T.A.R. LAZIO
21 APRILE 2008

PARTI: **FASTWEB S.P.A.** *(avv.ti Berbenni, de Vergottini)* **MINISTERO DELLE COMUNICAZIONI - ISPETTORATO TERRITORIALE PER LA LIGURIA** *(avvocatura Gen. dello Stato)* **MINISTERO DELL'INTERNO**

Prestazioni obbligatorie a fini di giustizia • Obbligo di conservazione dei dati telematici • Inadempimento • Sussistenza • Sanzione amministrativa

Non si ravvisano argomenti di ordine testuale, ovvero sistematico per ritenere che l'operatività dell'art. 6, comma 1, del D.L. n. 144/05 sia subordinata alla previa adozione del regolamento attuativo, contemplato dall'ultimo comma del medesimo testo normativo; ulteriore corollario di ciò è che dalla data di entrata in vigore del D.L. n. 144/05 deve ritenersi obbligatoria la conservazione dei dati del traffico telefonico o telematico (anche non soggetti a fatturazione), limitatamente alle informazioni che consentono la tracciabilità degli accessi.
La conclusione di tale ragionamento è che l'art. 6, comma 1, del D.L. n. 144/05 si pone come legittimo fondamento dell'obbligo di conservazione dei files di log, richiesti con l'ordine di esibizione, la cui violazione ha portato all'irrogazione della sanzione gravata.

FATTO E SVOLGIMENTO DEL PROCESSO. — Con atto notificato nei giorni 14 giugno 2007 e seguenti e depositato il successivo 27/6 la società ricorrente, premesso che la Procura della Repubblica presso il Tribunale di La Spezia, nell'ambito del procedimento penale n. 3080/06/44-2 R.G., emetteva ordine di esibizione nei confronti di « Telecom Italia Network S.r.l. e di ogni altro provider che eventualmente risulterà essere stato utilizzato » »al fine di acquisire copia dei« files di log completi di *caller id*, inerenti gli anni 2005 e 2006 relativi agli accessi all'indirizzo di posta elettronica oceanomare64@virgilio.it », e che in data 5 luglio 2006 detto ordine le veniva trasmesso dalla Polizia Postale di La Spezia con riferimento alla connessione avente I.P. 81.208.60.201 avvenuta il 29 marzo 2006 alle ore 15:24, espone di avere tempestivamente informato l'organo di polizia di non poter risalire ai dati richiesti in quanto la tecnologia di cui essa allora si avvaleva non lo consentiva.

Ciò nonostante con verbale n. 2 di accertamento e contestazione di violazione, elevato il 21 settembre 2006 dalla Polizia postale ai sensi della legge n. 689/81, e notificato a mezzo posta il 29 settembre 2006, veniva contestata a Fastweb la violazione dell'art. 96 del C.c.e. in materia di comunicazioni obbligatorie ai fini di giustizia ed inflitta sanzione amministrativa, pari ad euro 34.000,00 ai sensi del combinato disposto degli artt. 98, XIV comma, e 16 della legge n. 689/81.

Con memoria difensiva del 17 ottobre 2006 la deducente confermava che l'impossibilità di fornire i dati richiesti era dovuta al fatto che « fino al giorno 15 luglio 2006 non esisteva una infrastruttura tecnologica in grado di raccogliere e storicizzare i file di log delle connessioni transitate attraverso i router configurati con le regole di ''natting'', data la difficoltà tecnica relativa all'implementazione, selezione e conservazione dell'enorme mole di dati generata ».

Con l'ordinanza impugnata il Ministero delle Comunicazioni respingeva le argomentazioni espresse da Fastweb e confermava l'irrogazione della sanzione *ex* art. 98 del C.c.e., nel presupposto che nel caso in esame trova applicazione l'art. 6 della legge 31 luglio 2005, n. 155 (c.d. « legge Pisanu ») in tema di misure urgenti per il contrasto del terrorismo interna-

zionale, che impone agli operatori la conservazione, senza alcuna limitazione, dei dati relativi al traffico telematico.

Deduce a sostegno del ricorso i seguenti motivi di diritto:

1) In via preliminare: violazione dell'art. 9 del C.c.e.; illegittimità dell'ordinanza per l'erronea indicazione del termine e dell'autorità cui è possibile ricorrere ai sensi dell'art. 22-*bis* della legge n. 689/81, anziché ai sensi dell'art. 9 del C.c.e.

Va preliminarmente eccepita l'illegittimità dell'ordinanza impugnata con la quale si è disposto erroneamente che « avverso il presente provvedimento è ammessa opposizione, in carta semplice, al tribunale competente per territorio, entro trenta giorni dalla notificazione, ai sensi dell'art. 22-*bis* della legge n. 689/81 ».

Risulta infatti erronea l'indicazione del termine e dell'organo giurisdizionale (giudice ordinario) cui è possibile fare ricorso, in quanto la cognizione della presente controversia è devoluta in via esclusiva ed inderogabile alla giurisdizione esclusiva amministrativa ai sensi dell'art. 9 dello stesso C.c.e.

Giudice naturale della presente controversia è il T.A.R. del Lazio, vertendosi al cospetto di una controversia avente ad oggetto l'opposizione ad un provvedimento sanzionatorio di un organo periferico del Ministero delle Comunicazioni comminato ai sensi dell'art. 98, XIV comma, del C.c.e. per presunta violazione di quanto disposto dall'art. 96 del medesimo corpus normativo.

Dovendosi dunque adire il giudice amministrativo, non trova applicazione il termine stabilito dall'art. 22 della legge n 689/81, bensì quello ordinario di sessanta giorni stabilito per la proposizione del ricorso giurisdizionale avanti al giudice amministrativo.

È stato dunque indicato un termine inferiore a quello stabilito dalla legge, con conseguente lesione del diritto alla difesa di Fastweb, ed illegittimità del provvedimento impugnato.

2) Violazione dell'art. 96 del C.c.e. e dell'art. 6 del D.L. n. 144/2005, convertito nella legge n. 155/2005.

La piena operatività dell'art. 96 del C.c.e. è condizionata all'emanazione di un apposito repertorio cui è demandato il compito di individuare le c.d. prestazioni obbligatorie e di stabilire modalità, tempi di effettuazione delle prestazioni ed obblighi specifici degli operatori.

Fino all'approvazione del repertorio i tempi ed i modi delle prestazioni devono essere concordati con le autorità giudiziarie e continua a trovare applicazione il listino approvato con d.m. 26 aprile 2001.

Altra norma richiamata nel provvedimento sanzionatorio è l'art. 6 del D.L. n. 144/05, convertito nella legge n. 155/05 (c.d. legge Pisanu), recante misure urgenti per il contrasto del terrorismo internazionale.

Tale testo normativo, riformando l'art. 132 della legge sulla privacy, ha introdotto l'obbligo di custodia dei dati telematici ed ha subordinato l'attuazione di tale obbligo all'emanazione di uno specifico regolamento.

In tale contesto si pone la norma provvisoria dell'art. 6, I comma, la quale prevede una sorta di moratoria, riguardante le notizie di cui i fornitori, al momento dell'entrata in vigore della riforma, erano già in possesso, e non anche i dati la cui archiviazione è divenuta obbligatoria in forza della legge Pisanu.

Con riguardo a quanto contestato a Fastweb, nessuna norma le imponeva di conservare i files di log, prestazione non prevista nel listino di

cui all'art. 96 del C.c.e., né concordata con l'Autorità; al contempo, seppure prevista dall'art. 6 della legge Pisanu, essa non ha trovato concreta applicazione relativamente ai dati telematici, non essendo stato emanato il regolamento che definisce modalità, tempi di attuazione ed allocazione dei costi.

In ogni caso sarebbe illegittimo, implicando una sorta di analogia in malam partem, sanzionare ai sensi dell'art. 98 del C.c.e. una condotta prevista dall'art. 6 della legge Pisanu, e non già contemplata dall'art. 96 dello stesso C.c.e.

Si aggiunga ancora che la rete di Fastweb, diversamente dalla generalità di quelle degli altri operatori, è costruita sull'architettura di una MAN (metropolitan area network) che prevede l'utilizzo della NAT (network address translation) per la navigazione all'esteno della MAN; si tratta dunque di una tecnica che consiste nel modificare gli indirizzi IP (internet protocol) dei pacchetti in transito su un sistema.

Tale modalità di accesso ad internet non permetteva di svolgere attività di tracciamento storico (cioè di raccogliere e storicizzare i files di log).

A seguito della legge Pisanu Fastweb ha fatto ricorso ad un system integrator; i lavori di analisi sono iniziati nel luglio 2005, mentre la soluzione tecnologica è intervenuta nel maggio 2006; il costo totale di sviluppo di tale soluzione di tracciamento storico dei dati è stato di ben 3.755.000,00 euro che Fastweb ha sostenuto, benché ancora l'Amministrazione non abbia individuato né le modalità di conservazione dei dati, né abbia stabilito l'allocazione dei costi.

In ogni modo, dal 15 luglio 2006 Fastweb è in grado di raccogliere e storicizzare i files di log.

3) Eccesso di potere per illogicità e contraddittorietà della motivazione.

Il corredo motivazionale del provvedimento impugnato ne evidenzia l'illogicità e l'intrinseca contraddittorietà, nella misura in cui viene a sanzionare *ex* art. 98 del C.c.e. la violazione dell'art. 6 della legge Pisanu, piuttosto che la violazione dell'art. 96 dello stesso codice.

4) Violazione dell'art. 96 del C.c.e., dell'art. 6 della legge Pisanu, dell'art. 98 del C.c.e., nonché eccesso di potere in relazione alla violazione dei principi di legalità, determinatezza ed analogia.

La prestazione richiesta a Fastweb concerneva dunque la consegna di files di log; in realtà tale prestazione non poteva essere pretesa nei confronti della ricorrente, non essendone la stessa legittimamente in possesso.

Ex art. 96 del C.c.e. le prestazioni obbligatorie devono essere individuate in un apposito repertorio a tutt'oggi non ancora approvato; la norma aggiunge che fino all'approvazione del repertorio i tempi ed i modi sono concordati con le autorità e fino all'emanazione del decreto si applica il c.d. listino relativo alle prestazioni obbligatorie per gli organismi di comunicazione.

La conservazione di file di log non rientra nel disposto normativo dell'art. 96 del C.c.e., e non è dunque una registrazione telematica che Fastweb era tenuta ad archiviare e tenere a disposizione per soddisfare eventuali richieste dell'autorità giudiziaria.

È stata erroneamente applicato anche l'art. 6 della legge Pisanu in quanto, pur prevedendo la norma l'obbligo di conservazione dei file di log, non è ancora intervenuto il regolamento attuativo di cui al comma quarto.

Ai providers non sono dunque state fornite le specifiche tecniche per l'adempimento di tale obbligo.

5) Eccesso di potere e violazione di legge in relazione alla insussistenza dell'illecito amministrativo per la totale mancanza di colpevolezza in capo a Fastweb.

Fastweb non è stata in grado di adempiere alla prestazione in questione, in quanto il sistema utilizzato all'epoca dei fatti, e rispondente a tutte le prescrizioni all'epoca vigenti, non le permetteva di raccogliere e storicizzare i file di log.

Nessuna colpa di ciò può essere addebitata alla ricorrente, la quale, non appena entrata in vigore la legge Pisanu, pur in assenza di obblighi specifici, ha avviato lo studio di fattibilità e progettazione per fornire il proprio sistema di una soluzione che fosse in gradi di permettere il tracciamento storico dei dati (TSD); all'esito delle verifiche, è emersa l'inesistenza nel mercato di una soluzione tecnologica per adeguare la rete Fastweb alle nuove finalità, e per tale motivo la deducente ha fatto ricorso ad un system integrator.

Si è reso necessario lo sviluppo di alcuni prototipi ed un notevole impegno di risorse e mezzi al fine di giungere alla soluzione attualmente in esercizio.

In assenza di colpa non può ritenersi configurabile la fattispecie dell'illecito amministrativo contestato, come si desume dall'art. 3 della legge n. 689/81.

Si è costituito in giudizio, senza svolgere difese, il Ministero delle Comunicazioni.

All'udienza del 10 aprile 2008 la causa è stata trattenuta in decisione.

DIRITTO. — 1. Con il primo motivo viene dunque dedotta l'illegittimità dell'impugnata ordinanza — ingiunzione per violazione dell'art. 9 del C.c.e., in ragione dell'erronea indicazione del termine e dell'Autorità cui è possibile ricorrere, che avrebbe determinato una compressione del diritto alla difesa, prefigurando come applicabile la disciplina di cui agli artt. 22 e 22-*bis* della legge 24 novembre 1981, n. 689.

La censura non appare meritevole di positiva valutazione.

Occorre invero considerare come, secondo il consolidato indirizzo della giurisprudenza, sia amministrativa, che ordinaria in tema di sanzioni amministrative, l'omessa od erronea indicazione nel provvedimento impugnato del termine e dell'Autorità cui ricorrere, *ex* art. 3, IV comma, della legge 7 agosto 1990, n. 241, concreta una mera irregolarità, e non incide sulla legittimità dell'atto, consentendo solo la possibilità di ottenere la concessione dell'errore scusabile, al fine di attivarsi nella giusta sede (in termini, *ex multis*, Cons. Stato, Sez. VI, 16 maggio 2006, n. 2763; Cass., Sez. II, 31 maggio 2006, n. 12895; Cass., Sez. III, 12 marzo 2005, n. 5456; Cons. Stato, Sez. V, 31 gennaio 2003, n. 501; Cass., Sez. I, 6 marzo 2003, n. 3340).

Ora, nel caso di specie, appare indubbia l'applicabilità dell'art. 9 del D.Lgs. 1 agosto 2003, n. 259, con conseguente individuazione della giurisdizione esclusiva del giudice amministrativo, e competenza del T.A.R. del Lazio, con sede in Roma.

L'enucleazione, nell'ordinanza — ingiunzione gravata, del Tribunale ordinario come Autorità cui proporre opposizione, ed il (connesso) ter-

mine di trenta giorni, se non può comportare il beneficio della rimessione in termini, essendo stato rispettato il termine più breve, non è idonea a determinare alcuna conseguenza ulteriore, non solo perché, in concreto, la ricorrente ha comunque potuto svolgere le proprie difese, ma anche nella considerazione che l'irregolarità opera ex ante ed in astratto, con la conseguenza che il provvedimento amministrativo affetto da vizio formale minore (quale è quello dedotto nel caso di specie) è un atto *ab origine* meramente irregolare, per definizione tale da non comportare l'annullabilità dell'atto, anche a prescindere dalla considerazione che con l'introduzione dell'art. 21 *octies* nel corpus della legge generale sul procedimento amministrativo si è determinata una dissociazione tra illegittimità (vera e propria) ed annullabilità del provvedimento.

2. Con il secondo mezzo di gravame viene dedotta la violazione del combinato disposto dell'art. 96 del C.c.e. e dell'art. 6 del D.L. 27 luglio 2005, n. 144, convertito nella legge 31 luglio 2005, n. 155, nel duplice assunto che nessuna delle due norme imponeva, allo stato, a Fastweb di conservare i files di log, richiedendo, la prima, la previa emanazione di un apposito repertorio, e la seconda l'adozione di uno specifico regolamento, e che comunque la rete utilizzata dalla deducente, fino al luglio '06, non era in grado di raccogliere e storicizzare i predetti dati.

La censura è infondata, e deve pertanto essere disattesa.

Ed infatti l'art. 96 del C.c.e. prescrive, al primo comma, che « le prestazioni a fini di giustizia effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie sono obbligatorie per gli operatori; i tempi ed i modi sono concordati con le predette autorità fino all'approvazione del repertorio di cui al comma 2 »; al quarto comma dispone altresì che « fino all'emanazione del decreto di cui al comma 2, secondo periodo, continua ad applicarsi il listino adottato con D.M. 26 aprile 2001 del Ministro delle Comunicazioni, pubblicato nella G.U.R.I. n. 104 del 7/5/2001 ».

Se ne inferisce la configurabilità di una categoria di « prestazioni obbligatorie », a fini di giustizia; le modalità ed i tempi di effettuazione, nonché gli obblighi specifici degli operatori sono individuati con apposito repertorio; fino all'approvazione di questo, i tempi ed i modi vanno concordati con le competenti Autorità giudiziarie.

A fronte, dunque, di una previsione generica di prestazioni obbligatorie, contenuta nel predetto art. 96 del C.c.e., il primo comma dell'art. 6 del D.L. n. 144/05, nella formulazione applicabile alla fattispecie controversa, sanciva che « a decorrere dalla data di entrata in vigore del presente decreto e fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE ... del 15 marzo 2006, e comunque non oltre il 31 dicembre 2007, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi, debbono essere conservati fino alla data di entrata in vigore del provvedimento legislativo di attuazione

della direttiva 2006/24/CE ... del 15 marzo 2006, e comunque non oltre il 31 dicembre 2007, dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore ».

La norma da ultimo indicata sembra dunque enucleare un obbligo incondizionato in capo ai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, finalizzato al contrasto del terrorismo internazionale (salvo l'esercizio dell'azione penale per i reati comunque perseguibili).

Ad avviso di parte ricorrente, l'operatività di tale norma sarebbe invece condizionata all'adozione del regolamento, previsto dall'ultimo comma dell'art. 6, con cui vengono definite le modalità ed i tempi di attuazione della previsione di cui al comma 3, lett. *a*), *b*), *c*) e *d*), anche in relazione alla determinazione e allocazione dei relativi costi.

L'assunto non appare al Collegio condivisibile, in quanto il regolamento, come ora evidenziato, è attuativo delle previsioni contenute nel terzo comma dell'art. 6 del D.L. n. 144/05, le quali recano modifiche all'art. 132 del D.Lgs. 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali), in tema di « conservazione di dati di traffico per altre finalità ».

Si tratta di prescrizioni solo in parte sovrapponibili a quella del primo comma dell'art. 6, ma certamente non coincidenti e sotto il profilo teleologico, finalistico, e sotto il profilo contenutistico.

Conseguentemente non si ravvisano argomenti di ordine testuale, ovvero sistematico per ritenere che l'operatività dell'art. 6, I comma, del D.L. n. 144/05 sia subordinata alla previa adozione del regolamento attuativo, contemplato dall'ultimo comma del medesimo testo normativo; ulteriore corollario di ciò è che dalla data di entrata in vigore del D.L. n. 144 deve ritenersi obbligatoria la conservazione dei dati del traffico telefonico o telematico (anche non soggetti a fatturazione), limitatamente alle informazioni che consentono la tracciabilità degli accessi.

La conclusione di tale ragionamento è che l'art. 6, I comma, del D.L. n. 144/05 si pone come legittimo fondamento dell'obbligo di conservazione dei files di log, richiesti con l'ordine di esibizione, la cui violazione ha portato all'irrogazione della sanzione gravata.

È chiaro come allora, in tale contesto, non assume rilievo giuridico il fatto che la rete di Fastweb, all'epoca dell'ordine di esibizione, si avvalesse di una modalità di accesso ad internet che non consentiva di svolgere attività di tracciamento storico (e cioè proprio di raccogliere e storicizzare i files di log).

Al cospetto di un obbligo legale attuale, le difficoltà tecniche che hanno imposto alla società ricorrente di fare ricorso ad un system integrator, e di sviluppare una soluzione tecnologica complessa ed onerosa utile a conservare i dati, non sono utilmente opponibili; né, d'altro canto, viene fatta oggetto di censura l'incongruità dell'arco temporale messo a disposizione degli operatori per conformarsi alle nuove norme sui dati del traffico telefonico e telematico.

Resta, anzi, da osservare come il D.L. n. 144/05 sia entrato in vigore alla fine del luglio '05, mentre l'ordine di esibizione emesso dalla Procura della Repubblica della Spezia risale al 21 giugno 2006, e concerneva una connessione avvenuta il precedente 29 marzo 2006.

Non può dunque condividersi l'assunto difensivo di Fastweb in ordine alla inesigibilità della prestazione richiesta nei suoi confronti per il fatto di non essere legittimamente in possesso dei dati richiesti.

3. Con la terza e la quarta censura, che possono essere trattate congiuntamente, in quanto tra loro complementari, vengono ulteriormente ribaditi gli argomenti difensivi finora sviluppati, nella direzione, in particolare, della contraddittorietà della motivazione del provvedimento impugnato e della violazione del principio di legalità, per il fatto di avere quest'ultimo sanzionato, a tutto concedere, *ex* art. 98, XIV comma, del C.c.e. la violazione di un obbligo non fondato sull'art. 96 dello stesso codice.

Anche tali censure devono essere disattese.

Anzitutto va rilevata la coerenza del percorso motivazionale dell'ordinanza — ingiunzione, che, muovendo proprio dall'obiezione di Fastweb di non avere avuto (sino al 15 luglio 2006) una infrastruttura tecnologica in grado di raccogliere i files di log delle connessioni transitate attraverso i router configurati con le regole di « natting », la supera incentrando la propria decisione sulla portata dell'art. 6, I comma, del D.L. n. 144/05, norma che « impone in ogni caso e senza limitazioni di alcun genere la conservazione dei dati di traffico prodotto per l'accesso alle reti di comunicazione ».

Tale assunto, passando ad esaminare così il secondo profilo di contestazione, non determina peraltro un'applicazione analogica in malam partem dell'art. 96 del C.c.e., in quanto, come si è cercato supra di evidenziare, detta norma stabilisce che le prestazioni a fini di giustizia (effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie) sono obbligatorie per gli operatori, e la violazione di tali obblighi è sanzionata ai sensi del successivo art. 98, XIV comma.

Ora, l'art. 6, I comma, del D.L. n. 144/05 ha introdotto una nuova tipologia di « prestazione obbligatoria », di portata derogatoria rispetto anche alle disposizioni dell'art. 96 del C.c.e. con riguardo alle modalità ed ai tempi di effettuazione delle prestazioni stesse ed agli obblighi specifici degli operatori.

Tale profilo di specialità, derivante dalla portata incondizionata dell'art. 6, non esclude che l'obbligo di conservazione dei dati del traffico telefonico o telematico, da tale fonte derivante, costituisca una prestazione a fini di giustizia, ricadente comunque nell'ambito del più volte richiamato art. 96 del C.c.e., la cui violazione è dunque stata legittimamente sanzionata ai sensi dell'art. 98, XIV comma.

Più chiaramente, può ritenersi che la portata precettiva dell'art. 96 del C.c.e. sia stata (etero)integrata, in via provvisoria, ma cogente, sotto il profilo modale, dalla disposizione dell'art. 6 del D.L. n. 144/05; ma ciò, oltre a non violare il principio di legalità, non dà luogo neppure ad una non consentita interpretazione analogica, in quanto l'art. 96 è comunque norma che pone il precetto della obbligatorietà delle prestazioni effettuate a fini di giustizia.

4. Deve infine essere disatteso anche il quinto motivo di ricorso, con cui si lamenta l'insussistenza dell'elemento soggettivo della colpa (in

capo a Fastweb) necessario ad integrare l'illecito amministrativo, nella considerazione che l'infrastruttura tecnologica utilizzata all'epoca dei fatti non consentiva di raccogliere e storicizzare i files di log.

Ed invero, a fronte di un obbligo legale di conservazione dei dati del traffico telefonico o telematico (anche non soggetto a fatturazione), limitatamente alle informazioni che consentono la tracciabilità degli accessi, la inidoneità tecnologica dell'impianto non può integrare l'esimente della buona fede.

Occorre ricordare come l'art. 3 della legge n. 689/81 pone una presunzione di colpa in ordine al fatto vietato a carico di colui che lo abbia commesso, riservando a questi l'onere di provare di avere agito senza colpa.

Ne deriva che l'esimente della buona fede rileva come causa di esclusione della responsabilità amministrativa solo quando sussistano elementi positivi idonei ad ingenerare nell'autore della violazione il convincimento della liceità della sua condotta, e risulti che il trasgressore abbia fatto tutto il possibile per conformarsi al precetto di legge, onde nessun rimprovero possa essergli mosso (in termini, *ex multis*, Cass., Sez. II, 11 giugno 2007, n. 13610; Cass., Sez. II, 14 marzo 2007, n. 5894).

D'altro canto, a dimostrazione della inconfigurabilità di un errore (incolpevole ed inevitabile) sulla liceità del fatto sta la oggettiva considerazione che Fastweb si è successivamente attivata per conformarsi alla previsione dell'art. 6 del D.L. n. 144/05.

Né può parlarsi di un fisiologico tempo di adeguamento alle nuove prescrizioni legislative, atteso che, come già posto in evidenza, il D.L. n. 144/05 è stato pubblicato nella G.U. 27 luglio 2005, n. 173, mentre l'ordine di esibizione inadempiuto risale al 21 giugno 2006, e si colloca dunque a distanza di quasi un anno dall'entrata in vigore della norma.

In definitiva, l'errore sulla illiceità del fatto deve trovare causa in un fatto scusabile, certamente non identificabile nella mera asserita incertezza del contesto normativo, risultando, questa, una condizione sempre superabile con adeguata diligenza; ciò tanto più ove riguardi un operatore professionale, e cioè un soggetto nei cui confronti il dovere di conoscenza ed informazione in ordine ai limiti e condizioni del proprio operare è particolarmente intenso, con l'effetto che la sua condotta, sotto il profilo considerato, deve essere valutata con maggiore rigore (Cass., Sez. II, 11 ottobre 2006, n. 21779).

5. Le considerazioni che precedono impongono la reiezione del ricorso per l'infondatezza dei motivi dedotti.

Sussistono tuttavia giusti motivi per disporre tra le parti la compensazione delle spese di giudizio.

P.Q.M. — Il Tribunale Amministrativo Regionale per il Lazio - Sezione III-*ter*, definitivamente pronunciando sul ricorso in epigrafe, lo respinge.

Compensa tra le parti le spese di giudizio.

Ordina che la presente sentenza sia eseguita dall'Autorità amministrativa.

LA DISCIPLINA DEGLI OBBLIGHI DI CONSERVAZIONE DEI DATI TELEMATICI DA PARTE DEI PROVIDERS

1. Premessa.

La pronuncia in commento desta particolare interesse non solo perché il giudice amministrativo non siè ulteriormente determinato sulla disciplina *de qua*, ma anche perché, affermando un principio di diritto che, come si dirà, appare opinabile, offre l'opportunità di analizzare l'intera evoluzione del quadro normativo nazionale in materia di obblighi di conservazione dei dati telematici riconosciuti in capo ai *providers*.

La decisione in discorso verrà approfondita nelle pagine che seguono ma a chi scrive pare opportuno rilevare sin d'ora come la criticabilità della sentenza trovi sostegno non solo nella dottrina già espressasi al tempo dei fatti, ma pure nell'intervenuto D.Lgs. n. 109 del 30 maggio 2008 che, colmando la lacuna normativa allora esistente ha contribuito a smentire l'esegesi fornita dal T.A.R. del Lazio nell'aprile del 2008.

Per una corretta individuazione del tema, occorre però premettere che la regolamentazione di settore si è evoluta seguendo il mutare del rapporto fra *privacy* e sicurezza pubblica[1]. Tale, solo apparente, digressione è utile per cogliere a pieno il ruolo, non certo marginale, assunto nel settore *de quo* dal *provider*, il quale, trattando le informazioni degli utenti, può cooperare al corretto sviluppo delle indagini secondo una responsabilizzazione, a seconda dei casi, più o meno marcata[2].

Gli episodi di terrorismo internazionale registrati all'inizio del duemila hanno indotto il legislatore comunitario e nazionale ad intervenire mediante una serie di misure urgenti atte a contrastarne l'*escalation*.

Relativamente al quadro nazionale, occorre qui richiamare l'art. 6 del D.L. n. 144/05, convertito in legge n. 155/05 (*c.d. legge Pisanu)*.

La norma in parola, come si vedrà, intervenendo sul regime delle responsabilità in capo ai *providers*, ha dettato una nuova disciplina in tema di conservazione dei dati derivanti dal traffico telefonico e telematico, più specificatamente, ha ampliato gli obblighi di custodia delle informazioni, al contempo introducendo una disciplina transitoria.

Quindi, mentre con riferimento ai dati ricavati dal traffico telefonico, sin dal 2003, era presente nel nostro ordinamento un esplicito, e immediatamente vigente, obbligo di conservazione, per le informazioni telematiche, diversamente, il dovere di custodia è stato previsto solo nel 2005, subordinandolo comunque all'emanazione di un apposito regolamento attuativo.

La regolamentazione della materia è stata poi da ultimo incisa dal D.Lgs. 30 maggio 2008 n. 109. Preliminarmente importa osservare che

---

[1] Cfr. C. Fatta, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in questa *Rivista* 2008, 395 ss.

[2] Per un confronto tra le valutazioni effettuate sul tema nell'ordinamento nordamericano e in quello europeo, Vedi G.L. Perdonò, *Le responsabilità penali collegate all'uso di internet fra comparazione e prospettive di riforma*, in questa *Rivista* 2007, 323 ss.

tale decreto, avvalorando l'opinabilità della decisione indicata, ha modificato la disciplina di settore e, oltre ad abrogare parzialmente il già citato art. 6 della legge n. 155/05, ha concretamente individuato le categorie di dati (anche telematici) da preservare, così rendendo concretamente efficace l'obbligo di conservazione in capo ai *providers* (nel 2005 previsto solo in via programmatica).

2. Il caso oggetto della controversia e i contenuti della decisione.

Conviene illustrare anzitutto la fattispecie sottoposta all'esame del T.A.R.

La vicenda veniva originata dall'irrogazione di una sanzione amministrativa nei confronti di un *provider* che, alla richiesta delle autorità competenti, non era stato in grado di fornire copia di determinati *files* di *log*.

La sanzione irrogata per questo mancato adempimento veniva poi confermata dalla successiva ordinanza-ingiunzione emessa dal Ministero delle Comunicazioni.

Il presupposto fondante per la determinazione in discorso era da rinvenire nella ritenuta sussistenza, in capo al fornitore di servizio, di un incondizionato obbligo di conservazione dei dati telematici, asseritamente discendente dall'applicabilità al caso in esame dell'art. 6 della legge n. 155/05.

Su queste basi, il giudice amministrativo adito, condividendo l'opinione dell'amministrazione, ha ritenuto che la norma *de qua* « (...) *impone agli operatori la conservazione, senza alcuna limitazione, dei dati relativi al traffico telematico* (...) ».

Quindi, con la pronuncia oggetto di questo commento, il giudice amministrativo, determinandosi sulla portata applicativa del menzionato art. 6, ha ricondotto l'obbligo di conservazione dei dati telematici al comma 1 della norma anziché al successivo comma 3. Invero, mentre il comma 1 dettava una disciplina transitoria che, in quanto tale, si applicava alle sole prescrizioni già in vigore prima del 2005; il comma 3 innovava la disciplina in materia e, novellando l'art. 132 del decreto legislativo 30 giugno 2003, n. 196 (*c.d.* Codice della *Privacy*), individuava un inedito obbligo di conservazione dei dati telematici comunque subordinandolo, ai sensi del seguente comma 4, all'emanazione di uno specifico regolamento attuativo.

Come meglio si argomenterà nelle pagine che seguono le determinazioni a cui è giunto il T.A.R. paiono criticabili sotto diversi profili.

3. Disciplina normativa vigente in materia sino all'emanazione della *c.d.* « legge Pisanu »: obbligo di conservazione dei soli dati telefonici.

Come già detto, la materia che qui ci occupa è stata sin dall'origine regolamentata avendo come parametro di riferimento il rapporto *privacy*-sicurezza pubblica, per queste ragioni l'analisi non può che partire dalla Direttiva 2002/58/CE.

La disposizione comunitaria appena richiamata si occupa del trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche, sicché, in un contesto in cui l'esigenza princi-

palmente perseguita sembra essere quella di tutela della *privacy*[3], l'art. 15[4] (riservando agli Stati membri la possibilità di adottare misure legislative atte a garantire la sicurezza nazionale mediante la conservazione dei dati utili all'accertamento e al perseguimento dei reati) rappresenta un'eccezione.

Il legislatore italiano ha deciso di esercitare la facoltà in discorso con l'art. 132 del D.Lgs. n. 196/2003 (*c.d.* Codice della *Privacy*), adeguando poi di volta in volta la disciplina *ivi* contenuta al mutare della valutazione politica in ordine al rapporto fra sicurezza collettiva e diritto alla riservatezza.

In origine l'obbligo di conservazione incombente sui fornitori si riferiva tassativamente ed esclusivamente ai « *dati relativi al traffico telefonico* ». Questa formula, che ovviamente impediva di ricomprendere la documentazione dei collegamenti ad *internet* nell'ambito del dovere di custodia, è stata però messa in discussione per il crescente ricorso alle nuove tecnologie da parte delle organizzazioni terroristiche.

Conseguentemente si intervenne per la prima volta sulla materia *de qua* col D.L. n. 354/2003.

In sede d'elaborazione fu attentamente valutata la relazione fra le emergenti esigenze investigative e la tutela della *privacy*, ad ogni modo, se nella prima versione del provvedimento si ritenne prioritario l'interesse alla repressione dei reati, e coerentemente veniva previsto un esplicito riferimento all'obbligo di conservazione delle informazioni provenienti dalla « rete », nella versione definitiva dello stesso D.L. furono effettuate valutazioni diverse e il legislatore scelse di eliminare la clausola di ampliamento dell'obbligo di custodia ai dati telematici[5].

---

[3] A sostegno di tale affermazione basti richiamare gli accorgimenti predisposti dalla stessa direttiva 2002/58/CE per evitare che la divulgazione dei dati transitati e conservati nelle strutture di rete possa ledere il diritto alla riservatezza degli utenti. Fra le tante, a titolo meramente esemplificativo, si possono ricordare: il generale divieto di memorizzare i dati relativi alle comunicazioni (art. 5); nonché l'obbligo di cancellare o di rendere anonimi i dati relativi al traffico di comunicazioni (art. 6).

[4] Tale articolo stabilisce che: « (...) Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea (...) ».

[5] L'art. 132 del Cod. della *Privacy*, come novellato dal D.L. 354/03, statuiva come segue: « *Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione dei reati.*

Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico sono conservati dal fornitore per ulteriori ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) *del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.*

Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pub-

Tale formulazione fu preferita sulla scorta di due principali argomentazioni.

Da una parte, fu rilevato che l'esigenza di tutela della *privacy* sconsigliava la creazione d'una gigantesca banca-dati, dietro la quale sarebbe stato facile intravedere il pericolo d'una schedatura di massa[6].

Dall'altra parte, furono portate ragioni di carattere economico.

Con specifico riferimento a queste ultime fu evidenziato che, per archiviare una massa di materiali così imponente, i *providers* avrebbero dovuto sopportare costi particolarmente alti, ciò avrebbe avuto delle ripercussioni a cascata: aumento delle tariffe applicate agli utenti, chiusura dei gestori più piccoli o, addirittura, concretizzazione del rischio che, per compensare le maggiori spese, i dati venissero usati per finalità improprie[7].

Sulla base di questi argomenti, il legislatore scelse di non prescrivere alcun obbligo di conservazione con riguardo al traffico telematico[8], limitandosi a consentire l'apprensione di quei soli dati che i *providers* avrebbero comunque conservato a fini contabili[9].

---

blico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. (...)».

[6] Cfr. gli interventi di C. FALANGA (Camera, seduta del 26 gennaio 2004, n. 412) e B.M. MAGNOLFI (Commissione giustizia della Camera, seduta del 14 gennaio 2004).

[7] Cfr. C. FALANGA (Camera dei deputati, seduta del 28 gennaio 2004, n. 414); S. COLA (Camera, seduta del 28 gennaio 2004, n. 414); L. VITALI (Commissione giustizia della Camera, seduta del 14 gennaio 2004); P. FOLENA (Camera, sedute del 26 gennaio 2004, n. 412 e del 28 gennaio 2004, n. 414); B.M. MAGNOLFI (Camera dei deputati, Commissione giustizia, seduta del 14 gennaio 2004, nonché assemblea, seduta del 26 gennaio 2004, n. 412); B.M. MAGNOLFI (Commissione giustizia della Camera, seduta del 14 gennaio 2004).

[8] Tra l'altro, tale la scelta seguiva la direttrice già tracciata nell'ambito della convenzione del Consiglio d'Europa sul *cybercrime* (Budapest, 23 novembre 2001, ratificata in Italia con la Legge 18 marzo 2008, n. 48). Infatti, il Comitato di esperti sulla criminalità nello spazio cibernetico, allora incaricato di estendere il progetto, non riuscì a raggiungere il consenso intorno all'idea di obbligare i fornitori di ciascun Paese firmatario a conservare sistematicamente, per un certo periodo, i dati di traffico.

[9] Ai sensi dell'art. 123 dello stesso Codice della *Privacy* allora vigente: «*I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.*

Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento.

Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'ac-

4. Emanazione del D.L. 27 luglio 2005 n. 144 convertito, con modificazioni, in legge 31 luglio 2005, n. 155: ampliamento degli obblighi di conservazione dei fornitori anche alle informazioni derivanti dal traffico *internet*.

Nel 2005 il legislatore italiano riformò nuovamente la materia della conservazione dei dati a fini di giustizia.

Il passaggio dalla vecchia alla nuova regolamentazione non fu tuttavia repentino, si scelse di intervenire per gradi, subordinando l'entrata in vigore del novellato art. 132 del Cod. della *Privacy* all'emanazione di una serie di prescrizioni attuative. Nel frattempo avrebbe trovato applicazione una specifica disciplina transitoria che, fino alla piena efficacia della nuova normativa, avrebbe sospeso i vincoli legislativi già vigenti[10].

certamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto.

Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione».

[10] L'art. 6 della legge n. 155/05 così disponeva: «*A decorrere dalla data di entrata in vigore del presente decreto e fino al 31 dicembre 2007, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi, debbono essere conservati fino al 31 dicembre 2007 dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.*

All'articolo 55, comma 7, del decreto legislativo 1º agosto 2003, n. 259, le parole: "al momento dell'attivazione del servizio" sono sostituite dalle seguenti: "prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.). Le predette imprese adottano tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici riportati su un documento di identità, nonché del tipo, del numero e della riproduzione del documento presentato dall'acquirente ed assicurano il corretto trattamento dei dati acquisiti".

All'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: "al traffico telefonico", sono inserite le seguenti: "inclusi quelli concernenti le chiamate senza risposta";

b) al comma 1, sono aggiunte, in fine, le seguenti parole: "mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi";

c) al comma 2, dopo le parole: "al traffico telefonico", sono inserite le seguenti: "inclusi quelli concernenti le chiamate senza risposta";

d) al comma 2, dopo le parole: "per ulteriori ventiquattro mesi", sono inserite le seguenti: "e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi";

e) al comma 3, le parole: "giudice su istanza del pubblico ministero o" sono sostituite dalle seguenti: "pubblico ministero anche su istanza";

f) dopo il comma 4 è inserito il seguente:

"4-bis. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo

Già una mera lettura della norma evidenzia le tre direttrici prescelte dal legislatore:

i) si allargano gli obblighi di custodia addossati ai fornitori, estendendoli ad informazioni che, prima, dovevano essere cancellate;

ii) si introduce una disciplina transitoria che sospende, per un certo periodo, ogni obbligo di distruggere i dati raccolti;

iii) infine, si cambia la suddivisione delle incombenze tra giudice e pubblico ministero: il baricentro del sistema si sposta verso il secondo organo, le cui prerogative crescono sensibilmente.

Tralasciando il terzo profilo, non di interesse per il caso che qui ci occupa, nelle pagine che seguono ci si soffermerà sui primi due aspetti, aspetti che, lo si ripete, la pronuncia qui commentata pare non aver correttamente colto.

Con riferimento al punto *sub i*) va rilevato come l'art. 6, comma 3, lettere a, b, c e d della novella, sia intervenuto sull'art. 132 Cod. *Privacy*, accrescendo gli obblighi di conservazione *ivi* regolati. L'ampliamento in discorso attiene non solo alle caratteristiche dei dati (estende ad esempio l'obbligo di conservazione alle chiamate telefoniche senza risposta) ma anche, ed è ciò che qui rileva, al *genus* degli stessi.

In altri termini, con specifico riguardo alla fattispecie di interesse in questo scritto, con la novella del 2005 sono stati introdotti nel nostro ordinamento nuovi doveri di custodia dei dati derivanti dal traffico telematico, anche se, per espressa statuizione del legislatore[11], queste disposizioni non potranno considerarsi operative sino a quando non sarà stato emanato un apposito regolamento applicativo capace di determinare « *modalità* », « *tempi di attuazione* » e « *allocazione dei* (...) *costi* »[12].

Questa scelta appare non solo coerente con le perplessità di natura economica che in sede di prima modifica dell'art. 132 del Codice della *Privacy*[13] avevano impedito l'introduzione di un esplicito riferimento ai dati telematici ma, vieppiù, si mostra doverosa. Infatti, secondo la dottrina occupatasi del tema: « (...) *almeno per quanto riguarda i collegamenti alla rete, non si poteva fare altrimenti: i providers sarebbero stati all'improvviso caricati d'un compito improbo, perché la massa delle in-*

---

possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati'''.

Con regolamento adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri interessati, sentito il Garante per la protezione dei dati personali, sono definiti le modalità ed i tempi di attuazione della previsione di cui al comma 3, lettere a), b), c) *e* d), *del presente articolo, anche in relazione alla determinazione e allocazione dei relativi costi, con esclusione, comunque, di oneri per il bilancio dello Stato.* ».

[11] Cfr. art. 6, comma 4, del D.L. 144/05.

[12] Nel parere reso, il 29 luglio 2005, alle Commissioni I e II della Camera dei deputati, il Comitato per la legislazione ha esattamente osservato che gli effetti della regola « *sono destinati a prodursi in un momento differito rispetto all'entrata in vigore del decreto legge, in quanto si rinvia la definizione di specifici aspetti [...] a successivi atti di natura non legislativa, senza peraltro stabilirne [...] i termini di emanazione* ».

[13] Cfr. paragrafo 3.

formazioni da archiviare è davvero imponente; così, (...) *nuovi obblighi di custodia, sono demandati ad un futuro regolamento* (...) »[14].

Per quanto attiene al profilo *sub ii*), basti dire che l'art. 6, comma 1, del più volte citato D.L. n. 144, introduceva una sorta di « *moratoria* »[15], in quanto tale, capace di sospendere l'efficacia solo ed esclusivamente su disposizioni normative regolarmente vigenti.

5. *Ius superveniens*: il D.Lgs. n. 109/08 come chiave interpretativa della sentenza.

Successivamente alla pronuncia che qui si commenta, il panorama normativo in materia di obblighi di custodia delle informazioni telematiche è stato ulteriormente innovato in maniera tale da ulteriormente evidenziare l'erroneità della decisione resa dal T.A.R. del Lazio.

L'analisi dello *ius superveniens* non può non iniziare dal D.L. n. 248/2007 che, intervenendo sull'art. 6, comma 1, della legge n. 155/05 e prorogando i termini della *data retention* fino al 31 dicembre 2008, ha aggiunto che « (...) *a decorrere dalla data di entrata in vigore del presente decreto e fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE del Parlamento Europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico* (...) ».

La direttiva comunitaria appena richiamata, emanata in armonia con quella relativa alla *privacy* (2002/58/CE) che vieta la generazione di ciò che non sia già necessario alla normale operatività del servizio, aveva quale obiettivo l'armonizzazione, nell'ambito comunitario, delle diverse discipline nazionali dettate in tema lotta al terrorismo internazionale. In particolare essa riguardava la conservazione di dati generati o trattati nella fornitura di servizi di comunicazione elettronica e, al paragrafo 23, statuiva « (...) *dato che gli obblighi dei fornitori di servizi di comunicazioni elettroniche dovrebbero essere proporzionati, la presente direttiva prescrive che essi conservino soltanto i dati generati o trattati nel processo di fornitura dei loro servizi di comunicazione. Nella misura in cui tali dati non sono generati o trattati da detti fornitori, non sussiste alcun obbligo di conservarli* (...) ».

L'Italia ha recepito la direttiva in discorso col già menzionato D.Lgs. n. 109/2008.

L'art. 2 di detto provvedimento normativo, abrogando tacitamente il comma 1 (ed esplicitamente il comma 4) dell'art. 6 della legge n. 155/05, ha modificato parzialmente l'art. 132 del Codice della *privacy*.

Non solo, con il proprio art. 5, il decreto *de quo* ha ulteriormente inciso sul Codice in parola inserendovi l'art. 162 *bis* che, per la prima volta, definisce uno specifico regime di « *Sanzioni in materia di conservazione dei dati di traffico* ».

---

[14] Vedi A. Camon, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.*, 2005, 2, p. 594 ss.

[15] Così la relazione al disegno di legge di conversione del decreto.

Sempre con il citato D.Lgs. n. 109, sono state individuate le « *Categorie di dati da conservare per gli operatori di telefonia e comunicazione elettronica* ». Tali dati sono stati meglio specificati « *[ne]i dati necessari per determinare la data, l'ora e la durata di una comunicazione* », con particolare riferimento all'accesso a internet sono stati individuati nella « (...) *data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;* (...) » (art. 3 lettera *c*) punto 2.1).

Da quanto precede emerge quindi che lo *ius superveniens*, colmando la carenza normativa che connotava la disciplina di settore al tempo della causa, ha messo in luce la *ratio* sottesa alle disposizioni allora vigenti. Specificatamente ha evidenziato l'insussistenza — allora — di obblighi di conservazione di dati derivanti dal traffico *internet*.

6. Considerazioni conclusive.

In conclusione: la sentenza qui commentata, presupponendo al tempo dei fatti pienamente efficaci e quindi disattesi gli obblighi di conservazione introdotti dall'art. 6 della legge Pisanu (L. n. 155/05), ha confermato la sanzione nei confronti del *provider*. Il ragionamento che ha portato il giudice adito a pronunciarsi in tali termini si presta però ad una lettura critica, in particolar modo, con riferimento alle affermazioni secondo cui: « (...) *il regolamento* (*ndr* di cui al comma 4 dell'art. 6 del D.L. n. 144/05) *è attuativo delle previsioni contenute nel terzo comma dell'art. 6 del D.L. n. 144/05, le quali recano modifiche all'art. 132 del D.Lgs. 30 giugno 2003, n. 196* (...) *Si tratta di prescrizioni solo in parte sovrapponibili a quella del primo comma dell'art. 6, ma certamente non coincidenti e sotto il profilo teleologico, finalistico, e sotto il profilo contenutistico* (...) ».

In realtà i commi 1 e 3 dell'art. 6 erano stai concepiti dal legislatore secondo una relazione diretta.

Infatti, assodato che l'emanazione del regolamento rappresentava *conditio sine qua non* per l'operatività dell'obbligo di conservazione dei dati telematici, la disciplina transitoria non poteva dirsi riferibile alle informazioni derivanti dal traffico telematico in quanto, allora, per questa tipologia di dati non sussisteva alcuna previsione normativa in tal senso.

Tale interpretazione non solo si mostra coerente con le valutazioni effettuate in sede di elaborazione del D.L. n. 354/03 circa le difficoltà economiche che avrebbero altrimenti incontrato i *providers* nel trovarsi inaspettatamente obbligati a conservare una tale enormità di informazioni (cfr. *sub* 3), ma è anche l'unica esegesi capace di chiarire la portata della norma senza contrastare con la natura transitoria della stessa.

Sicché, in considerazione di tutto ciò che precede e anche alla luce del richiamato *ius superveniens*, dal quale è desumibile un'ulteriore conferma in tal senso, i canoni interpretativi utilizzati dal giudice nella formulazione della sentenza meglio indicata in premessa appaiono discutibili, specie con riferimento all'affermazione secondo cui il comma 1 dell'art. 6 enucleerebbe « (...) *un obbligo incondizionato* (...) ».

Chi scrive, condividendo l'opinione della dottrina già espressasi sul tema, ritiene che il precetto in discorso riguardasse solo le informazioni che i fornitori erano già obbligati a conservare ciò in quanto, al tempo dei fatti, mancava una puntuale disciplina attuativa la quale, come visto, è intervenuta solo nel 2008 col D.Lgs. n. 109.

ANTONIO TOLONE