribuire alla creazione di macchinazioni fraudolente e diminuire la fiducia dei consumatori nelle comunicazioni elettroniche, si potrebbe aggiungere al testo introduttivo del capo 7 una sottosezione, intitolata "Frode di identità", in cui indicare che sia la riservatezza sia la tempestiva eliminazione dei dati personali eccedenti contribuiscono a prevenire l'usurpazione d'identità.

Nell'affrontare le questioni di autenticazione, occorre tuttavia tenere presente che, in linea di principio, le persone devono poter usare i servizi pubblici elettronici in modo anonimo. Pertanto, prima di presentare qualsiasi proposta o modifica in materia di autenticazione, è necessaria un'analisi approfondita sull'accessibilità dei servizi elettronici, poiché la comunicazione libera è essenziale. Dall'analisi potrebbe emergere che molte forme di frode possono essere neutralizzate rendendo obbligatoria l'autenticazione da parte dei fornitori di servizi. Sarebbero auspicabili ricerche in materia.

Documento di lavoro dei servizi della Commissione, sezione 7.1 - Obbligo di adottare misure di sicurezza, e poteri delle autorità nazionali di regolamentazione di determinare e controllare l'applicazione tecnica

In questa sezione si avanza l'idea che il quadro attuale lasci un margine di manovra eccessivo ai fornitori di servizi per quanto riguarda la valutazione dell'adeguatezza delle rispettive misure di sicurezza. Considerate le crescenti minacce alla sicurezza, il documento propone di chiarire i termini usati all'articolo 4 della direttiva sull'ePrivacy per rendere più efficaci le misure di sicurezza.

Questo chiarimento si tradurrebbe in nuovi obblighi, quali l'adozione di misure per affrontare gli incidenti di sicurezza, l'obbligo di rispettare le linee guida delle autorità di regolamentazione e l'introduzione di disposizioni contrattuali per informare i consumatori delle misure da adottare in caso di violazione della sicurezza.

In primo luogo, non è chiaro quale sia l'apporto innovativo di tali proposte rispetto al quadro attuale, a parte codificare ciò che probabilmente già costituisce un'aspettativa standard per la maggior parte delle autorità di regolamentazione. È improbabile, ad esempio, che un'autorità di regolamentazione consideri che un fornitore di servizi, le cui misure di sicurezza non contemplino procedure per affrontare gli incidenti di sicurezza e minimizzare l'impatto sui consumatori, rispetti la direttiva sull'ePrivacy.

In secondo luogo, il fatto che un fornitore di servizi ignori le indicazioni dell'autorità di regolamentazione dovrebbe già permettere di stabilire in una certa misura se tale fornitore abbia violato l'articolo 4 della direttiva sull'ePrivacy. È quindi difficile capire in che modo obbligando i fornitori a seguire tali indicazioni si possano ottenere benefici maggiori di quelli associati ad un'applicazione responsabile delle disposizioni vigenti da parte delle autorità di regolamentazione.

In terzo luogo, la previsione di disposizioni contrattuali per informare i consumatori dei passi che possono compiere in caso di violazione della sicurezza sembra essere una pura operazione di facciata.

Prevedendo l'obbligo di tali disposizioni, le proposte inoltre rischiano di aggravare gli oneri normativi non solo a carico del settore ma anche a carico dell'autorità di regolamentazione. Data la natura del settore, le autorità di controllo della protezione dei dati non possono emanare disposizioni in materia di sicurezza sotto forma di istruzioni vincolanti. Le misure devono essere specifiche rispetto al singolo settore; esse cambiano troppo in fretta per consentire ad un'autorità di monitorare l'intero settore, e ovviamente ci sono molti esperti specializzati in sicurezza che hanno migliori strumenti per fornire consulenze in questa materia e svolgere controlli.

I chiarimenti e le istruzioni vincolanti dovrebbero provenire da un'autorità specifica del settore e non da specialisti della protezione dei dati. È inoltre importante evitare una regolamentazione

troppo pesante, come indicato dallo stesso documento di lavoro (nota 30) *"per affrontare le questioni di sicurezza occorre andare oltre la regolamentazione".*

Documento di lavoro dei servizi della Commissione, sezione 7.2 – Notificazione delle violazioni della sicurezza da parte degli operatori di rete e dei fornitori di servizi Internet

Alla luce delle osservazioni di cui sopra, il Gruppo di lavoro Articolo 29 accoglie favorevolmente la proposta di esigere la notificazione delle violazioni della sicurezza; tuttavia, va rilevato che la comunicazione non stabilisce alcuna sanzione per il caso in cui un operatore di rete o un fornitore di servizi Internet ometta di informare l'autorità nazionale di regolamentazione.

Il Gruppo di lavoro Articolo 29, inoltre, ritiene che il settore potrebbe temere che questa misura costituisca un "trattamento speciale" per un settore specifico, dato che per altri settori non esiste un siffatto obbligo di notificazione. Il Gruppo di lavoro Articolo 29 riconosce tuttavia che tali obblighi sono un "tema scottante" di attualità e, cosa più importante, che si tratta di una regolamentazione "leggera", che impone pochi oneri supplementari a carico dei fornitori di servizi che applicano misure appropriate, trattandosi di un effettivo strumento deterrente basato sul mercato per coloro che cercano scappatoie.

D'altro canto, va segnalato che nessuna delle violazioni della sicurezza che di recente hanno fatto notizia negli Stati Uniti (Choicepoint, LexisNexis, Bank of America, Time Warner, ecc.) ha riguardato fornitori di servizi Internet. Il Gruppo di lavoro Articolo 29 suggerisce di estendere l'obbligo di notificazione anche agli intermediari che forniscono dati (data brokers), alle banche o altri fornitori di servizi on-line. Pur non essendo per definizione fornitori di servizi Internet, tali soggetti sono i più interessati dalle violazioni della sicurezza.

Secondo la proposta, i fornitori di servizi Internet devono notificare la violazione della sicurezza solo ai clienti che ne sono stati vittima. Tuttavia, in caso di violazioni importanti (la Comunicazione non intende definire i vari gradi di violazione né quando una violazione debba essere notificata), tutti i clienti del fornitore di servizi Internet devono essere informati della violazione e non solo le "vittime". La proposta normativa dovrebbe fissare regole per classificare i diversi gradi di violazione.

Fornitori di infrastrutture di accesso e fornitori di servizi

La comunicazione distingue tra fornitori di infrastrutture di accesso e fornitori di servizi. L'articolo 3 dell'attuale direttiva sull'ePrivacy definisce il trattamento dei dati a cui si applica la regolamentazione. Mentre in passato era chiaro chi dovesse essere considerato fornitore di servizi di comunicazione elettronica accessibili al pubblico, gli sviluppi nel settore delle comunicazioni elettroniche potrebbero rendere più difficile per i consumatori sapere chi è che effettivamente presta un servizio. In effetti essi possono accedere a un servizio attraverso un portale e nel servizio possono intervenire varie parti.

Rispetto ad attività quali la prestazione dell'informativa e del consenso,, non sempre è chiaro a chi spetti informare gli utenti o a chi si debba prestare il consenso. Allo stesso tempo può esserci il rischio che i fornitori di servizi reindirizzino erroneamente gli utenti verso un fornitore di accesso o di rete, se questo è il soggetto che si occupa di aspetti specifici del servizio in senso tecnico.

Guardando in prospettiva al ruolo specifico dei fornitori di infrastrutture di accesso e dei fornitori di servizi, probabilmente vale la pena di analizzare se le regolamentazioni in materia di trattamento dei dati personali e di tutela della vita privata nel settore delle comunicazioni elettroniche necessitino di essere approfondite per prevenire eventuali malintesi sui destinatari di tali regolamentazioni. La proposta normativa dovrebbe quindi apportare chiarimenti anziché generare maggiore confusione.

4. Conclusioni

Il Gruppo di lavoro Articolo 29 ha accolto con favore la possibilità di fornire le sue osservazioni sulla revisione del pacchetto relativo alle comunicazioni elettroniche, con particolare attenzione alla direttiva sull'ePrivacy. Il Gruppo di lavoro Articolo 29 desidera innanzitutto raccomandare il miglioramento delle misure di sicurezza e vuole sottolineare che nel migliorare la sicurezza delle infrastrutture dovrebbero essere tenuti seriamente in considerazione la tutela degli utenti e lo sviluppo della loro fiducia nelle comunicazioni elettroniche.

Il Gruppo di lavoro Articolo 29 suggerisce, inoltre, di affrontare le questioni relative alle applicazioni on-line, tra cui le problematiche di sicurezza, la responsabilità degli operatori, e la definizione dello status giuridico e del responsabile del trattamento.

Il Gruppo di lavoro Articolo 29 desidera sottolineare che, pur essendo favorevole ad un miglioramento delle misure di sicurezza, non è favorevole ad alcuna misura che comporti o possa comportare una maggiore sorveglianza o il blocco dei contenuti.

Il Gruppo di lavoro Articolo 29 si riserva la possibilità di esprimere ulteriori commenti sulla direttiva alla luce della sua evoluzione.

Bruxelles, 26 settembre 2006

Per il gruppo di lavoro

Il vicepresidente
Jose Luis Piñar Mañas