Milano, 16 febbraio 2007

RAPPORTO DEL COMITATO PER IL CONTROLLO INTERNO E PER LA CORPORATE GOVERNANCE AL CONSIGLIO DI AMMINISTRAZIONE

1. Premesse

1.1. Il presente rapporto è stato redatto dal COMITATO PER IL CONTROLLO INTERNO E PER LA CORPORATE GOVERNANCE ad esito delle attività svolte e degli accertamenti effettuati dal COMITATO medesimo nel corso del 2006 e fino alla metà di febbraio del corrente anno con riferimento alle seguenti materie:

- vicende concernenti l'*ex* responsabile della *Funzione Security*, Giuliano Tavaroli;
- sicurezza della rete e servizi all'Autorità Giudiziaria;
- dati di traffico, *privacy* e informazioni sui dipendenti.

1.2. Si precisa che, ai sensi dell'art. 12 del Codice di Autodisciplina della Società, il COMITATO ha funzioni consultive e propositive nei confronti del Consiglio di Amministrazione. In particolare (e per quanto interessa ai presenti fini), il COMITATO assiste il Consiglio nell'espletamento dei compiti relativi al sistema di controllo interno; valuta il piano di lavoro preparato dai preposti al controllo interno e riceve le relazioni periodiche degli stessi; riferisce al Consiglio, almeno semestralmente, sull'attività svolta e sull'adeguatezza del sistema di controllo interno.

1.3. Il COMITATO è composto interamente da Amministratori indipendenti (Guido Ferrarini, Francesco Denozza, Domenico De Sole e Marco Onado). Ai suoi lavori partecipa il Presidente del Collegio Sindacale o altro sindaco di volta in volta designato dallo stesso. Ove ritenuto opportuno, in relazione alle tematiche da trattare, il COMITATO e il Collegio Sindacale si riuniscono congiuntamente.

1.4. Si precisa altresì che, ai sensi dell'art. 11 del Codice di Autodisciplina della Società, il Consiglio di Amministrazione definisce le linee guida del sistema di controllo interno e ne verifica il corretto funzionamento con riferimento alla gestione dei rischi aziendali. L'Amministratore all'uopo delegato (attualmente il Vice Presidente Esecutivo, Carlo Buora) definisce gli strumenti e le modalità di attuazione del sistema di controllo interno, in esecuzione degli indirizzi stabiliti dal Consiglio di Amministrazione; assicura l'adeguatezza complessiva del sistema stesso, la sua concreta funzionalità, il suo adeguamento alle modificazioni delle condizioni operative e del panorama legislativo e regolamentare.

1.5. Al fine di verificare il corretto funzionamento del sistema di controllo interno il Consiglio di Amministrazione si avvale, oltre che del COMITATO, di un preposto

dotato di un adeguato livello di indipendenza e di mezzi idonei allo svolgimento della funzione. Tale preposto - attualmente individuato nella società consortile TELECOM ITALIA AUDIT & COMPLIANCE SERVICES, che ha all'uopo incaricato il suo Presidente Armando Focaroli - riferisce del suo operato al Vice Presidente Esecutivo, al COMITATO ed al Collegio Sindacale.

1.6. Il Vice Presidente Esecutivo dà attuazione agli interventi sul sistema di controllo interno che si rendano necessari in esito alle attività di verifica svolte, a tal fine nominando uno o più preposti. Nel 2005, per meglio coordinare l'attuazione del sistema di controllo interno, è stato creato il ruolo di *Group Compliance Officer*. Nel corso del 2006, per assicurare il coordinamento al vertice della gestione dei rischi, da una parte è stato istituito un apposito Comitato di *Risk Management*, presieduto da Carlo Buora e composto dei responsabili delle Direzioni centrali interessate; dall'altra parte, nell'ambito di TELECOM ITALIA AUDIT & COMPLIANCE SERVICES, è stata costituita la funzione *Group Risk Officer*.

1.7. I principi del sistema di controllo interno sono enunciati dall'art. 11, comma 6, del Codice di Autodisciplina e specificati, tra l'altro, nel Modello Organizzativo. Questo Modello, adottato ai sensi del d.lgs. n. 231/2001, si articola in "principi di comportamento con la Pubblica Amministrazione" e in "schemi di controllo interno" nei quali sono elencate le principali fasi di ogni processo, sono evidenziati gli eventuali reati perpetrabili e vengono definite le attività preventive di controllo finalizzate ad evitare i relativi rischi. Il Modello Organizzativo 231 è sottoposto a revisione periodica in conseguenza dell'esperienza applicativa e dell'estensione della disciplina 231 a nuove fattispecie. Un apposito Organismo di Vigilanza (OdV), composto da un Sindaco (Ferdinando Superti Furga che lo presiede), un Amministratore indipendente (Guido Ferrarini) e il preposto al controllo interno (Armando Focaroli), vigila - con il supporto di un'apposita funzione denominata *231 Support Group* - sull'osservanza del Modello e ne propone - con la collaborazione di uno *Steering Committee* composto dei Dirigenti responsabili delle funzioni interessate - le necessarie modifiche.

1.8. La parte del sistema di controllo interno concernente il *reporting* economico/finanziario è anche interessata dall'applicazione del *Sarbanes-Oxley Act*, che prevede sia una certificazione sui relativi controlli interni da parte del CEO e del CFO, sia una attestazione dei revisori circa l'adeguatezza dei controlli in materia, ai sensi della *Section* 404 della medesima legge. La Società è attualmente impegnata in un importante progetto diretto ad assicurare la piena e corretta applicazione di tale disciplina e, quindi, il perfezionamento dei controlli interni di tipo contabile e finanziario (Progetto 404). L'attestazione dei revisori sarà rilasciata, per la prima volta, con riferimento al bilancio del presente esercizio.

2. Le attività svolte dal COMITATO

2.1. Gli accertamenti relativi alla vicenda *Security*, in una prima fase, hanno interessato solo la funzione di *Internal Audit* e l'OdV (v. sotto il n. 3.1). Peraltro, nella riunione del 4 maggio 2005, al COMITATO vennero fornite una prima generica informativa, nel *Report* trimestrale del Preposto al Controllo Interno, circa l'*audit* in materia di *Security*; nonchè un'informativa riservata in ordine all'avviso di garanzia notificato a Giuliano Tavaroli.
In data 15 luglio 2005, il COMITATO ricevette un'informativa sulla autosospensione di Giuliano Tavaroli - in data 4 maggio 2005 - dal suo incarico dirigenziale e sull'intendimento di attribuirgli un incarico consulenziale in materia di antiterrorismo.
Il Consiglio di Amministrazione ebbe analoga informativa in data 26 luglio 2005, quando fu anche informato della nomina di Giovanni Penna quale responsabile *ad interim* della Funzione *Security*.

2.2. Il COMITATO è stato più direttamente investito delle tre materie oggetto di questo rapporto a partire dal 2006, nelle riunioni qui sotto specificate:

2.2.1. riunione del 30 marzo 2006: esame delle notizie di stampa relative a presunte irregolari attività di intercettazione e utilizzo improprio di dati di traffico della clientela; in merito alla vicenda Tavaroli: segnalazione, da parte del Preposto al Controllo Interno, i) dell'intervento di *audit* effettuato nel febbraio/marzo 2005, ii) dell'acquisizione da parte dell'Autorità Giudiziaria delle relative risultanze, nonché iii) dell'attivazione di misure organizzative correttive dichiarate idonee; del che fu fatta relazione al Consiglio di Amministrazione della Società in data 8 maggio 2006;

2.2.2. riunione (congiunta con il Collegio Sindacale) del 12 giugno 2006: esame delle tematiche di *compliance* (rete, sistemi informatici, servizi per l'Autorità Giudiziaria); in merito alla vicenda Tavaroli, al COMITATO fu segnalata la presentazione di un esposto all'Autorità Giudiziaria; di ciò venne fatta relazione al Consiglio di Amministrazione in data 5 luglio 2006, quando venne anche esaminato un documento riguardante le materie oggetto di questo Rapporto;

2.2.3. riunione (congiunta con il Collegio Sindacale) del 29 settembre 2006: analisi dell'Ordinanza di custodia cautelare emessa dal Giudice per le indagini preliminari presso il Tribunale di Milano nei confronti, tra gli altri, di Giuliano Tavaroli (ordinanza che è divenuta di pubblico dominio a seguito della pubblicazione integrale del provvedimento a mezzo internet presso il sito www.ilvelino.it); esame delle irregolarità nel trattamento di dati di traffico e delle attività svolte dalla Società per conformarsi al Provvedimento dell'Autorità Garante per la *Privacy* del 1° giugno 2006;

2.2.4. riunione (congiunta con il Collegio Sindacale) del 3 ottobre 2006: prosecuzione dell'esame della questione *Privacy*;

2.2.5. riunione (congiunta con il Collegio Sindacale) del 12 ottobre 2006: audizioni del Vice Presidente Esecutivo, di *KPMG Advisory*, della società di revisione *Reconta Ernst & Young* (che illustrava le verifiche aggiuntive da svolgere con riferimento alle vicende della Funzione *Security*) e dello studio *Davis Polk and Wardwell* in merito ai profili di rilevanza delle vicende descritte dal punto di vista del diritto statunitense (applicabile alla Società in quanto quotata al *NYSE*); informativa circa i pareri richiesti a consulenti esterni su vari aspetti di diritto italiano in merito alle vicende oggetto di questo Rapporto;

2.2.6. riunione (congiunta con il Collegio Sindacale) del 24 ottobre 2006: esame del parere del Professor Mucciarelli sui profili di rilevanza della vicenda Tavaroli alla stregua del d.lgs. n. 231/2001 (v. sotto il § 3.5); incontro con *KPMG Advisory* e con il *Management* per un aggiornamento sui temi oggetto del presente Rapporto;

2.2.7. riunione (congiunta con il Collegio Sindacale) del 31 ottobre 2006: audizione del Vice Presidente Esecutivo in merito al funzionamento del Comitato di *Risk Management* dallo stesso presieduto ed al coordinamento tra i lavori di tale Comitato e del COMITATO per una più efficace gestione dei rischi in genere ed una adeguata reazione alle recenti vicende in particolare; nonché in merito all'attuale assetto della Funzione *Security* e ad altre problematiche di tipo organizzativo coinvolte dalle recenti vicende;

2.2.8. riunione (congiunta con il Collegio Sindacale) del 12 dicembre 2006: verifica sullo stato di avanzamento delle attività della Società in merito alle iniziative di *IT compliance* e aggiornamento sulla vicenda Tavaroli;

2.2.9. riunione (congiunta con il Collegio Sindacale) del 31 gennaio 2007: acquisizione delle prime risultanze delle procedure di verifica aggiuntive intraprese dalla società di revisione *Reconta Ernst & Young* in merito alle vicende riguardanti la Funzione *Security*; esame con il Vice Presidente Esecutivo delle vicende riguardanti Fabio Ghioni e il c.d. "*Tiger Team*";

2.2.10. riunione del 16 febbraio 2007: aggiornamento sullo stato di avanzamento delle attività della Società in merito alle iniziative di *IT compliance*; comunicazioni da parte della società di revisione *Reconta Ernst & Young* circa il prosieguo del programma di lavoro; chiarimenti su modalità e tempi di riscontro da parte della Società in ordine alle richieste dell'Autorità Giudiziaria con riferimento all'episodio di accesso abusivo alla rete informatica di RCS.

3. Informazioni ricevute e attività svolte dal COMITATO

Nel corso delle riunioni indicate nel paragrafo precedente, i competenti uffici della Società hanno informato il COMITATO dei fatti verificatisi, esponendo le loro valutazioni, come di seguito sintetizzati.

3.1. *Vicenda Security*

3.1.1. *Audit e riorganizzazione*

3.1.1.1. Nel febbraio/marzo 2005 venne effettuato un *audit* interno sull'acquisto di prestazioni professionali e consulenze da parte della Funzione *Security* - attività di *Intelligence*. Obiettivo dell'*audit* (non inserito nel Piano 2005, ma effettuato su richiesta dell'A.D. Carlo Buora, anche a fronte della crescita della voce di spesa concernente tale Funzione) era la valutazione del correlativo sistema di controlli interni mediante accesso remoto (per via informatica) alla documentazione e con approfondimenti/richieste specifici presso il responsabile della Funzione.

3.1.1.2. Il *report* finale non segnalava criticità specifiche, pur evidenziando, in generale, un sistema di controllo interno debole, con consistente ricorso ad acquisti al di fuori della procedura ordinaria (i c.d. acquisti in deroga erano il 60% del totale degli acquisti di questa tipologia di servizi) e con accentramento presso il responsabile della Funzione sia della scelta del fornitore, sia della rilevazione del servizio reso che dell'autorizzazione al pagamento delle fatture.

Nella premessa dell'*executive summary*, si evidenziava che il periodo considerato «è stato caratterizzato da un'intensa attività di 'contrasto' che sicuramente ha influenzato il '*modus operandi*' dell'intera struttura» (con riferimento implicito alle note vicende in Brasile). Nelle conclusioni del medesimo documento, si dava atto delle «difficoltà oggettive di poter realizzare un sistema di controllo 'tradizionale' in relazione alla delicatezza delle attività riguardate».

Delle risultanze dell'*audit* il responsabile Armando Focaroli informava i vertici della Società ed informalmente anche i membri dell'OdV, i quali condividevano la necessità di porre rimedio alle debolezze riscontrate rafforzando il sistema di controllo interno della Funzione *Security*.

Della questione l'OdV si occupava formalmente nella riunione del 31 maggio 2005, quando riceveva da Armando Focaroli l'illustrazione riassuntiva dei risultati dell'intervento di *audit* sugli acquisti di prestazioni professionali e consulenze da parte della Funzione *Security*. L'OdV, condivisa l'esigenza di un sistema di controllo basato sulla separazione dei ruoli operativo e di supervisione, chiedeva di essere costantemente aggiornato.

3.1.1.3. Frattanto, Giuliano Tavaroli riceveva, in data 3 maggio 2005, un avviso di garanzia dal quale risultavano pendenti nei suoi confronti indagini per ipotesi di violazione del segreto di ufficio e associazione a delinquere. Erano svolte perquisizioni presso gli uffici di Telecom Italia ed acquisiti, da parte della Polizia Giudiziaria, i documenti relativi all'*audit* della Funzione *Security*.

In data 12 maggio, l'Autorità Giudiziaria richiedeva alla Società le fatture emesse da alcuni fornitori della Funzione medesima.

Veniva, quindi, attivata una *task force* interdirezionale per la verifica preventiva, ai fini del pagamento, delle fatture pervenute dai fornitori indicati. Cessava il conferimento di incarichi ai medesimi fornitori.

3.1.1.4. Non appena ricevuto l'avviso di garanzia, Tavaroli chiedeva di essere esonerato dalla prestazione lavorativa con effetto immediato e per un periodo di tre mesi. In data 5 luglio 2005 era risolto il rapporto di lavoro con Tavaroli, a decorrere dal 31 luglio, con trattamento economico *standard*.

Al suo posto era nominato, come responsabile *ad interim* della Funzione *Security*, Giovanni Penna, con decorrenza dal 1° agosto 2005.

In data 19 luglio 2005, era conferito a Tavaroli, previa intesa con le autorità governative a seguito del noto attentato di Londra (come riferito dal Presidente dott. Tronchetti Provera nella riunione del Consiglio di Amministrazione del 26 luglio 2005 e dall'avv. Chiappetta nella riunione del COMITATO del 15 luglio 2005), un incarico di consulenza nella materia dell'anti-terrorismo, per la durata di un anno e per il compenso di 50.000 euro. In data 23 settembre, era conferita a Tavaroli, in relazione a detto incarico, una procura di carattere istituzionale, senza poteri di acquisto.

L'incarico di consulenza - poi esteso alla materia della *business continuity*, senza modifiche di compenso e durata - cessava nel marzo 2006, con revoca della procura in data 19 giugno.

3.1.1.5. Proseguiva la riorganizzazione della Funzione *Security* nel senso sopra indicato.

Dapprima si ipotizzava la creazione di una società consortile analoga a TELECOM ITALIA AUDIT & COMPLIANCE SERVICES; poi prevaleva la scelta di ristrutturare dall'interno la Funzione, distinguendo i ruoli operativi da quelli di controllo.

A seguito delle modifiche introdotte, il Responsabile della Funzione *Security* (individuato dal gennaio 2006 nella persona di Gustavo Bracco, Direttore della *Funzione Human Resources and Organization*) non opera direttamente, bensì svolge attività di supervisione ed indirizzo; dispone, inoltre, di una funzione di *staff* per l'attività di pianificazione e controllo

che assicura la correttezza amministrativa, il supporto documentale dell'operatività e la pertinenza della spesa agli obiettivi.
Dell'intervenuta riorganizzazione era data informativa all'OdV in data 28 febbraio 2006: Armando Focaroli dichiarava che l'esigenza di un adeguato sistema di controllo interno nel settore *intelligence* della Funzione *Security* era stata soddisfatta dalle misure prese. Nella medesima riunione era approvata la relazione dell'OdV per il 2005, nella quale era fornita informativa sia sui risultati dell'*audit* che sulle misure organizzative adottate per rimediare alle carenze riscontrate.
Analogamente, nella riunione del COMITATO del 30 marzo 2006 il dott. Focaroli spiegava che - come già riferito all'Organismo di Vigilanza nell'aprile/maggio 2005 (v. sopra 3.1.1.2) - "all'inizio del 2005 TI Audit ha svolto una verifica sulle spese di consulenze e prestazioni professionali della struttura [*Security*] a fronte di una loro importante e rapida crescita, peraltro motivata da ragioni oggettive. L'intervento di *audit* evidenziò alcune criticità in termini non di irregolarità sostanziale, ma di inadeguatezza del sistema di controllo a causa del forte accentramento di compiti in capo al responsabile. […]Ai rilievi da parte dell'*internal auditor* sono seguite comunque misure organizzative correttive, ferme le peculiarità della specifica tipologia di servizi».

3.1.1.6. In definitiva, il problema posto in evidenza dal rapporto di *audit* era prospettato dal *Management* come di natura essenzialmente organizzativa e la Società si era attivata per dare risposte idonee sul piano organizzativo.
Non si ritennero sussistere elementi per ulteriori interventi in considerazione di:

a. la natura particolare del settore (e il momento molto delicato dal punto di vista della sicurezza internazionale, prima ancora che aziendale). Ciò rendeva credibile che per alcune attività particolarmente delicate si evitasse di conservare presso la Società documenti e altri risultati delle indagini;
b. gli ottimi risultati raggiunti da Tavaroli in recenti vicende (ad esempio quella della Kroll in Brasile, in cui addirittura venne presentata una lettera formale di scuse a Telecom Italia);
c. la non materialità delle cifre in gioco dal punto di vista degli effetti possibili sul bilancio e del giudizio complessivo sui controlli interni della Società.

3.1.2. *Emersione di nuove informazioni*

3.1.2.1. La questione assumeva diversa fisionomia alla fine del 2005, quando il difensore di Cipriani inoltrava (peraltro solo a Pirelli) una richiesta che faceva sorgere il dubbio circa l'effettivo svolgimento delle prestazioni fatturate a Telecom Italia. La Società (come anche Pirelli) incaricava un

legale esterno di effettuare una verifica in relazione alle fatture già a suo tempo liquidate alle aziende collegate a Cipriani.

3.1.2.2. Nella riunione del COMITATO, già citata, del 30 marzo 2006 il consigliere Francesco Denozza «domanda chiarimenti sulle notizie comparse sulla stampa quotidiana circa presunti pagamenti irregolari effettuati dalla Funzione *Security*». Il *Management* affermava che, alla luce delle verifiche sino ad allora effettuate ed ancora in corso a quella data, i pagamenti effettuati dalla Società apparivano giustificati da prestazioni effettivamente rese.

3.1.2.3. L'indagine del legale esterno si concludeva il 21 aprile 2006 e metteva in evidenza che in molti casi non era stato possibile ricostruire l'oggetto della prestazione. Le dimensioni delle cifre (8,5 milioni stimati per il periodo tra il 30 maggio 2002 e il 3 novembre 2004) non erano peraltro tali da determinare giudizi negativi sulla qualità dei controlli interni (e tanto meno la condizione di *material weakness* ai sensi della legislazione statunitense), anche in considerazione del fatto che il problema sul piano strettamente procedurale era stato risolto da oltre un anno. La Società inoltrò immediatamente un dettagliato esposto all'Autorità Giudiziaria in data 8 giugno 2006.

3.1.2.4. Il COMITATO sollecitava Armando Focaroli, nella riunione del 3 ottobre 2006, a chiedere agli esponenti del vertice dell'azienda all'epoca dei fatti (Tronchetti Provera, Buora e Ruggiero) e ai loro primi riporti (17 dirigenti complessivamente) di verificare se, nel periodo marzo 2003 - maggio 2005, fossero stati dati incarichi a Tavaroli e, in caso affermativo, quale fosse stato il contenuto e quali le modalità di affidamento e di ottenimento dei risultati.

Su 20 persone interpellate, 10 hanno risposto affermativamente e hanno fornito indicazioni su contenuti, modalità di affidamento e di ottenimento dei risultati, che non mettono in evidenza criticità.

3.1.2.5. Dal provvedimento del GIP si apprendeva della distruzione di documenti amministrativi da parte di dipendenti Pirelli e Telecom Italia. Il Collegio Sindacale ha richiesto all'*auditor* interno di effettuare una verifica in merito a eventuali ulteriori episodi di segno analogo che potessero essere accaduti nell'ambito della Società. Tale verifica ha portato ad un esito negativo.

3.1.2.6. Sono in corso, da parte dei revisori di *Reconta Ernst & Young*, verifiche in relazione agli acquisti effettuati dalla Funzione *Security* nel periodo 2001-2006, con l'obiettivo primario di valutare l'esistenza di eventuali impatti sul bilancio di Telecom Italia. Nelle riunioni del 31 gennaio e del 16 febbraio 2007 il COMITATO è stato aggiornato circa l'avanzamento del

programma di lavoro, che - come concordato con la Società - è stato predisposto sulla base degli *standard* di revisione di riferimento e della disciplina Consob. Le verifiche svolte, che hanno riguardato tutti i fornitori comunque citati nell'ordinanza del GIP, non evidenziano impatti "*material*" sui bilanci.

3.1.2.7. La Società ha proseguito nella collaborazione con l'Autorità Giudiziaria, presentando ulteriori esposti in data 19 ottobre, 6 dicembre e 14 dicembre 2006.

3.1.2.8. E' continuata l'attività di "manutenzione" del Modello Organizzativo 231, anche prendendo spunto dalle vicende oggetto di esame.
In particolare:

- Lo *Steering Committee* 231 di Gruppo ha approvato una integrazione allo schema di controllo "Agenti e Mediatori" del Modello Organizzativo: tale integrazione è volta ad inserire nei rapporti contrattuali della Società con tali soggetti una specifica clausola che prevede il divieto, posto a carico dell'agente/mediatore, di cessione del credito e/o di mandato all'incasso. In tal modo si intende garantire che solo l'agente o il mediatore possa essere l'effettivo destinatario del pagamento. Eventuali deroghe a tale previsione contrattuale verrebbero evidenziate nei flussi informativi trimestrali all'Organismo di Vigilanza, così come verrebbero evidenziati i pagamenti effettuati in luogo diverso da quello di residenza/domicilio/sede legale dell'agente o del mediatore.
- La stessa integrazione è stata estesa ad altri schemi di controllo del Modello Organizzativo, con l'approvazione di un'analoga modifica degli schemi di controllo relativi a "Consulenze e prestazioni professionali", "Sponsorizzazioni" e "Acquisti di beni e servizi".
- Con riguardo a "Consulenze e prestazioni professionali", la Società ha proceduto, anche su specifica richiesta del Collegio Sindacale, ad una verifica dell'efficacia e dell'efficienza delle procedure in vigore, con particolare attenzione alle operazioni effettuate "in deroga". Al riguardo, in un primo momento, è stata emessa dal Vice Presidente Esecutivo una disposizione a tenore della quale era escluso - salva esplicita autorizzazione del medesimo Vice Presidente Esecutivo - il ricorso a deroghe alle procedure previste dal Modello Organizzativo e, più in generale, dal sistema di controllo interno. Successivamente, a partire dal mese di gennaio 2007 è divenuta operativa una apposita procedura per la gestione e il pagamento delle fatture c.d. "fuori sistema", che prevede, per fatture relative a importi superiori a una determinata soglia e comunque là dove se ne ravvisi l'opportunità, l'autorizzazione da parte del Vice Presidente Esecutivo. Nel contempo è stata introdotta una specifica reportistica periodica a fini di verifica e monitoraggio del fenomeno.

3.1.2.9. Come riferito nella riunione del COMITATO del 16 febbraio 2007, è proseguita la riorganizzazione del settore *Security*, mediante trasferimento all'unità revisione tecnica di TELECOM ITALIA AUDIT & COMPLIANCE SERVICES delle attività tecniche di *IT Security*, concentrando l'azione della *Security* sulla sicurezza "logica" delle informazioni (vale a dire definizione di *policies* in tema di protezione delle informazioni, individuazione degli *owner* di processo/sistema...). E' in corso la revisione del sistema di qualificazione dei fornitori di "Servizi di investigazione" così come dei fornitori di "*Executive Protection*", mentre è prevista la definizione di una normativa di *vendor rating* allo scopo di valutare le prestazioni dei fornitori. Il monitoraggio sarà effettuato secondo i criteri fissati nella procedura generale già utilizzata per vari comparti merceologici di acquisto e basata sulle valutazioni della qualità tecnica, amministrativa e commerciale.

3.2. *La sicurezza della rete e i servizi all'Autorità Giudiziaria*

Per "sistemi dell'Autorità Giudiziaria" si intende un insieme di sistemi destinati ad erogare prestazioni obbligatorie a cui sono soggetti per legge gli operatori di telecomunicazioni. Si ricorda che le intercettazioni disposte dall'Autorità Giudiziaria avvengono in strutture diverse da quelle della Società. La Società, infatti, ha rinunciato a partecipare alle gare per l'organizzazione delle relative sale d'ascolto, ma adempie soltanto all'obbligo di legge, imposto a tutti gli operatori, di convogliare le utenze di cui le Procure hanno disposto il controllo verso le numerazioni prescelte, indicate dalle Procure stesse.

3.2.1. Il COMITATO ha esaminato più volte nel corso del 2006 il tema in questione. In particolare nelle riunioni del 30 marzo 2006 e 12 giugno 2006 è stato a esso riferito che:

a. la Società, dopo un significativo riassetto nel 2003, ha apportato nel 2005 una serie di modifiche all'assetto organizzativo per offrire un interfaccia unitario centralizzato all'Autorità Giudiziaria, così da migliorare qualità e tempestività del servizio;
b. la struttura organizzativa è stata razionalizzata con la creazione della Funzione SERVIZI AUTORITÀ GIUDIZIARIA (SAG), mediante l'integrazione in unico polo delle strutture della Società (già operanti nel CENTRO NAZIONALE AUTORITÀ GIUDIZIARIA (CNAG) collocato nell'ambito di *Security*) e di Tim dedicate alle prestazioni obbligatorie. La responsabilità del SAG è stata attribuita al responsabile della funzione affari legali (disposizioni organizzative del 25 novembre 2005);
c. le procedure adottate offrono la massima garanzia, in quanto le intercettazioni avvengono materialmente in locali nella disponibilità della Autorità Giudiziaria. In particolare, i responsabili di settore hanno

affermato che «la tematica delle intercettazioni è totalmente sotto controllo né presenta criticità di sorta» (riunione del COMITATO del 12 giugno 2006);

d. i sistemi di supporto alle attività di intercettazione del mobile sono stati a suo tempo oggetto di certificazione da parte della società CSQ, applicando gli *standard* definiti dal BSI - *British Standard Institute* (*standard* ex BS7799, equivalente a ISO 27001).

3.2.2. In definitiva, il tema "intercettazioni" in senso stretto non ha mai presentato criticità alla luce delle informazioni fornite al COMITATO.

3.2.3. Esiste, peraltro, un problema più generale di tutela della *privacy* con riferimento al trattamento di dati giudiziari e alla gestione dei flussi informativi relativi alle prestazioni obbligatorie erogate all'Autorità Giudiziaria su cui è intervenuta, con provvedimento generale nei confronti di tutti i gestori, l'Autorità Garante per la *Privacy* in data 15 dicembre 2005 prescrivendo l'adozione entro 180 giorni di specifici accorgimenti e misure atti a garantire maggiormente la protezione dei dati trattati. Le prescrizioni (afferenti ad aspetti organizzativi; alla sicurezza dei flussi informativi con l'Autorità Giudiziaria; alla protezione dei dati trattati per scopi di giustizia) riguardano la forma e l'autenticità dei decreti della Magistratura di inizio attività, la modalità di trasmissione della relativa documentazione, la gestione dei profili di autorizzazione e l'attribuzione dei diritti di accesso alle risorse informatiche: questioni che, quanto meno rispetto ai primi due aspetti, presuppongono un confronto e la collaborazione con l'Amministrazione della Giustizia.

Il 20 giugno 2006 Telecom Italia ha riscontrato il provvedimento del 15 dicembre 2005, trasmettendo una relazione sull'ottemperanza alle prescrizioni ricevute (necessariamente parziale, poiché alcune di esse richiedono per la loro attuazione la disponibilità delle Procure della Repubblica a dotarsi di soluzioni tecniche idonee).

Il 20 settembre 2006 l'Autorità Garante per la *Privacy* ha emanato un nuovo provvedimento in merito ai servizi per l'Autorità Giudiziaria, recante l'ordine a tutti i gestori telefonici di ultimare entro 90 giorni l'adozione delle prescrizioni di cui al precedente atto del 15 dicembre 2005, finalizzate a mettere in sicurezza i dati trattati e i flussi informativi relativi alle attività connesse alle prestazioni fornite alla Magistratura.

3.2.4. Su questi aspetti la Società ha chiesto la consulenza di *KPMG Advisory*. Quest'ultima nella riunione del 31 ottobre 2006 ha rappresentato al COMITATO:

a. la mancanza di un quadro unitario, completo ed aggiornato del perimetro dei sistemi in ambito SAG;

b. che il sistema Circe (vale a dare l'applicativo informatico per l'esecuzione delle prestazioni obbligatorie a favore della Magistratura in

ambito mobile) manifesta alcune debolezze che possono generare rischi potenziali di sicurezza, nonché difficoltà nella verifica *ex post* della coerenza delle attività svolte rispetto a quanto disposto dalle autorità;

c. che è stata rilevata una discontinuità nel processo di integrazione fra i sistemi di intercettazione del fisso e del mobile nel corso del tempo.

Peraltro, nella riunione del 16 febbraio 2007 il *management* ha riferito al COMITATO in merito ai risultati del censimento effettuato. Allo stato attuale dell'*assessment* sono stati identificati 23 sistemi utilizzati in via esclusiva per ottemperare alle richieste dell'Autorità Giudiziaria e 14 sistemi che supportano l'erogazione di servizi funzionali anche all'erogazione di prestazioni obbligatorie verso l'Autorità Giudiziaria. Nel frattempo, il progetto volto all'adeguamento rispetto al Provvedimento del Garante per la *Privacy* del 20 settembre 2006 è stato sostanzialmente concluso entro il termine prescritto, ciò di cui è stato dato riscontro al Garante in apposito documento inoltrato il 22 dicembre 2006. Resta fermo che il corretto funzionamento delle soluzioni implementate dipende dall'adozione da parte delle Procure di strumenti adatti alla ricezione e all'invio di comunicazioni secondo i protocolli sicuri che sono stati definiti.

3.2.5. Proseguono, nel frattempo, le attività di *assessment* di medio periodo anche al fine della razionalizzazione e integrazione delle varie strutture e procedure oggi esistenti. Sia sui sistemi utilizzati per le prestazioni obbligatorie che sui sistemi a supporto sono in corso analisi e valutazioni delle applicazioni informatiche utilizzate e dei relativi processi gestiti, al fine di determinare, con la consulenza di *KPMG Advisory*, eventuali rischi e aree di miglioramento.

3.3. *Dati di traffico, privacy e informazioni sui dipendenti*

3.3.1. Il tema si è proposto all'attenzione del COMITATO all'inizio del 2006, quando si verificava l'aggravarsi di fenomeni di impropria diffusione di dati personali di clienti (dati di traffico), da parte di dipendenti infedeli.

Un nuovo caso, in particolare, presentava una significativa differenza rispetto al passato. Fino a quel momento, ogni volta che il fenomeno era emerso, il responsabile era stato prontamente individuato e gli erano state applicate sanzioni, fino al licenziamento. Nel nuovo caso, peraltro, non si era in grado di individuare il responsabile.

Anche in considerazione di ciò, in marzo l'A.D. Carlo Buora convocava un gruppo di lavoro interdirezionale sul tema della sicurezza e della tutela dei dati di traffico. Dalle analisi di questo gruppo emergeva, in particolare, l'incompleta mappatura degli applicativi informatici che gestiscono dati di traffico, con conseguente indisponibilità dell'informazione in ordine al numero di soggetti autorizzati ad accedere a tali dati.

3.3.2. Nel corso della riunione del COMITATO del 12 giugno, il *Management* manifestava comunque la sua fiducia nella qualità dei controlli in proposito. Come da apposita nota distribuita in detta sede: «Preme comunque evidenziare come i sistemi di controllo abbiano retto nel senso che, sia pure *ex post*, i *file* di *log* estratti abbiano consentito di individuare senza dubbio gli autori dell'illecito sia nei casi di violazioni compiute dal personale dei Servizi per l'Autorità Giudiziaria che nei casi del personale di altre strutture».

3.3.3. Sempre nel corso della citata riunione, il COMITATO era informato che nel corso dell'ispezione dell'Autorità Garante per la *Privacy* era "emersa la presenza di un applicativo" (Radar) che non risponde agli *standard* aziendali di sicurezza e ai requisiti di legge. La Società, peraltro, aveva subito disposto il blocco del sistema Radar e segnalato la vicenda all'Autorità Giudiziaria.

3.3.4. In data 1° giugno 2006, anche a seguito del ricorso di un utente, l'Autorità Garante per la *Privacy* prescriveva alla Società di adottare entro 120 giorni una serie di misure a protezione dei dati di traffico in assenza delle quali avrebbero dovuto cessare il trattamento dei dati.

3.3.5. La risposta della Società, rispetto ad una situazione che andava delineandosi diversa e più preoccupante di quella fino a tale momento percepibile, si sostanziava in:

a. un incarico a *KPMG Advisory* per la rilevazione e l'analisi indipendente dello stato della sicurezza dei processi e dei sistemi IT della Società, con particolare riferimento a quelli che trattano dati di traffico;
b. la definizione di un progetto trasversale rispetto all'intera organizzazione aziendale, organizzato sui tre livelli strategico, di coordinamento e operativo, che ha coordinato interventi su 132 applicazioni aziendali. Va rilevato che, anche a detta dei fornitori di tecnologia, Telecom Italia è una delle prime imprese al mondo, e certamente la prima in Italia, ad affrontare tali problematiche in un contesto operativo di grandi dimensioni;
c. un impegno (già realizzato) di risorse interne della Società per 2 milioni di ore/lavoro, con un investimento stimato in oltre 30 milioni di euro per il 2006 (7 milioni per gli anni 2007-08).

Il 29 settembre era presentato all'Autorità Garante per la *Privacy* un documento descrittivo dell'attività svolta, delle iniziative ancora in corso e dei problemi tecnici dell'azione di adeguamento (anche perché, alla stregua della disciplina nazionale, l'applicazione dei requisiti in materia di firma elettronica è particolarmente onerosa). Il 30 ottobre 2006 veniva altresì presentato al Garante un documento di aggiornamento sulle attività svolte sino a tale data.

Nella riunione del COMITATO del 12 dicembre 2006 il *Management* ha precisato che le attività sino ad allora realizzate in adempimento al provvedimento del Garante cd. dei 120 giorni avevano messo in sicurezza i sistemi che - sempre nella valutazione manageriale - sono rilevanti per l'efficace svolgimento dell'attività d'impresa.

3.3.6. Alla riunione del COMITATO del 12 dicembre sia *KPMG Advisory* sia il responsabile *IT Governance* della Società hanno presentato un aggiornamento sugli interventi nel frattempo realizzati e sulla tempistica di quelli ancora in corso.

3.3.7. Con provvedimento in data 7 dicembre 2006 l'Autorità Garante per la *Privacy* deliberava di prorogare al 31 marzo 2007 il termine per completare l'attuazione delle prescrizioni contenute nel provvedimento del 1° giugno 2006. Il lavoro di adeguamento svolto dalla Società risulta così positivamente apprezzato.

3.3.8. Nella riunione del 16 febbraio 2007, con riferimento ai sistemi che trattano dati di traffico, il COMITATO è stato informato che, rispetto alle 35 applicazioni che ancora presentavano criticità alla data del 30 settembre 2006, risulta a oggi sicuramente completata l'attività di adeguamento per 31 applicazioni. L'adeguamento delle restanti 4 applicazioni (sistemi che forniscono servizi a valore aggiunto, che sono complessi, ma a bassa criticità) sarà completato nel pieno rispetto del termine previsto dal provvedimento di proroga del 7 dicembre 2006. Come richiesto da tale provvedimento, il 31 gennaio 2007 è stato consegnato al Garante un apposito documento di aggiornamento sullo stato delle attività.

3.3.9. Il COMITATO, dalla lettura del provvedimento del GIP, apprendeva di un problema relativo alla raccolta di informazioni su dipendenti. In particolare, secondo il magistrato (che ha impiegato parole assai severe) la *Security* avrebbe raccolto informazioni su un certo numero di dipendenti nel periodo febbraio-agosto 2004.

3.3.10. L'indagine compiuta dalla Direzione del Personale ha messo in evidenza che:

a. i controlli sono stati disposti per iniziativa di Tavaroli, che avrebbe rappresentato alla Direzione del Personale di *Wireline* la necessità di disporre degli elenchi del personale risultato idoneo all'assunzione, in relazione al pericolo di infiltrazioni terroristiche;
b. in due casi pervenne (verbalmente) alla Direzione del Personale di *Wireline* l'indicazione di non idoneità. I due candidati non vennero assunti;
c. la Direzione del Personale ha dichiarato di ignorare i metodi di indagine utilizzati da Tavaroli.

3.3.11. Nella relazione del Direttore *Human Resources* del Gruppo si precisa che «non risulta l'esistenza di alcuna *policy* in materia né che sia stata data alcuna specifica disposizione in merito da parte dei responsabili di gestione del personale».

3.4. Di recente, da notizia apparsa sulla stampa, risulterebbe una censura alla Società in relazione alle richieste dell'Autorità Giudiziaria con riferimento all'episodio di accesso abusivo alla rete informatica RCS: le verifiche effettuate dal *Management* permettono di escludere che vi siano stati ritardi, mentre confermano che alcune delle risposte all'Autorità Giudiziaria sono state predisposte dal dott. Ghioni, oggetto poi di un provvedimento restrittivo concernente anche tale episodio.

3.5. Il Prof. Avv. Francesco Mucciarelli ha formulato un suo parere in risposta al quesito che gli è stato proposto circa l'eventuale configurabilità a carico di Telecom Italia di una responsabilità ai sensi del d.lgs. 231/01 per i fatti di cui all'ordinanza del GIP.
A tale quesito il professionista ha dato risposta negativa.
Premesso che tra i reati contestati nel provvedimento del GIP solo i fatti di corruzione rientrano nell'elenco *ex* d.lgs. 231/01 e che il sig. Tavaroli, unico *ex* dipendente Telecom Italia indagato per fatti di corruzione, è da considerare (in via di assunzione prudenziale) soggetto apicale (come inteso dal d.lgs. 231), il fatto corruttivo contestato, allo stato attuale delle conoscenze, ha unicamente ad oggetto la dazione a pubblici ufficiali di somme di denaro, da parte del sig. Cipriani, per il tramite di società italiane ed estere allo stesso riferibili, per l'acquisizione di informazioni non legittimamente disponibili a terzi.
Osserva il Prof. Mucciarelli che nessuna contestazione è stata mossa a Telecom Italia in riferimento al d.lgs. 231/01, in quanto i fatti di reato posti in essere appaiono commessi in danno alla Società e non a vantaggio o nell'interesse della stessa; a tale considerazione si accompagna quella per cui le condotte illecite sarebbero state realizzate al di fuori della consapevolezza dei vertici aziendali.
Per altro verso, la tipologia degli altri reati contestati, ed in particolare il reato associativo e le ipotesi di appropriazione indebita pluriaggravata, deporrebbe nel senso di un interesse del tutto distonico rispetto a quello dell'ente e accrediterebbe anche l'ipotesi che tali condotte siano state realizzate attraverso modalità tali da tenerne celata la reale natura. Quest'ultima considerazione sembra al Prof. Mucciarelli particolarmente significativa, in quanto uno dei requisiti necessari per escludere la responsabilità diretta dell'ente, quando il fatto sia commesso da un soggetto apicale, consiste nell'elusione fraudolenta dei modelli organizzativi esistenti.
Ovviamente il parere reso dal professionista si basa sulle conoscenze allo stato disponibili e si regge su alcune valutazioni che sono state finora espresse dall'Autorità Giudiziaria in merito alla qualificazione dei fatti, nell'ambito di incolpazioni che, per loro natura, devono essere considerate provvisorie.

4. Proposte

4.1. Il COMITATO, sulla base di quanto riferito dal *Management* e dai consulenti, nonché di quanto risulta dai provvedimenti dell'autorità Giudiziaria e dell'Autorità Garante per la *Privacy*, ritiene necessario che le azioni già avviate dalla Società vengano integrate e rafforzate in modo da dare risposte definitive e tranquillizzanti riguardo alla correttezza dell'organizzazione e dei comportamenti.
In questa prospettiva è indispensabile avviare e/o concludere, nel più breve tempo possibile, le seguenti iniziative:

4.1.1. completa attuazione delle richieste dell'Autorità Garante per la *Privacy*, di cui al provvedimento del 1° giugno 2006 (la cui scadenza è stata prorogata al 31 marzo 2007), in esecuzione del piano già programmato;

4.1.2. tempestiva attuazione delle misure individuate dal *Management* con il supporto di *KPMG Advisory*, riepilogate nella consulenza relativa allo stato della sicurezza dei processi e dei sistemi IT della Società;

4.1.3. accertamento dei motivi che hanno impedito un'adeguata percezione dei rischi collegati alla *compliance* con la normativa in materia di *privacy* e proposta di misure conseguenti;

4.1.4. completamento dell'indagine di *Reconta Ernst & Young* sulle ricadute e gli effetti sul bilancio di quanto emerso nel settore *Security*;

4.1.5. verifica dell'adeguatezza organizzativa del settore *Security*, anche alla luce degli interventi già messi in atto, con particolare attenzione ai presidi per il rispetto della correttezza operativa e all'efficacia dei controlli;

4.1.6. valutazione circa l'efficacia delle misure di prevenzione previste in materia di consulenze dal Modello Organizzativo *ex* d.lgs. n. 231;

4.1.7. accertamenti in ordine agli aspetti della vicenda Tavaroli che potrebbero ancora toccare la struttura organizzativa della Società. E in particolare: i) chiarimenti su quanto riferito dal GIP circa la posizione di Tavaroli dopo il maggio 2005 («Risulta dagli atti che per un certo periodo, anche dopo il suo allontanamento dalla dirigenza del settore *Security*, egli abbia mantenuto un ruolo attivo in Telecom, operando in particolare dalla Romania») [p. 337]"; ii) verifiche se, anche in riferimento al punto precedente, dopo il maggio 2005 dipendenti o funzioni della Società abbiano, al di fuori dello specifico incarico consulenziale a Tavaroli in materia di terrorismo, consentito a Tavaroli stesso di accedere a dati aziendali;

4.1.8. accertamenti su eventuali comportamenti di oggettiva agevolazione da parte di uffici o singoli dipendenti/collaboratori della Società all'acquisizione e al

trattamento di dati riservati o comunque estranei alle attitudini professionali dei candidati all’assunzione; adozione di procedure che assicurino il rispetto della normativa in materia.