ARTICOLO 29 – Gruppo di lavoro per la tutela dei dati personali

00451/06/IT
WP 118

Parere 2/2006 sugli aspetti di tutela della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica

Adottato il 21 febbraio 2006

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

istituito con direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafi 1, lettera c), e 3 della richiamata direttiva,

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

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

Il gruppo di lavoro articolo 29 è consapevole del diffondersi di diversi servizi di comunicazione online, in particolare di servizi gratuiti di posta elettronica via web e servizi connessi. Tale espansione suscita preoccupazione quanto alla tutela della riservatezza delle comunicazioni, a causa soprattutto delle prassi attuali dirette a controllare le comunicazioni per eliminare spam o virus o individuare contenuti predeterminati.

Il gruppo sa anche che i provider di servizi Internet (*Internet service provider* o "ISP") e i provider di servizi di posta elettronica (*e-mail service provider* o "ESP") applicano filtri per proteggere la rete e le apparecchiature, nonché, in casi più limitati, per controllare le comunicazioni a fini commerciali. Esso ritiene, tuttavia, che in alcuni casi l'uso di tali filtri possa contravvenire alla normativa vigente sulla protezione dei dati che andiamo a descrivere, forse anche perché l'applicazione di questa normativa ai nuovi tipi di servizi non è sempre chiara.

Obiettivo principale del presente documento è fornire alcune indicazioni sul problema della riservatezza delle comunicazioni di posta elettronica e, più nello specifico, sul filtraggio delle comunicazioni on line. Si pone soprattutto il problema di stabilire se la scansione delle comunicazioni di norma effettuata da ISP e ESP per una serie di finalità configuri un'intercettazione e se e in quale modo tale intercettazione sia giustificabile.

Pertanto, il presente documento esamina in particolare le disposizioni sulla riservatezza delle comunicazioni elettroniche di cui all'articolo 5, paragrafo 1, della direttiva 2002/58 relativa alla vita privata e alle comunicazioni elettroniche, le altre disposizioni pertinenti che sono parte dell'acquis comunitario e le norme nazionali di attuazione.

II. QUADRO GIURIDICO SULLA PROTEZIONE DEI DATI E SUL RISPETTO DELLA VITA PRIVATA NELLE COMUNICAZIONI DI POSTA ELETTRONICA

A) Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

La riservatezza nelle comunicazioni è garantita conformemente agli strumenti internazionali relativi ai diritti dell'uomo, in particolare alla Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali ("CEDU") e alle costituzioni degli Stati membri, ma anche dalle due direttive dell'UE su cui ci soffermeremo in seguito.

L'articolo 8 della CEDU sancisce il diritto di ciascuno al rispetto della vita privata e della corrispondenza e stabilisce le condizioni in cui si possono giustificare eventuali limitazioni di tale diritto. La Corte europea dei diritti umani ("Corte") ha in più occasioni applicato l'articolo 8 in relazione alla corrispondenza ordinaria.

---

[1] GU L 281del 23.11.1995, pag. 31, consultabile al seguente indirizzo: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

Intercettare, aprire, leggere una lettera, ritardarne la consegna o ostacolarne l'invio sono tutti atti che configurano violazione dell'articolo 8 della CEDU[2]. Dalle decisioni della Commissione e dalla giurisprudenza della Corte si può concludere che le comunicazioni di posta elettronica rientrano quasi certamente nel disposto dell'articolo 8 CEDU, combinando entrambe le nozioni di "vita privata" e "corrispondenza"[3]. Le parti che scambiano messaggi di posta elettronica possono quindi plausibilmente aspettarsi che le loro comunicazioni non siano oggetto di controllo da parte di terzi, pubblici o privati.

Il diritto al rispetto della "corrispondenza" non riguarda solo la sua segretezza, ma anche il diritto di inviare e ricevere tale corrispondenza[4]. Si può pertanto concludere che il divieto generale di inviare o ricevere posta elettronica contravviene all'articolo 8 della CEDU.

Gode del diritto al rispetto della vita privata e della corrispondenza chiunque rientri nella giurisdizione di uno degli Stati contraenti della CEDU; ciò vale per tutti i soggetti che partecipino ad una comunicazione. Nella causa A/Francia (1993) la Corte ha statuito che la registrazione di una conversazione telefonica con il consenso di una sola delle parti costituisce ingerenza nel diritto al rispetto della corrispondenza dell'altra parte della comunicazione.

Ai sensi della CEDU, gli Stati contraenti possono effettuare intercettazioni legittime di corrispondenze, anche elettroniche, o prendere altre misure, se necessarie per le finalità della convenzione e conformi all'interpretazione della CEDU nella giurisprudenza della Corte. Per intercettazione si può intendere l'acquisizione da parte di terzi dell'accesso al contenuto e/o ai dati sul traffico relativi a comunicazioni private fra due o più interlocutori, compresi i dati sul traffico relativi all'uso di servizi di comunicazione elettronica, che configuri violazione del diritto al rispetto della vita privata e alla segretezza della corrispondenza. Tali intercettazioni sono inammissibili se non soddisfano tre criteri fondamentali, ai sensi dell'articolo 8, paragrafo 2 della CEDU e dell'interpretazione fornitane dalla Corte:

"… una base giuridica, la necessità di tali misure in una società democratica e la conformità con una delle finalità legittime elencate nella convenzione…"

Nei rapporti privati, però, lo strumento più pertinente per l'esercizio dei diritti della convenzione è la dottrina delle obbligazioni positive delle parti contraenti, in base alla quale queste ultime non soltanto hanno l'obbligo di astenersi da ogni ingerenza, ma anche quello di adoperarsi affinché quei diritti possano essere realmente esercitati, non solo nei confronti dell'autorità pubblica ma anche nell'ambito dei rapporti interpersonali. Donde l'obbligo di provvedere a un adeguato quadro giuridico per il loro esercizio.

---

[2] Nella causa Niemitz (1992) la Corte ha statuito che le lettere già recapitate al destinatario rientrano nel campo d'applicazione dell'articolo 8 della CEDU. Sempre in quella sede la Corte affermava che vanno tutelate non soltanto le comunicazioni private ma anche la corrispondenza sul posto di lavoro. Nelle cause Klass (1978), Malone (1984) e Huvig (1990), la Corte ha deciso che anche le conversazioni telefoniche rientrano nel disposto dell'articolo 8. Per gli altri mezzi di comunicazione, rileva la decisione della Commissione nel caso Mersch (1985) secondo la quale la captazione di qualunque forma di comunicazione configura un'ingerenza nel disposto dell'articolo 8.

[3] Tale conclusione trova conferma nel fatto che nella maggior parte degli Stati membri è vietato controllare i messaggi di posta elettronica e che a livello internazionale e nazionale sono state create specifiche potestà per l'intercettazione delle comunicazioni di posta elettronica.

[4] Golder (1975), punto 43: "Impedire finanche di iniziare una corrispondenza costituisce la forma più radicale di "ingerenza" (articolo 8, paragrafo 2) nell'esercizio del "diritto al rispetto della corrispondenza"; è inconcepibile che ciò fuoriesca dal disposto dell'articolo 8 laddove la mera supervisione vi rientra indiscutibilmente". Configura ingerenza anche il trattenimento della corrispondenza ricevuta (Schöneberger & Durmaz, 1988)

L'articolo 6, paragrafo 2 del trattato sull'Unione europea afferma esplicitamente che l'Unione rispetta i diritti fondamentali quali sono garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e quali risultano dalle tradizioni costituzionali comuni degli Stati membri, in quanto principi generali del diritto comunitario. Secondo l'articolo 52, paragrafo 3 della Carta dei diritti fondamentali dell'UE, il significato e la portata dei diritti ivi contenuti sono uguali a quelli conferiti dalla CEDU. Tale disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa.

B) Disposizioni specifiche applicabili alla riservatezza delle comunicazioni di posta elettronica

Come si è già detto, la riservatezza delle comunicazioni è garantita anche da due direttive dell'UE. Nel valutare questo particolare aspetto è necessario interpretare le disposizioni di entrambe le direttive alla luce della CEDU e della giurisprudenza della Corte europea dei diritti umani di cui sopra.

La direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("direttiva sulla protezione dei dati") istituisce un regime giuridico orizzontale per la tutela dei diritti individuali alla protezione dei dati. In relazione al trattamento dei dati personali, la richiamata direttiva fa riferimento al diritto al rispetto della vita privata sancito dall'articolo 8 della CEDU[5]. La libertà di ricevere o di comunicare informazioni è riconosciuta anch'essa in quanto rientrante nella libertà di espressione di cui all'articolo 10 CEDU[6]. Inoltre, stando al considerando 47, deve essere considerata responsabile del trattamento dei dati personali la persona che ha emanato il messaggio di posta elettronica contenente quei dati, mentre il provider di posta elettronica sarà di norma considerato il responsabile del trattamento dei dati personali supplementari necessari per la funzionalità del servizio.

La direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ("direttiva e-privacy") si applica al trattamento dei dati personali connesso alla fornitura di reti di comunicazione elettronica accessibili al pubblico nella Comunità. Le disposizioni di questa direttiva precisano e integrano la direttiva sulla protezione dei dati. La riservatezza delle comunicazioni è tutelata, in particolare, dal suo articolo 5 che recita:

"... Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente ..."

Inoltre, ai sensi dell'articolo 4 della direttiva e-privacy "*Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete*".

---

5 Considerando 10: "considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario"

6 Considerando 37: "considerando che il trattamento di dati personali a scopi giornalistici o di espressione artistica o letteraria, in particolare nel settore audiovisivo deve beneficiare di deroghe o di limitazioni a determinate disposizioni della presente direttiva ove sia necessario per conciliare i diritti fondamentali della persona con la libertà di espressione ed in particolare la libertà di ricevere o di comunicare informazioni, quale garantita in particolare dall'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali"

Rilevante in materia è anche la direttiva sul commercio elettronico, in particolare le disposizioni relative alla responsabilità di ISP ed ESP in base alle quali gli Stati membri non impongono a tali prestatori un obbligo generale di sorveglianza. Tale obbligo costituirebbe infatti violazione della libertà di informazione e della segretezza della corrispondenza (articolo 15 della direttiva sul commercio elettronico[7]).

III. SCANSIONE DEL CONTENUTO DEI MESSAGGI DI POSTA ELETTRONICA

Alla luce di questo contesto giuridico si pone il problema della compatibilità con il diritto dell'UE della scansione delle comunicazioni di norma effettuata da ISP e ESP per una serie di finalità.

La maggior parte dei provider provvedono in effetti alla scansione dei messaggi e-mail: è una prassi di routine finalizzata al filtraggio degli spam, al rilevamento dei virus, alla ricerca e al controllo ortografico, all'inoltro, alla risposta automatica, all'aggiunta di flag per contrassegnare messaggi urgenti, alla conversione delle e-mail in entrata in messaggi di testo per telefoni cellulari, al salvataggio automatico e all'ordinamento in cartelle, alla conversione di URL di testo in link cliccabili.

Andiamo quindi a esaminare il quadro giuridico che disciplina lo screening effettuato per i seguenti fini: (A) individuare virus, (B) filtrare spam (C) ricercare contenuti predeterminati.

A) Scansione effettuata per individuare virus

La scansione antivirus consiste nel verificare i file alla ricerca di virus conosciuti. In alcuni casi, alla scansione segue l'eliminazione del virus, processo mediante il quale il virus individuato viene rimosso dal file che potrà essere quindi utilizzato in modo sicuro. La scansione avviene di solito non appena il messaggio raggiunge i server del provider. Molti provider includono nei loro servizi la scansione antivirus, nell'intento di proteggersi e di proteggere gli utenti da virus pericolosi. Gli utenti, però, spesso non sono in grado di disattivare la scansione automatizzata che è attiva per default.

Nell'esaminare i fondamenti giuridici che legittimano tale prassi, il gruppo articolo 29 ritiene che i sistemi di filtraggio installati e attivati dai provider di posta elettronica per individuare i virus potrebbero trovare giustificazione nell'obbligo di adottare misure tecniche ed organizzative appropriate al fine di garantire la sicurezza dei servizi prestati da tali provider, ai sensi dell'articolo 4 della citata direttiva e-privacy.

In effetti, posto che il recapito di mail contenenti virus può provocare l'arresto del sistema del provider di posta elettronica (oltre a danneggiare altri documenti e i software nelle apparecchiature terminali dell'utente finale), e impedire quindi la trasmissione di altre comunicazioni di posta elettronica, il gruppo articolo 29 considera la scansione effettuata a tal fine una misura di sicurezza tesa a proteggere il sistema del responsabile del trattamento (il provider di servizi di posta elettronica), rientrante –come si è già detto- negli obblighi imposti al fornitore di servizi di comunicazione elettronica dall'articolo 4 della direttiva e-privacy.

Il gruppo articolo 29 ritiene che l'attivazione di filtri per gli scopi dell'articolo 4 possa essere compatibile con l'articolo 5 della richiamata direttiva.

Il gruppo sottolinea, in particolare, che le misure di cui sopra devono essere conformi con i principi generali del diritto comunitario.

---

[7] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

Esso ritiene, inoltre, che nel predisporre i sistemi di filtraggio i provider provvedano a garantire l'esecuzione del contratto di servizi concluso con i clienti, i quali si aspettano di ricevere e inviare messaggi di posta elettronica con un certo grado di sicurezza. Di conseguenza, il trattamento di dati effettuato dai provider di servizi e-mail nel predisporre sistemi di filtraggio può essere legittimato anche ai sensi dell'articolo 7, lettera b) della direttiva sulla protezione dei dati, il quale prevede il trattamento "*necessario all'esecuzione del contratto concluso con la persona interessata*".

Premesso che, in ragione di quanto esposto, la scansione antivirus potrebbe essere lecita per salvaguardare la sicurezza dei servizi a norma dell'articolo 4 della direttiva e-privacy e/o per la mera esecuzione del contratto a norma dell'articolo 7, lettera b) della direttiva sulla protezione dei dati, ferma restando la riservatezza della comunicazione, il gruppo articolo 29 ricorda l'obbligo per i provider di servizi e-mail di garantire il rispetto di quanto segue:

a) il contenuto dei messaggi e relativi allegati deve rimanere segreto ed essere rivelato soltanto ai destinatari;

b) in caso di presenza di virus, il software antivirus deve offrire adeguate garanzie di riservatezza;

c) la scansione antivirus effettuata sotto forma di scansione del contenuto dovrebbe applicarsi automaticamente ed esclusivamente per questa finalità; il contenuto, cioè, non può essere analizzato per nessun'altra ragione.

Andrebbero inoltre fornite informazioni sulle attività di scansione (vedi infra).

B) Scansione effettuata per individuare spam[8]

I provider ISP e ESP ricorrono a diverse tecniche per impedire che messaggi indesiderati (non necessariamente solo commerciali), cioè gli spam, raggiungano i destinatari.

Una di queste tecniche è la cosiddetta lista di blocco (o lista nera, *black list*), un elenco cioè nel quale vengono inseriti gli indirizzi IP di certi server e le classi IP dinamiche assegnate a certi ISP[9]. Tale tecnica non costituisce, tuttavia, oggetto di analisi nel presente documento.

Il filtraggio antispam è ormai divenuto una pratica necessaria. Se i servizi di posta elettronica non filtrassero i messaggi per individuare gli spam, questi finirebbero per congestionare il flusso di mail in entrata e i sistemi diventerebbero probabilmente sempre più lenti e inefficienti, fino a rendere il servizio praticamente inutilizzabile per l'utente. Ne conseguirebbero ovviamente lo scontento dei consumatori e possibilità ridotte di fornire un servizio mail sicuro e affidabile.

---

8 Il documento OCSE dal titolo "*Anti Spam Regulations*" realizzato dalla *Spam Task Force* nel marzo 2005 (DSTI/CP/ICCP/SPAM(2005)1 afferma, descrivendo il concetto di spam: "*Il termine "spam" è usato comunemente nei media internazionali e nelle dichiarazioni politiche di diversi paesi, ma non esiste un consenso globale sulla sua definizione. Pur riferendosi globalmente allo stesso fenomeno, i vari paesi ne danno una definizione corrispondente anzitutto al proprio contesto locale. Nel mettere a punto una politica antispam è essenziale comprendere e definire chiaramente la natura di questo fenomeno, differenziando lo spamming dalle prassi legittime."*

9 Con questa tecnica, il provider di posta elettronica non fa filtraggio ma si limita a bloccare (ovvero rifiuta di accettare) le mail provenienti da server o classi IP presenti in una *black list*, senza controllarne il contenuto. Sebbene, in linea di principio, meno invasiva per la vita privata del filtraggio basato sui contenuti, la pratica delle black list può porre il problema della libertà di parola e di espressione e del diritto al rispetto della corrispondenza e a ricevere tale corrispondenza, come riconosciuto dall'articolo 8 della CEDU nelle successive interpretazioni della Corte.

Pur non costituendo di per sé una minaccia per la sicurezza dei servizi dei provider ESP, quanto piuttosto per la funzionalità generale della rete e del servizio di posta elettronica in particolare, gli spam possono tuttavia rendere l'ESP incapace di fornire quel servizio. Il gruppo articolo 29 ritiene che l'articolo 4 della direttiva e–privacy, che fa obbligo ai provider di posta elettronica di adottare misure tecniche ed organizzative appropriate al fine di garantire la sicurezza dei loro servizi, riguardi tanto la sicurezza dei provider ESP e dei servizi di rete propriamente detti, quanto la funzionalità generale della rete e dei servizi di posta elettronica. La sicurezza dei provider ESP è un problema nella misura in cui influisce sul servizio da essi prestato. Per questo motivo, il gruppo articolo 29 ritiene che l'articolo 4 possa applicarsi anche a questa situazione. In altri termini, le minacce alla funzionalità generale dei servizi di posta elettronica e di rete possono giustificare l'applicazione di filtri antispam da parte dei provider ISP e ESP. Se si considerano gli effetti prodotti dagli spam, anche nell'eventualità che lo spammer diffonda solo poche informazioni al giorno attraverso messaggi di posta elettronica, ma a un numero molto elevato di destinatari, si consolida l'argomento a favore dell'applicazione dell'articolo 4 della direttiva e-privacy poiché, persino in quell'eventualità, l'invio di un numero così contenuto di mail potrebbe bloccare il traffico Internet e pregiudicare gravemente l'affidabilità, la sicurezza e l'efficienza dei servizi di posta elettronica in generale. Inoltre, per questi stessi motivi il gruppo ritiene che il filtraggio dei messaggi possa giustificarsi anche in forza dell'articolo 7, lettera b) della direttiva sulla protezione dei dati, posto che, senza filtri antispam, il provider ESP non potrebbe eseguire correttamente il contratto di servizi di cui è parte la persona interessata, ossia il destinatario.

D'altro canto, il gruppo teme il rischio dei "falsi positivi", che siano cioè filtrati come spam messaggi legittimi "desiderati", i quali non sarebbero quindi recapitati. Esso ritiene che il fatto di filtrare e trattenere messaggi presumibilmente indesiderati possa costituire non solo una limitazione della libertà di parola, ma anche una violazione dell'articolo 10 della CEDU, e configurare pertanto ingerenza nella sfera delle comunicazioni private[10].

In considerazione di ciò, nonostante l'applicazione dell'articolo 4 della direttiva e-privacy, e nell'intento di tutelare il principio della libertà di comunicazione riconosciuto dall'articolo 10 CEDU e la riservatezza delle comunicazioni di cui all'articolo 5 della richiamata direttiva e all'articolo 8 CEDU, il gruppo articolo 29 invita caldamente i provider di posta elettronica ad attenersi alle seguenti raccomandazioni, il cui scopo principale è dare ai destinatari dei messaggi di posta elettronica il controllo delle comunicazioni che, in linea di principio, sono loro indirizzate:

a) il gruppo articolo 29 incoraggia la prassi consistente nel permettere agli abbonati di disapplicare i filtri antispam, controllare i messaggi classificati come spam per accertare se effettivamente lo siano, e stabilire quali "tipi" di spam debbano essere filtrati. Il Gruppo, inoltre, accoglie con favore la possibilità offerta agli abbonati da alcuni provider ESP di abilitare nuovamente e con facilità la scansione dei messaggi di posta elettronica al fine di individuare spam;

b) il gruppo caldeggia anche lo sviluppo di strumenti di filtraggio che l'utente possa installare o configurare nelle apparecchiature terminali o in server terzi o nel server del provider, e che gli diano la possibilità di controllare i messaggi che desidera o non desidera ricevere, anche per ridurre i costi inerenti allo scaricamento di messaggi elettronici indesiderati di cui al considerando 44 della direttiva 2002/58/CE. Il gruppo guarda inoltre con favore alla ricerca di nuovi strumenti antispam che possano risultare meno invasivi per la vita privata.

[10] Come afferma la Corte nel caso Schöneberger & Durmaz, 1988.

In aggiunta a quanto sopra, il gruppo ricorda ai provider di servizi di posta elettronica i quali effettuano lo screening delle mail per individuare spam, che a norma dell'articolo 10 della direttiva sulla protezione dei dati hanno l'obbligo di informare gli abbonati, in modo chiaro e univoco, della loro politica antispam; su questo punto si rimanda alla sezione IV del presente parere. Il provider deve anche assicurare la segretezza delle mail filtrate, che non devono essere utilizzate per nessun altro scopo.

C) Scansione effettuata alla ricerca di contenuti predeterminati

Il gruppo articolo 29 osserva che alcuni provider di posta elettronica si riservano il diritto di controllare e persino eliminare eventuali contenuti predeterminati[11], nei quali figurerebbero per esempio materiali asseritamente illegali o che il destinatario, utente di quel particolare servizio, non desidera ricevere. La tecnica applicata per questo tipo di screening è molto simile a quella in uso per individuare virus e spam.

Diversamente dallo screening effettuato per individuare virus, la scansione delle mail a scopo di ricerca di contenuti predeterminati, benché considerati asseritamente illeciti, non può essere assimilata a una misura tecnica e organizzativa necessaria per salvaguardare la sicurezza dei servizi di posta elettronica ai sensi dell'articolo 4 della direttiva e-privacy. Il provider ESP non rischia, in effetti, di essere danneggiato, né di dover interrompere le comunicazioni a causa del materiale contenuto nelle mail. La scansione a scopo di ricerca di tale materiale non trova quindi legittimazione nella necessità del provider di salvaguardare la sicurezza del servizio. Il gruppo teme, inoltre, che applicando tale tipo di filtraggio i provider di posta elettronica assurgano a censori delle comunicazioni elettroniche private, bloccando per esempio messaggi i cui contenuti siano magari perfettamente leciti, interferendo con ciò gravemente nella libertà di parola, pensiero e informazione. Il gruppo desidera sottolineare che l'individuazione di contenuti predeterminati o asseritamente dannosi non rientra negli obblighi standard dei provider, ma potrebbe essere offerta, come si dirà in seguito, quale servizio a valore aggiunto.

Di conseguenza, il gruppo articolo 29 ritiene che, in forza dell'articolo 5, paragrafo 1 della direttiva e-privacy, sia fatto divieto ai provider di posta elettronica di filtrare, memorizzare o intercettare in altro modo comunicazioni e relativi dati sul traffico alla ricerca di contenuti predeterminati senza il consenso degli utenti, salvo quando siano autorizzati legalmente a norma dell'articolo 15 della richiamata direttiva, così come attuata nel diritto degli Stati membri.

---

[11] Si vedano le Condizioni generali per l'Utilizzo del Servizio (CGUS) di Yahoo!: L'Utente riconosce che Yahoo! non effettua costantemente un controllo preventivo dei Contenuti. Tuttavia Yahoo! e i soggetti da lei designati si riservano il diritto discrezionale - senza per questo assumere alcun obbligo al riguardo - di controllare preventivamente, rifiutare o rimuovere un qualsiasi Contenuto accessibile tramite il Servizio. Fatto salvo quanto previsto sopra, Yahoo! e i soggetti da lei designati si riservano il diritto di rimuovere qualsiasi Contenuto che costituisca violazione delle presenti CGUS o che risulti in altro modo reprensibile. L'Utente si impegna a valutare compiutamente e a sopportare tutti i rischi associati all'utilizzo di un Contenuto, incluso l'eventuale affidamento da lui riposto sulla veridicità, completezza o utilità di tale Contenuto. A tal fine, l'Utente dovrebbe evitare di fare affidamento sui Contenuti diffusi tramite il Servizio, incluse a mero titolo di esempio le informazioni contenute in Yahoo! Bacheca, Yahoo! Gruppi e in tutte le altre parti del Servizio. L'Utente riconosce e accetta che Yahoo! abbia il diritto di memorizzare i Contenuti e le informazioni sul rispettivo account e di rivelarli a terzi (...) ove ciò sia richiesto dalla legge ovvero perché Yahoo! ritenga in buona fede che ciò sia necessario per: adempiere a procedure legali; applicare le CGUS; replicare alle contestazioni secondo cui i Contenuti violano diritti di terzi; rispondere alle Vs. richieste rivolte al Servizio Assistenza Clienti; proteggere i diritti, i beni o l'incolumità di Yahoo!, dei suoi utenti e di terzi.

IV. OBBLIGO DI INFORMARE

Oltre all'articolo 5 della direttiva e-privacy, il trattamento di dati personali teso a conoscere il contenuto e/o i dati sul traffico in relazione a comunicazioni private deve conformarsi anche a vari requisiti della direttiva sulla protezione dei dati.

Questa direttiva introduce, fra l'altro, l'obbligo di informare l'interessato del trattamento dei suoi dati personali. In particolare, l'articolo 10, recante la rubrica "*Informazione della persona interessata*", fa obbligo al responsabile del trattamento di fornire alla persona presso la quale effettua la raccolta dei dati che la riguardano almeno alcune informazioni, fra cui l'identità del responsabile del trattamento e le finalità del trattamento cui sono destinati i dati. Inoltre, l'articolo 6, paragrafo 1, lettera a) sempre di questa direttiva stabilisce che i dati personali debbano essere trattati lealmente e lecitamente, rafforzando con ciò l'obbligo, per il responsabile del trattamento, di garantire la totale trasparenza circa le condizioni del trattamento di quei dati.

Per quanto riguarda l'applicazione di filtri antispam e antivirus, il gruppo articolo 29 considera adeguata la prassi dei provider ESP consistente nell'informare gli abbonati nell'ambito delle condizioni contrattuali previste per il servizio.

In aggiunta a quanto sopra, i provider ESP hanno anche il dovere di conformarsi all'articolo 4 della direttiva e-privacy a norma del quale, nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati. Se poi il rischio per la sicurezza è al di fuori della portata dei possibili rimedi esperibili dal fornitore, spetta al fornitore informare gli utenti e gli abbonati delle misure che questi ultimi possono prendere per proteggere la sicurezza delle loro comunicazioni.

V. ALTRI SERVIZI CONNESSI ALLA POSTA ELETTRONICA

Il gruppo articolo 29 osserva lo sviluppo di un nuovo tipo di prodotti e servizi software, come il *Didtheyreadit* ("L'hanno letto?"), il cui scopo è verificare se un messaggio di posta elettronica sia stato aperto.

Questo genere di servizio consente all'abbonato di sapere a) se il destinatario di una sua mail l'ha letta, b) il momento in cui l'ha letta, c) quante volte l'ha letta (o quanto meno aperta), d) se è stata inoltrata a terzi e e) a quale server di posta elettronica, compresa la sua localizzazione. Permette anche di sapere quale tipo di navigatore web e di sistema operativo utilizzi il destinatario.

Il trattamento dei dati è effettuato segretamente, all'insaputa cioè del destinatario della mail presso il quale i dati sono raccolti. Inoltre, al destinatario non è data facoltà di accettare o rifiutare tale raccolta di dati. In buona sostanza, a differenza dei sistemi classici di conferma di ricezione (*acknowledgement*), con questi nuovi prodotti il destinatario di un messaggio di posta elettronica non ha la possibilità di accettare o rifiutare che le informazioni di acknowledgement siano trattate e inoltrate all'utente del software.

Il gruppo articolo 29 esprime tutte le sue riserve su questo trattamento, in quanto vengono registrati e trasmessi dati personali relativi al comportamento del destinatario senza il suo univoco consenso. Tale trattamento effettuato all'insaputa dell'interessato contravviene ai principi di protezione dei dati che esigono lealtà e trasparenza nella raccolta dei dati stessi, conformemente all'articolo 10 della direttiva sulla protezione dei dati.

Per poter svolgere un'attività di trattamento dati che consista nel reperire, presso il destinatario di un messaggio di posta elettronica, dati che confermino se egli abbia letto il messaggio e se e quando l'abbia inoltrato a terzi, è necessario il suo univoco consenso. Nessun altro fondamento giuridico può legittimare tale trattamento. Pertanto, il trattamento di dati effettuato all'insaputa dell'interessato

contravviene al principio in base al quale il consenso deve essere manifestato in maniera inequivocabile, come sancisce l'articolo 7 della direttiva sulla protezione dei dati.

VI. CONCLUSIONI

Il gruppo articolo 29 ha ritenuto utile pubblicare il presente parere a fronte dell'evidente incertezza circa la compatibilità dell'attività di filtraggio delle comunicazioni di posta elettronica, nonché per rispondere alla richiesta di orientamenti formulata dalle parti interessate.

Il gruppo invita i provider di posta elettronica a tener conto, nel fornire i loro servizi, degli orientamenti e delle raccomandazioni espressi nel presente parere. Inoltre, coerentemente con la scelta di promuovere tecnologie che integrino i requisiti di protezione dei dati e tutela della privacy nella realizzazione di infrastrutture e sistemi di informazione, ivi comprese le apparecchiature terminali, il gruppo articolo 29 invita i produttori e gli sviluppatori di programmi di gestione della posta elettronica a progettare e mettere a punto sistemi rispettosi della vita privata, riducendo al minimo il trattamento di dati personali e limitandolo a quanto strettamente necessario e proporzionato alle finalità del trattamento.

Bruxelles, 21 febbraio 2006

Per il Gruppo

Il Presidente
Peter Schaar