AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

ALLEGATO A alla delibera n. 420/19/CONS

Esiti del market test di cui alla determina n. 2/19/DRS

1. Premessa

Come noto ed a conclusione di una estesa ed altresì complessa attività di vigilanza, nella seduta del 25 luglio 2018 il Consiglio – contestualmente all'adozione della delibera n. 396/18/CONS rivolta a Telecom Italia - ha altresì deciso l'avvio di un procedimento di contestazione di addebito al medesimo operatore (nel seguito TIM, Telecom Italia o Telecom), ai sensi dell'articolo 3, comma 4-bis, dell'allegato A alla delibera n. 581/15/CONS, per violazioni consistenti nella mancata adozione, ai sensi dell'art. 41 del Codice delle comunicazioni elettroniche, di idonee misure per garantire la riservatezza dei dati clienti degli OLO in occasione dell'apertura di ticket di guasto o disservizi su linea fissa (cd. *trouble ticket* o *TT*).

A valle della contestazione di cui in premessa, notificata in data 11 dicembre 2018, TIM, avvalendosi della facoltà di cui all'articolo 13 del regolamento sanzioni (delibera n. 581/15/CONS), ha presentato, nei termini regolamentari, un preliminare documento di impegni e poi il documento definitivo in data 29 gennaio, dopo essere stata ascoltata in audizione in data 16 gennaio 2019.

Il documento di impegni, corredato dalla relazione istruttoria della Direzione reti e servizi di comunicazioni elettroniche, è stato poi sottoposto al vaglio del Consiglio in data 25 giugno 2019 che ne ha valutata l'ammissibilità e decisa la pubblicazione per il conseguente *market test*.

Rileva a riguardo che, contestualmente, al Consiglio è stata sottoposta anche l'informativa sulla parallela conclusione del tavolo tecnico con gli operatori di cui alla delibera n. 396/18/CONS, i cui argomenti risultano convergenti e/o complementari a quelli di cui agli impegni in oggetto. A tal riguardo appare opportuno rammentare che l'ordine rivolto a TIM, di cui alla delibera n. 396/18/CONS, è essenzialmente motivato dalla necessità di individuare un set di interventi finalizzati a non rendere intellegibili, se

non a personale TIM ben identificato e autorizzato, i dati dei clienti degli OAO che avviano una procedura di *assurance.*

Con determina direttoriale n. 2/19/DRS del 5 luglio 2019 gli impegni sono stati pubblicati sul sito *web* dell'Agcom per il confronto critico con il mercato.

Giova rammentare, in proposito, che l'articolo 16 del Regolamento (comma 1) oltre alla possibilità di formulare osservazioni (sugli impegni) da parte degli OAO, contempla la facoltà di replica da parte dell'interessato (comma 4) su tali osservazioni.

Si riporta, di seguito, una sintesi delle osservazioni degli OAO e della replica di TIM.

2. Gli impegni di TIM e le osservazioni degli OAO

Nei termini regolamentari sono rispettivamente pervenute le note degli operatori Sky Italia, Fastweb, Vodafone Italia, Tiscali, Wind Tre e BT Italia sulle misure proposte da TIM.

Al fine di semplificare la lettura e la valutazione delle osservazioni prodotte dal mercato in ordine alle misure proposte da TIM di seguito si riporta ciascuno degli impegni e le relative osservazioni degli OAO:

IMPEGNO n. 1: introdurre una misura di protezione specifica anche sui sistemi di delivery*. In tal senso TIM si impegna ad individuare una soluzione tecnica che possa essere condivisa anche dagli OAO, che impedisca la visualizzazione di dati sensibili (nome e cognome cliente, CF/PIVA e recapito telefonico) in caso di qualunque operazione di estrazione singola o massiva di ordinativi da parte di qualunque personale autorizzato all'accesso tramite interfaccia grafica (GUI) al sistema, quindi outsourcers, personale TIM Wholesale e OAO. A tal proposito saranno create delle nuove profilature ad hoc per gli utenti dei sistemi che permettono di visualizzare da interfaccia grafica (GUI)i dati sensibili solo da parte di personale autorizzato, per la cui attività lavorativa è necessario accedere a queste informazioni, escludendo tale possibilità per tutti gli altri utenti dei sistemi. In logica di full equivalence la misura sarà estesa anche al caso di ordinativi retail di TIM. In altri termini anche per gli ordinativi di TIM retail né gli outsourcers né il personale di TIM wholesale potrà estrarre i suddetti dati sensibili. Per quanto riguarda il sistema NOW, le modifiche proposte dovranno essere preventivamente concordate anche con gli OAO, poiché tale sistema viene utilizzato da personale OAO.*

- Un operatore evidenzia che l'introduzione di un processo di criptazione a tutela dei dati, attraverso l'introduzione di *log*, era stato già oggetto di valutazione positiva da parte del mercato in occasione del tavolo tecnico successivo all'adozione della delibera n. 396/18/CONS, sede in cui se ne era auspicata l'estensione (oltre che all'*assurance*) anche al *delivery*, ragione per la quale la misura non sarebbe connotata da alcun elemento di novità. Essa inoltre, attesa la genericità dei contenuti, non apparrebbe in grado di soddisfare il preteso requisito

del miglioramento delle condizioni di concorrenzialità rimuovendo i profili antiregolamentari delle condotte contestate.

- A livello generale un operatore ritiene non vi sia un valore aggiunto negli impegni poiché TIM si è già dotata di un Codice di comportamento per la riservatezza dei dati degli OAO ed "*ha stabilito, tra gli altri provvedimenti, misure tecnologiche ed organizzative idonee a garantire la separazione dei sistemi informativi delle unità organizzative preposte alla gestione della Rete da quelli delle Funzioni commerciali preposte alla vendita di servizi alla clientela finale, proponendosi di verificare nel tempo il rispetto, l'adeguatezza e l'efficacia di tali misure*".

  Gli impegni proposti dunque si limiterebbero a duplicare, seppur con qualche piccola modifica, quanto già in essere e non presentano alcun *quid pluris* rispetto a quanto l'operatore già dovrebbe garantire in base agli obblighi regolamentari vigenti.

  Nel merito l'operatore rileva che la principale misura proposta, cioè "*il sistema di profilatura ad hoc*", rappresenta un impegno futuro, non ben definito né nel tipo di soluzione tecnica, in quanto deve essere concordato con gli OAO nel caso abbia impatto su di essi, né nelle tempistiche di implementazione.

- Secondo un operatore l'impegno proposto di introdurre una "*misura di protezione specifica*" anche sui sistemi di *delivery* confermerebbe la inadeguata attenzione prestata fino ad oggi da TIM alle modalità trattamento dei dati *wholesale* degli OAO contenenti informazioni commerciali sensibili - quali nome e cognome del cliente, CF/P.IVA e recapito telefonico - disattendendo gli obblighi regolamentari e sottovalutando le segnalazioni degli operatori pervenute da anni anche per il tramite dell'Autorità. La previsione di gestire la visualizzazione di dati sensibili del cliente appare come un requisito minimo per preservare il dato commerciale sensibile dal possibile utilizzo illecito da parte di soggetti interni a TIM o terzi che lavorano per conto e sotto la responsabilità di TIM che hanno accesso a tali informazioni ed è una misura di base che avrebbe dovuto, pertanto, essere già implementata all'inizio della fornitura del servizio *wholesale* da parte di TIM. Lo stesso operatore fa presente che in passato ha più volte segnalato la "vulnerabilità" dei sistemi TIM e richiesto l'adozione di misure minime per la tutela dei dati dei propri clienti quali, ad esempio, l'introduzione di un sistema di profilazione degli utenti con accesso al sistema NOW, l'inibizione della possibilità di estrazioni massive, l'eliminazione del dato sensibile. TIM si era già impegnata a sviluppare un sistema di gestione degli accessi ai dati sensibili […], dimostrando di essere conscia della mancanza di requisiti minimi di cautela nella gestione dei dati sensibili nei propri processi.

  Inoltre l'impegno n. 1 non costituirebbe, di per sé, uno strumento idoneo a garantire il non riproporsi della condotta illecita, quanto piuttosto uno strumento minimo - che avrebbe dovuto già essere implementato nel passato - che TIM decide di utilizzare per fare fronte alle proprie responsabilità.

  Ciò detto l'operatore segnala, in ogni caso, che nel documento oggetto di analisi TIM si impegna ad estendere la misura che gestisce la visualizzazione dei dati

sensibili anche al personale autorizzato all'accesso tramite interfaccia grafica GUI appartenente ad *outsourcers*, a TIM *wholesale* e agli OAO. Con riferimento agli *outsourcers* che lavorano direttamente per TIM e/o al personale tecnico dedicato alle attività *on field*, l'operatore ritiene utile la definizione di un documento che elenchi le tipologie di permessi di accesso e l'utilizzo dei dati da parte di tutti. È infatti utile che TIM dia evidenza di quali soggetti interni/esterni hanno accesso alle informazioni e di come verrà definita e gestita la profilatura degli accessi. Inoltre non viene fornita alcuna indicazione in merito ai tempi di implementazione della misura, ai dettagli utili per capire come verrebbe implementata ed alle relative garanzie di *security* e monitoraggio degli accessi al fine di impedire il fenomeno di fuoriuscita dei dati.

In ogni caso, l'operatore evidenzia come la misura proposta, nella migliore delle ipotesi, potrebbe limitare il numero di soggetti non autorizzati che hanno visibilità sui dati dei clienti *wholesale* e dei relativi ordini di *provisioning*/*assurance* su rete TIM, ma non risolve il problema dell'utilizzo di dati *wholesale* a fini *retail*, in quanto vi sarebbero comunque soggetti "autorizzati" (sia interni che esterni) alla visualizzazione e conoscenza di tali dati e quindi non viene fornita alcuna garanzia sull'efficacia della misura alla prevenzione/interruzione del fenomeno.

Pertanto, secondo l'operatore, l'impegno proposto non soddisferebbe i requisiti di cui alla delibera n. 581/15/CONS con riferimento a:

- Art. 13, comma 1, secondo cui l'impegno proposto deve migliorare le condizioni della concorrenza nel settore rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure;
- Art. 13, comma 5, secondo cui l'impegno proposto deve indicare in dettaglio gli obblighi che l'operatore si dichiara disposto ad assumere ed i relativi tempi di attuazione.

- Un operatore ritiene che l'impegno così come formulato risulti generico e lacunoso in quanto non è fornita alcuna indicazione o dettaglio in merito alla "soluzione tecnica" ed ai relativi tempi di implementazione, contravvenendo quindi all'art. 13 del Regolamento di cui all'Allegato A della delibera n. 581/15/CONS laddove è previsto che *"la proposta definitiva deve indicare in dettaglio gli obblighi che l'operatore si dichiara disposto ad assumere ed i relativi tempi di attuazione"*.

  L'operatore evidenzia, altresì, che la circostanza in base alla quale tale soluzione dovrebbe essere *"preventivamente concordata con gli OAO"* (che non dispongono delle informazioni e delle conoscenze dei sistemi di TIM necessarie a valutare l'efficacia di una eventuale soluzione tecnica sui suoi sistemi) comporterebbe un ritardo considerevole nell'attuazione della stessa laddove, invece, la gravità e l'importanza della condotta contestata raccomanderebbe l'adozione tempestiva di misure a tutela e garanzia del rispetto degli obblighi di riservatezza di cui all'art. 41, comma 3, del Codice delle comunicazioni elettroniche

- Un operatore osserva che tale proposta, per quanto apprezzabile, sia da ritenersi non sufficiente a porre rimedio alle pratiche scorrette, in quanto l'adozione di una soluzione tecnica che impedisca la visualizzazione dei dati sensibili in caso di qualunque operazione di estrazione singola o massiva di ordinativi non dovrebbe, a parere della scrivente, essere limitata alla sola fase di estrazione dei dati dei clienti, ma andrebbe estesa a tutte le fasi in cui vi sia la possibilità di accedere ai dati sensibili in esame, il cui accesso dovrebbe comunque essere inibito in ogni passaggio del processo che implichi l'utilizzo di tali dati.

  Lo stesso rispondente sottolinea, infatti, che l'utilizzo improprio dei dati dei clienti avviene non solo e non tanto a seguito dell'operazione di estrazione dei dati, ma altresì in occasione del contatto volto alla definizione dell'appuntamento per installare la linea (o risolvere il guasto) e proprio nella circostanza specifica dell'esecuzione dei lavori presso la sede del cliente.

  In secondo luogo, l'operatore commenta la dichiarazione di TIM di voler inibire la visualizzazione dei dati sensibili da parte di "*qualunque personale autorizzato all'accesso tramite interfaccia grafica (GUI) al sistema"*, in quanto appare chiaro che vi siano una molteplicità di soggetti "utenti dei sistemi", che hanno accesso ai dati senza averne apparentemente titolo, senza alcuna profilatura ed indipendentemente dalla reale necessità di accedere a tali dati.

  L'OAO fa presente che, nella sua proposta di impegni, Telecom non ha specificato quali siano i soggetti interni e/o esterni titolari, ad oggi, della possibilità di estrarre le informazioni dai sistemi, essendoci solo un generale riferimento, da parte di TIM, al *"personale autorizzato, per la cui attività lavorativa è necessario accedere a queste informazioni, escludendo tale possibilità per tutti gli altri utenti dei sistemi".* Ciò premesso, l'operatore ritiene che Telecom debba esplicitare soggetti, motivazioni e modalità che legittimino operazioni di accesso e di estrazione sui sistemi in cui sono contenuti dati sensibili dei clienti.

- Un operatore ritiene corretto proteggere le informazioni sensibili dei clienti degli OAO anche sui sistemi di *provisioning* della stessa TIM, indipendentemente da chi li usa, sia personale interno che terze parti che operano per conto di TIM. Per tale ragione ritiene corretto condividere la soluzione tecnica con gli altri OAO, ma si sottolinea la necessità di distinguere con chiarezza ciò che viene visualizzato sulle GUI delle diverse applicazioni in uso al personale di TIM o alle sue terze parti, da ciò che viene reso disponibile nelle cosiddette estrazioni: mentre le prime sono per loro natura "evanescenti", le seconde hanno carattere di permanenza e si prestano ad un utilizzo *a posteriori;* entrambe tuttavia devono mostrare solo quella parte di informazioni sensibili che attengono all'attività lavorativa di ciascun utilizzatore. Inoltre, poiché le estrazioni sono memorizzate in un file che potrebbe non essere immediatamente cancellato, esso non deve essere trasmesso ad enti aziendali o a terze parti diversi da quello che ha prodotto l'estrazione medesima. Infine, con riferimento alle visualizzazioni, l'OAO sottolinea l'importanza della disponibilità selettiva delle informazioni sensibili, da applicare ad ogni tipo di applicazione di TIM, sia quelle fruibili da postazioni fisse sia quelle in mobilità come le app.

IMPEGNO n. 2: Istituire dei tavoli tecnici con gli OAO:

- *per analizzare congiuntamente i casi da loro segnalati e darne riscontro anche ad AGCom;*
- *per condividere un processo per poter effettuare «dei test civetta» utilizzando clienti reali (es. forniti da OAO) per l'assurance e rendere pubblici gli esiti di tali test.*
- *In tale ambito TIM si impegna a mettere a punto una modalità di effettuazione dei test civetta su base richiesta per l'assurance secondo i seguenti criteri:*

a) Per ogni numero rientrante nel test civetta viene lanciato uno script che modifica il campo "recapito telefonico" nei vari sistemi preposti alla risoluzione del guasto;

b) In base all'eventuale numero chiamato chi raccoglierà la chiamata sarà in grado di individuare il sistema da cui è stato prelevato il dato.

- Su tale iniziativa un rispondente non ha osservazioni da fare se non evidenziare il fatto che ricorrere ad una misura per una verifica di casi critici evidenzia la scarsa incidenza ed efficienza dell'impegno n.1.

- Secondo un operatore tale impegno non può essere considerato una misura atta a tutelare la corretta gestione dei dati sensibili *wholesale* poiché TIM si impegna *ex post* rispetto all'utilizzo scorretto dei dati *wholesale* ad effettuare analisi in merito alle segnalazioni presentate dagli operatori.

  Pertanto l'impegno proposto da TIM di analizzare congiuntamente con gli OAO i casi segnalati appare tardivo ed inefficace.

  In generale la previsione di istituire dei tavoli tecnici - peraltro già attivi sull'*assurance* e già previsti per il *delivery* - non si può configurare come un impegno di TIM.

  Peraltro la previsione di effettuare "dei test civetta" costituisce un meccanismo di test e verifica del funzionamento tecnico del sistema di gestione degli accessi proposto da TIM. Da questo punto di vista quindi non costituisce un impegno autonomo quanto una fase necessaria e scontata del primo Impegno.

  Sottolinea in ogni caso come il test proposto sembri essere circoscritto al solo processo di *assurance* e non anche al processo di *delivery*, fortemente impattato nell'ultimo periodo dal fenomeno del contatto scorretto.

  La proposta di effettuare dei "test civetta" appare in ogni caso anch'essa tardiva poiché TIM, a conferma della propria buona condotta, avrebbe potuto effettuare autonomamente i test ad esempio su proprie utenze "fittizie".

  Anche in questo caso l'impegno proposto non soddisferebbe i requisiti di cui alla delibera n. 581/15/CONS con riferimento a:

- Art. 13, comma 1, relativamente al fatto che l'impegno proposto deve migliorare le condizioni della concorrenza nel settore rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure;
- Art. 13, comma 5, relativamente al fatto che l'impegno proposto deve indicare in dettaglio gli obblighi che l'operatore si dichiara disposto ad assumere ed i relativi tempi di attuazione.

- Un operatore osserva criticamente che tale proposta di impegni non appare altro che il mero recepimento di quanto ordinato a TIM dall'Autorità nella delibera n. 396/18/CIR recante le misure urgenti finalizzate ad impedire l'uso improprio dei dati *wholesale* di *assurance* per fini di contatto commerciale. Inoltre, il rispondente rappresenta che tali misure sono da ritenersi inidonee a rimuovere in modo stabile le conseguenze anti-competitive dell'illecito e migliorare le condizioni della concorrenza nel settore.
- Sulla proposta di TIM di istituire dei tavoli tecnici con gli OAO, un operatore riscontra come detti tavoli tecnici – istituiti già a suo tempo con Telecom – abbiano prodotto scarsi risultati, al punto che l'Autorità è dovuta intervenire con la delibera n. 396/18/CONS per individuare una soluzione che mettesse fine al fenomeno delle pratiche scorrette.

  Relativamente ai "test civetta" da effettuare congiuntamente, l'operatore osserva l'insufficienza di tale misura, in quanto può consentire, secondo quanto dichiarato da TIM, solo di "*individuare il sistema da cui è stato prelevato il dato*" ma non anche chi abbia prelevato il dato stesso, atteso che al medesimo sistema hanno accesso una molteplicità di soggetti.
- Sulla istituzione dei tavoli tecnici con gli OAO, un operatore si dichiara favorevole e concorda con la proposta di analizzare congiuntamente i casi anomali segnalati dagli operatori alternativi.

  Tuttavia, l'OAO rappresenta la scarsa chiarezza dell'obiettivo dei test civetta e la scarsa comprensibilità dei loro criteri guida che, secondo lo stesso, dovrebbero essere riformulati più chiaramente.

IMPEGNO n. 3: Trasmettere ad AGCOM periodicamente:

- *L'esito delle verifiche del grado di correlazione tra rientri in TIM e le segnalazioni di guasto ricevute sui sistemi wholesale di rete, fatte con la procedura richiesta con la delibera n. 396/18/CONS. L'esito, in caso di correlazione significativa, dei controlli sui soggetti che svolgono attività commerciale retail per TIM e a cui tali ordini sono riconducibili.*

- Un operatore ritiene che la trasmissione ad Agcom di tali informazioni per la diretta verifica di quest'ultima è da considerarsi positiva sebbene già prevista dalla delibera n. 396/18/CONS.

- Un rispondente non ha osservazioni specifiche sul punto essendo esse assorbite nelle considerazioni che precedono. Lo stesso sostiene, infatti, che complessivamente non vi sono elementi innovativi tali da far ritenere che le misure di cui agli impegni in oggetto siano la soluzione alle condotte abusive di cui all'atto di contestazione n. 3/18/DRS.

  Secondo il rispondente, in presenza di comportamenti di rilevante gravità, come quelli in essere, l'Autorità dovrebbe rigettare gli impegni in nome del prevalente interesse a che tali comportamenti siano sanzionati o comunque formino oggetto di accertamento.

- Secondo un OAO la proposta di TIM di mettere in correlazione i rientri in TIM e le segnalazioni di guasto trasmesse appare inadeguata a scongiurare ulteriori condotte illecite e ad essere considerata idonea ai sensi degli impegni per evitare una sanzione per violazione della normativa vigente.

  La numerosità dei rientri in TIM non esonera quest'ultima dalla responsabilità sulla *malpractice* nell'utilizzo dei dati *wholesale*. Il divieto sancito dall'art. 41 del CCE resta valido a prescindere dagli esiti che la violazione produce; pertanto il controllo proposto da TIM sui soggetti che svolgono attività commerciale per proprio conto e a cui tali ordini sono riconducibili sarebbe del tutto inadeguato.

  In questo senso non può avere alcuna valenza il concetto di "correlazione significativa" tra rientri in TIM e le segnalazioni di guasto ricevute dai sistemi *wholesale* di rete, essendo tale valutazione è del tutto soggettiva.

  Evidenzia in ogni caso come né i risultati dell'analisi di correlazione né la metodologia utilizzata (quale, ad esempio, la finestra temporale di analisi a partire dalla data di guasto che è stata utilizzata) siano stati condivisi con il mercato ed è pertanto impossibile esprimere un giudizio compiuto. L'analisi poi è stata svolta solo in relazione all'*assurance*, mentre nulla è stato proposto per il *delivery*.

  Si tratta al più di un misura che TIM avrebbe già dovuto implementare da tempo per assicurare la *compliance* alla normativa sui dati *wholesale* e come tale non può avere valenza di impegno pro-concorrenziale.

  Neppure l'impegno 3 proposto soddisferebbe, quindi, i requisiti di cui alla delibera n. 581/15/CONS con riferimento al già citato articolo 13, commi 1 e 5.

  L'impegno proposto da TIM non sarebbe in grado di migliorare le condizioni di concorrenza nel settore, non rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure, trattandosi al più di una misura interna a TIM per tentare di misurare l'entità del fenomeno di utilizzo di dati *wholesale* a fini *retail* senza alcun impatto positivo sulla concorrenza, o ancora peggio a tentare di ottenere la legittimazione da parte di AGCOM sul comportamento scorretto posto in essere (anche qui ex post). Analogamente agli impegni 1 e 2 anche l'impegno 3 non indica nel dettaglio i relativi tempi di attuazione.

- Un altro rispondente non ha commenti specifici sul punto in quanto assorbiti dal commento sull'impegno n. 2.

- Un rispondente richiede, in un'ottica di maggiore trasparenza, una modifica di tale impegno per la condivisione con gli altri operatori delle evidenze che TIM trasmetterà ad AGCOM.
- Sulla proposta di TIM di effettuare dei controlli sui soggetti che svolgono attività commerciale per TIM in caso di correlazione significativa tra le segnalazioni di guasto e gli episodi di rientro in TIM, un OAO concorda ma ritiene necessario stabilire una "soglia di significatività", superata la quale TIM procederà a detti controlli, i quali dovrebbero essere descritti con precisione da TIM.

IMPEGNO n. 4: formazione del personale

- *Trasmettere entro 60 giorni dall'eventuale approvazione degli Impegni, a tutto il personale aziendale della direzione Wholesale nonché alle eventuali società esterne attive in modalità System Unico o per conto di TIM, coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO, un documento informativo che illustri i principali obblighi vigenti in materia di parità di trattamento interna/esterna nonché le regole di condotta che detto personale deve seguire nei contatti con i clienti degli OAO. In particolare, detto documento conterrà il richiamo a tutti i divieti di uso commerciali dei dati privilegiati e sarà aggiornato con cadenza annuale per 5 anni.*
- *Realizzare, entro 6 mesi dall'eventuale approvazione degli Impegni, un programma di formazione, anche in modalità on-line, relativo al documento informativo di cui al punto precedente, cui dovrà partecipare tutto il personale tecnico di TIM che entra in contatto con i clienti finali degli OAO. Il programma di formazione verrà indirizzato anche alle imprese terze di cui TIM si avvale per le attività di assurance e delivery.*

- Anche su tale iniziativa un rispondente esprime un apprezzamento complessivamente negativo atteso che, dato il ruolo e le dimensioni di TIM, una adeguata formazione del proprio personale così come di quello esterno con cui collabora dovrebbe rappresentare l'ovvia applicazione del più volte ribadito principio di garanzia di parità interna/esterna cui TIM deve assolvere, ragione quest'ultima per valutare siffatta misura non come una novità e da respingere per tale ragione come impegno oltre che per la genericità con cui è stato presentato.

  Sul punto osserva inoltre che, essendo l'obbligo di parità di trattamento già oggetto di precedenti e risalenti procedimenti (tra cui quello di cui alle delibere nn. 351/08/CONS e 718/08/CONS), la misura presentata nel procedimento di che trattasi evidenzia il fatto che TIM non sia stata – a partire dal 2008 – in grado di organizzarsi efficacemente in modo da disincentivare il personale – proprio o con cui collabora – dal porre in essere condotte scorrette tali quali quelle che hanno generato il fenomeno qui osservato.

- Un rispondente non ha osservazioni specifiche.
- L'impegno 4, secondo un rispondente, riprende alla lettera il contenuto degli impegni proposti dalla stessa TIM nell'ambito del procedimento A514 (tuttora pendente) davanti ad AGCM relativo alle strategie anticompetitive poste in essere da TIM nell'ambito del mercato dei servizi di accesso alla rete di telecomunicazioni e nel mercato dei servizi di telecomunicazioni al dettaglio, al fine di ostacolare lo sviluppo concorrenziale dei mercati *wholesale* e *retail* dei servizi a banda larga e ultralarga in Italia.

  A tal fine AGCOM ha, a più riprese, prescritto a TIM, in qualità di operatore notificato, di separare, mediante opportune misure organizzative, le divisioni interne preposte alla gestione della rete da quelle preposte alla vendita dei servizi finali, al fine di assicurare che i dati comunicati dall'operatore alternativo non siano impiegati da TIM per avvantaggiarsi indebitamente nella competizione sul mercato dei clienti finali (art. 2, comma 2, *lett. d*) della delibera n. 152/02/CONS; art. 8 della delibera n. 4/06/CONS; art. 17 bis, comma 2, *lett. c*) e § 26 della delibera n. 274/07/CONS; art 55, comma 1, *lett. d*) ed *e*) della delibera n. 731/09/CONS; 64, comma 1, *lett. c*), *d*) ed *e*) e comma 2 della delibera n. 623/15/CONS).

  L'impegno in esame si limita a proporre, secondo l'OAO, misure rimediali che non apportano alcun valore aggiunto rispetto a quello che TIM sarebbe già tenuta a fare sin dalla delibera n. 152/02/CONS recante "*Misure atte a garantire la piena applicazione del principio di parità di trattamento interna ed esterna da parte degli operatori aventi notevole forza di mercato nella telefonia fissa"*.

  È infatti evidente, secondo il rispondente, che il rispetto degli obblighi di non discriminazione/parità di trattamento da parte di TIM implichi, di per sé, la necessità di formare tutto il personale di cui essa si avvale per l'"*attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO*" circa "*i principali obblighi vigenti in materia di trattamento interna/esterna*".

  Diversamente opinando, aggiunge lo stesso operatore, si potrebbe affermare che dal 2002 ad oggi TIM non abbia posto in essere alcuna concreta misura per garantire la piena applicazione del principio di parità di trattamento interna ed esterna.

  A tali dirimenti considerazioni aggiunge che le misure proposte sono generiche ed indeterminate, essendo del tutto omesse informazioni essenziali ai fini della verifica delle stesse, quali:

  - la descrizione dettagliata del documento illustrativo da trasmettere al personale *wholesale* e alle società esterne coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO;

- la descrizione dettagliata del programma di formazione cui dovrà partecipare il personale tecnico di Telecom che entra in contatto con i clienti finali dei concorrenti;
- la descrizione delle "modalità on-line" di formazione.

L'Impegno in esame sarebbe per l'operatore peraltro:

- contraddittorio in quanto da un lato, prevede che il documento illustrativo debba essere trasmesso "*a tutto il personale aziendale della direzione Wholesale nonché alle eventuali società esterne attive in modalità system unico o per conto di Telecom, coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO*", dall'altro, prevede di realizzare un programma di formazione dedicato solamente al "*personale tecnico di Telecom che entra in contatto con i clienti finali degli OAO*";
- incompleto in quanto il programma di formazione dovrebbe essere esteso anche alla rete commerciale di Telecom compresi gli eventuali call center esterni di cui quest'ultima si avvale;
- inefficace in quanto non prevede misure di monitoraggio, *enforcement* e sanzione in caso di violazione o comportamenti non in linea con tali indicazioni. Qualunque impegno, infatti, dovrebbe secondo Fastweb prevedere quantomeno un meccanismo di verifica che consenta all'Autorità ed ai soggetti impattati (OAO) di valutare l'effettiva formazione del personale impiegato da TIM, nonché adeguati meccanismi sanzionatori nel caso di mancato rispetto degli obblighi di non discriminazione o utilizzo delle informazioni *wholesale* sia da parte di dipendenti TIM sia da parte di call center/agenzie che operano per conto di TIM e/o altri soggetti (come i *system*);
- non verificabile in quanto non prevede strumenti che consentano di verificare, da un lato, la correttezza della condotta degli agenti commerciali, delle imprese terze e dei *system* che lavorano per conto di Telecom, dall'altro, l'applicazione da parte di quest'ultima del descritto regime sanzionatorio.

Anche gli impegni 4 proposti non soddisfano, per l'operatore, i requisiti di cui alla delibera n. 581/15/CONS con riferimento all'articolo 13, commi 1 e 5 ed, in particolare, con riferimento al comma 5, in quanto non vengono forniti i necessari dettagli sulle modalità di attuazione e sul contenuto delle attività di formazione, sulle sanzioni per mancata ottemperanza, sui meccanismi (indipendenti) da TIM di verifica del rispetto delle linee guida da personale interno ed esterno operante per TIM.

- Sulla proposta di TIM un operatore evidenzia, in via preliminare, la totale noncuranza di TIM nei confronti della regolamentazione sulla parità di trattamento.

In secondo luogo, il rispondente rileva come gli impegni in questione siano già stati proposti da TIM all'AGCM nell'ambito del procedimento A514 e siano stati, già in tale ambito, rigettati in quanto ritenuti inidonei a rimuovere i profili anticoncorrenziali oggetto di istruttoria.

In conclusione, alla luce delle considerazioni e delle osservazioni presentate, l'OAO ritiene che la proposta definitiva di impegni di TIM di cui alla determina n. 2/19/DRS, non portando alla immediata e stabile interruzione dei comportamenti non in linea con le regole, sia inidonea a migliorare le condizioni di concorrenza nel settore e non costituisca misura idonee a rimuovere le conseguenze anti-competitive dell'illecito. Ne consegue che essi andrebbero, a parere della stessa, rigettati.

- Un operatore fa presente che l'Autorità ha in più sedi già prescritto a Telecom Italia di adottare opportune modifiche organizzative atte a separare le divisioni interne deputate alla gestione della rete da quelle deputate alla vendita dei servizi finali al fine di garantire che i dati comunicati dall'operatore alternativo non siano utilizzati da TIM per avvantaggiarsi indebitamente nella competizione sul mercato dei clienti finali. TIM sarebbe, pertanto, venuta meno all'osservanza della delibera n. 152/02/CONS, recante "Misure atte a garantire la piena applicazione del principio di parità di trattamento interna ed esterna da parte degli operatori aventi notevole forza di mercato nella telefonia fissa".

  L'operatore sottolinea, altresì, la somiglianza degli impegni adottati ai fini del procedimento in oggetto con quelli proposti in altre sedi e in tempi diversi (i primi risalenti al 2008 e riconosciuti dall'AGCOM come *remedies* con delibera n. 731/09/CONS; i secondi risalenti al 2017 e presentati da Telecom nell'ambito del procedimento AGCM A514) e che, secondo l'OAO, avrebbero già dovuto essere messi in atto da Telecom. Ciò implica, a parere del rispondente, che tale impegno rappresenti esclusivamente un mero adempimento ad un obbligo regolamentare ai sensi della delibera n. 152/02/CONS.

  Entrando nel merito della misura proposta, l'OAO ritiene che detto impegno sia carente di specificità, in quanto non fornisce informazioni di dettaglio del documento da diffondere al personale *wholesale* e alle società esterne coinvolte nei processi di *provisioning* ed *assurance* delle linee di accesso presso il domicilio dei clienti degli operatori; di completezza, in quanto non prevede l'estensione del programma di formazione anche alla rete commerciale di Telecom (compresi gli eventuali call center esterni di cui quest'ultima si avvale); di verificabilità, in quanto non prevede alcun meccanismo di verifica che possa consentire di valutare l'effettiva formazione del personale impiegato da TIM.

  In base a quanto espresso nelle proprie considerazioni, l'operatore ritiene che gli impegni proposti da Telecom non offrano sufficienti garanzie a tutela della riservatezza dei dati dei clienti in possesso di Telecom e, di conseguenza, non rappresentino una misura sufficiente a scongiurare in via definitiva il ripetersi di comportamenti illeciti.

- Un operatore ritiene che tale misura sia insufficiente e tardiva, in quanto essa costituisce già un obbligo per TIM e, per tale ragione, già rigettata dall'Autorità Antitrust all'esito del procedimento A514.

IMPEGNO n. 5: Funzione di vigilanza sugli impegni assunti

In ottemperanza all'articolo 13, comma 5, della delibera n. 581/15/CONS, TIM propone ad Agcom di svolgere la funzione di vigilanza sugli impegni assunti da TIM.

- Due rispondenti non hanno osservazioni sul punto.
- Un operatore osserva che l'art. 13, comma 5, della delibera n. 581/15/CONS stabilisce che la proposta definitiva di impegni, oltre ad indicare in dettaglio gli obblighi che l'operatore si dichiara disposto ad assumere ed i relativi tempi di attuazione, deve in ogni caso prevedere la funzione di vigilanza in capo ad una struttura indipendente che, a seconda delle dimensioni dell'impresa e del contenuto degli impegni, può essere appositamente costituita.

  TIM ha proposto che sia AGCOM a svolgere tale funzione di vigilanza sugli impegni assunti da TIM.

  Tale impegno, ad avviso del rispondente, non è conforme alle previsioni della delibera n. 581/15/CONS in quanto la stessa AGCOM ha sempre e comunque un obbligo di vigilanza sugli impegni assunti dagli operatori e quindi non fa che ribadire le funzioni già previste dalla normativa, senza assolvere a quanto previsto invece dall'articolo richiamato che indica chiaramente una struttura indipendente diversa da AGCOM stessa.

  Infatti, lo stesso articolo 18 della delibera n. 581/15/CONS prevede che sia AGCOM ad effettuare verifiche sull'attuazione degli impegni.

  L'attività di verifica sull'attuazione degli impegni prevista espressamente in capo ad AGCOM avrebbe peraltro la finalità di evidenziare all'organo collegiale eventuali criticità nell'attuazione da parte dell'operatore degli impegni assunti, "*ai fini dell'adozione dei conseguenti provvedimenti*".

  L'operatore ritiene che un medesimo soggetto, nel caso di specie la stessa Autorità, non possa al contempo svolgere, da un lato, un'attività di vigilanza in qualità di soggetto indipendente e, dall'altro, di verifica sulla corretta attuazione delle misure, segnalando eventuali criticità che potrebbero riguardare anche la misura stessa relativa all'attività di vigilanza svolta.

  Ne deriverebbe che lo stesso soggetto si troverebbe a rivestire contemporaneamente sia il ruolo di vigilato che di vigilante, in palese violazione del requisito di indipendenza richiesto espressamente dalle stesse disposizioni regolamentari applicabili al caso di specie.

  Da quanto sopra dovrebbe necessariamente conseguire che una struttura di vigilanza costituita solo per un terzo dall'Autorità non può essere ritenuta

indipendente ai sensi dell'articolo 13, comma 5, del Regolamento, tantomeno potrà essere ritenuta indipendente ed idonea a svolgere le attività di vigilanza cui è deputata una struttura costituita unicamente dall'Autorità.

- Un operatore rinvia alle osservazioni di cui al punto precedente**.**

- Due operatori non svolgono commenti sul punto ritenendo la misura in generale generica e tardiva.

3. Esame e valutazione, dell'Autorità, in ordine alle osservazioni prodotte dagli OAO

3.1 Osservazioni generali

I. Un rispondente osserva che l'introduzione di un processo di criptazione a tutela dei dati, attraverso l'introduzione di *log*, era stato già oggetto di valutazione positiva da parte del mercato in occasione del tavolo tecnico successivo all'adozione della delibera n. 396/18/CONS, sede in cui se ne era auspicata l'estensione (oltre che all'*assurance*) anche al *delivery*, ragione per la quale la misura non sarebbe connotata da alcun elemento di novità.

A tale riguardo l'Autorità ritiene che, relativamente al *provisioning*, tale misura non è oggetto di obbligo regolamentare; va da sé, dunque, che la stessa introduce una innovazione rispetto al vigente quadro regolamentare. Il fatto che tale misura fosse stata ritenuta, dagli osservatori, ipoteticamente auspicabile conferma la propria valenza pro-concorrenziale.

II. Un operatore ha osservato, in relazione alla proposta di impegni numero 2 relativa ai tavoli tecnici e ai *test* civetta, che la stessa non appare altro che il mero recepimento di quanto ordinato a TIM dall'Autorità nella delibera n. 396/18/CONS. Analogo discorso vale per l'impegno 3 sulla verifica del grado di correlazione tra segnalazioni di guasto e i rientri in TIM.

A tale riguardo si richiama che, effettivamente, in tale delibera l'Autorità ha ordinato a TIM di introdurre delle *idonee procedure di controllo interno per la verifica periodica del grado di correlazione tra rientri in TIM e le segnalazioni di guasto ricevute sui sistemi wholesale di rete. In caso di correlazione significativa, TIM attiva controlli sui soggetti che svolgono attività commerciale retail per TIM e a cui tali ordini sono riconducibili, al fine di accertare eventuali violazioni contrattuali, di cui sopra, circa il divieto di acquistare liste di clienti in disservizio che sono attestati su rete TIM. Analoghe procedure di controllo dovranno essere attivate in caso di chiamata commerciale ai "numeri civetta", eventualmente indicati dagli OAO e di cui si è detto sopra, attivando controlli al fine di accertare violazioni contrattuali circa i divieti sull'uso di informazioni sui clienti disserviti. Tali misure sono comunicate all'Autorità, entro 60 giorni dalla notifica del provvedimento, per valutarne l'adeguatezza e l'efficacia.*

L'Autorità ritiene, condividendo il rilievo dell'operatore, che sarebbe opportuno che TIM estendesse tali misure alla fase di *provisioning*, non prevista dalla citata delibera.

III. In via generale, un rispondente rileva che Telecom si è già dotata di un Codice di comportamento per la riservatezza dei dati degli OAO ed "*ha stabilito, tra gli altri provvedimenti, misure tecnologiche ed organizzative idonee a garantire la separazione dei sistemi informativi delle unità organizzative preposte alla gestione della Rete da quelli delle Funzioni commerciali preposte alla vendita di servizi alla clientela finale, proponendosi di verificare nel tempo il rispetto, l'adeguatezza e l'efficacia di tali misure*". Gli impegni proposti dunque, funzionali alla criptazione dei dati sensibili del cliente e alla formazione del personale, rappresenterebbero una misura di base che avrebbe dovuto pertanto essere già implementata da parte di TIM. A tal fine l'operatore osserva come l'Autorità abbia già imposto a TIM, in qualità di operatore notificato, di separare, mediante opportune misure organizzative le divisioni interne preposte alla gestione della rete da quelle preposte alla vendita dei servizi finali, al fine di assicurare che i dati comunicati dall'operatore alternativo non siano impiegati da TIM per avvantaggiarsi indebitamente nella competizione sul mercato dei clienti finali (art. 2, comma 2, *lett. d*) della delibera n. 152/02/CONS; art. 8 della delibera n. 4/06/CONS; art. 17 bis, comma 2, *lett. c*) e § 26 della delibera n. 274/07/CONS; art 55, comma 1, *lett. d*) ed *e*) della delibera n. 731/09/CONS; 64, comma 1, *lett. c*), *d*) ed *e*) e comma 2 della delibera n. 623/15/CONS).

A tale riguardo l'Autorità fa rilevare che l'art. 64 della delibera n. 623/15/CONS prevede, in relazione al tema della separazione dei sistemi, quanto segue (comma 1):

d. la gestione di dati e informazioni relative ai servizi di accesso acquistati dagli operatori interconnessi sia separata da quella relativa ai dati accessibili dalle divisioni di vendita dei servizi finali;

e. i sistemi informativi e gestionali relativi ai dati degli operatori alternativi siano gestiti da personale differente da quello preposto alle attività commerciali verso i clienti finali e che tali sistemi e le relative informazioni non siano accessibili al personale delle unità organizzative commerciali che forniscono servizi ai clienti finali.

2. Telecom Italia garantisce che il personale della funzione cui sono attribuite le competenze relative alla fornitura dei servizi di accesso all'ingrosso di cui al presente provvedimento non svolga alcuna attività commerciale di vendita presso i clienti finali.

Il comma 4 dello stesso articolo prevede che:

Telecom Italia, entro il 30 giugno di ogni anno, presenta sotto la propria responsabilità una relazione annuale, certificata da un soggetto terzo, che comprovi la separazione tra sistemi informativi della funzione cui sono attribuite le competenze relative alla fornitura dei servizi di accesso all'ingrosso di cui al presente provvedimento e quelli delle funzioni commerciali che forniscono servizi agli utenti finali. Tale relazione indica, inoltre, quali misure siano adottate per

impedire l'utilizzo dei dati riservati relativi alla clientela degli operatori da parte delle divisioni commerciali dell'operatore notificato che forniscono servizi agli utenti finali.

Si osserva che la vigente regolamentazione focalizza la propria attenzione sulla separazione dei sistemi informativi relativi ai clienti degli operatori *wholesale* dai sistemi con i dati dei clienti *retail* di TIM e sulla separazione del personale addetto al trattamento dei relativi dati (ossia separazione tra sistemi informativi e personale *retail* e *wholesale*).

Telecom ha, a tale riguardo, annualmente prodotto la relazione di certificazione della corretta implementazione della richiesta separazione.

In particolare TIM ha adottato misure di riservatezza per garantire la ***separazione (fisica e logica) dei sistemi informativi*** delle funzioni di rete e delle funzioni commerciali e per impedire l'utilizzo dei dati della clientela degli OLO in possesso delle Funzioni di Rete e *Wholesale* da parte delle divisioni commerciali di TIM. Di seguito una sintesi delle misure come certificate:

Separazione dei sistemi informativi

Per quanto attiene alla separazione dei sistemi informativi, essa viene attuata adottando i seguenti principi:

- ✓ *Separazione fisica:*
  - *È in essere una "separazione fisica" tra i sistemi informativi della Direzione Wholesale e Technology e quelli delle direzioni commerciali retail di TIM. Il personale Wholesale dedicato alla commercializzazione dei servizi wholesale utilizza propri sistemi informativi per la commercializzazione e la fatturazione dei servizi forniti agli OLO; il personale Retail non accede a tali sistemi;*
- ✓ *Separazione logica:*
  - *Il sistema informativo che contiene dati riservati dell'OLO e/o della sua clientela è "acceduto" da personale dell'area Commerciale Retail attraverso profili di accesso che non consentono la visualizzazione e/o gestione dei suddetti dati riservati;*
  - *L'accesso ai dati riservati dell'OLO e/o della sua clientela da parte di personale dell'area Commerciale Retail è ammesso per la sola gestione di specifici eventi di business preventivamente censiti ed autorizzati.*

Misure di riservatezza

Per quanto attiene alle misure di riservatezza, esse vengono attuate adottando i seguenti principi:

- ✓ *Misure di riservatezza sui sistemi informativi:*
  - *Controllo delle abilitazioni per accesso utente e accesso diretto (ove presente) e procedure operative per la gestione degli accessi;*

- *Impiego di informative all'accesso a sistemi che contengono dati riservati dell'OLO e/o della sua clientela e labeling della reportistica prodotta da tali sistemi;*
- *Regole a protezione delle postazioni utente con accesso a sistemi contenenti dati riservati dell'OLO e/o sua clientela.*

✓ *Misure di riservatezza organizzative:*

- *Codice di Comportamento per la riservatezza dei dati relativi alla clientela degli Altri Operatori Autorizzati;*
- *Clausole contrattuali per Terze Parti ed Outsourcers;*
- *Formazione a tutto il personale interessato dai temi della Delibera 152/02/CONS e della Delibera 623/15/CONS;*
- *Gruppo di Lavoro permanente interfunzionale con il compito di assicurare che tutte le implementazioni di nuovi processi operativi, sistemi e cambiamenti organizzativi avvengano nel rispetto della Delibera 152/02/CONS e Delibera 623/15/CONS;*
- *Classificazione delle informazioni riservate dell'OLO e/o sua clientela e relativa gestione.*

<u>*Conclusioni della certificazione tecnica*</u>

✓ *Valutazione delle misure di riservatezza sui sistemi informativi*

Con riferimento ai principi espressi dalla Delibera 152/02/CONS, articolo 2, comma 7, e dalla Delibera 623/15/CONS, articolo 64, comma 4 è stato riscontrato quanto segue:

- *i sistemi informativi dell'area Commerciale Retail sono separati da quelli dell'area Rete/Wholesale;*
- *i sistemi informativi dell'area Commerciale Retail, contenenti dati riservati dell'OLO e/o della sua clientela, posseggono misure di riservatezza che non consentono alle divisioni dell'area Commerciale Retail l'utilizzo non autorizzato dei suddetti dati;*
- *i sistemi informativi dell'area Rete e Wholesale posseggono misure di riservatezza che non consentono alle divisioni dell'area Commerciale Retail l'utilizzo dei dati riservati dell'OLO e/o della sua clientela.*

✓ *Valutazioni sulle misure di riservatezza organizzative*

Oltre alle azioni previste sui sistemi appartenenti all'area di indagine 2016, TIM ha attuato una serie di ulteriori misure organizzative (cosiddette "non sui sistemi") atta a garantire il rispetto, da parte del personale, delle raccomandazioni della Delibera 152/02/CONS, articolo 2, comma 7, e della Delibera 623/15/CONS, articolo 64, comma 4.

In particolare si evidenzia che:

- *è stata effettuata in data 19 giugno 2017 una nuova emissione del Codice di Comportamento previsto dalle Delibere 152/02/CONS e 623/15/CONS e del Codice di Comportamento conseguente agli impegni assunti da TIM ed approvati con la Delibera 718/08/CONS. Così facendo TIM si impegna continuativamente a tutelare la confidenzialità dei dati riservati dell'OLO e/o della sua clientela nei confronti del personale dell'area commerciale Retail, e a rafforzare la responsabilità di ogni dipendente verso il continuo rispetto della riservatezza dei dati riservati dell'OLO e/o della sua clientela e della parità di trattamento in generale;*
- *è stato aggiornato l'elenco dei referenti per il rispetto degli adempimenti previsti dalle Delibere 152/02/CONS e 623/15/CONS in coerenza con le variazioni dell'assetto organizzativo di TIM;*
- *è stata completata l'integrazione nei contratti già in essere e nei nuovi contratti con società terze interessate dalla tematica di cui alle Delibere 152/02/CONS e 623/15/CONS, dell'apposita clausola contrattuale a tutela della riservatezza dei dati riservati dell'OLO;*
- *è stato effettuato un programma di formazione dedicato alle risorse impattate dalle Delibere 152/02/CONS e 623/15/CONS. Inoltre è stata riscontrata, presso le funzioni oggetto di Site Visit, una diffusa conoscenza della problematica connessa alla gestione dei dati riservati dell'OLO ed una profonda sensibilità del personale nei confronti degli obblighi derivanti dalle Delibere 152/02/CONS e 623/15/CONS.*

Ciò premesso, l'Autorità osserva come nessuna delle misure già previste consente di far fronte al fatto che vi possa essere comunque un dipendente "infedele" (anche della divisione rete) che, in modo autonomo, possa divulgare i dati dei clienti a presunti *call center* per tornaconto personale.

Le misure oggetto della delibera n. 396/18/CONS e degli impegni in questione sono funzionali proprio ad individuare eventuali abusi da parte di quei soggetti che, funzionalmente, hanno titolo ad utilizzare i dati dei clienti *wholesale*.

D'altra parte l'Autorità ha avviato un procedimento sanzionatorio nei confronti di TIM non per non aver attuato le misure di cui sopra (ossia quelle definite dall'art. 64 della delibera n. 623/15/CONS) ma per non essersi, in modo diligente, attivata per introdurre misure aggiuntive, quali quelle oggi proposte, come la criptazione e il *log* degli accessi. Ciò alla luce della stessa denunzia di condotte fraudolente poste in essere, possibilmente, anche a danno di TIM stessa (la stessa ha effettuato diverse denunce a differenti Procure delle Repubblica per i fatti di che trattasi diffusi in buona parte del territorio nazionale).

Pertanto le osservazioni di alcuni rispondenti, su tale questione, non colgono nel segno e sono da rigettare.

3.2 Osservazioni tecniche sugli impegni

Appaiono condivisibili una serie di osservazioni di merito che di seguito si riportano.

Impegno 1

In primo luogo è opportuno che TIM fornisca maggiori dettagli sulla soluzione tecnica dell'impegno 1 oltre che sulle tempistiche di implementazione.

La misura proposta limita il numero di soggetti autorizzati che hanno visibilità sui dati dei clienti *wholesale* e dei relativi ordini di *provisioning*/*assurance* su rete TIM. A tale riguardo, in replica ad un commento ricevuto, è evidente che non si annulla il rischio di fuoriuscita dei dati per la ragione che non è controllabile in assoluto la volontà fraudolenta di un dipendente/operatore disonesto e infedele, di TIM come degli OAO. Però, con la misura proposta, sarà più facile individuare il punto di uscita e il responsabile.

Si condivide comunque l'osservazione relativa all'adozione di una soluzione tecnica che impedisca la visualizzazione dei dati sensibili in caso di qualunque operazione di estrazione singola o massiva di ordinativi che andrebbe estesa, quindi, a tutte le fasi in cui vi sia la possibilità di accedere ai dati sensibili in esame, il cui accesso dovrebbe comunque essere inibito in ogni passaggio del processo che implichi l'utilizzo di tali dati.

Nella sua proposta di impegni, Telecom non ha specificato, inoltre, quali siano i soggetti interni e/o esterni titolari ad oggi della possibilità di estrarre le informazioni dai sistemi, essendoci solo un generale riferimento, da parte di TIM, al *"personale autorizzato, per la cui attività lavorativa è necessario accedere a queste informazioni, escludendo tale possibilità per tutti gli altri utenti dei sistemi".* Ciò premesso, si ritiene opportuno che Telecom espliciti quali siano le figure professionali, i motivi e le modalità che legittimino operazioni di accesso e di estrazione sui sistemi in cui sono contenuti dati sensibili dei clienti.

Impegno 2

In relazione all'Impegno 2 si condivide la richiesta che sia esteso al processo di *provisioning*. Inoltre sarebbe necessario meglio chiarire la modalità di realizzazione dei test civetta.

Si condivide l'opportunità che l'analisi di correlazione sia svolta anche per il *delivery e* che siano forniti maggiori dettagli sull'analisi di correlazione e la metodologia utilizzata (quale, ad esempio, la finestra temporale di analisi a partire dalla data di guasto che è stata utilizzata, la "soglia di significatività", superata la quale TIM procederà a detti controlli, i quali dovrebbero essere descritti con precisione da TIM).

Impegno 3

Analogamente agli impegni 1 e 2 anche l'impegno 3 non indica nel dettaglio i relativi tempi di attuazione.

Impegno 4

In relazione all' Impegno 4 si condivide la richiesta, a TIM, di inviare all'Autorità quanto segue:

1. il documento illustrativo da trasmettere al personale *wholesale* e alle società esterne coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO;
2. la descrizione del programma di formazione cui dovrà partecipare il personale tecnico di Telecom che entra in contatto con i clienti finali dei concorrenti;
3. la descrizione delle "modalità on-line" di formazione.

Inoltre,

4. si ritiene che TIM debba verificare la congruenza dei seguenti passaggi laddove, da un lato, TIM prevede che il documento illustrativo debba essere trasmesso "*a tutto il personale aziendale della direzione Wholesale nonché alle eventuali società esterne attive in modalità system unico o per conto di Telecom, coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO*", dall'altro, prevede di realizzare un programma di formazione dedicato solamente al "*personale tecnico di Telecom che entra in contatto con i clienti finali degli OAO*";

L'Autorità non condivide, viceversa, l'osservazione di un OAO secondo cui la proposta sia inefficace in quanto non prevede misure di monitoraggio, di verifica del grado di formazione, *enforcement* e sanzione in caso di violazione o comportamenti non in linea con tali indicazioni. Infatti resta in capo all'Autorità il compito di svolgere la necessaria attività di vigilanza e sanzionatoria, indipendentemente dagli impegni di TIM.

Si condivide l'osservazione di alcuni OAO secondo cui il programma di formazione debba essere rivolto anche alla divisione commerciale di TIM (compresi gli eventuali *call center* esterni di cui quest'ultima si avvale).

Impegno 5

Un rispondente ha osservato che la funzione di vigilanza non potrebbe essere svolta dall'Agcom ai sensi del Regolamento sui procedimenti sanzionatori.

A tale riguardo si richiama il testo dell'articolo 13, comma 5, della delibera n. 581/15/CONS laddove prevede che "*La proposta definitiva deve indicare in dettaglio gli obblighi che l'operatore si dichiara disposto ad assumere ed i relativi tempi di attuazione e deve in ogni caso* ***prevedere la funzione di vigilanza in capo ad una struttura indipendente*** *che, a seconda delle dimensioni dell'impresa e del contenuto degli impegni,* ***può*** *essere appositamente costituita*".

L'Autorità ha in diversi casi approvato impegni in cui si è ritenuto di costituire la struttura di vigilanza con la partecipazione di soggetti nominati dall'operatore e di funzionari dell'Autorità. La *ratio* della norma, infatti, è quella di obbligare il soggetto proponente ad una vigilanza esterna a sé stesso.

Ciò evidentemente, ed in ogni caso, non impedisce che sia l'Autorità stessa ad assolvere pienamente alla funzione di vigilanza e di controllo di cui all'articolo 18 del Regolamento, le cui attività non risultano disgiunte né differenziabili da quelle di cui al richiamato articolo 13, comma 5, bensì complementari. Inoltre l'esercizio in via esclusiva della funzione di vigilanza e controllo ad opera dell'Autorità stessa risponde meglio ad esigenza di snellezza e maggiore speditezza delle attività di interlocuzione con l'operatore vigilato, qualora ne ricorra la necessità. Ciò, infatti, è quanto di prassi seguito in diversi procedimenti.

L'osservazione pertanto è priva di pregio e la correlativa emenda non ritenuta necessaria.

4. La replica di TIM alle osservazioni degli OAO

Preliminarmente rileva che, con nota del 19 luglio 2019 TIM, in relazione al fenomeno dell'utilizzo illegittimo di dati sui clienti, ha fornito i risultati di alcune verifiche che di seguito si riassumono brevemente.

TIM ha, in primo luogo, richiamato che le fasi di lavorazione di un *trouble ticket* rendono individuabili quattro momenti di possibile fuoriuscita dei dati dei clienti non tutti gestiti da TIM, ovvero:

I. *in primis*, quanto l'operatore inserisce sul portale *wholesale* le notizie relative al guasto, incluso il nome e cognome del cliente e il numero di telefono; a tale fase è associata quella di utilizzo, tramite credenziali di accesso rilasciate da parte degli OAO a persone specifiche a loro riferibili, dei dati inseriti, come meglio chiarito di seguito;

II. quando i dati sui guasti sono presenti sui sistemi di TIM deputati, affinché il proprio personale ne pianifichi la gestione;

III. quando TIM *Wholesale*, attraverso *Wholesale Operation*, dispaccia l'ordine presso le società che operano per TIM (call center), che a loro volta eseguono una cosiddetta diagnosi di primo livello. Si tratta di un intervento da remoto, cioè condotto attraverso una *call* con il cliente dell'operatore che ha inserito il guasto. In questa fase potrebbe essere chiuso il TT laddove il problema sia di facile soluzione. Questa è una fase che TIM affida sempre a società esterne;

IV. se il TT non ha soluzione in questa fase, quando l'ordine è gestito da TIM *on field*, cioè attraverso l'inoltro a società esterne che lavorano con TIM o a tecnici interni a TIM secondo una logica di efficienza basata sulla distribuzione territoriale degli ordini.

TIM, nell'ottica di risalire alla genesi dei fenomeni di *malpractice* commerciale, ha svolto una serie di controlli sui propri sistemi in relazione alla prima fase (fase I) di processo di un ordine (di segnalazione guasto): ovvero quando personale addetto dell'operatore alternativo accede al portale *wholesale* di TIM per inserire l'anagrafica del proprio cliente disservito o per svolgere altre funzioni ammesse sui dati dei clienti degli OAO.

A tale scopo sono state avviate, da TIM, anche una serie di verifiche relative all'utilizzo da parte del personale OAO dell'accesso al portale Wholesale di TIM. Infatti, nel momento in cui un OAO firma un contratto per uno dei tanti servizi wholesale con TIM, l'attuazione dello stesso avviene *in primis* abilitando il personale, indicato dall'OAO, ad accedere alle procedure di delivery e *assurance* relative allo specifico contratto. L'abilitazione consiste nel fornire le credenziali di accesso alla singola persona ad un'area riservata nell'ambito della quale è possibile utilizzare le funzionalità di *delivery* e *assurance*, nonché di eseguire in autonomia *report* ed *export* dai sistemi relativamente ai dati di pertinenza, quali: dati linea, dati cliente, ordinativi di lavoro e guasti.

Una volta acquisite le informazioni dai sistemi informatici per uso proprio (mediante export sui propri dispositivi) non è possibile effettuare da parte di TIM nessun controllo sull'eventuale diffusione di tali dati.

Nel corso del normale monitoraggio sull'utilizzo dei propri sistemi informatici, è stata condotta un'analisi volumetrica sugli accessi effettuati nel primo semestre del 2019 nel Portale *Wholesale*.

Sono stati analizzati gli accessi effettuati nel primo semestre del 2019. Gli accessi sono stati effettuati da circa [*omissis*] account OAO autorizzati e sono avvenuti da circa [*omissis*] indirizzi IP diversi.

Si sono evidenziati i seguenti fenomeni anomali:

- accessi concorrenti da parte dello stesso account da IP diversi. Si può presumere che le stesse credenziali di accesso siano state utilizzate da più persone in contemporanea e da postazioni diverse;
- una forte polarizzazione del traffico proveniente da specifici IP e specifici account: [*omissis*] account hanno generato il [*omissis*] del totale delle richieste/accessi;
- gli accessi sono avvenuti anche da IP non italiani;
- in alcuni casi, dal medesimo indirizzo IP vengono effettuati accessi con Account di diversi OAO.

Le suddette evidenze sono state anche oggetto di denuncia alla Procura della Repubblica presso il Tribunale di Roma in data 1 agosto 2019, affinché la stessa possa svolgere gli approfondimenti investigativi ritenuti necessari, e verificare la rilevanza penale dei fatti e, qualora ravvisi condotte delittuose, perseguire a norma di legge gli eventuali responsabili.

Alla luce di quanto sopra esposto, TIM ritiene di aver fatto e di continuare a fare, quindi, tutto ciò che è nelle sue disponibilità. Tuttavia, come chiaramente emerge anche dai media - da ultimo l'operatore richiama lo speciale andato in onda su SKY TG24 il 12 settembre u.s. dal titolo "i predoni dei dati" - si tratta di un fenomeno fraudolento che può essere contrastato solo se si individua una soluzione di sistema. In questo, secondo TIM, il ruolo dell'Autorità può essere fondamentale nel promuovere tra tutti gli Operatori l'adozione di un *Codice di Comportamento* che tracci le linee guida delle modalità con cui un Operatore può acquisire i propri clienti.

Quanto alle repliche sulle osservazioni degli OAO al documento di Impegni, con nota del 20 settembre 2019, TIM ha comunicato di aver accolto in parte le richieste del mercato ed integrato gli impegni.

Di seguito si riportano gli Impegni di TIM evidenziando in rosso le integrazioni effettuate, nella nota del 20 settembre, a seguito del *market test*:

Impegno 1

"Introdurre una misura di protezione specifica anche sui sistemi di delivery: TIM si impegna ad individuare, entro 30 giorni dall'approvazione degli impegni, una soluzione tecnica che possa essere condivisa anche dagli OAO, che impedisca la visualizzazione di dati sensibili (nome e cognome cliente, CF/Partita IVA e recapito telefonico) in caso di qualunque operazione di estrazione singola o massiva di ordinativi da parte di qualunque personale autorizzato all'accesso tramite interfaccia grafica (GUI) al sistema, quindi outsourcers, personale TIM Wholesale e OAO. In proposito saranno create delle nuove profilature ad hoc per gli utenti dei sistemi, con diversi livelli autorizzativi di accesso e tracciamento degli stessi accessi, che permettano di visualizzare da interfaccia grafica i dati sensibili solo dal personale autorizzato, per la cui attività lavorativa è necessario accedere a queste informazioni, escludendo tale possibilità per tutti gli altri utenti dei sistemi. In logica di full equivalence la misura sarà estesa anche al caso di ordinativi retail TIM. In altri termini anche per gli ordinativi di TIM retail né agli outsourcers né il personale di TIM wholesale potrà estrarre i suddetti dati sensibili. Per quanto riguarda il sistema NOW, le modifiche proposte dovranno essere preventivamente concordate anche con gli OAO perché tale sistema viene utilizzato anche da personale OAO".

Impegno 2

"Istituire dei tavoli tecnici con gli OAO:

- *per analizzare congiuntamente i casi da loro segnalati e darne riscontro anche ad AGCom;*
- *per condividere un processo per poter effettuare «dei test civetta» utilizzando clienti reali (es. forniti da OAO) per l'assurance e per il delivery e rendere pubblici gli esiti di tali test.*
- *In tale ambito TIM si impegna a mettere a punto una modalità di effettuazione dei test civetta su base richiesta per l'assurance e per il delivery secondo i seguenti criteri:*
    - *per ogni numero rientrante nel "test civetta" viene lanciata uno script che modifica il campo "recapito telefonico" nei vari sistemi preposti alla risoluzione del guasto;*
    - *in base all'eventuale numero chiamato chi raccoglierà la chiamata sarà in grado di individuare il sistema da cui è stato prelevato il dato"*

Impegno 3

"Trasmettere ad AGCom periodicamente: l'esito delle verifiche del grado di correlazione tra rientri in TIM e le segnalazioni di guasto ricevute sui sistemi wholesale di rete, fatte con la procedura richiesta con la Delibera 396/18/CONS. L'esito, in caso di correlazione significativa, dei controlli fatti sui soggetti che svolgono attività commerciale retail per TIM e a cui tali ordini sono riconducibili".

"Predisporre entro 30 giorni dall'approvazione degli impegni una procedura analoga a quella fatta per la correlazione tra guasti e rientri, che consenta di correlare i rientri in TIM e gli ordini di attivazione da parte degli OAO. L'esito delle suddette verifiche sarà periodicamente trasmesso ad AGCom".

Impegni 4-5

"Trasmettere, entro 60 giorni dall'eventuale approvazione degli Impegni, a tutto il personale aziendale della direzione Wholesale nonché alle eventuali società esterne attive in modalità System Unico o per conto di TIM, coinvolte nei lavori di attivazione e riparazione delle linee di accesso presso il domicilio dei clienti degli OAO, un documento informativo che illustri i principali obblighi vigenti in materia di parità di trattamento interna/esterna nonché le regole di condotta che detto personale deve seguire nei contatti con i clienti degli OAO. In particolare, detto documento conterrà il richiamo a tutti i divieti di uso commerciali dei dati privilegiati e sarà aggiornato con cadenza annuale per 5 anni. TIM si impegna a fornire preliminarmente ad AGCom il suddetto documento per sue eventuali osservazioni

"Realizzare, entro 6 mesi dall'eventuale approvazione degli Impegni, un programma di formazione, anche in modalità on-line, relativo al documento informativo di cui al punto precedente, cui dovrà partecipare tutto il personale tecnico di TIM che entra in contatto con i clienti finali degli OAO. Il programma di formazione verrà indirizzato anche alle imprese terze di cui TIM si avvale per le attività di assurance e delivery. TIM si impegna inoltre, a fornire tutta la documentazione necessaria alle società esterne di rete di cui si avvale perché sensibilizzino il proprio personale al rispetto di quanto nelle stessa previsto.

"In ottemperanza all'art. 13, comma 5, della Delibera 581/15/CONS, TI propone ad AGCOM di svolgere la funzione di vigilanza sugli impegni assunti da TI a cui garantisce il supporto di proprio personale e/o consulenti esterni."