AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

DELIBERA N. 9/26/CIR

APPROVAZIONE DELLA PROPOSTA DI IMPEGNI PRESENTATA DALLA SOCIETÀ R&D COMMUNICATION S.R.L. AI SENSI DELLA LEGGE N. 248/06, DI CUI AL PROCEDIMENTO SANZIONATORIO CONT. N. 2/25/DRS

L'AUTORITÀ

NELLA riunione della Commissione per le infrastrutture e le reti del 26 febbraio 2026;

VISTA la legge 14 novembre 1995, n. 481, recante "*Norme per la concorrenza e la regolazione dei servizi di pubblica utilità. Istituzione delle Autorità di regolazione dei servizi di pubblica utilità*";

VISTA la legge 31 luglio 1997, n. 249, recante "*Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo*", di seguito denominata Autorità;

VISTA la direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il "*Codice europeo delle comunicazioni elettroniche*";

VISTO il decreto legislativo 1° agosto 2003, n. 259 recante "*Codice delle comunicazioni elettroniche*";

VISTA la legge 24 novembre 1981, n. 689, recante "*Modifiche al sistema penale*";

VISTA la legge 7 agosto del 1990, n. 241, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";

VISTO il decreto-legge 3 ottobre 2006, n. 262, recante "*Disposizioni urgenti in materia tributaria e finanziaria*";

VISTO il decreto legislativo 2 luglio 2010 n. 104 recante "*Attuazione dell'articolo 44 della legge 18 giugno 2009 n. 69, recante delega al Governo per il riordino del processo amministrativo*";

VISTO l'articolo 14-*bis, comma 1,* del decreto-legge 4 luglio 2006, n. 223, convertito in legge 4 agosto 2006, n. 248, recante "*Integrazione dei poteri dell'Autorità per le garanzie nelle comunicazioni*";

VISTA la delibera n. 223/12/CONS, del 27 aprile 2012, recante "*Regolamento concernente l'organizzazione e il funzionamento dell'Autorità per le garanzie nelle*

comunicazioni", come modificata, da ultimo, dalla delibera n.58/25/CONS del 6 marzo 2025;

VISTA la delibera n. 286/23/CONS" del 1° novembre 2023, recante "*Modifiche al Regolamento di procedura in materia di sanzioni amministrative e impegni di cui all'allegato A alla delibera n. 410/14/CONS come modificato, da ultimo, dalla delibera n.437/22/CONS*", di seguito denominato Regolamento sanzioni;

VISTA la delibera n. 12/23/CIR, del 3 maggio 2023 recante "*Regolamento sull'utilizzo dei caratteri alfanumerici che identificano il soggetto mittente nei servizi di messaggistica aziendale (SMS ALIAS)*";

VISTA la sentenza n. 1692 del TAR del Lazio (Sezione Quarta) del 29 gennaio 2024, di annullamento, *in parte qua*, della delibera n. 12/23/CIR;

VISTO l'atto di accertamento e contestazione Cont. n. 2/25/DRS notificato alla società RDCOM s.r.l. in data 31 luglio 2025 recante " *Contestazione alla società R&D COMMUNICATION s.r.l. per violazione dell'articolo 7, comma 1, di cui all'allegato "A" alla delibera n. 12/23/CIR*";

VISTO il documento definitivo di Impegni della società RDCOM del 27 novembre 2025 sottoposto a Market test in data 30 dicembre 2026 con determina n.10/25/DRS;

VISTI gli esiti del Market test, di cui al punto che precede, concluso senza osservazioni critiche del mercato in data 29 gennaio 2026;

VISTI tutti gli atti formati ed acquisiti dalla Direzione reti e servizi di comunicazioni elettroniche;

CONSIDERATO quanto segue:

Premessa

In esito ad attività di vigilanza sul diffuso fenomeno di CLI *spoofing* ed in particolare ad attività di illegittimo utilizzo di SMS con *Alias* di provenienza extraterritoriale, è stato avviato un procedimento sanzionatorio con provvedimento Cont.2/25/DRS a carico della società RD COMMMUNICATION s.r.l., nella specifica qualità di Fornitore di Transito (FT) per avere consentito di veicolare in Italia SMS con *Alias* proveniente da soggetto estero non autorizzato in Italia (società avente sede in Svizzera) secondo la chiara disposizione dell'articolo 11 del CCE e, dunque, di non avere bloccato il traffico violando, per tale via, l'obbligo regolamentare di cui all'articolo 7, comma1, della delibera n.12/23/CIR.

E' altresì utile rappresentare preliminarmente ed in estrema sintesi a riguardo che la delibera regolamentare n. 12/23/CIR, ha delimitato le modalità d'uso dei caratteri

alfanumerici (*Alias*) che identificano il soggetto mittente nei servizi di messaggistica aziendale (SMS) al fine di contrastare, per tale categoria di servizi, possibili usi illegittimi della stessa, considerando che la manipolazione dei dati identificativi può generare anche tentativi di frode a danno degli utenti finali riceventi.

Dalle richiamate attività istruttorie di vigilanza è infatti emerso che la società RDCOM (così nel seguito) è risultata coinvolta in traffico con identificativo del mittente alterato agevolando l'illegittima attività di manipolazione delle informazioni relative all'originazione della comunicazione contenute nel campo CLI, con l'effetto finale di impedire al soggetto ricevente la chiamata -in questo caso l'SMS- l'individuazione corretta di chi abbia originato la comunicazione simulando un mittente differente e apparentemente legittimo.

Giova comunque altresì evidenziare che, nel caso di specie, si è trattato di un unico SMS recapitato attraverso l'uso di identificativo mittente alfanumerico (*Alias*) "BNL" con CLI imputabile ad un unico numero mobile nazionale.

Rileva a riguardo che la medesima Società di seguito alla notifica del provvedimento Cont. 2/25/DRS si è avvalsa della facoltà *ex lege* di presentare, nei rituali termini di cui all' articolo 13 del richiamato Regolamento, un documento preliminare e poi definitivo di "Impegni", che è stato sottoposto, come noto, alla preliminare valutazione di ammissibilità nel corso della già cennata seduta della CIR del 17 dicembre, finalizzata al confronto critico con il mercato di riferimento (*market test*).

Nella seduta del 17 dicembre 2025 la Commissione, ha preso atto dell'istruttoria preliminare della Direzione Reti, con previa valutazione di non manifesta inammissibilità della proposta definitiva di impegni presentata da RDCOM, ai sensi dell'articolo 14, comma 3, del Regolamento.

Pertanto, con determina n. 10/25/DRS del 30 dicembre 2025, si è provveduto alla pubblicazione sul sito *web* della proposta definitiva di impegni, invitando - come previsto dall'art. 16 del Regolamento - i terzi interessati a fare pervenire le proprie osservazioni.

Rileva a riguardo che allo scadere del trentesimo giorno del 29 gennaio 2026 non sono pervenute osservazioni da parte dei terzi interessati sul documento definitivo di Impegni.

Quadro normativo e regolamentare

Giova evidenziare che l'episodio si colloca all'interno del "*Regolamento sull'utilizzo dei caratteri alfanumerici che identificano il soggetto mittente nei servizi di messaggistica aziendale (SMS ALIAS)*", - Allegato A alla delibera n. 12/23/CIR che in particolare all'articolo 3 (*Definizione dei ruoli nella fornitura del servizio di*

messaggistica aziendale) indentifica i soggetti cui è attribuito un ruolo - "n*ell'ambito della fornitura e gestione di servizi di MAA…*" - tra cui - alla lett. *d)* - il "*fornitore del servizio di transito di messaggistica (FT)*" stabilendone - al successivo articolo 7 - i relativi "*Obblighi*" specificamente (al comma 1) statuendo che: "*Il FT blocca la messaggistica con codifica non decimale esclusivamente se non ricevuta da soggetti in possesso dell'autorizzazione generale del Ministero delle Imprese e del Made in Italy e specificamente da FS o da altro FT. I messaggi bloccati sono inseriti in un elenco e sono mensilmente comunicati all'Autorità.*".

A tal riguardo è bene fin d'ora rammentare anche che la delibera citata è stata solo in parte incisa dalla sentenza 29 gennaio 2024, n. 1692 del TAR del Lazio (Sezione Quarta) in esito al ricorso demolitorio dell'intera delibera n. 12/23/CIR proposto da un operatore.

La citata pronuncia in accoglimento solo parziale del ricorso "…*nei limiti indicati in parte motiva, e, per l'effetto,* ***annulla le previsioni di cui all'art. 2, comma 10, dell'allegato A alla delibera n. 12/23/CIR e di cui all'art. 2, comma 1 e comma 2, della delibera stessa***" (enfasi aggiunta).

Tuttavia, la pronuncia non ha autorizzato affatto un superamento della regolamentazione in ordine agli obblighi di cui al richiamato articolo 7, comma 1, atteso che al contrario, ne ha, invece, confermato la validità ritenendo che persista "… ***l'obbligo, in capo agli operatori del settore … di verificare la titolarità, in capo a ciascuno dei soggetti con cui vengano scambiati SMS con Alias, delle autorizzazioni acquisite dal MIMIT***" (enfasi aggiunta).

Si osserva, infatti, a riguardo che il giudice adito non ha ritenuto sussistesse che tali obblighi di verifica fossero eccessivamente gravosi ritenendo, invece, che sia necessario piuttosto "*…operare una verifica incrociata anche delle informazioni fornite da ciascun UM che richieda la registrazione di un Alias consultando pubblici registri come il Registro Imprese o l'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata (INI-PEC) e verificando il possesso, da parte del soggetto che richiede la registrazione dell'Alias, dei poteri di legale rappresentanza dell'azienda mittente della messaggistica*" rilevando che non siano emersi concreti elementi atti a comprovare una "*eccessiva onerosità dei nuovi obblighi…,* ***che richiedono il compimento di una mera attività di consultazione di pubblici registri****, come il Registro Imprese, l'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata (INI-PEC) e gli elenchi degli operatori autorizzati di comunicazioni elettroniche pubblicati sul sito del Ministero delle Imprese e del Made in Italy*" (v.p.to 14 della sentenza; enfasi aggiunta).

Attività che RDCOM non ha evidentemente svolto.

Appare infatti palese, nel caso che ci occupa, che l'essere la Società svizzera (partner commerciale di RDCOM) sprovvista dell'autorizzazione ex art. 11 del Codice delle comunicazioni elettroniche deriva evidentemente dal fatto che RDCOM ha omesso una semplice, quanto possibile, verifica sul sito del MIMIT (attività svolta agevolmente dalla scrivente in sede di indagini istruttorie) e ne è stata ben consapevole, come si evince dal contratto prodotto dalla medesima RDCOM stipulato con il partner straniero nonché dai riscontri forniti durante le cennate attività di verifica, come di seguito riportate.

La posizione della società RDCOM

Negli scritti, depositati agli atti dell'istruttoria di vigilanza, risulta *per tabulas* che la società sanzionanda ha comunque invocato, assumendone valore esimente, la convinzione in buona fede che la parziale demolizione del contenuto deliberativo regolamentare ad opera del Giudice Amministrativo la esonerasse dallo svolgere controlli sulla regolarità della posizione autorizzativa in Italia del *partner* commerciale straniero, unilateralmente ritenendo di avere ricevuto e veicolato il suddetto SMS, conformemente a quanto disposto dal TAR Lazio sull'unilaterale assunto che, in buona sostanza, "…*ad avviso del T.A.R., non sussiste alcuna valida giustificazione per l'imposizione di un blocco generalizzato del traffico SMS con Alias proveniente dall'estero*" poiché "… *imporre il blocco degli SMS rispetto al traffico estero proveniente da imprese senza stabile organizzazione sul territorio italiano (e, conseguentemente, prive di autorizzazione generale) condurrebbe proprio al medesimo risultato contrastato dalla giurisprudenza amministrativa*.".

A siffatte considerazioni la stessa Società ha aggiunto, evidenziandone la limitata portata offensiva dell'accaduto, che, trattandosi di un unico caso rilevato di SMS, con Alias artefatto, non fosse da escludere che si trattasse di un *gap* del sistema informatico, pur sempre possibile, benché la soglia di attenzione di RDCOM sulla regolarità dei flussi di traffico sia asseritamente massima, evidenziando a riguardo "*il significativo e costante impegno ... nella prevenzione dello spam, delle pratiche di "CLI spoofing" e, in generale, degli usi illegittimi della messaggistica con Alias*".

La compulsata Società affermando la molteplicità delle verifiche costantemente svolte, ha sottolineato in ordine al caso specifico "… *che il mancato blocco dell'SMS in questione, ..., rappresenta un evento isolato dovuto alla (fisiologica) fallibilità dei sistemi informatici…*".

Il documento definitivo di Impegni del 27 novembre 2025

Il programma di impegni proposto in versione definitiva ed integrata in data 27 novembre 2025, allegato alla presente deliberazione di cui è parte integrante, è costituito da 5 misure di carattere programmatico ed organizzativo connotate dalla stabile

permanenza nei propri sistemi inserite con le modalità e le caratteristiche riportate nel seguito.

Impegno 1: implementazione di un sistema automatizzato di verifica delle autorizzazioni MIMIT e gestione avanzata del traffico non conforme.

"*RDCOM si impegna a sviluppare e integrare nella propria piattaforma Smpp3 una funzionalità che, prima di accettare e instradare traffico con Alias verso la rete nazionale, esegua una verifica automatica e in tempo reale, interfacciandosi con gli elenchi pubblici degli operatori autorizzati tenuti dal Ministero delle Imprese e del Made in Italy (MIMIT).*

Sul punto, si precisa ulteriormente che l'adozione di tale processo automatizzato è finalizzata a un duplice obiettivo: da un lato, incrementare l'accuratezza del controllo minimizzando l'incidenza dell'errore umano; dall'altro, ottimizzare l'efficienza operativa riducendo sensibilmente i tempi di verifica. La soluzione proposta garantisce dunque l'applicazione delle misure di blocco sul traffico non conforme con maggiore precisione e tempestività.

Nel caso in cui la suddetta verifica restituisse esito negativo (soggetto non autorizzato), il sistema adotterà in via primaria la misura del blocco automatico della messaggistica con codifica non decimale, cioè della messaggistica con Alias. Anche in questo caso, l'automatismo avrebbe il vantaggio di bloccare in tempi rapidi il traffico non conforme.

L'obiettivo è dunque quello di automatizzare e rendere certa l'applicazione dell'art. 7, comma 1, dell'Allegato A alla Delibera 12/23/CIR, garantendo che tutto il traffico SMS/MMS con Alias, ricevuto in qualità di Fornitore di Transito (FT), provenga esclusivamente da soggetti (FS o altri FT) in possesso della necessaria autorizzazione generale.

Resta inteso che, qualora gli elenchi pubblici del MIMIT non risultassero aggiornati, RDCOM si impegna comunque ad effettuare una valutazione del singolo caso in modalità non automatizzata, al fine di consentire il transito del traffico legittimo, previa verifica manuale della documentazione prodotta dall'operatore partner.

Tempi di attuazione: con riferimento alle tempistiche, si conferma l'implementazione di tali misure entro 30 giorni lavorativi dalla notifica del provvedimento finale.

Sul punto, si precisa ulteriormente che i tempi di lavorazione prevedono una fase iniziale di studio degli strumenti messi eventualmente a disposizione da parte del MIMIT (a titolo esemplificativo: accesso al database dell'albo dei soggetti autorizzati), i quali,

se disponibili, potrebbero determinare una riduzione delle tempistiche sopra indicate. In assenza di tali strumenti, si farà riferimento ai file pdf pubblicati sul sito ufficiale dell'Autorità."

- **valutazione sull'Impegno 1.**

Relativamente alla prima parte dell'"*Impegno 1*" ovvero sull'implementazione della funzionalità del blocco dell'*Alias* prima dell'instradamento, nel caso di soggetto non autorizzato la Società RDCOM ha evidenziato che la saliente novità consiste nell'implementazione di un controllo automatizzato e in tempo reale sugli elenchi dei soggetti autorizzati, superando il controllo manuale previsto dalla regolamentazione vigente. Si è in particolare sottolineato che il sistema, così organizzato e attivato, riceverà automaticamente gli aggiornamenti dagli elenchi pubblici e dalla collaborazione costante con gli operatori e soggetti terzi e sarà dunque in grado di bloccare il traffico non autorizzato in tempo reale *bypassando* in tal modo il più lento e la ben possibile incompletezza di informazioni tipiche di un sistema solo manuale. L'adozione di una procedura *software* va aldilà della "semplice" verifica manuale imposta dalla normativa attuale che dispone *sic et simpliciter* solo un obbligo di verifica.

Infatti la misura proposta e predisposta con l'implementazione descritta sostituisce la verifica manuale che sconta l'evidente limite connesso proprio alla modalità dell'aggiornamento soggetto ad un controllo da parte dell'operatore fisico sui sistemi e sui *data base* che generalmente, e nella migliore delle ipotesi, può essere svolto quotidianamente, semmai anche più di una volta, per aggiornare il *database* dei soggetti autorizzati (ad es. inserendo o eliminando il soggetto autorizzato o meno in base alla verifica sugli elenchi pubblici) ma ciò evidentemente non assicura un costante e più pervasivo intervento come quello invece proposto da RDCOM che avviene attraverso un sistema automatizzato che aggiorna costantemente ed in tempo reale lo stesso *database* agevolandone oggettivamente il controllo, ivi incluso ogni minimo cambiamento intervenuto sugli elenchi pubblici degli operatori autorizzati tenuti dal Ministero delle Imprese e del Made in Italy (MIMIT).

La misura, dunque, così implementata appare meritevole di accoglimento poiché oggettivamente appare connotata da una stabile permanenza nei sistemi della Società proponente e di indubbio miglioramento relativo all'attuale assetto regolamentare aggiungendovi un *quid pluris* oggettivamente apprezzabile.

Impegno 2: potenziamento dei sistemi anti-frode tramite analisi avanzata e intelligenza artificiale.

"*RDCOM si impegna a completare lo sviluppo e a mettere in produzione un sistema avanzato basato su intelligenza artificiale (AI) per l'analisi degli Alias e dei contenuti. Tale sistema, interrogato tramite API interne, includerà:*

a) il rilevamento di Alias fraudolenti: implementazione di algoritmi di ricerca semantica e corrispondenza di similarità per rilevare e bloccare varianti di Alias che imitano brand noti (es. "IntesaSanpa0lo" vs "IntesaSanpaolo");

b) la classificazione dei contenuti: messa in opera di un classificatore MLP (Multi-Layer Perceptron), addestrato internamente su dataset specifici, per identificare e bloccare messaggi con contenuti riconducibili a schemi fraudolenti. Sul punto, si chiarisce ulteriormente che l'"addestramento" consiste nel somministrare al modello campioni di traffico reale, che verranno classificati utilizzando algoritmi di riconoscimento del contenuto attraverso l'utilizzo di basi dati già classificati. La verifica dell'efficacia del modello passerà poi attraverso una fase di ottimizzazione, con successiva somministrazione diretta di campioni "critici" già riconosciuti come "falsi positivi" o "falsi negativi";

c) l'integrazione con fonti esterne: arricchimento dei database interni tramite l'integrazione con fonti community-driven (es. Tellows) per l'aggiornamento quasi in tempo reale di blacklist di URL e numerazioni sospette presenti all'interno del contenuto (a titolo esemplificativo, un messaggio contenente la frase "ottieni il tuo fantastico bonus del 30%, richiamaci al numero …" verrebbe bloccato qualora tale numerazione fosse presente nelle blacklist come indicatore di attività fraudolenta).

Al fine di garantire la massima trasparenza, RDCOM si rende altresì disponibile a consentire a codesta Autorità la visione delle modalità di funzionamento del sistema AI sviluppato, nell'ottica di un dialogo costruttivo e costante, previa assunzione da parte dell'Autorità medesima dei necessari obblighi di riservatezza a tutela dei diritti di RDCOM, ivi inclusi i relativi diritti di proprietà intellettuale.

L'obiettivo è innalzare il livello di sicurezza proattiva per prevenire fenomeni di spoofing, smishing e altre attività fraudolente.

Tempi di attuazione: con riferimento alle tempistiche, si propone l'implementazione di tali misure entro 60 giorni lavorativi dal completamento dell'impegno n. 1.

Sul punto, è opportuno precisare come la tempistica di cui sopra è giustificata e dipende, più che dall'implementazione iniziale degli algoritmi e dallo sviluppo dell'applicazione, dalla necessità di "addestrare" il sistema: ridurre i tempi di "addestramento" comporterebbe analisi meno precise, con conseguente e possibile

aumento di errori da parte del sistema (come bloccare Alias conformi o lasciare transitare Alias fraudolenti).

Se l'Autorità lo riterrà utile, RDCOM si rende comunque disponibile a produrre una "versione beta" del sistema con un anticipo di circa 10 giorni lavorativi rispetto alla tempistica sopra indicata, di modo che il relativo funzionamento possa essere valutato dalla stessa Autorità, pur tenendo presente che i risultati saranno inevitabilmente meno precisi rispetto a quelli che potrà ottenere la versione definitiva.".

- **Valutazioni sull'impegno 2**

Su siffatta iniziativa la società ha definito e soprattutto evidenziato la consistenza del "*potenziamento*" di cui è stata sostenuta l'efficacia.

Infatti RDCOM ha precisato a riguardo che il sistema non si limiterebbe al solo blocco dell'SMS, come visto relativamente al punto che precede, ma è basato sull'utilizzo anche di controlli antifrode basati su intelligenza artificiale finalizzata a verificare la congruità dei contenuti dei messaggi rispetto al mittente. La misura proposta, cioè, allestirebbe un sistema che si sviluppa, come descritto, in tre fasi, e di cui ai punti a; b) e c) del documento di impegni.

Infatti, al punto *a)* del documento è a dirsi che il sistema che la società si impegna a predisporre è utile a identificare numeri segnalati come fraudolenti e quindi bloccare i messaggi sospetti in tempo reale.

A tal riguardo la Società prevede l'implementazione di algoritmi di ricerca semantica e similarità per rilevare e bloccare varianti di *Alias* che imitano *brand* noti. Sul punto RDCOM ha altresì evidenziato che la rilevazione automatica di Alias alterati rappresenta un oggettivo vantaggio rispetto all'attuale controllo manuale svolto dal *team* dedicato di RDCOM. Il sistema antifrode automatizzato che, peraltro si sta già implementando, consente di bloccare tentativi di frode tramite Alias alterati che potrebbero sfuggire ai controlli manuali degli operatori autorizzati.

L'intervento di cui sopra è poi integrato dall'implementazione di cui al punto successivo *b).* In ordine a tale misura giova evidenziare che si procede con la classificazione anche dei contenuti dei messaggi recapitati con *Alias* tramite un modello di intelligenza artificiale che richiede l'addestramento e la popolazione del medesimo modello per mezzo di un classificatore basato su un ampio *dataset* di messaggi - sia legittimi che fraudolenti - per identificare e bloccare i tentativi, ad esempio, di *phishing* attraverso l'utilizzo di *Alias* provenienti da soggetti non legittimati e dunque già potenzialmente sospetti di veicolare messaggi scorretti. Naturalmente ciò prevede forme di collaborazione con autorità e operatori terzi, come definito al punto *c)* per l'integrazione del *database/classificatore* che necessita, come intuibile, dell'inserimento

di un volume considerevole di dati finalizzato a contemplare in modo quanto più vasto possibile la casistica delle fattispecie di messaggi illeciti.

A tal riguardo giova sottolineare che, al fine di inserire nel modello di AI il maggior numero di informazioni e dati, RDCOM ha anche avviato una *partnership* con una società tedesca specializzata nel raccogliere e catalogare casi significativi di tentativi di frode o CLI *spoofing*, anche attraverso lo scambio di informazioni ricevuti da soggetti privati che ne sono stati vittime. Ciò inevitabilmente incide sui tempi di realizzazione e messa a punto dell'implementazione della misura proposta che, così come indicato nel documento di impegni, è possibile completare in 90 giorni, ferma restando la disponibilità a consentire all'Autorità la visione delle modalità di funzionamento del sistema di AI sviluppato nell'ottica della massima trasparenza e collaborazione.

Si soggiunge a tal riguardo che anche la tempistica (60 giorni dall'implementazione dell'impegno "1") appare coerente con lo sviluppo di una iniziativa articolata e complessa, quale quella proposta, che però, una volta implementata, potrebbe rappresentare un valido modello risolutivo delle notorie criticità connesse al *CLI spoofing* e anche una soluzione estensibile ad altri soggetti compartecipi in tale segmento di mercato.

Infine, risulta apprezzabile in siffatto contesto anche l'atteggiamento particolarmente collaborativo della Società proponente che ha pure predisposto una soluzione "alternativa" (cd. *Beta*) qualora si ritenessero lunghi i tempi di attuazione dell'Impegno "2", ovviamente evidenziando una minore efficacia della misura connessa ad una minore quanto evidente "popolazione del sistema".

Impegno 3: collaborazione con operatori, terzi e Autorità.

"*RDCOM si impegna a promuovere attivamente l'interoperabilità e la condivisione delle proprie soluzioni tecnologiche, al fine di rafforzare la sicurezza dell'intero ecosistema delle comunicazioni elettroniche, attraverso le seguenti misure:*

a) condivisione e interoperabilità: RDCOM si impegna a rendere disponibili, su base volontaria, report aggregati periodici su Alias non conformi e traffico sospetto ad altri operatori del settore e alle Autorità competenti, contribuendo così alla creazione di un ecosistema più trasparente e sicuro;

b) supporto agli operatori: la Società si impegna a favorire l'interoperabilità con altri operatori autorizzati, condividendo prassi e standard tecnici finalizzati a garantire che il traffico venga instradato secondo criteri di sicurezza, affidabilità e conformità normativa;

c) supporto all'Autorità: RDCOM si rende disponibile a consentire l'accesso al sistema di intelligenza artificiale per l'analisi dei contenuti e degli Alias, da parte delle Autorità competenti. L'attivazione di tale funzionalità sarà subordinata all'adozione di adeguate misure di controllo degli accessi, tracciabilità delle interrogazioni, in conformità alla normativa vigente in materia di sicurezza e protezione dei dati, oltre che all'assunzione dei più ampi obblighi di riservatezza da parte delle Autorità medesime, a salvaguardia di ogni più ampio diritto di RDCOM;

d) educazione e strumenti per i clienti: la Società si impegna inoltre a sviluppare strumenti accessibili ai propri clienti per la verifica e registrazione degli Alias, nonché a promuovere campagne informative sull'importanza della conformità normativa nella gestione del traffico di messaggistica.

Tempi di attuazione: con riferimento alle tempistiche, si propone l'implementazione di tali misure entro 60 giorni lavorativi dal completamento dell'impegno n. 2.".

- **Valutazioni sull'impegno 3**

Anche con riferimento a tale iniziativa valgono le positive considerazioni svolte al punto che precede attesa l'evidente complementarità delle indicate misure con la complessità della struttura proposta. Risulta a tal riguardo positivamente apprezzabile l'aspetto di cooperazione che la Società è disposta a realizzare attraverso l'interlocuzione con i soggetti presenti nel segmento di mercato di riferimento aprendosi a una proficua quanto virtuosa collaborazione "*…condividendo prassi e standard tecnici finalizzati a garantire che il traffico venga instradato secondo criteri di sicurezza, affidabilità e conformità normativa"* e – non meno significativamente – l'apertura a verifiche anche molto penetranti da parte dell' Autorità finalizzata concretamente al rafforzamento della sicurezza al sistema delle comunicazioni elettroniche impegnandosi ad una apprezzabile disponibilità a rendere visibili – per coloro i quali lo richiedessero – i report periodici ed aggregati "*…su Alias non conformi e traffico sospetto ad altri operatori del settore e alle Autorità competenti*" contribuendo in tal modo a realizzare, attraverso un trasparente sistema di rapporti tra soggetti interessati, un sistema complessivamente più trasparente e sicuro.

In ordine a siffatte iniziative anche la tempistica proposta appare coerente, atteso che la Società proponente RDCOM ha però evidenziato che una contrazione dei tempi di realizzazione allo stato può rappresentare un realistico *vulnus* del sistema che si vuole realizzare correlato alla tipicità dello stesso ed in ragione della necessità di interfacciarsi con operatori, soggetti terzi ed istituzioni per il maggior popolamento possibile del

database e, quindi, della sua massima efficienza. Un tempo più ampio garantisce infatti una maggiore efficacia del sistema poiché maggiormente arricchito di dati.

Impegno 4: reporting e monitoraggio interno

" *RDCOM si impegna a fornire all'Autorità, con cadenza semestrale per i primi 12 mesi dalla notifica del provvedimento finale, una relazione contenente lo stato di attuazione degli impegni e le statistiche relative ai messaggi con Alias bloccati in conformità all'art. 7 della Delibera 12/23/CIR.*

L'obiettivo è garantire la massima trasparenza nei confronti dell'Autorità e consentire una facile verifica del rispetto degli impegni e della normativa vigente.

Con riferimento alle tempistiche, si propone l'invio della prima relazione al termine del primo semestre solare successivo alla notifica del provvedimento finale.".

Impegno 5: istituzione di una funzione di vigilanza indipendente

*Ai sensi dell'articolo 13, comma 5, dell'Allegato A alla Delibera n. 286/23/CONS, RDCOM si impegna a costituire una struttura indipendente (la "**Struttura**") per il monitoraggio della corretta esecuzione degli impegni, con l'incarico di fornire all'Autorità un resoconto semestrale sull'attuazione degli stessi, per un periodo di 12 mesi a decorrere dalla notifica del provvedimento finale.*

Con riferimento alla composizione e alle modalità di funzionamento della Struttura, RDCOM propone una struttura indipendente appositamente costituita, convocata in esito all'accoglimento degli impegni, composta – fermo restando diverse indicazioni da parte dell'Autorità – da due membri: un funzionario designato dall'Autorità e un dipendente di RDCOM.

Quanto al funzionamento della Struttura, saranno previste nel corso dei 12 mesi di validità dell'attività di vigilanza riunioni periodiche con frequenza almeno semestrale, nell'ambito delle quali verrà verificata la corretta implementazione degli impegni. La Struttura redigerà una relazione finale della propria attività di vigilanza da trasmettere all'Autorità al termine del periodo di validità degli impegni.

La misura risponde all'esigenza di agevolare il monitoraggio da parte dell'Autorità sull'attuazione degli impegni, ha una funzione di garanzia circa la stabilità delle misure nel tempo e assolve allo scopo di consentire un dialogo continuo e costruttivo sulle corrette modalità di implementazione degli obblighi.".

- ***Valutazioni sugli Impegni 4 e 5.***

Rileva su tali specifici punti, del documento definitivo di Impegni, che le misure ivi indicate ai punti 4 e 5 del documento e relative ai tempi di elaborazione di *report*, così

come relativamente alle caratteristiche dell'unità di monitoraggio, deputata alla verifica dell'adempimento da parte di RDCOM degli impegni assunti, si stabilisce in questa sede che, come di prassi, sia la tempistica dei *report* da fornire che la composizione dell'unità deputata al monitoraggio degli impegni assunti – la cui presenza è peraltro obbligatoria ai sensi e per gli effetti dell'articolo 13, comma 5, - sono definiti dall'Autorità in esito alla valutazione degli impegni stessi.

A tal riguardo, quindi, nell'ambito della definitiva decisione da assumersi per gli adempimenti da monitorare e relativamente all'impegno "5" riferito alla "*struttura*" deputata al monitoraggio si ritiene ammissibile la proposta composizione consistente di un rappresentante di RDCOM e di un funzionario di Agcom all'occorrenza supportato da un ulteriore funzionario per l'esame del dato tecnico.

Relativamente poi alla tempistica dei *report* appare accettabile anche l'invio del primo di questi dopo i primi 6 mesi di approntamento e implementazione delle misure che – come riferito nel documento – hanno tempi realistici di completamento di tutte le misure proposte di 5/6 mesi. Per siffatta ragione appare conseguentemente coerente disporre che il periodo di monitoraggio sia di 24 mesi complessivi decorrenti dalla notifica del provvedimento deliberativo.

Conclusioni

Richiamando le precedenti valutazioni di merito dei singoli impegni presentati si osserva che le misure contenute nell'intero documento risultano già *prima facie* e relativamente al contesto regolamentato, di tale conclusiva fase valutativa, complessivamente apprezzabili e altresì sintomatiche di un serio e stabile intervento da parte della Società proponente poiché rivelano non solo un carattere preventivo di contrasto al fenomeno oggetto di contestazione, ma l'estensione *pro futuro*, e dunque stabile, delle iniziative assunte con i correlati positivi effetti prodotti dagli interventi programmati per aggiungere un *quid pluris* all'attuale regolamentazione.

Le iniziative societarie soprattutto riferite negli impegni contrassegnati come "Impegno 1, 2 e 3" assumono poi particolare valenza poiché l'implementazione ulteriore del blocco automatico di tutte le chiamate di dubbia provenienza, attraverso un controllo che, svolto in tempo reale e con l'elaborazione di modelli che, attraverso l'utilizzo di AI, consentono un efficace aggiornamento su numerazioni e *blacklist* di URL sospetti.

A tanto si aggiunge che anche la popolazione di *database* e *dataset* sempre più ampi di elaborazione di casistiche utili a contrastare un fenomeno, che diventa sempre più aggressivo e sofisticato di manipolazione delle informazioni relative al CLI, anche riferite al mercato specifico - qui di interesse - dell'uso di SMS con *Alias.* Peraltro, proprio per la particolare tipologia di rapporti economici in cui essi sono utilizzati (banche,

organizzazioni, istituti pubblici, ecc.) quanto si propone di realizzare – da parte di RDCOM - merita particolare attenzione attesa la maggiore probabilità di veicolare - attraverso gli stessi SMS – tentativi molto aggressivi di *marketing* o di *spoofing* con intento fraudolento.

Il positivo apprezzamento condotto, non solo esaminando la documentazione ma anche il confronto con la Società stessa (svoltosi in audizione) fonda anche sulla manifestata e dichiarata disponibilità, rivelata da RDCOM, a collaborare fattivamente e proattivamente con l'Autorità – e specificamente attraverso l'Impegno 3 – consentendo l'accesso al sistema di AI approntato per l'analisi dei contenuti elaborati per le finalità sopra descritte in totale trasparenza.

Parimenti e infine non va trascurato il positivo effetto derivante dalla pubblicazione degli impegni che costituirà una *best practice* e un riferimento per gli altri operatori, i quali saranno indotti ad alzare la soglia della qualità delle proprie attività di monitoraggio sull'interconnessione transfrontaliera.

Tanto premesso, si ritengono ammissibili gli impegni presentati dalla società RDCOM s.r.l connessi al procedimento sanzionatorio Cont. n. 2/25/DRS vincolandola all'obbligo di esatto adempimento dei medesimi, risultando soddisfatti, sia i requisiti preliminari richiesti dalla regolamentazione vigente, sia quelli sostanziali, ivi inclusi quelli relativi all'unità di monitoraggio.

L'esame delle misure, così come presentate, nel loro insieme, contengono infatti i requisiti di miglioramento stabile richiesto per la loro ammissibilità potendo essere, dunque, per tali fini favorevolmente e definitivamente accolte poiché esse appaiono oggettivamente utili a migliorare le condizioni della concorrenza nel settore, rimuovendo le conseguenze anti-competitive dell'illecito attraverso idonee e stabili misure, atteso che quanto la società intende realizzare potenzia le attuali previsioni regolamentari di cui alla delibera n.12/23/CIR e, per l'effetto, comportano anche tangibili e sostanziali benefici per l'utenza finale in termini di connessa ed auspicabile riduzione delle chiamate di disturbo, oggetto di segnalazione o, quanto meno dei molesti tentativi di frode.

Definitivamente concludendo se ne delibera, quindi, l'approvazione, per le ragioni fin qui descritte, nonché l'esecuzione degli stessi con la pubblicazione sul sito *web* dell'Autorità del presente provvedimento con annesso il documento di impegni di RDCOM s.r.l. nella versione definitiva del 27 novembre 2025, e correlata sospensione del procedimento sanzionatorio Cont. n. 2/25/DRS ai sensi e per gli effetti dell'articolo 17, comma 6, del Regolamento;

VISTA la relazione sul procedimento di impegni della Direzione Reti e le risultanze istruttorie;

RITENUTO, in conclusione, che gli impegni definitivi presentati da RDCOM s.r.l. in data 27 novembre 2025 – allegati al presente provvedimento - risultano, ad una valutazione complessiva, idonei a migliorare le condizioni della concorrenza nel settore rimuovendo le conseguenze anticompetitive dell'illecito attraverso idonee e stabili misure;

RITENUTO, pertanto, di ordinare l'esecuzione e di disporre l'obbligatorietà dei suddetti impegni a carico della società proponente RDCOM s.r.l. ai sensi e per gli effetti dell'articolo 17, comma 6, del Regolamento di cui all'allegato "A" alla delibera n.286/23/CONS, in ragione della accertata loro meritevolezza rispetto ai fini previsti dalla legge, sospendendo, nel contempo, il procedimento sanzionatorio Cont. n. 2/25/DRS fino alla verifica dell'effettivo adempimento degli stessi;

UDITA la relazione del Commissario Antonello Giacomelli, relatore ai sensi dell'art. 31 del "*Regolamento concernente l'organizzazione e il funzionamento dell'Autorità*";

DELIBERA
Articolo unico
(Approvazione degli impegni di RDCOM s.r.l.)

1. Gli impegni presentati in data 27 novembre 2025 da RDCOM s.r.l., ai sensi dell'art. 13 dell'allegato "A" alla delibera n. 286/23/CONS, sono approvati e resi obbligatori per la società nei termini sopra descritti, ed allegati al presente provvedimento di cui costituiscono parte integrante e sostanziale.
2. L'Autorità esaminerà con cadenza periodica, e comunque per un periodo di 24 mesi dalla notifica del presente provvedimento, l'attuazione degli impegni attraverso l'unità di monitoraggio costituita con separato atto della Direzione reti e servizi di comunicazioni elettroniche.
3. Il procedimento sanzionatorio di cui all'atto di contestazione Cont. n. 2/25/DRS resta sospeso fino alla verifica dell'effettivo adempimento degli impegni.
4. RDCOM s.r.l. provvede alla esecuzione degli Impegni, nel rispetto dei termini indicati nel testo allegato al presente provvedimento. I suddetti termini decorrono dalla data di notifica del presente provvedimento alla società.
5. Ai sensi dell'art. della delibera n. 286/23/CONS, la mancata attuazione degli impegni comporta, previa diffida, la revoca del provvedimento di approvazione degli impegni stessi, la sanzione ai sensi dell'art. 30, comma 12, del Codice per l'inottemperanza all'ordine di esecuzione di cui al comma 1, e la ripresa del procedimento sanzionatorio per la violazione precedentemente contestata.

Il presente atto può essere impugnato davanti al Tribunale Amministrativo Regionale del Lazio entro 60 giorni dalla notifica dello stesso.

La presente delibera è notificata alla parte e pubblicata sul sito *web* dell'Autorità.

Roma, 26 febbraio 2026

IL PRESIDENTE
Giacomo Lasorella

IL COMMISSARIO RELATORE
Antonello Giacomelli

Per attestazione di conformità a quanto deliberato
IL SEGRETARIO GENERALE
Giovanni Santella