# REGIONE LIGURIA

**Comitato Regionale per le Comunicazioni**

**Deliberazione n. 32 del 16 novembre 2022**

Sono presenti i componenti del Comitato:

| | | |
|---|---|---|
| **TOFI** | Vinicio | Presidente |
| **ANSALDO** | Massimo | Componente |
| **CORRADO** | Leda Rita | Componente |

Svolge le funzioni di Segretario il funzionario Tiziana Salvatori

**Oggetto**: DEFINIZIONE DELLA CONTROVERSIA XXXXX XXXXX / FASTWEB SPA – PROCEDIMENTO GU14/488813/2022.

## IL COMITATO REGIONALE PER LE COMUNICAZIONI

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*";

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

VISTA la delibera n. 73/11/CONS, del 16 febbraio 2011, recante "*Regolamento in materia di indennizzi applicabili nella definizione delle controversie tra utenti e operatori*", di seguito denominato *Regolamento sugli indennizzi* come modificato da ultimo dalla delibera n. 347/18/CONS;

VISTA la delibera n. 203/18/CONS, del 24 aprile 2018, recante "*Approvazione del Regolamento sulle procedure di risoluzione delle controversie tra utenti e operatori di comunicazioni elettroniche*", come modificata, da ultimo, dalla delibera n. 390/21/CONS;

VISTA la legge della Regione Liguria 25 marzo 2013 n. 8, "Istituzione, organizzazione e funzionamento del Comitato regionale per le comunicazioni";

VISTA la Convenzione per l'esercizio delle funzioni delegate in tema di comunicazioni, sottoscritta tra l'Autorità per le garanzie nelle comunicazioni, il Consiglio regionale della Regione Liguria e il Comitato regionale per le comunicazioni ligure in data 19 dicembre 2017;

VISTA l'istanza dell'utente XXXXX XXXXX, del 08/01/2022 acquisita con protocollo n. 0004588 del 08/01/2022;

VISTI gli atti del procedimento;

CONSIDERATO quanto segue:

### 1. La posizione dell'istante

Nella propria istanza l'utente ha descritto la vicenda dedotta in controversia nei termini che seguono:

In qualità di intestatario della linea avente numero 324XXXX870, il signor XXXXX, dal mese di Luglio 2021, riscontrava le seguenti anomalie: riceveva da subito OTP per varie applicazioni e servizi commerciali che non ha mai né scaricato, utilizzato o creato account per esse ed in seguito notava addebiti per telefonate eseguite verso l'estero (Tunisia, Rep. Democratica del Congo...). Contattava più volte il call center di Fastweb ma senza trovare soluzione al problema. Nonostante il reclamo scritto Fastweb non riscontrava nulla. Il signor XXXXX è stato conseguentemente obbligato ad eseguire la disdetta, spiegando all'operatore dettagliatamente l'accaduto.

Richieste:

- Restituzione delle somme relative alle chiamate estere mai eseguite.

- Predisposizione equo indennizzo pecuniario.

REPLICA ISTANTE

Alla memoria dell'Operatore l'istante ha replicato con nota del seguente tenore:

"L'operatore, riferisce che i fatti oggetto dell'istanza non possano essere riconducibili ad una responsabilità di Fastweb, ma verso soggetti terzi; inoltre la compagnia telefonica ribadisce che la casistica non possa rientrare nelle competenze del Co.Re.com, quando il Co.Re.com stesso è messo a disposizione per la risoluzione delle controversie tra utenti e operatori telefonici. L'Autorità per le Garanzie nelle Comunicazioni è un'Autorità che svolge funzioni di regolamentazione e vigilanza nei settori delle telecomunicazioni. Posto che l'operatore non abbia dato alcuna prova di non avere avuto alcuna responsabilità su quanto è accaduto e soprattutto sulla salvaguardia dei dati personali e quindi non ha dimostrato in nessun modo di aver fatto tutto quanto necessario per impedire a soggetti terzi di ottenere la possibilità di utilizzare la linea intestata alla parte istante, si ritiene che, la violazione dei dati, possa considerarsi imputabile a Fastweb S.p.A, la quale avrebbe dovuto aver cura sia della custodia dei dati

personali, sia dei reclami eseguiti e in tal modo da constatare con quale metodo i cybercriminali, abbiano potuto riuscire a carpire i dati.

Preme precisare che la frode informatica possa essere avvenuta solo in conseguenza alla violazione dei dati personali del signor XXXXX. Prima di tutto, il nostro associato, contattava il Call Center di Fastweb, per riferire gli accadimenti e richiedeva il blocco delle chiamate verso l'estero. L'operatore non risolveva il problema e non dava neppure indicazioni utili a riguardo. La scrivente associazione inviata reclamo scritto tramite PEC, al quale l'operatore non si è prestato di rispondere; di conseguenza il signor XXXXX inviava la disdetta per la SIM reclamando l'accaduto e veniva avviata la conciliazione paritetica, anche al fine di ottenere documentazione che provasse che l'operatore avesse adottato tutti i sistemi di sicurezza utili all'inviolabilità dei dati del suo Cliente. Pur non essendo le paritetiche, sedi per integrazioni documentali, le stesse conciliazioni sono utili a valutare la controversia, onde evitare l'avanzamento della stessa in altre sedi e danno modo di poter replicare per la valutazione della casistica in maniera approfondita e raggiungere quindi un accordo. Tuttavia Fastweb S.p.A ha solamente provveduto a non ritenersi responsabile dell'accaduto, riscontrando con la sola frase: "i fatti non sono imputabili a Fastweb S.p.A ma a terzi".

Al fine di far comprendere i dettagli a codesta spettabile Autorità, si espone l'ordine cronologico della vicenda.

Il nostro aderente è stato presumibilmente vittima, di una truffa digitale realizzata attraverso l'acquisizione fraudolenta di dati personali. Soggetti terzi, sono entrati in possesso del numero di cellulare del signor XXXXX e il medesimo numero è stato utilizzato per inviare messaggi, per chat di whatsapp, creare account su vari siti e anche per eseguire chiamate verso l'estero, con – inoltre - la possibilità che la numerazione, possa essere stata utilizzata per altri scopi illeciti e per cui si è esposta opportuna querela onde evitare al consumatore, di essere accusato di presunti reati di profilo penale.

Il signor XXXXX era cliente Iliad Italia S.p.A e avendo già avuto questo problema con il vecchio operatore, riteneva utile passare a Fastweb S.p.A in quanto, esponendo il problema del caso a quest'ultima compagnia

telefonica, la stessa compagnia gli garantiva che un simile caso con Fastweb S.p.A non sarebbe potuto accadere, in quanto l'operatore sosteneva di avere un sistema operativo sicuro.

Avvenuto il passaggio da Iliad Italia S.p.A a Fastweb S.p.A, per due settimane, in effetti il signor XXXXX non riscontrava più anomalie. Successivamente, invece si trovava nuovamente con credito telefonico esaurito e con messaggi su whatsapp che non aveva mai inviato. L'app di Whatsapp, lo avvertiva del fatto che il numero di telefonia mobile – oggetto della controversia – non fosse più registrato sul suo telefono, ma su altro dispositivo.

Dal tabulato telefonico delle chiamate in uscita, è risultato che dalla numerazione di cui il signor XXXXX aveva titolarità, siano state effettuate chiamate con il suo numero di telefono verso numeri esteri.

Di conseguenza avvertiva subito l'operatore, che però gli confermava che non si riscontravano anomalie sulle chiamate in uscita.

Sembrerebbe che il nostro associato sia stato vittima presumibilmente di una tecnica usata per mettere in piedi un attacco informatico che viene definito come Port Out Scam.

In pratica il cyber criminale avrebbe eseguito una specie di portabilità di numero dalla SIM della vittima, alla sua.

In italiano questo attacco informatico è meglio noto come dirottamento della SIM, in quanto sposterebbe il numero di telefono dalla scheda SIM della vittima alla SIM del malintenzionato.

Il signor XXXXX eseguiva disdetta a Fastweb tramite PEC, essendo costretto quindi a rinunciare/perdere il suo numero di cellulare e spiegando i dettagli a Fastweb S.p.A e reclamando gli accadimenti, ma ancora senza ottenere nessun riscontro da parte dell'operatore. Eseguiva integrazione alla denuncia (allegato 3).

PREMESSO CHE: le normative europee e la legislazione nazionale di recepimento, si preoccupano di garantire la sicurezza dei dati personali imponendo specifici obblighi di protezione a carico anche delle compagnie telefoniche.

La vigente disciplina europea, fa riferimento alla tutela della privacy in particolare gli obblighi di protezione dei dati.

In particolare, giova analizzare la disciplina contenuta nel Regolamento UE 2016/679, del Parlamento Europeo e del Consiglio, del 27 aprile 2016, applicabile a decorrere dal 25 maggio 2018 e noto anche come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

La normativa in tema di protezione dei dati personali fornisce il quadro generale al quale devono ispirarsi i fornitori di servizi di pagamento per impedire l'accesso abusivo di terzi alle banche dati che custodiscono gli elementi identificativi dei propri clienti, in modo da scongiurare il possibile compimento di operazioni illecite.

Nell'ordinamento interno l'originaria disciplina della materia era contenuta nella legge 31 dicembre 1996, n. 675, adottata in attuazione della direttiva 95/46/CE ed abrogata, a decorrere dal 1° gennaio 2004, a seguito dell'entrata in vigore del Codice sulla Privacy, introdotto con il d.lgs. 30 giugno 2003, n. 196. Il Codice è stato poi integralmente riformato con il d.lgs. 10 agosto 2018, n. 101, che ha adeguato l'ordinamento nazionale al regolamento (UE) n. 2016/679, entrato in vigore il 25 maggio 2018, che ha abrogato la direttiva 95/46/CE. Pertanto, la materia è attualmente disciplinata sia dal Regolamento UE (GDPR), sia dal Codice Privacy, così come modificato ed adeguato alla normativa europea dal d.lgs. 101/2018. La normativa introdotta dal Regolamento europeo si concentra sul principio dell'accountability, che si sostanzia nell'obbligo posto in capo ai titolari del trattamento dei dati personali di valutare le informazioni in loro possesso ed il loro conseguente valore, al fine di approntare le misure tecniche ed organizzative, adeguate a mettere al sicuro tali dati. Il principio di accountability impone una gestione responsabile che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali, ai principi sanciti dal Regolamento e dalla legislazione nazionale.

Dalla normativa europea emerge chiaramente la volontà del legislatore di instaurare un apparato di tutela in relazione ai trattamenti effettuati, individuando i necessari oneri che il titolare del trattamento deve porre in

essere per assicurare il necessario standard di sicurezza, legislativamente previsto.

Rispetto al Codice Privacy del 2003, si abbandona l'intento di ancorare i titolari del trattamento a previsioni minime di sicurezza, diversamente preferendo la loro responsabilizzazione, affidando ad essi l'incarico di comprendere l'importanza dei dati in proprio possesso; di decidere autonomamente le misure tecniche ed organizzative che si ritengono necessarie per assicurare la effettiva tutela dei dati personali, in considerazione della realtà produttiva in cui si opera; di dimostrare di aver adottato i necessari adempimenti con l'osservanza delle adeguate misure, per soddisfare gli standard di tutela richiesti. A tal fine, l'art. 5 del GDPR prevede espressamente i principi generali applicabili al trattamento dei dati personali. In particolare, esso richiama i principi della liceità e correttezza, riprendendo altri concetti quali la trasparenza, la minimizzazione, l'esattezza, la limitazione di conservazione, l'integrità e la riservatezza.

L'operatore, è quindi tenuto ad adottare tutti quegli strumenti che siano inerenti al contesto di riferimento e che mettano al sicuro i dati in loro possesso. E nell'evolversi di questa controversia, Fastweb S.p.A non ha inserito alcuna prova che dimostri che abbia adottato le giuste misure di sicurezza, onde evitare la violabilità dei dati. Nonostante il reclamo nostro e la prima istanza di conciliazione, non è stata prodotta infatti alcuna documentazione che sollevi l'operatore da qualsiasi responsabilità. Nel definire le misure di sicurezza da adottare, il paragrafo 1 dell'articolo 32 prevede alla lettera b) "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e alla lettera c) "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico". Infine, la lettera d) prevede il ricorso ad una procedura che ha l'obiettivo di "testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento". Il secondo paragrafo dell'articolo richiede inoltre che si valuti "l'adeguato livello di sicurezza" e che si tenga conto dei rischi presentati dal trattamento che derivano "dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o

comunque trattati". Pertanto, la norma individua una serie di misure tecniche e di condotte che misurano il grado di diligenza che il responsabile del trattamento dei dati personali ha l'obbligo di adottare, dal punto di vista tecnico e organizzativo; nel contempo, essa pone in evidenza i rischi che potrebbero emergere dalla distruzione, dalla perdita o dalla modifica dei dati, e fa emergere la tipologia dei danni che potrebbero derivare dalla violazione dei necessari obblighi di protezione. Entrando invece nel merito delle richieste l'articolo 82 del Regolamento europeo sancisce al primo paragrafo che chiunque subisca un danno "materiale o immateriale" (ossia, patrimoniale o non patrimoniale), causato da una violazione del GDPR, ha diritto ad ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento dei dati personali. Viene così riconosciuta espressamente l'ammissibilità anche del danno non patrimoniale e vengono identificati gli elementi necessari per la nascita dell'obbligazione risarcitoria: la condotta attiva o quella omissiva contraria al regolamento; il danno; il rapporto causa-effetto tra questi. Il legislatore pone al centro della fattispecie il soggetto debole del rapporto, costruendo la disposizione attorno al danneggiato ed al suo diritto al risarcimento. Per quanto concerne le tipologie di danni risarcibili, l'art. 82 GDPR afferma che l'interessato può richiedere il risarcimento dei danni materiali e immateriali. In pratica dovrà essere risarcito ogni tipo di danno che l'interessato possa subire dalla violazione dei suoi dati personali, quali: la perdita del controllo dei dati personali; la limitazione dei loro diritti; il furto o l'usurpazione d'identità; perdite finanziarie; perdita di riservatezza dei dati personali; o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

RITENUTO CHE: ben sapendo che questa sede non possa riconoscere il risarcimento del danno, l'Autorità per le Garanzie nelle Comunicazioni svolge funzioni di regolamentazione e vigilanza nei settori delle telecomunicazioni e mette a disposizione questa piattaforma per la risoluzione delle controversie tra utenti e operatori di telefonia e potrebbe conseguentemente accertare quella che, stando a tutto quanto esposto e documentato dal signor XXXXX risulterebbe responsabilità dell'operatore e potrebbe quindi predisporre a sua valutazione indennizzo pecuniario relativo, consentendo inoltre e successivamente al consumatore, di adire

nelle sedi giudiziali per ottenere il risarcimento del danno. Per tutto quanto suesposto, la scrivente associazione a tutela dei consumatori RICHIEDE: a codesta spettabile Autorità, di accogliere l'istanza.

## 2. La posizione dell'operatore

Nella propria memoria l'Operatore ha evidenziato quanto segue:

"In via preliminare, Fastweb eccepisce l'inammissibilità dell'avversa domanda atteso che, come già rilevato nel corso del verbale di conciliazione paritetica, i fatti oggetto di istanza integranti gli estremi della presunta frode informatica: "non sono imputabili a Fastweb ma a terzi" e, conseguentemente, non rientrano nella competenza dell'Ill.mo Corecom adito, bensì dell'Autorità Giudiziaria ordinaria.
Inoltre, l'avversa prospettazione è generica, non supportata da alcuna prova documentale e come tale nulla. Peraltro, all'epoca dei fatti "luglio 2021" controparte non era ancora cliente Fastweb per la linea 3247448870, atteso che la relativa proposta di abbonamento è stata sottoscritta il 19.8.2021 e, da quanto sopra, deriva la carenza di legittimazione passiva in capo a Fastweb.

In ogni caso, Fastweb non è certo responsabile del presunto invio: "OTP per varie applicazioni e servizi commerciali che non ha mai né scaricato, utilizzato o creato account per esse", avendo ad oggetto il contratto unicamente i servizi telefonici. Se terzi non autorizzati hanno inviato otp e/o avviato non meglio specificati servizi commerciali non è imputabile a Fastweb. Né lo scrivente operatore è responsabile di presunte chiamate verso stati esteri di cui controparte non indica né la data né gli importi. Peraltro, come detto, il contratto mobile è stato sottoscritto il 19.8.2021 e nella prima fattura emessa dopo l'attivazione dell'utenza mobile non sono presenti addebiti per chiamate verso l'estero. Da ultimo, si evidenzia che è del tutto assente la prova di invio/ricezione dell'asserito reclamo.

Conclusivamente si insiste per il rigetto delle avverse domande, in quanto infondate in fatto ed in diritto."

## 3. Motivazione della decisione

Preliminarmente si osserva che l'istanza soddisfa i requisiti di ammissibilità e procedibilità previsti dall'art.14 del Regolamento.

Alla luce di quanto emerso nel corso dell'istruttoria, le richieste formulate dalla parte devono essere respinte come di seguito precisato.

Per quanto riguarda la richiesta di "Restituzione delle somme relative alle chiamate estere mai eseguite." non è possibile in quanto non vi è alcuna documentazione relativa a telefonate effettuate all'estero se non un elenco predisposto dall'Associazione UNC, che rappresenta l'istante, non suffragate da alcun documento probatorio.

Ai sensi della Delibera Agcom n. 70/12/CIR sull'onere della prova, questa ha stabilito che "La domanda dell'utente dovrebbe essere rigettata nel merito, qualora lo stesso non adempia l'onere probatorio su di lui incombente".

Inoltre la contestazione e la relativa richiesta di indennizzo pecuniario verte sulla presunta "truffa digitale realizzata attraverso l'acquisizione fraudolente di dati personali" come denunciato nella querela, presentata contro ignoti, dal Sig. XXXXX ai Carabinieri della Stazione di Ceva e ancora pendente. Proprio per la natura della problematica rappresentata, il Corecom, organo amministrativo, non è competente in materia, trattasi di un'attività di esclusiva pertinenza dell'Autorità Giudiziaria ordinaria. E, quindi, onere dell'istante richiedere l'intervento della magistratura per tutelare la propria posizione ed evitare eventuali utilizzi illeciti dei propri dati.

Infine, la possibilità di riconoscere il rimborso delle spese necessarie per l'espletamento della procedura, liquidate secondo criteri di equità e proporzionalità, è previsto dall'articolo 20, comma 6, del Regolamento che sancisce inoltre che nel determinare rimborsi ed indennizzi si tenga conto "del grado di partecipazione e del comportamento assunto dalle parti anche in pendenza del tentativo di conciliazione e può riconoscere altresì il rimborso delle spese necessarie e giustificate per l'espletamento della procedura liquidate secondo criteri di equità e proporzionalità".

Nel caso di specie, tenuto conto dell'integrale rigetto delle domande proposte dall'utente si ritiene che nulla può essere disposto a carico

dell'operatore in tal senso, atteso che non è stato accertato alcun addebito nei confronti dello stesso. Il mancato riconoscimento delle spese di procedura segue la soccombenza delle domande principali.

**DELIBERA**

**Articolo 1**

**1.** Per i motivi riportati in premessa, che qui si confermano integralmente, in merito all'istanza avanzata da XXXXX XXXXX il Comitato delibera il RIGETTO dell'istanza come sopra specificato.

**2.** Il presente provvedimento costituisce un ordine ai sensi e per gli effetti dell'articolo 98, comma 11, del d.lgs. 1° agosto 2003, n. 259.

**3.** È fatta salva la possibilità per l'utente di richiedere in sede giurisdizionale il risarcimento dell'eventuale ulteriore danno subito.

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 alle parti e pubblicata sul sito *web* dell'Autorità.

| IL SEGRETARIO | IL PRESIDENTE |
|---|---|
| Tiziana Salvatori | Avv. Vinicio Tofi |

*Documento prodotto in originale informatico e firmato digitalmente ai sensi del "Codice dell'Amministrazione Digitale" (D.Lgs. n.82/2005 e s.m.i.)*