Caso Peppermint - Internet

Caso Peppermint - Internet : illecito "spiare" gli utenti che scambiano file musicali e giochi - Le società private non possono svolgere attività di monitoraggio sistematico per individuare gli utenti che si scambiano file musicali o giochi su Internet. (dal sito Garante della Privacy - comunicato stampa del 13 marzo 2008)

Caso Peppermint - Internet: illecito "spiare" gli utenti che scambiano file musicali e giochi - Le società private non possono svolgere attività di monitoraggio sistematico per individuare gli utenti che si scambiano file musicali o giochi su Internet. (dal sio Garante della Privacy comunicato del 13 marzo 2008)

Internet: illecito "spiare" gli utenti che scambiano file musicali e giochi

Le società private non possono svolgere attività di monitoraggio sistematico per individuare gli utenti che si scambiano file musicali o giochi su Internet.

L'Autorità per la privacy ha chiuso l'istruttoria avviata sul "caso Peppermint", la società discografica che aveva svolto, attraverso una società informatica svizzera (la Logistep, utilizzata anche dalla società Techland con riferimento a *software* relativi a giochi), un sistematico monitoraggio delle reti *peer to peer* (P2P). Tramite l'utilizzo di *software* specifici, le società avevano individuato numerosissimi indirizzi IP (che identificano i *computer* collegati ad Internet) relativi a utenti ritenuti responsabili dello scambio illegale di *file*: erano poi risaliti ai nomi degli utenti, anche italiani, al fine di potere ottenere un risarcimento del danno.

Il Garante, richiamando anche la decisione dell'omologa Autorità svizzera, ha ritenuto illecita l'attività svolta dalle società.

Innanzitutto, ha ricordato il Garante, la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti. É stato, poi, violato il principio di finalità: le reti P2P sono finalizzate allo scambio tra utenti di dati e file per scopi personali. L'utilizzo dei dati dell'utente può avvenire, dunque, soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno).

Infine non sono stati rispettati i principi di trasparenza e correttezza, perché i dati sono stati raccolti ad insaputa sia degli interessati sia di abbonati che non erano necessariamente coinvolti nello scambio di file.

Sulla base del provvedimento del Garante (di cui è stato relatore Mauro Paissan), le società che hanno effettuato il monitoraggio dovranno ora cancellare, entro il 31 marzo, i dati personali degli utenti che hanno scambiato *file* musicali e giochi attraverso il sistema P2P.

Roma, 13 marzo 2008

Internet - Caso Peppermint: illecito "spiare" gli utenti che scambiano file musicali e giochi - 28 febbraio 2008

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli,

Caso Peppermint - Internet

segretario generale;

VISTE le recenti ordinanze con le quali il Tribunale di Roma –come richiesto da questa Autorità – ha rigettato alcuni ricorsi con i quali le società Peppermint Jam Records GmbH (di seguito, Peppermint), casa discografica con sede in Germania e Techland sp. z. o.o. (di seguito, Techland), società che elabora e commercializza giochi elettronici avente sede in Polonia, intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica la comunicazione delle generalità di soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer to-peer*;

RILEVATO che tali ricorsi si basavano sull'attività svolta per conto e su autorizzazione delle predette società da Logistep AG (di seguito, Logistep), società svizzera che, attraverso un'attività di monitoraggio delle reti *peer-to-peer* effettuata tramite un *software* proprietario, aveva individuato numerosi indirizzi Ip i cui titolari erano stati considerati responsabili della predetta condotta illecita;

VISTA la nota del 25 maggio 2007 con la quale l'Autorità ha avviato accertamenti volti a verificare la liceità e la correttezza dei trattamenti di dati personali svolti dalle predette società, alle quali è stato quindi chiesto di comunicare ogni informazione e documentazione utile per valutare le modalità con le quali, anche avvalendosi dell'attività di altri soggetti, sono stati concretamente raccolti e utilizzati i dati personali di utenti identificati o identificabili; rilevato che con tale nota si è chiesta, altresì, collaborazione e cooperazione alle autorità di protezione dei dati personali dei Paesi nei quali risultano stabilite le società medesime (Repubblica federale tedesca, Polonia e Svizzera);

VISTE le note del 18 giugno e del 5 luglio 2007 con le quali l'avv. Otto Mahlknecht, che ha curato gli interessi delle società Peppermint e Techland, nel richiamare le deduzioni formulate nei diversi procedimenti giudiziari, ha fornito altri elementi conoscitivi sul funzionamento del software utilizzato da Logistep nell'attività svolta su incarico delle altre due società, allegando la perizia di un esperto del settore;

VISTA la nota del 19 giugno 2007 con la quale Logistep ha fornito altre informazioni in merito alla propria attività e ha comunicato l'avvio di un'attività di collaborazione con l'autorità svizzera di protezione dati finalizzata a verificare la liceità dell'attività svolta;

VISTA la comunicazione del 20 giugno 2007 con la quale l'autorità polacca per la protezione dei dati ha rappresentato di aver effettuato un accertamento ispettivo e di aver rilevato che Techland non ha svolto direttamente le attività necessarie per individuare le persone che scambiano illecitamente su reti *peer-to-peer* il *software* da essa sviluppato, e che tali attività sono state svolte, su propria autorizzazione, da Logistep, nonché da Logistep Polska, e curate poi dallo studio legale italiano dell'avv. Otto Mahlknecht;

VISTA la nota del 22 giugno 2007 dell'autorità per la protezione dei dati personali per la Bassa Sassonia;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito, *"Codice"*) e, in particolare, gli artt. 11, 13 e 122 del Codice;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Mauro Paissan;

Caso Peppermint - Internet

PREMESSO

1. Oggetto del provvedimento

Il presente provvedimento ha per oggetto la liceità e correttezza del trattamento di dati personali relativi a utenti identificabili operanti su reti *peer-to-peer* (di seguito, anche "p2p") che è stato effettuato a cura dapprima di Logistep AG e Logistep Polska su autorizzazione di Peppermint e Techland e, poi, presso il predetto studio legale italiano. Tale trattamento è avvenuto in due fasi:

a) la prima, è consistita nella raccolta e nell'elaborazione automatizzata, anche nell'ambito di banche dati, di innumerevoli informazioni di carattere personale estratte tramite reti peer-to-peer per mezzo di un *software* denominato "*file sharing monitor*" (di seguito, *fsm*) utilizzato da Logistep;
b) la seconda, si è basata sulla richiesta all'autorità giudiziaria italiana in sede civile di ordinare a taluni fornitori di servizi di comunicazione elettronica di rivelare le generalità degli intestatari degli interessati. A seguito di alcune prime pronunce del Tribunale di Roma che hanno provveduto in tal senso (*cfr*. *causa Peppermint c/ Wind telecomunicazioni S.p.A., ordinanza del 18 agosto 2006 confermata, in sede di reclamo cautelare della Wind, con ordinanza del 22 settembre 2006 e, attualmente, in attesa che il giudice determini le modalità di attuazione dell'ordinanza di accoglimento; causa Peppermint c/Telecom Italia S.p.A., ordinanza del 28/29 novembre 2006, riformata in sede di reclamo della Peppermint con ordinanza del 9 febbraio 2007*), il predetto legale ha inviato diverse centinaia di lettere a persone individuate quali intestatari di una linea di collegamento a Internet. Con tali lettere si è contestata la violazione dei diritti derivanti dalla produzione di fonogrammi e si è proposta una risoluzione bonaria, alternativa anche alla denuncia in sede penale, basata sul rispetto di alcune condizioni comprensive di un versamento di 330 euro.

Il presente provvedimento non riguarda, invece, la connessa questione oggetto più specificamente delle predette controversie instaurate presso il Tribunale di Roma nelle quali si è costituito anche il Garante e in cui, a modifica del primo orientamento giurisprudenziale sopramenzionato, il Tribunale ha statuito che i fornitori di servizi di comunicazione elettronica, allo stato della legislazione vigente, non possono comunicare in sede giurisdizionale civile a Peppermint e Techland i nominativi degli interessati ritenuti responsabili di violazioni del diritto d'autore in rete. Ciò, stante la specifica disciplina della conservazione dei dati di traffico, prevista solo per finalità di accertamento e repressione di reati (art. 132 del Codice; *cfr*. causa Peppermint e Techland c/Wind Telecomunicazioni S.p.A.,ordinanza 14 luglio 2007; causa Peppermint e Techland c/ Telecom Italia S.p.A.,ordinanza 14 luglio 2007; causa Peppermint c/ Wind telecomunicazioni S.p.A., ordinanza 26 ottobre 2007; *cfr*.,anche, comunicato stampa del 17 luglio 2007, pubblicato sul sito *web* dell'Autorità).

Tale profilo della comunicazione dei dati di traffico è stato esaminato, da ultimo, dalla Corte di giustizia delle Comunità europee la quale si è pronunciata su una questione per molti aspetti simile (sentenza 29 gennaio 2008, pronunciata nella causa C-275/06 Promusicae c/ Telefonica de Espana Sau).

La Corte ha confermato che il diritto comunitario consente agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale -a esclusione, quindi, dei processi civili- il dovere di conservare e mettere a disposizione i dati sulle connessioni e il traffico generati dalle comunicazioni effettuate durante la prestazione di un servizio della società dell'informazione. La Corte ha rilevato che anche i dati di traffico conservati per finalità di fatturazione non possono essere utilizzati in *"controversie diverse da quelle insorgenti tra i fornitori e gli utilizzatori, relative ai motivi della memorizzazione dei dati avvenuta per attività previste dalle disposizioni [dell'art. 6 della direttiva 2002/58/Ce]"* (*cfr*. art. 123 del Codice); da ciò, ha escluso la possibilità

che tali dati potessero essere messi a disposizione per controversie civili relative ai diritti di proprietà intellettuale *(cfr. punto 48 della sentenza; artt. 15, n. 2, e 18 della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della Società dell'informazione, in particolare il commercio elettronico, nel mercato interno; artt. 8, nn. 1 e 2 direttiva 2001/29/Ce sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; art. 8 direttiva 2004/48/Ce sul rispetto dei diritti di proprietà intellettuale; artt. 17, n. 2 e 47 Carta dei diritti fondamentali dell'Unione europea).*

2. Risultanze istruttorie e funzionamento del *software fsm*

Nelle centinaia di lettere inviate a utenti in Italia, il legale che ha agito per conto di Peppermint ha dichiarato che sulla base dei risultati acquisiti grazie al predetto software *"antipirateria"* appositamente realizzato, ritenuto di assoluta affidabilità e attendibilità, è stato possibile accertare che:

- ciascun destinatario delle lettere aveva violato il diritto d'autore a partire dalla linea di rete Internet risultante nella rispettiva titolarità, mettendo indebitamente file musicali a disposizione di terzi;
- ciò, risultava avvenuto mediante un *software* di condivisione contemporanea di file (c.d. *peer-to-peer*) che altri utenti risultavano aver utilizzato per connettersi al p.c. dei destinatari delle lettere e per scaricare i file musicali da una cartella a questo dedicata.

Lo scambio di file via Internet rientra nella nozione di *"comunicazione"* anche quando ha per oggetto contenuti protetti dal diritto d'autore, tenuto conto che la nozione stessa include lo *"scambio o la trasmissione di informazioni"*, *"tramite un servizio di comunicazione elettronica accessibile al pubblico"*, tra *"un numero finito di soggetti"* (*cfr*. art. 2, lettera d), primo periodo, della direttiva 2002/58/CE e art. 4, comma 1, lett. l) del Codice). Quest'ultimo riferimento tende a distinguere l'ambito delle *"comunicazioni private"* da quello delle *"comunicazioni al pubblico"*. La circostanza che il sistema peer-to-peer consenta l'accesso a un numero potenzialmente elevato di utenti non rende *"infinito"*, o del tutto indeterminabile, il numero dei soggetti della comunicazione. Quest'ultima, è infatti rivolta non a una platea indistinta di utenti, ma a soggetti delimitati che possono essere identificati. Manca, tra l'altro, la simultaneità e l'unicità della trasmissione che sono caratteristiche qualificanti di una *"comunicazione al pubblico"* (come è nel caso del "servizio di radiodiffusione" -c.d. *broadcasting*-, espressamente escluso dall'ambito applicativo della nozione di comunicazione elettronica: *cfr*., anche, art. 4, comma 2, lett. a) del Codice).

L'attività di ricognizione condotta da Logistep risulta essersi focalizzata su due importanti reti p2p, GNUtella e eDonkey e utilizzando il sistema *software fsm*, sviluppato integrando e modificando software liberamente disponibili sulla rete per collegarsi a reti p2p.

Il *software fsm* consente:

a) usuali operazioni effettuabili tramite i comuni *client*, eccettuata la condivisione di *file* eventualmente scaricati dalla rete;
b) l'archiviazione a scopo di documentazione di tutte le informazioni usualmente caratterizzate da *"volatilità"*, perché non necessarie una volta che la trasmissione dei *file* è avvenuta;
c) di correlare le attività sulle reti p2p di un determinato utente al variare dell'indirizzo Ip assunto, nonché del provider utilizzato (il *clock* del programma risulta sincronizzato con una sorgente esterna, mentre viene tenuta traccia dell'identificativo *Guid*, generato al momento dell'installazione dei *client*).

In sostanza, il *software fsm* permette di tenere traccia della disponibilità in rete di un certo *"contenuto"*; di

verificarne l'effettiva possibilità di acquisizione, effettuandone lo scaricamento (*download*), ovvero la copia in rete dalle aree di condivisione degli utenti che ospitano quel contenuto verso i propri computer; di verificarne la segnatura digitale con algoritmo SHA1 o MD5 (in dipendenza dal protocollo p2p utilizzato); di controllarne la diffusione, verificando l'esistenza di altre condivisioni presuntivamente riferibili a una pregressa attività di "*download*" (sul presupposto che la quasi totalità degli utenti che condividono uno specifico contenuto lo abbiano a loro volta acquisito da un'altra fonte nella rete, tranne eventualmente il soggetto che originariamente lo abbia messo per la prima volta in condivisione, con una specifica segnatura digitale).

In particolare, il sistema *fsm* consente la raccolta dei seguenti dati: indirizzi Ip dell'offerente, il nome e il valore *Hash* del *file*, la misure del *file*, l'*user name*, il Guid, la data e l'ora del *download*.

In altre parole, come emerge dalla stessa perizia prodotta dall'avv. Mahlknecht, il *software fsm* accerta da chi, e quando, viene offerto quale *file* per un *downloading* e da chi, quando e per quanto tempo viene effettivamente copiato tale *file*; riconosce i tentativi dei partecipanti di sistemi di condivisione *file* di modificare il loro indirizzo Ip; organizza tali informazioni in una banca dati.

Anche se non risulta in atti che il sistema *fsm* svolga attività intrusive o installazioni di *software* o di altri componenti sul terminale dell'utente che partecipa al *file sharing*, e sebbene non risultino allo stato significativi elementi di diversità nelle modalità di funzionamento di tale *software* rispetto ai normali *client* che agiscono sulle reti p2p, il trattamento svolto da Logistep su incarico di Peppermint e Techland non può comunque ritenersi lecito.

3. Profili di illiceità e non correttezza del trattamento

Il trattamento in questione è stato inizialmente effettuato a partire da un Paese (la Svizzera), dotata di una legge di protezione dei dati e che ha ratificato la Convenzione di Strasburgo n. 108/1981, e la cui autorità di protezione dei dati ne ha già dichiarato, per questa parte, l'illiceità.

La Préposé fédéral à la protection des donne et à la transparence (PFPDT), con una recente pronuncia adottata all'esito di un procedimento avviato anche su impulso di questa Autorità, ha ritenuto che il trattamento svolto da Logistep su incarico di Peppermint e Techland e che ha riguardato anche informazioni memorizzate su p.c. di utenti italiani, ha violato alcuni princìpi fondamentali della legge federale sulla protezione dei dati personali (decisione del 9 gennaio 2008).

E' risultato in particolare violato il principio di liceità (in ragione del fatto che la raccolta dei dati è stata effettuata in mancanza di una base legale esplicita). Si è ritenuto in secondo luogo violato il principio di finalità (in quanto la registrazione sistematica dei dati degli utenti ha perseguito scopi diversi da quelli tipici delle reti *peer-to-peer*). Non sono stati, altresì, rispettati i princìpi di buona fede e trasparenza, in quanto la raccolta dei dati è avvenuta senza che gli interessati potessero esserne consapevoli (sia per le circostanze nelle quali la raccolta è avvenuta, sia perché non informati) e i dati possono essere stati raccolti all'insaputa di abbonati che non sono, necessariamente, i soggetti coinvolti nello scambio dei dati. Infine, è risultato violato il principio di proporzionalità (in quanto il diritto alla segretezza delle comunicazioni è risultato limitabile solo nell'ambito di un bilanciamento con un diritto di pari grado e, quindi, allo stato, non per l'esercizio di un'azione civile).

Non risultano in atti elementi più specifici di valutazione delle modalità di trattamento di dati che è stato effettuato a cura di Logistep Polska, il quale, qualora si sia svolto con le modalità sopraindicate, si è posto anch'esso in violazione dei princìpi di trasparenza, finalità, correttezza e buona fede richiamati sia dalla Convenzione di Strasburgo, sia dalla direttiva 95/46/Ce e dalla stessa disciplina nazionale di protezione dati (*cfr*. art. 5 Conv. n. 108/1981 cit., art. 6 direttiva 95/46/Ce).

I trattamenti in esame, effettuati in modo massivo e capillare per un periodo di tempo prolungato e nei riguardi di un

numero elevato di soggetti, hanno consentito di tenere traccia analitica delle operazioni compiute da innumerevoli, singoli utenti relativamente a specifici contenuti protetti dal diritto d'autore.

Per le modalità con le quali la raccolta dei dati è stata svolta, si è configurata un'attività di monitoraggio vietata a soggetti privati dalla direttiva 2002/58/Ce (art. 5; *cfr*. art. 122 del Codice).

Le reti p2p sono finalizzate allo scambio fra utenti di dati e *file* per scopi sostanzialmente personali, mentre il *software fsm* "non è destinato allo scambio di dati, ma al monitoraggio ed alla ricerca di dati, che utenti di reti P2P mettono a disposizione a terzi" (*cfr*. nota del 5 luglio 2007 dell'Avv. Otto Mahlknecht). I dati che gli utenti mettono in rete possono essere utilizzati per le finalità per le quali tale pubblicazione avviene (*cfr*., fra gli altri, *Provv*. del 14 giugno 2007, doc. *web* n. 1424068). L'utilizzo dei dati dell'utente delle reti *peer-to-peer* può, quindi, avvenire per le finalità sue proprie e non già, in modo non trasparente, per scopi ulteriori, quali quelli perseguiti da Logistep, Peppermint e Techland.

Il trattamento è risultato viziato anche sotto il profilo della trasparenza e della correttezza, posto che non è stata fornita alcuna informativa preliminare agli utenti. Dalla descrizione resa dalle società sul funzionamento del software *fsm* si è potuto rilevare che, mentre gli indirizzi Ip sono stati acquisiti da un terzo rispetto agli utenti (il *tracker*), gli altri dati (ossia, i *file* offerti in condivisione, data e ora del *download*) sono stati raccolti direttamente presso gli interessati.

Il Tribunale di Roma ha riconosciuto, per tali informazioni, la natura di *"dati personali"* relativi a utenti identificabili i quali dovevano essere informati di tale ulteriore e inatteso trattamento *(v. anche Parere del Gruppo Art. 29 del 18 gennaio 2005 in materia di diritti di proprietà intellettuale, nel quale è stato rilevato che nessun dato personale può essere raccolto senza che l'interessato sia correttamente e preventivamente informato, in maniera trasparente, sulle eventuali modalità di controllo e sull'identità del soggetto che lo effettua, prima che il trattamento abbia inizio e prima che l'interessato fornisca i dati personali attraverso il download).*

4. Conclusioni

Come premesso, una seconda fase del trattamento dei dati connesso all'invio delle lettere è avvenuta nel territorio dello Stato, utilizzando dati personali relativi a persone identificabili e raccolti illecitamente.

Si rende pertanto necessario, a definizione della complessa istruttoria preliminare, provvedere in ordine all'ulteriore utilizzazione di tali dati sul territorio dello Stato. Ciò, senza che occorra proseguire gli accertamenti per verificare anche se, e in quale misura, la disciplina italiana di protezione dei dati trovi in tutto o in parte applicazione anche alla prima fase di raccolta automatizzata dei dati, alla luce della disposizione normativa secondo cui la legge italiana si applica ai trattamenti effettuati da soggetti stabiliti nel territorio di un Paese non appartenente all'Unione europea il quale impieghi, per il trattamento, strumenti situati nel territorio dello Stato (quali i *p.c.* degli utenti italiani, dai quali Logistep ha chiaramente tratto gli indirizzi Ip: art. 5 del Codice).

In ragione delle predette risultanze non possono che confermarsi le valutazioni di illiceità e non correttezza già tratteggiate nelle memorie di costituzione in giudizio nelle controversie dinanzi al Tribunale di Roma –e note alle controparti –, e conseguentemente disporsi il divieto nei confronti delle predette tre società di ulteriore utilizzazione dei dati personali raccolti illecitamente, nonché la loro cancellazione entro il termine del 31 marzo 2008.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d) del Codice dispone, nei termini di cui in motivazione, nei confronti di Peppermint Jam Records GmbH, Techland sp. z. o.o. e Logistep AG, il

Caso Peppermint - Internet

divieto dell'ulteriore trattamento dei dati personali relativo a soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer-to-peer* e ne dispone la cancellazione entro il termine del 31 marzo 2008.

Roma, 28 febbraio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli