

## Allegato B alla delibera n. 334/20/CIR

### DOCUMENTO DI CONSULTAZIONE

#### **I. Premessa**

Le vigenti norme nazionali (Codice delle Comunicazioni Elettroniche, art. 55, comma 7<sup>1</sup>) prevedono, nel caso di nuovi contratti di servizi di telefonia mobili e personali o nel caso di integrazione di contratti o di portabilità del numero per cambio operatore (MNP), l'identificazione del soggetto contraente da parte degli operatori di comunicazione elettronica anche nel caso di richieste effettuate per via telematica.

Tuttavia, a oggi, non sono esplicitamente previsti nella normativa vigente obblighi di identificazione dei clienti nell'ambito della fornitura di alcune prestazioni accessorie, quali la sostituzione di una SIM card, operazione spesso gestita presso un *dealer* dell'operatore.

La sostituzione della SIM può avvenire per diverse motivazioni, quali il deterioramento della card, la necessità di sostituzione del formato della SIM (incluso il caso di eSIM) nel caso di contestuale sostituzione dell'apparecchio telefonico con uno più moderno, furto o smarrimento della SIM e infine, come detto, nel caso della portabilità del numero in occasione di un cambio operatore.

Rispetto a tali fattispecie, di recente l'Autorità ha registrato un aumento preoccupante di segnalazioni di casi di sostituzione SIM, per passaggio ad altro operatore o per presunto furto o deterioramento, all'insaputa dell'utente finale titolare della SIM.

Sebbene siano già in corso attività per consentire di contrastare e prevenire fenomeni fraudolenti che coinvolgono direttamente, in particolare, gli istituti bancari, va tenuto in considerazione che fenomeni di sostituzione della SIM all'insaputa dell'utenza finale possano avere obiettivi diversi da quello di un furto di denaro eludendo le procedure di sicurezza nei servizi di *home banking* (c.d. *SIM swap*).

Infatti, la sostituzione della SIM di un utente da parte di un soggetto terzo non autorizzato e malintenzionato può permettere allo stesso di entrare in possesso anche di ulteriori dati riservati, rispetto a quelli utili per un effettuare un furto per via telematica presso gli istituti bancari, come per esempio il furto di dati personali sensibili utilizzati anche al fine di effettuare ulteriori attività dolose.

Nella fornitura di diversi servizi, attraverso l'utilizzo di reti telematiche, è prassi comune che gli utenti siano informati per *e-mail* o via SMS in tempo reale delle richieste di servizi

---

<sup>1</sup> Il Codice delle Comunicazioni Elettroniche, art. 55, comma 7, prevede che "Ogni impresa è tenuta a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che sono identificati prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.). Le predette imprese adottano tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici riportati su un documento di identità, nonché del tipo, del numero e della riproduzione del documento presentato dall'acquirente ed assicurano il corretto trattamento dei dati acquisiti. L'autorità giudiziaria ha facoltà di accedere per fini di giustizia ai predetti elenchi in possesso del centro di elaborazione dati del Ministero dell'interno".

in corso e, in particolare, in alcuni casi, dello stato di avanzamento e di ogni singolo passaggio della procedura necessaria per soddisfare la richiesta.

Tale prassi non è però abitualmente utilizzata nella fornitura di tutti i servizi o prestazioni connesse a quelli di comunicazione elettronica, come i servizi mobili. Una prestazione priva di informazioni di sicurezza sul processo in corso è proprio quello che riguarda la sostituzione di una SIM, che di solito avviene nei punti vendita commerciali con marchio degli operatori mobili, ma che potrebbe essere effettuata anche per via telematica.

Considerati, sulla scorta delle attività di vigilanza condotte a seguito della ricezione delle segnalazioni di tali truffe informatiche, gli effetti che questa carenza di sicurezza sta causando a un numero sempre crescente di utenti finali, risulta necessario, nel quadro regolamentare di riferimento per gli operatori di telefonia mobile, per un verso rendere maggiormente solidi i processi telematici di portabilità del numero mobile, per altro, introdurre delle procedure che prevedano la fornitura all'utente titolare della SIM di opportune notifiche sul cambio SIM in corso e connessi consensi, garantendo maggiore sicurezza delle operazioni e maggiori possibilità di controllo in caso di sostituzione di una SIM.

Tali misure appaiono ancora più necessarie considerato che, nella gestione di tali operazioni, non sussiste, a oggi, un'adeguata segregazione informatica dei dati sensibili sui clienti rispetto all'accesso da parte dei titolari dei punti vendita degli operatori mobili diffusi sul territorio nazionale, il cui operato non risulta facilmente controllabile da parte del fornitore del servizio mobile.

A tal fine, pertanto, si propone l'introduzione di nuove procedure che gli operatori di telefonia mobile dovranno seguire nel caso di sostituzione di SIM e, in generale, nell'ambito delle procedure di MNP, al fine incrementare la sicurezza dell'utenza.

## ***II. I principi ispiratori della proposta di regolamentazione***

La proposta di integrazione regolamentare dell'Autorità si basa principalmente sui seguenti principi:

1) estensione a tutti i casi di cambio SIM dell'obbligo di identificazione del soggetto a cui viene data in uso una SIM (fisica o tramite caricamento via etere del profilo su eSIM) sia presso il *dealer* sia in caso di richiesta per via telematica, attuando le vigenti norme in tema di identificazione. Ciò è dovuto al fatto che in alcuni casi di cambio SIM potrebbero non essere attualmente adottate le medesime procedure e ciò potrebbe costituire una possibile debolezza del sistema in termini di sicurezza;

2) in tutti i casi di sostituzione della SIM, il fornitore di servizi mobili deve verificare, mediante identificazione, che il richiedente sia il titolare del contratto. In particolare:

- nel caso in cui il cliente si rivolga, per la sostituzione della SIM, al proprio operatore, il *dealer* dovrà richiedere al cliente un documento di identità e la vecchia SIM (e trattenerla nel caso di immediata attivazione della nuova; a quanto noto, infatti, in questa fase si sono verificate frodi mediante falsificazione dei documenti o per mancata esibizione degli stessi, come sopra riportato al punto 1);

- nel caso in cui il cliente si rivolga per la sostituzione della SIM ad altro operatore, fermo restando che il cliente deve essere identificato ai fini del nuovo contratto e dovrebbe essere regolamentato l'obbligo di effettuare fotocopia della vecchia SIM, operazione abitualmente posta in essere, occorrerà valutare gli opportuni adeguamenti nell'ambito delle procedure per la portabilità del numero mobile per ridurre la probabilità di sostituzione non autorizzate di SIM richieste da soggetti diversi dal reale contraente (per errore o in caso di frode). Infatti, sulla base delle attuali procedure di MNP il rigetto della richiesta di passaggio si basa semplicemente o sulla verifica della correttezza dell'associazione del numero telefonico con il Codice Fiscale (casi di abbonamento) o con il numero seriale della SIM (casi di traffico prepagato). Un primo esempio di frode potrebbe essere quello messo in opera da un soggetto che richieda il passaggio di un numero di un altro cliente, comunicando il corretto numero seriale della vecchia SIM o il Codice Fiscale, appartenenti al suddetto legittimo cliente intestatario e di cui, il malintenzionato, è venuto a conoscenza. In tal caso la procedura di passaggio può andare a buon fine e va a riguardare un altro cliente che, per l'effetto, perde il numero. Al fine di rafforzare la sicurezza del processo, si ritiene necessario che tutti i dealer effettuino i necessari controlli sui documenti, ma anche che il rigetto della richiesta di MNP si basi, nell'ambito della procedura regolamentata, sulla verifica **sia del Codice Fiscale sia del numero seriale della SIM** considerando più complesso che vengano forniti entrambi corretti (anche grazie alla previsione di cui al punto 5);
- i due parametri (Codice Fiscale e numero seriale della SIM) sono già presenti nel sistema MNP e l'obbligo di presentazione, al dealer, di entrambi rafforzerebbe il controllo che, sulla base delle segnalazioni ricevute, se basato sul solo numero seriale della SIM si è rilevato insufficiente. Parimenti, l'utilizzo del solo Codice Fiscale risulta inadeguato in quanto facilmente individuabile da possibili frodatori. Pertanto, si ritiene che l'obbligo di presentare al dealer entrambi i dati possa incrementare la sicurezza del processo.

Il principio di cui sopra si applica, in particolare, nel caso di SIM smarrita o rubata laddove il cliente si rivolga, per la sostituzione, a un nuovo operatore richiedendo la MNP. Le attuali procedure di MNP non prevedono alcun controllo in caso di smarrimento della SIM. In tal caso potrebbe verificarsi un errore di portabilità laddove venga digitato, al momento di inserimento dell'ordine, un numero telefonico errato. Fermo restando l'obbligo di identificazione ai fini del contratto, in questo caso il cliente dovrà esibire, oltre alla denuncia, un documento con il Codice Fiscale. In tal caso la procedura di MNP dovrebbe sempre prevedere la verifica del Codice Fiscale (anche nel caso di traffico prepagato);

- In definitiva, sia nel caso in cui il cliente si rivolga al dealer del proprio operatore sia che richieda la MNP presso altro dealer, il dealer dovrà effettuare una copia di un documento d'identità del soggetto richiedente, di un documento attestante il Codice Fiscale, nonché della SIM o, eventualmente, della denuncia alle autorità competenti di smarrimento o furto della stessa. Per richieste per via telematica, oltre all'identificazione, come previsto dalle norme vigenti, dovrà essere previsto l'invio anche della copia della medesima documentazione richiesta in caso in cui ci si rivolga al dealer. La procedura di inserimento dati dovrebbe garantire, comunque,

l'impossibilità di finalizzare la stessa se non vengono caricati a sistema la scansione dei documenti citati;

3) in tutti i casi di sostituzione della SIM, il fornitore di servizi mobili invia sempre un messaggio SMS per informare il cliente che è stata richiesta la sostituzione della SIM e gli chiede conferma (a esempio mediante inserimento di una OTP) al fine di proseguire con le ulteriori procedure necessarie per esaudire la richiesta. In assenza di conferma esplicita, cosa che si verifica nei casi di SIM smarrita, rubata o guasta, si introduce un principio di attesa di un adeguato tempo (per esempio 72 ore) nel corso del quale il cliente, per altra via (ad esempio tramite e-mail o fornitura di un altro numero cellulare all'operatore) potrà essere informato del cambio SIM e, nel caso di cambio all'insaputa dell'utente, bloccare il processo.

A tal fine ai numeri mobili "principali" sono associati altri numeri mobili ed e-mail, validati con opportuna procedura di test, a cui verranno inviate le informazioni relative al processo di sostituzione della SIM, eventualmente limitando l'invio della OTP al solo numero principale e fornendo informazioni del processo ai numeri ed e-mail associati. Eventuali variazioni dopo l'adesione al contratto dei numeri ed e-mail associati dovrà avvenire sempre adottando criteri di sicurezza basati su OTP.

Ciò premesso, quando il cliente riceve l'informazione che si sta procedendo con la sostituzione della SIM, deve sempre avere la possibilità di bloccare tale processo in modo semplice, anche solo inviando un SMS ad un numero prefissato, concordato tra tutti gli operatori mobili e l'Autorità, con codice "40", ovvero chiamando il *customer care* e svolgendo la procedura in autonomia o parlando con un operatore, nonché accedendo ad un'area riservata sul sito *web* dell'operatore;

4) nel caso di numeri mobili utilizzati per servizi M2M, verso i quali le comunicazioni testuali sarebbero inefficaci, deve essere concordata ed individuata preventivamente con l'utente la numerazione a cui inviare una OTP per la conferma della propria volontà;

5) in generale, in tutti i casi di cui sopra, l'OTP inviata al cliente e il numero seriale della SIM sono gestiti dai sistemi degli operatori e non sono resi accessibili né al *dealer* né al *customer care* dell'operatore stesso, in quanto, essendo elementi riservati ed utilizzati per la validazione delle richieste di cambio SIM, la loro diffusione potrebbe essere causa di elusione dei sistemi di sicurezza previsti dalle norme;

6) il cliente, in generale, è informato dall'operatore a cui si è rivolto, via SMS e via e-mail, delle fasi di fornitura del servizio richiesto, anche in caso di rigetto della richiesta di MNP, riportando le motivazioni descritte nella delibera n. 147/11/CIR.