COPIA
TELECOM

Ct 1990/10 – Avv. Fiorentino

AVVOCATURA GENERALE DELLO STATO

***

TRIBUNALE DI ROMA

IX Sezione – G.D. Dott.ssa Antonella Izzo

R.G. 81826/09

per il **GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**, in persona del Presidente in carica, *ope legis* rappresentato e difeso dall'Avvocatura generale dello Stato, nei cui uffici domicilia in Roma, alla via dei Portoghesi, 12

interventore

contro

FAPAV – FEDERAZIONE ANTIPIRATERIA AUDIOVISIVA, in persona del legale rappresentante pro tempore, elettivamente domiciliata in Roma, vicolo Orbitelli, 31, presso lo studio dell'Avv. Prof. Vincenzo Zeno – Zencovich, che la rappresenta e difende unitamente all'Avv. Mario Gallavotti

ricorrente

e nei confronti di

TELECOM ITALIA S.P.A, in persone del legale rappresentante pro tempore, elttivamente domiciliata in Roma, via Ajaccio, 14, rappresentata e difesa dall'Avv. Arturo Leone e dall'Avv. Alessandro Berti Arnoaldi Veli

resistente

Comparsa di intervento

nel procedimento cautelare introdotto con ricorso depositato in data 3 dicembre 2009.

Fatto

L'Associazione FAPAV – Federazione AntiPirateria AudioVisiva (in proseguo, per brevità: FAPAV) – ricorre al Tribunale civile di Roma, ai sensi dell'art. 156 della legge n. 633 del 1941 (legge sul diritto d'autore) e dell'art. 700 cod. proc. civ., lamentando l'illecita acquisizione di opere audiovisive protette da parte di clienti Telecom, società fornitrice del servizio di accesso alla rete Internet.

L'Associazione chiede, in via d'urgenza, di:

«*1. Ordinare a Telecom Italia di comunicare alle Autorità di pubblica sicurezza tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette p. e p. dagli artt. 171 ss. l.d'a.*

2. Ordinare a Telecom Italia di adottare tutte le misure, sia tecniche che amministrative, per impedire ovvero ostacolare l'accesso ai siti – elencati nel ricorso – usualmente utilizzati per accedere a e riprodurre illecitamente contenuti audiovisivi non disponibili al pubblico;

3. Ordinare a Telecom Italia di informare i propri utenti in ordine alla natura illecita delle condotte di riproduzione di opere audiovisive non disponibili al pubblico, comunicando altresì che tali condotte costituiscono condotte contrattualmente vietate ai sensi del contratto di accesso ad Internet e, per l'effetto, che la prosecuzione di tali condotte potrà dare luogo alla risoluzione del contratto medesimo.

4. In ogni caso adottare ogni altro provvedimento idoneo a salvaguardare il buon diritto della ricorrente».

La ricorrente ha dedotto che «*a partire dal 2008 ha commissionato una serie di ricerche volte ad accertare la dimensione, in Italia, del fenomeno della illecita messa a disposizione di opere audiovisive protette, attraverso la rete internet. I risultanti evidenziano come il fenomeno sia in continuo aumento ed abbia raggiunto ormai livelli che mettono a repentaglio la sopravvivenza dell'industria audiovisiva*», con svariati milioni di episodi di accesso illecito.

FAPAV sostiene, inoltre, che «*dalla medesima ricerca è risultato che ben più della metà dei casi di messa a disposizione e riproduzione è avvenuta utilizzando la rete dalla società Telecom Italia», per una percentuale indicata tra il 57% ed il 65%". L'illecito sarebbe stato attuato da parte dei clienti Telecom accedendo, attraverso la rete della medesima, a siti «notoriamente utilizzati per la messa a disposizione delle copie 'pirata' di opere audiovisive protette*», come *Theprivatebay.org, BitTorrent portal site, Vedogratis, Angelmule.com*, ecc..

A sostegno della domanda, la ricorrente ha invocato:

• l'art. 28 del D. Lgs. N. 259 del 2003 (Codice delle comunicazioni elettroniche);

• gli artt. 14 e 17 del D. Lgs. N. 70 del 2003 (Disposizioni sul commercio elettronico);

• l'art. 163 della Legge 22 aprile 1941, n. 633 (Legge sul diritto d'autore), e successive modificazioni ed integrazioni.

La ricorrente afferma di avere diffidato Telecom a «*porre in atto le misure tecniche, amministrative e giuridiche per impedire l'abuso della convenzione internet da parte dei propri abbonati. In particolare è stato chiesto a Telecom Italia di disattivare e/o bloccare l'accesso ai siti attraverso i quali avviene la illecita riproduzione di opere audiovisive protette, nonché di comunicare alle Autorità di Pubblica Sicurezza i dati idonei a consentire l'adozione delle misure di competenza di quest'ultima*».

A tale intimazione Telecom avrebbe risposto con nota del 26 giugno 2009, nella quale ha opposto un rifiuto.

Diritto.

***I* Motivi dell'intervento del Garante**.

L'Autorità, in considerazione del suo ruolo e dei suoi compiti istituzionali, intende costituirsi nel giudizio istaurato innanzi all'adito Tribunale, a tutela dell'interesse pubblico, in considerazione delle particolari questioni di diritto, relative alla protezione dei dati personali, coinvolte nel procedimento giudiziario *de quo* e che rivestono una rilevanza decisiva in ordine all'esito del medesimo.

In particolare, come si dimostrerà nel punto II che segue, si ritiene probabile che gli elementi posti a fondamento del ricorso in oggetto siano il risultato di un illecito trattamento di dati personali e,come tali, siano inutilizzabili anche nel presente giudizio (art. 11, comma 2 del D.Lgsl. 30 giugno 2003 n. 196, recante il Codice in materia di protezione dei dati personali – d'ora in avanti, per brevità: "Codice" – secondo il quale «*(i) dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*»).

In secondo luogo, si deve rilevare che il *petitum* della ricorrente – come si mostrerà nel punto III che segue – sembra implicare la richiesta (di ordinare) alla Società Telecom di effettuare di un trattamento di dati personali illecito, per la sua contrarietà alle vigenti disposizioni, nazionali e

comunitarie, in tema di tutela della riservatezza; trattamento che il Garante, per di più, ha già espressamente vietato alla resistente, in una precedente occasione (Prescrizione del Garante 10 gennaio 2008, adottata ai sensi dell'art. 154, 1 c del Codice, all. 1).

***

***II* Modalità di acquisizione dei dati presentati da FAPAV ai fini del ricorso**.

Nel ricorso mancano precise indicazioni sulle modalità tecniche attraverso le quali la ricorrente ha raccolto le fonti di prova della presunta acquisizione illecita di opere protette, essendosi essa limitata ad asserire, genericamente, di avere "commissionato una serie di ricerche" per accertare le dimensioni del fenomeno denunciato, senza neppure precisare a quale soggetto tali ricerche siano state commissionate. Sta di fatto che da tali "ricerche" sarebbe emerso sia il numero di (presunti) episodi di accesso illecito ad opere protette (otre due milioni e duecentomila), sia, altresì, il dato che tale accesso sarebbe stato attuato soprattutto da clienti Telecom (si indica una percentuale tra il 57% ed il 65% del totale degli accessi), come risulterebbe dagli indirizzi IP, facenti capo a tale operatore di rete.

La ricorrente, quindi, ammette di avere acquisito e raccolto gli indirizzi IP di destinazione dei file, scaricati dalla rete, contenenti le opere protette. Ciò impone di verificare se FAPAV, o chi per essa, al fine di procurarsi gli elementi posti a fondamento del ricorso in oggetto, abbia effettuato un monitoraggio degli utenti della rete internet connessi a determinati siti (indicati dal ricorrente come «*siti notoriamente utilizzati per la messa a disposizione in rete di copie pirata di opere audiovisive protette*»), e dei file da questi acquisiti, individuando gli indirizzi IP dei medesimi utenti.

Tale accertamento è necessario in quanto, ove si fosse effettivamente verificato il paventato monitoraggio sistematico degli utenti della rete internet, FAPAV avrebbe svolto un illecito trattamento di dati personali altrui, come appresso dimostrato.

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).

Orbene, l'art. 122 del Codice vieta, in generale, l'uso di una rete di comunicazione elettronica per monitorare le operazioni degli utenti, rinviando ad apposito codice di deontologia l'individuazione dei limiti e dei presupposti entro i quali l'uso della rete sopra indicato, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbia espresso il consenso, sulla base di una previa informativa che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento (sul punto v. anche la direttiva 2002/58/CE).

Pertanto, anche secondo i dettami del diritto comunitario, l'utilizzo dei dati degli utenti della rete internet connessi a siti per scambio di file può avvenire solo per le finalità proprie dell'attività stessa della connessione e non già, in modo occulto, per scopi ulteriori, quali il monitoraggio dell'attività svolta da tali utenti. Giova ricordare, a tale proposito, che nel parere reso il 18 gennaio 2005 in materia di diritti di proprietà intellettuale dai rappresentanti delle Autorità Garanti nell'ambito del Gruppo costituito ai sensi dell'art. 29 della direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, 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* (All. 1-bis).

Pertanto, fermo restando che il Garante ha già avviato, in relazione alle proprie competenze istituzionali, un autonomo procedimento di controllo sulla liceità e correttezza dei trattamenti già effettuati dalle

ricorrenti nei casi di specie, si segnala, in questa sede, la necessità che il Giudice adito verifichi le modalità di acquisizione, da parte di FAPAV, dei dati personali in argomento, tenuto conte che, come detto, ai sensi dell'art. 11, comma 2, del Codice i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati neppure in sede processuale. Tale orientamento è condiviso dalla giurisprudenza di codesta Sezione che, in una causa relativa alla medesima materia, ha affermato: «*Il possesso dei dati parziali avuto dalle ricorrenti sui presunti autori delle violazioni lamentate, ossia i codici IP e GUID, sempre in virtù della disciplina dettata dal D. Lgs. 196/2003 risulta illecito, trattandosi di dati acquisiti in assenza di autorizzazione dell'Autorità garante per la privacy (in base all'art. 37) e del consenso informato dei diretti interessati (artt. 13 e 23) [...] la connotazione illecita dell'acquisizione dei citati codici IP e GUID da parte delle ricorrenti determina la completa inutilizzabilità di tali dati anche in sede giudiziale, ai sensi dell'art. 11, II comma, del medesimo decreto, sicché gli stessi non possono costituire la base giudiziaria [...] per la valutazione del Giudice in ordine alla fondatezza della domanda*» (Trib. Roma, Sez. IX civile specializzata in materia di proprietà industriale e intellettuale, Ordinanza del 14 luglio 2007, Techland e Peppermint vs. Wind Telecomunicazioni e Garante – intervenuto -, all. 2).

***

***III* Divieto di monitoraggio dei contenuti della navigazione in internet**.

Il petitum di FAPAV, nella parte in cui chiede al Giudice di ordinare a Telecom di comunicare alle Autorità di pubblica sicurezza «*tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette p.p. dagli artt. 171 e ss. della Legge sul diritto d'autore*», risulta estremamente generico, non indicando la natura dei dati di cui si chiede la comunicazione.

Pare potersi ipotizzare, in linea con quanto prospettato anche dalla resistente, che con tale generica formulazione FAPAV intenda chiedere al Giudice adito di ordinare a Telecom di comunicare alle suddette Autorità (anch'esse, genericamente indicate), tutti gli indirizzi IP dei propri clienti

che accedono, in ipotesi, ai siti in questione, previo monitoraggio dei contenuti della navigazione sul web degli utenti Telecom.

Una tale richiesta, se effettivamente avanzata dal ricorrente, non potrebbe essere accolta dal Giudice adito, per la sua contrarietà alle vigenti disposizioni, nazionali e comunitarie, in tema di tutela della riservatezza.

In particolare, gli articoli 123 e 132 del Codice stabiliscono il divieto generale di conservazione dei dati relativi al traffico (art. 123, comma 1), con le seguenti eccezioni:

- è consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2), o, previo consenso dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica, per la durata all'uopo necessaria (art. 123, comma 3);

- è prescritta la conservazione, per dodici mesi, da parte del fornitore del servizio, per finalità di accertamento e repressione (non di prevenzione) dei reati, dei dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni. Entro tale termine, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante;

- è previsto, infine (comma 4-*ter*), che il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a

novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

Appare, pertanto, evidente che, secondo la legge, fatte salve le specifiche ipotesi sopra ricordate di richiesta da parte del Ministro dell'Interno o di un suo delegato, il fornitore dei servizi informatici può comunicare i dati di traffico telematico – conservati per un limitato periodo ed unicamente per le finalità sopra indicate – esclusivamente a fronte di decreto motivato del pubblico ministero, ovvero su istanza del difensore dell'imputato o della persona sottoposta alle indagini, con le modalità indicate dall'articolo 391-quater c.p.p..

Tale normativa è il frutto del bilanciamento, effettuato dal legislatore nazionale, tra i due diritti, entrambi fondamentali, all'accertamento e repressione dei reati e alla riservatezza, ritenendo che il sacrificio del secondo possa essere giustificato, e per un periodo limitato, unicamente in caso di lesione di interessi della collettività protetti dal diritto penale. A tale proposito, si ricorda che la Corte Costituzionale con sentenza 372/2006 ha respinto la eccezione di legittimità costituzionale dell'art. 132 nella parte in cui permetteva la conservazione dei dati di traffico per ulteriori 24 mesi per finalità di repressione soltanto di determinati reati, giustificando la ragionevolezza del diverso trattamento con la gravità dei reati stessi e richiamando la necessità di un bilanciamento tra il diritto alla riservatezza e gli interessi tutelati dal diritto penale.

Per quanto riguarda il diritto comunitario, si ricorda che gli articoli 123 e 132 del Codice costituiscono la trasposizione, nell'ordinamento italiano, degli articoli 5, 6 e 15 della direttiva 2002/58/Ce, in materia di trattamento dei dati personali e di tutela della vita privata nel settore delle

comunicazioni elettroniche. L'articolo 5 di tale direttiva impone un divieto di conservazione dei dati sul traffico relativi agli abbonati ed agli utenti, quando non siano più necessari ai fini della trasmissione delle comunicazioni.

Questo divieto conosce le seguenti eccezioni:

- un primo gruppo di eccezioni si rinvengono nei paragrafi 2 e 3 del citato articolo 6 della direttiva 2002/58/CE: si tratta della conservazione dei dati che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione (par. 2), nonché dei dati rispetto ai quali l'abbonato o l'utente abbia consentito il trattamento ai fini della commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto (par. 3). Il trattamento di questi dati deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività (par. 5);

- altre eccezioni si rinvengono nell'art. 15, par. 1, della direttiva, che consente agli Stati membri di adottare disposizioni legislative che prevedano un obbligo di conservazione dei dati sul traffico, quando ciò risulti necessario per la salvaguardia della sicurezza nazionale, della difesa o della sicurezza pubblica o, ancora, per la prevenzione, ricerca, accertamento o perseguimento dei reati o dell'uso non autorizzato del sistema di comunicazione elettronica.

A proposito di tale ultima eccezione, si osserva che per "uso non autorizzato" deve intendersi l'uso non autorizzato dal provider che metta in pericolo l'integrità o la sicurezza del sistema di comunicazione, come si desume anche dai lavori preparatori della direttiva (cfr Corte di Giustizia, sentenza 29 gennaio 2008, causa C-275/06, *Promusicae*, punto 52). In tal senso militano anche argomenti di ordine sistematico: la circostanza, cioè, che l'articolo 15 della direttiva 2002/58/CE, nel riprodurre alla lettera alcune delle eccezioni previste dall'articolo 13 della direttiva 95/46/CE, ha omesso di richiamarne altre e, in particolare, quella contenuta nella lettera g) (la quale allude a restrizioni del diritto alla riservatezza dei dati a fini di salvaguardia "dei diritti e delle libertà altrui").

Peraltro, la Repubblica italiana non si è, legittimamente, avvalsa della facoltà, concessale dall'art. 15 della direttiva 2002/58/CE, di imporre la conservazione dei dati a fini di repressione e accertamento anche dell' "uso non autorizzato del sistema di comunicazione elettronica" .

Da ultimo, giova richiamare la già sentenza *Promusicae*, nella quale la Corte di Giustizia delle Comunità europee, in un caso analogo a quello in esame, ha ribadito che oltre ai diritti di proprietà intellettuale e di autore risulta coinvolto «*(...) anche un altro diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata (...)*» (cfr. punto 63 della sentenza).

Nella sentenza, la Corte richiama la necessità di una conciliazione «*(...) degli obblighi connessi alla tutela di diversi interessi fondamentali: da una parte, il diritto al rispetto della vita privata e, dall'altra, i diritti alla tutela della proprietà e ad un ricorso effettivo*» (punto 64) e, dopo aver chiarito che il diritto comunitario non impone agli Stati membri di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile, evidenza come – anche negli Stati membri, tra i quali non vi è l'Italia, che, avvalendosi di tale margine di discrezionalità (comunque funzionalizzata al rispetto di un «*giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario*»), ciò abbiano consentito – «*le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità*» (punto 70 della sentenza).

Vi è, quindi, anche da parte del Giudice europeo un forte richiamo alla necessità di bilanciamento tra i valori costituzionali della tutela della proprietà e quelli, di rilievo certo non minore, relativi alla libertà e alla segretezza delle comunicazioni e delle riservatezza della vita privata.

I contorni di tale giudizio di bilanciamento, nel caso dell'ordinamento nazionale, sono già stati chiaramente delineati nella già sentenza n. 372/2006 della Corte costituzionale.

Tale ricostruzione trova decisivo conforto nella giurisprudenza di codesta Sezione, formatasi in occasione di diversi giudizi che, come nel caso *de quo*, opponevano la tutela del diritto d'autore alla salvaguardia della riservatezza degli utenti di internet (Ordinanza del 17 marzo 2008, Techland e Peppermint vs. Tiscali all. 4; id. Ordinanza del 14 luglio 2007, Techland e Peppermint vs. Wind Telecomunicazioni, con intervento del Garante, all. 2; id, Ord. del 14 luglio 2007, Techland e Peppermint vs. Telecom con intervento del Garante, all. 5; id, Ord. 12 ottobre 2007, Wind vs. Peppermint, con intervento del Garante, all. 6; id., Ord. 12 ottobre 2007, Wind vs. CDV Software Entertainment, con intervento del Garante, all. 7).

Non sussiste, pertanto, alcuna fonte normativa che consenta una comunicazione di dati quale quella invocata da FAVAP nella propria domanda. Il legislatore nazionale ha, infatti, operato, come già ricordato, un delicato bilanciamento di interessi tra il diritto alla riservatezza degli utenti dei servizi telefonici e di comunicazione elettronica e le esigenze di accertamento e repressione dei reati, vale a dire esigenze di sicurezza della collettività e ha inteso sacrificare la tutela di un diritto costituzionalmente garantito quale quello alla riservatezza dei propri dati solo per tali finalità di interesse pubblico, e non anche per la tutela di diritti di singoli, a contenuto economico.

Occorre, inoltre, aggiungere che è da escludersi che la pretesa di FAPAV possa condurre ad imporre legittimamente a Telecom - finanche per ordine giudiziale - il monitoraggio e la conservazione dei dati relativi ai contenuti della navigazione sul web degli utenti Telecom, onde accertarne l'eventuale connessione ai siti indicati dalla ricorrente e comunicarne le generalità, successivamente, all'Autorità di pubblica sicurezza.

Si ricorda, infatti, che la legge consente la conservazione temporanea dei soli dati relativi al traffico telematico con espressa esclusione dei contenuti delle comunicazioni (art. 132 del Codice).

A tale proposito si ricorda che il Garante, nell'esercizio della sua potestà, ha già prescritto a Telecom quanto segue: (Prescrizione del 10 gennaio 2008, ex art. 154, 1 c del Codice, in Bollettino 90/gennaio 2008, doc. web n. 1524263, citata ed allegata):

«1. Nel rispetto del principio secondo il quale i dati non devono essere formati e conservati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio, i fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica possono formare e conservare soltanto i dati di traffico telematico che devono essere necessariamente generati e che devono rimanere temporaneamente nella loro disponibilità, essendo necessariamente correlati ad attività tecniche strumentali alla resa dei servizi offerti e alla loro eventuale fatturazione (artt. 3, 11 e 123 del Codice).

Il fornitore di accesso, "mediatore" della comunicazione, deve conservare esclusivamente i dati di traffico telematico funzionali a fornire ad abbonati e utenti e a fatturare il servizio di connessione alla rete.

Il fornitore di accesso non deve quindi conservare in qualunque forma informazioni sui siti visitati dagli utenti.

La necessità del pieno rispetto del predetto principio, derivante dalla funzione stessa svolta dal gestore e dai suoi limiti, va evidenziata anche alla luce della constatazione che il trattamento dei dati di traffico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, stante la natura particolarmente delicata delle informazioni trattate la cui conoscenza può avere importanti ripercussioni sulla sfera personale di più soggetti interessati. Tali dati richiedono, per la loro conoscibilità, adeguate garanzie, considerata la loro "accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore" (cfr., fra l'altro, Corte cost., 26 febbraio-11 marzo 1993, in G.U. 17 marzo 1993 e Corte cost., 14 novembre 2006, n. 372).

Per il traffico telematico, peraltro, vista la particolarità delle informazioni trattate, si pongono specifiche criticità rispetto alle comunicazioni telefoniche, potendosi non di rado riscontrare una sostanziale identificazione fra il dato esteriore della comunicazione elettronica e il contenuto della stessa. Alcuni dati di traffico telematico, apparentemente "esterni" alla comunicazione elettronica (come, ad esempio, le pagine web visitate o gli indirizzi Ip di destinazione), coincidono

di fatto, nella maggior parte dei casi, con il "contenuto" della comunicazione medesima, consentendo, tra l'altro, di ricostruire direttamente o indirettamente relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

In questo quadro, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, va anche tenuto specificamente conto del fatto che l'art. 132 del Codice, nel prescrivere la conservazione temporanea dei dati di traffico per finalità di accertamento e repressione di reati, specifica puntualmente, con riferimento al traffico telematico, che devono essere esclusi dalla conservazione "i contenuti delle comunicazioni" (art. 132 del Codice)».

Sulla base di tale motivazione, il provvedimento in parola ha vietato a Telecom, ai sensi dell'art. 154, comma 1, lett. d) del Codice, ogni trattamento di dati personali consistente, in particolare:

1. nell'interposizione di sistemi informatici tra l'utente e i siti della rete ai quali questi accede, nella misura in cui i medesimi sistemi non siano strumentali alla resa del servizio di accesso alla rete Internet e determinino una raccolta di dati eccedente e non necessaria per la fornitura del servizio stesso o per la sua eventuale fatturazione;

2. nella raccolta e nella conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche quando esse siano specificate con notazione Url o con mero indirizzo Ip di destinazione. Ciò, in riferimento sia al sistema relativo alla telefonia mobile denominato Ipms-Ip monitoring system, sia ad ogni altro sistema in cui gli stessi, o altri analoghi dati di traffico vengano formati.

Si dimostra, pertanto, l'illegittimità di una ipotetica imposizione ala convenuta dell'obbligo di effettuare il monitoraggio del contenuto della navigazione nel web dei propri utenti e, a fortiori, della comunicazione di tali dati a chicchessia, anche per il motivo logico che tali dati non possono essere né raccolti né conservati.

***

IV Insussistenza del periculum in mora

FAPAV si è rivolto al Giudice adito, ex art. 700 c.p.c., sostenendo che il requisito dell'urgenza sarebbe rappresentato dall'irreparabilità del danno in atto.

Occorre, pertanto, rilevare che la ricorrente, dopo avere ricevuto dalla resistente il rifiuto ad ottemperare all'intimazione a cessare i comportamenti ritenuti illegittimi (26 giugno 2009), ha atteso più di cinque mesi (18 novembre 2009, data del deposito in cancelleria del ricorso), per ricorrere all'Autorità giudiziaria, circostanza incompatibile con la ricorrenza di un danno in atto irreparabile.

Ci si chiede, inoltre, per quale ragione FAVAP abbia scelto di rivolgere al Giudice civile una domanda – sulla cui ammissibilità, invero, si dubita - volta ad ottenere che il medesimo ordini a Telecom Italia di comunicare alle Autorità di pubblica sicurezza i dati relativi ai propri abbonati al fine di prevenire/reprimere eventuali ipotesi di reato, invece di adire, piuttosto, il competente Giudice penale. L'avere scelto, da parte del ricorrente, una via giudiziaria così contorta, pare fare escludere, oltre che l'effettiva convinzione da parte di FAPAV del fondamento delle proprie ragioni, anche la reale urgenza dell'istanza formulata dalla medesima.

Ed infatti, sono prospettabili due ipotesi per spiegare il ricorso al Giudice civile per fare ordinare a Telecom di comunicare i dati in parola al Giudice penale (il quale solo, peraltro, può ordinare la comunicazione dei dati in argomento):

FAPAV è consapevole dell'illecita provenienza e dell'inaffidabilità degli elementi a supporto della propria richiesta, tali da non poter essere presi in considerazione dal Giudice penale; in tal caso non si vede come la medesima possa pretendere dal Giudice adito la comunicazione di dati personali di terzi all'Autorità di pubblica sicurezza, in spregio alle norme di tutela della riservatezza;

ovvero

FAPAV ritiene che i dati dalla medesima acquisiti siano bastevoli per dimostrare il torto subito; in tale caso, l'avere scelto la tortuosa via giudiziaria sopra indicata, anziché rivolgersi direttamente al giudice competente per ottenere la celere tutela degli interessi dei propri associati,

porta ad escludere la sussistenza del periculum sostenuto dalla medesima, ai fini di giustificare il ricorso alla procedura d'urgenza ex art. 700 c.p.c..

***

Alla stregua di quanto precede, si rassegnano le seguenti

conclusioni

"Piaccia all'On.le Tribunale respingere l'istanza proposta da FAPAV, con vittoria di spese, ai sensi dell'art. 152, comma 12 del Codice".

Produzioni come da indice del fascicolo.

Roma, 8 febbraio 2010

F.to Sergio Fiorentino
avvocato dello Stato