ADESSO GOOGLE PUÒ CONSERVARE ANCHE I NOSTRI SMS: ECCO QUALI SONO GLI IMPATTI SULLE INDAGINI ELETTRONICHE

Google ha atteso per anni che i singoli operatori mobili di tutto il mondo adottassero il protocollo RCS, che di fatto permette agli utenti di gestire gli SMS al pari dei messaggi scambiati con WhatsApp. A livello architetturale Google però impone l'introduzione di API per Jibe Cloud nelle reti degli operatori mobili a differenza di WhatsApp. A fine del 2019 Google ha deciso di non attendere oltre ed ha lanciato la funzionalità Chat nell'App "Messages" presente in tutti gli smartphone Android. Il provider RCS di Google è Jibe Mobile acquisito nel 2015. Leggendo i Termini del servizio di Jibe possiamo constatare che di fatto la gestione degli SMS è del tutto assimilabile ai messaggi di una chat, con la possibilità di allegare foto, video, audio e di conoscere lo stato degli altri utenti mentre digitano il messaggio. Sotto il profilo delle metodologie utilizzate nelle moderne indagini elettroniche questo rappresenta una svolta molto importante, poiché a Google adesso è affidato il compito di conservare i contenuti fino alla consegna del messaggio ai destinatari. Al contempo Google potrà tracciare le nostre attività mediante la formazione di metadati, che quindi andranno ad impoverire i classici tabulati di traffico telefonico nei quali gli SMS così scambiati non saranno più presenti. C'è anche un risvolto pratico per quanto attiene le classiche intercettazioni.

di Giovanni NAZZARO, *Lawful Interception Consultant* e *Security Manager*, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da 20 anni, esperto in *security*, *legal* e *compliance* in tali ambiti. Si occupa della progettazione dei sistemi d'intercettazione e di data retention e delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della "*Lawful Interception Academy*" dal 2014, è promotore della *LIA Certification* per la certificazione degli apparati e sistemi d'intercettazione e della formazione degli addetti alla funzione *Judiciary Authority Services (JAS)* presso gli operatori di telecomunicazioni mobili, fisse, wifi, satellitari. E' docente a contratto in Master Universitari di I e II livello.

Verso la fine di aprile di quest'anno è arrivata anche sugli smartphone Android italiani la compatibilità all'uso del protocollo RCS (Rich Communication Services) da parte di Google. L'App "Messages" per gestire gli SMS, e già pre-installata sugli smartphone, è stata aggiornata in modo che consentisse di gestire i messaggi anche tramite la rete dati, avvicinando di fatto l'utilizzo del classico SMS a quello tipico delle App più moderne come WhatsApp che permettono di allegare al testo immagini, audio o video.
La funzionalità che permette di inviare SMS su rete dati non è una novità, né tantomeno è stata rilasciata di recente per agevolare le comunicazioni in pieno periodo di restrizioni dei movimenti dovute al COVID-19: le prime applicazioni risalgono al mese di giugno 2019 in Inghilterra, Francia e Messico. Si tratta di un protocollo standardizzato per la prima volta dalla GSM Association (GSMA) nel 2007. Per molti anni la GSMA, Google e noi semplici utilizzatori siamo rimasti in attesa che gli operatori mobili attivassero il protocollo RCS ma probabilmente questi hanno atteso, per sfruttare al massimo questa tecnologia che di fatto permette loro un puro ricavo, dato che i classici SMS utilizzano i canali di segnalazione e quindi sono per loro a costo zero. D'altra parte i numeri non mentono (vedi figura 1).

Dalle stime pubblicate dalla GSMA sui volumi di SMS scambiati a livello mondiale il numero degli SMS risulta di 4 miliardi, cioè più del doppio rispetto ai messaggi scambiati con l'App "WhatsApp" che, da un certo punto di vista, deve la sua diffusione a partire dal 2009 proprio alla mancata applicazione del protocollo RCS. Infatti, se in passato fosse stato già presente un protocollo che permetteva di allegare foto e video al testo, WhastApp non si sarebbe diffuso fino a raggiungere, ad oggi, i 2 miliardi di utenti.

Nel 2019 Google ha deciso di non attendere oltre i singoli operatori mobili ed ha abilitato il protocollo RCS su tutti gli smartphone del mondo, sfruttando la propria App "Messages" ed erogando il servizio attraverso il proprio operatore Jibe Mobile (applicazione concreta della definizione "Over The Top" per Google). Agli operatori mobili tradizionali non è rimasto che adeguarsi e quindi sono passati ad un c.d. "profilo comune e universale" dei propri clienti, che ha permesso di interagire con gli utenti delle altre reti mondiali, in collaborazione con i produttori degli smartphone a cui le case madri affidano i processi produttivi, chiamati appunto Original Equipment Manufacturer (OEM).

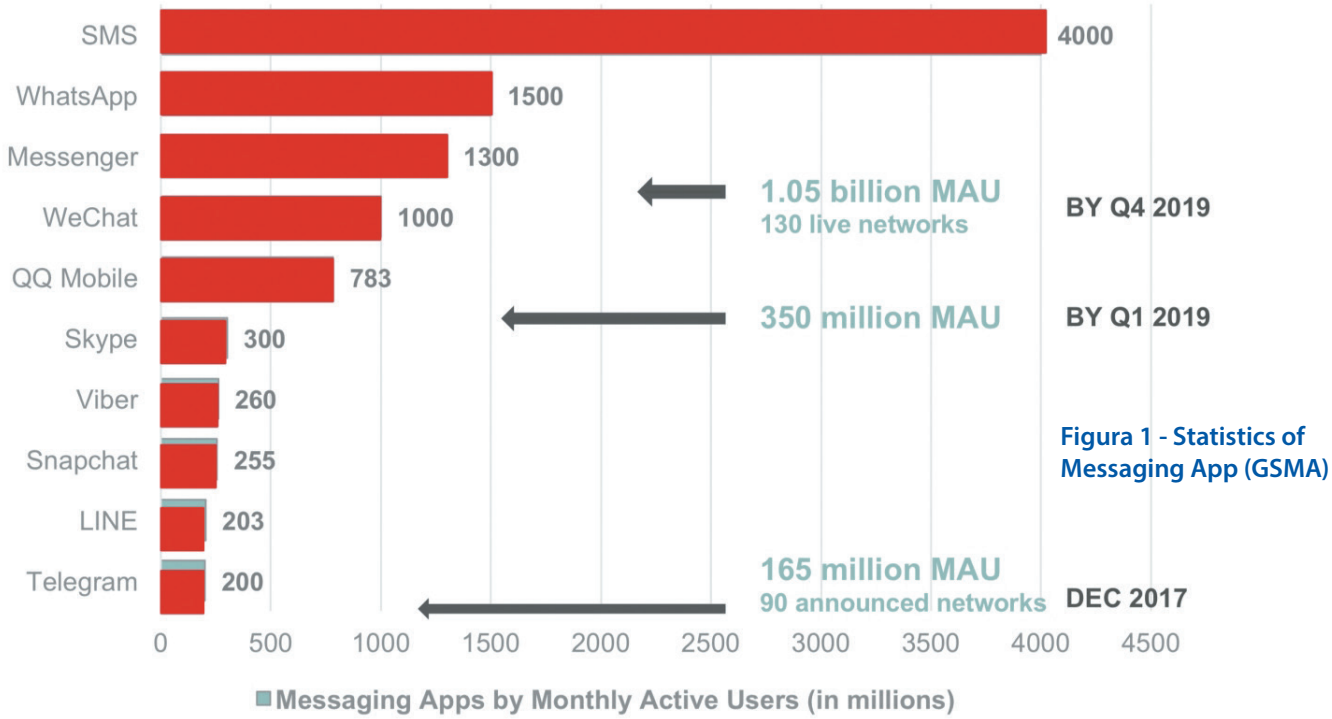

Figura 1 - Statistics of Messaging App (GSMA)

Il protocollo Rich Communication Services (RCS)

Il protocollo Rich Communication Services (RCS) è stato standardizzato dalla GSM Association (GSMA) per creare servizi di comunicazione inter-operatore basati sull'architettura IP Multimedia Subsystem (IMS). Questo aspetto costituisce la differenza principale rispetto ai servizi forniti dagli "Over The Top" (OTT) come ad esempio Viber, Whatsapp, ecc. IMS rende di fatto RCS uno standard universale, cioè interoperabile tra più fornitori di servizi, a differenza dei servizi degli OTT che invece sono utilizzati da comunità chiuse: per comunicare con un utente che ha Viber o Whatsapp dovremo utilizzare anche noi necessariamente la stessa App e la stessa architettura di rete.

Per RCS l'elemento di rete di base è IMS che consente la comunicazione peer-to-peer tra i client. Altri nodi di rete possono essere implementati dal Service Provider per fornire parti aggiuntive del set di funzionalità RCS.

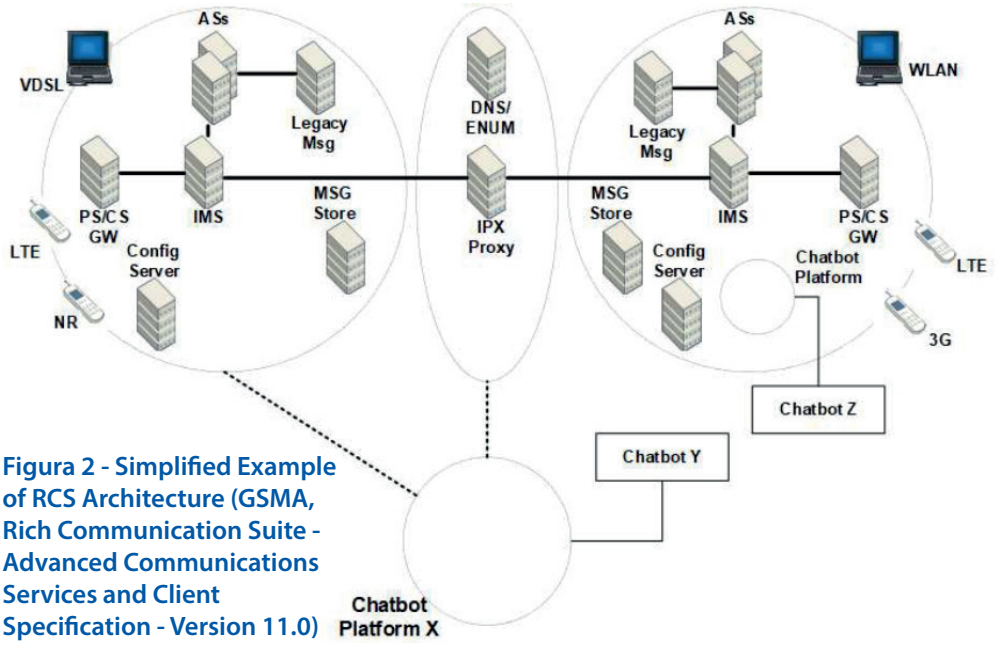

Figura 2 - Simplified Example of RCS Architecture (GSMA, Rich Communication Suite - Advanced Communications Services and Client Specification - Version 11.0)

La figura 2 illustra un esempio semplificato dell'architettura RCS: due fornitori di servizi RCS, a sinistra e a destra della figura, che si scambiano traffico tra loro attraverso l'IPX (IP Packet Exchange), al centro, utilizzando i meccanismi standard offerti dall'interoperabilità dell'Interfaccia Network-to-Network (NNI).

Il gateway PS / CS (GW) viene utilizzato per l'interazione tra la voce gestita dalla Circuit Switched (CS) e Packet Switched (PS), come ad esempio il Voice over Long Term Evolution (VoLTE). MSG Store è il server di archivio dei messaggi CPM (Converged IP Messaging). Legacy Msg si riferisce invece ai servizi Short Message Service (SMS) / Multimedia Message Service (MMS) che possono essere utilizzati tramite un IWF (Interworking Function) situato nel gruppo di Application Server (AS) che in aggiunta a questi può anche includere altre tipologia di nodi sfruttati dai servizi RCS, come ad esempio: Presence Server, Messaging Server, AS per il supporto della Funzionalità Chatbot.

La modalità per identificarsi sulla rete RCS dipende dal dispositivo utilizzato. Possiamo avere il classico smartphone (che lo standard chiama "primary device") in cui è presente una o più Subscriber Identity Module (SIM) associata alla propria numerazione telefonica (ad esempio IMPU / MSISDN). In questo caso l'App utilizzata (il client) può essere parte integrante dello smartphone ed è completamente integrato con le applicazioni native (rubrica, foto, galleria, browser di file, ecc.), come lo è l'APP "Messages" di Google, oppure può essere fornita da terze parti e quindi deve essere scaricata dal Play Store ed installata. In alternativa può essere utilizzato un dispositivo genericamente collegato ad Internet (chiamato dallo standard "secondary device") come ad esempio un computer portatile o un tablet senza SIM. Infatti, i servizi RCS possono anche essere implementati utilizzando un'identità non collegata alla rete mobile. In questo caso l'AS di turno dovrà utilizzare il tag "sip.instance" per l'identificazione. Utilizzando il protocollo SIP, RCS quindi non è immune al Caller ID spoofing. Proprio per tale motivo Google ha introdotto nella sua App la funzionalità di "SMS verificato".

Quando tale opzione è attiva e si riceve un SMS da un'azienda registrata su Google, il messaggio viene tradotto in un codice di autenticità leggibile solo dal nostro dispositivo. Google confronta questo codice con quello

inviati a Google dall'azienda. Se questi codici, detti anche hash del messaggio o HMAC (keyed-hash message authentication code) del messaggio, corrispondono allora Google conferma che il contenuto del messaggio è stato inviato dall'azienda e l'App "Messages" mostra informazioni sull'azienda, come il logo dell'azienda con un'icona "verificata".

L'App "Messages" di Google

L'App "Messagges" di Google per Android chiama le funzionalità offerte da RCS come "Chat", che è un nome più adatto e meno tecnico per i consumatori del servizio. L'attivazione delle funzionalità segue il principio di "opt-in": non appena è stata disponibile questa funzionalità gli utenti di Android hanno ricevuto una richiesta di aggiornamento della loro App per i messaggi. Anche l'attivazione successiva ha richiesto il consenso esplicito dell'utente.

Se stiamo utilizzando l'App di Google, compresi i servizi di RCS o di chat, vuol dire che abbiamo già accettato i Termini di servizio di Jibe Mobile di Google che chiariscono che le funzionalità di chat funzionano con i numeri di telefono, quindi possono coinvolgere altri fornitori di servizi, oltre al proprio. Utilizzando la "funzionalità di chat" si accetta che le capacità di utilizzo delle funzionalità da parte dei nostri contatti possano essere occasionalmente verificate per fornire il servizio stesso. Questo vuol dire che Google preleva di fatto la nostra rubrica.
È questo il dettaglio tecnico che caratterizza la già anticipata differenza principale tra RCS e altre App di chat: RCS non prevede un database centralizzato di chi possiede questa funzionalità, come invece accade per iMessage, per il quale Apple utilizza un database centrale chiamato "Apple Identity Service" che determina se la persona che stiamo contattando ha anche iMessage.

Questa opzione non è disponibile per RCS, perché utilizza un "modello federato" cioè un modello dove reti già esistenti di operatori diversi decidono di interconnettersi, ma ciascuno rimane responsabile dei server che consegnano i messaggi ai propri utenti. Questo vuol dire anche che non sarà più solo il nostro operatore a controllare la comunicazione dei nostri SMS. Nel dettaglio, quando si vuole inviare un nuovo SMS, avendo già abilitato la funzionalità chat, la nostra App invierà una query (notifica push) direttamente all'altro telefono. Questo "scambio di capacità" è stato definito come un modello "orientato ai punti", al contrario di quello di Apple per iMessage che è un modello basato sui server.

iMessage ci consente di ricevere il messaggio su tutti i nostri dispositivi contemporaneamente, a differenza di RCS che, essendo legato al numero di telefono, può recapitare il messaggio ad un solo dispositivo. La procedura di Google di utilizzo del Servizio, tuttavia, prende in considerazione anche il caso in cui ad un certo punto cambiamo smartphone: è possibile che il messaggio non arrivi al nuovo smartphone dove abbiamo trasferito la vecchia SIM. Nelle note circa la disattivazione del servizio, Google precisa che le funzionalità di chat potrebbero funzionare per circa 8 giorni dopo la rimozione della scheda SIM. In questo caso Google consiglia di disattivare la funzionalità di chat sul vecchio dispositivo oppure, se non è possibile farlo, perché è andato perso o rubato, attraverso un portale web dove occorre specificare il nostro numero di telefono. Questo vuol dire che l'associazione numero di telefono / dispositivo è temporanea ed è conservata da Google fino alla successiva verifica. È previsto infatti che Jibe invii di tanto in tanto un SMS per verificare il nostro numero di telefono. Questo aspetto potrebbe essere sfruttato da qualche male intenzionato per rubare i nostri SMS per un periodo di tempo limitato.

La piattaforma Jibe di Google

Il servizio è fornito dalla società Jibe Mobile con sede a Mountain View in California, ribattezzata così nel 2006 dall'iniziale Ascenna Mobile nata nel 2005, fondata da Amir Sarhangi (ex General Manager, Consumer Product Management in Vodafone Giappone) e Steve Schroeder con il finanziamento di Vodafone Ventures ed acquisita infine il 30 settembre 2015 da Google. Da settembre 2015 a febbraio 2019 Jibe Mobile ha lavorato per Google alla definizione dell'architettura, che ha consentito poi a tutti gli operatori mobili del mondo di interconnettersi, e allo stack protocollare per Android, che ha dato vita all'ultimo aggiornamento oggi disponibile per l'App "Messages", strumento di accesso ai servizi basati sul protocollo RCS.
Jibe consente ai classici operatori mobili di supportare il servizio RCS sulle loro reti senza

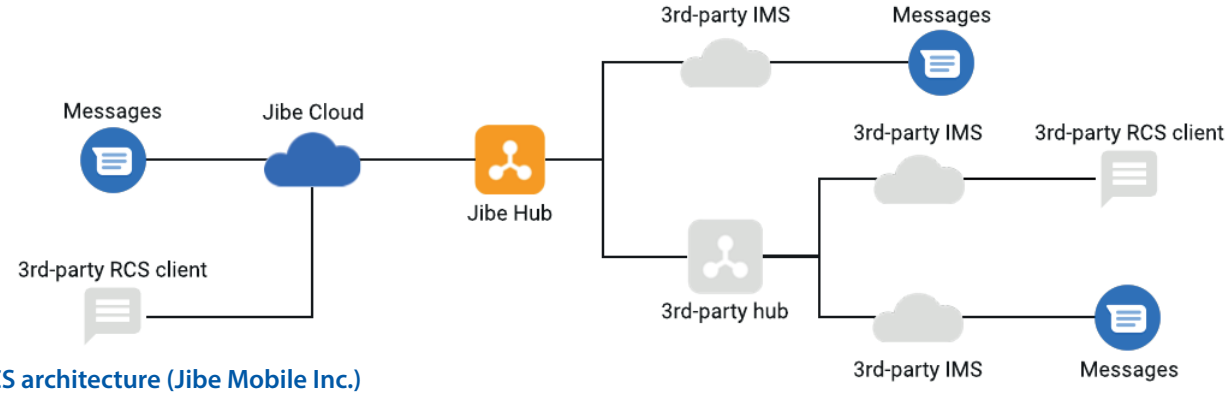

Figura 3 - RCS architecture (Jibe Mobile Inc.)

creare nuove infrastrutture. Il suo Hub, infatti, collega gli operatori abilitati, espande così la base di utenti e forza il disuso ai classici SMS. L'invio e la ricezione dei messaggi avviene tramite il backend RCS di Google via Internet, quindi potremo utilizzare il nostro smartphone sia tramite la rete mobile, ma anche utilizzando una qualunque rete Wi-Fi.

La piattaforma Jibe abilita il servizio RCS attraverso 3 componenti:

- Jibe Cloud che consente agli operatori mobili di supportare il servizio sulle loro reti senza creare nuove infrastrutture.;
- Jibe Hub che collega i gestori abilitati per RCS per espandere la base di utenti;
- le app "Messages" e "Carrier Services" per abilitare le funzionalità sui dispositivi Android.

Un SMS trasmesso tramite il protocollo RCS intraprende un processo in più fasi, passando attraverso le reti RCS di uno o più operatori mobili. Distinguiamo quindi due scenari, a seconda che mittente e destinatario appartengano o meno allo stesso operatore.

Quando un mittente e un destinatario si trovano sullo stesso operatore:

Figura 4 - RCS connections basic (Jibe Mobile Inc.)

- il mittente utilizza l'app "Messages" per inviare un SMS al destinatario;
- Jibe Cloud dell'operatore riceve il messaggio, determina che il destinatario utilizza il servizio cloud dello stesso operatore e consegna il messaggio al destinatario;
- il destinatario riceve il messaggio sul proprio dispositivo e può leggere e rispondere al messaggio nel proprio client RCS o nell'App "Messages".

Durante l'intero processo, Jibe Cloud si occupa anche di inviare una ricevuta di consegna al mittente quando il destinatario riceve il messaggio, una conferma di lettura una volta che il destinatario ha letto il messaggio ed un indicatore di digitazione mentre il destinatario compone una risposta.

Nel caso in cui l'operatore del mittente utilizza Jibe Cloud e l'operatore del destinatario utilizza un IMS di terze parti:

Figura 5 - RCS connections complex (Jibe Mobile Inc.)

- il mittente utilizza l'app "Messages" per inviare un messaggio RCS al destinatario;
- Jibe Cloud delll'operatore mittente riceve il messaggio, determina che il destinatario non è sullo stesso operatore e si connette a Jibe Hub;
- Jibe Hub inoltra il messaggio RCS al gestore del destinatario;
- il destinatario riceve il messaggio sul proprio dispositivo e può leggere e rispondere al messaggio.

Gli effetti sulle indagini elettroniche condotte dalle forze di polizia

Oltre agli aspetti appena esaminati, all'interno dei Termini di servizio di Jibe Mobile viene specificato anche che Google può scambiare le informazioni relative al nostro dispositivo, inclusi l'identificativo del dispositivo e gli identificativi caratteristici della scheda SIM, con gli altri operatori per verificare il nostro numero di telefono. Queste informazioni potrebbero essere conservate da Google per circa 1 mese anche dopo la disattivazione o l'inattività della funzionalità di chat.

L'aspetto rilevante a tal proposito è che la comunicazione è crittografata durante il trasporto ma non in tutti i punti, cioè il servizio non è completamente crittografato end-to-end quindi il nostro provider del servizio RCS potrà potenzialmente vedere il contenuto del messaggio e consegnarlo alle autorità competenti se richiesto. Il modello di funzionamento è analogo a quello che esiste oggi quando inviamo gli SMS tramite il consueto Centro Servizi (non preoccupatevi se l'App "Messages" vi dice che il numero di SMSC personalizzato è vuoto: per conoscere il numero del Centro servizi utilizzato o per modificarlo su uno smartphone Android occorre andare su Impostazioni>Info telefono>Stato>Rete>Numero centro SMS).

La possibilità di accedere ai contenuti in transito già esiste oggi, in quanto il nostro operatore mobile italiano potrebbe intercettare i contenuti degli SMS se l'autorità giudiziaria lo chiedesse mediante un opportuno decreto di autorizzazione. Con l'invio degli SMS tramite la funzionalità chat, così chiamata da Google, il nostro SMS utilizzerà la rete a pacchetto anziché quella a circuito, inoltre il provider del servizio non sarà più il nostro operatore mobile di appartenenza ma Jibe Mobile con sede in California. Di conseguenza il classico decreto italiano di autorizzazione alle intercettazioni telefoniche non sarà più sufficiente, occorrerà integrarlo con analogo decreto di intercettazione dati. L'operatore mobile italiano dovrebbe, tuttavia, adeguarsi in anticipo prima di poter accettare questo nuovo approccio, cioè dovrebbe **integrare i propri sistemi di Lawful Interception (LI) affinchè gestiscano il nuovo collegamento tra IMS Core Network e Jibe Cloud**. La modifica è necessaria in quanto nella sezione "In che modo proteggiamo i tuoi dati" nelle FAQ di Google, è precisato che le funzionalità di chat utilizzano la crittografia Transport Layer Security per proteggere i messaggi. Ciò significa che se si provasse ad intercettare i messaggi tra noi e Jibe, ad esempio sui nodi della rete del nostro operatore mobile, allora si visualizzerebbe solo del testo crittografato e illeggibile.

Se le funzionalità di chat sono fornite da Google ma il servizio RCS del destinatario viene fornito invece da un altro provider, i messaggi inviati verranno elaborati tramite il backend RCS di Google e poi indirizzati al servizio RCS del destinatario.

Per quanto attiene il trattamento dei contenuti da parte del provider, la logica di consegna degli SMS tramite protocollo RCS è la medesima utilizzata dal classico messaggio che sfrutta il Centro Servizi, nel senso che il messaggio è conservato dal provider fino a che il destinatario non diventa raggiungibile, fino ad un massimo di numero di ore che sceglie lo stesso provider. Jibe Mobile, e quindi Google, conservano i contenuti trasmessi fino alla consegna al suo destinatario. Tuttavia i tempi di conservazione possono superare ogni possibile previsione, fino ad arrivare all'indefinito, poiché occorre considerare che gli SMS inviati come chat possono coinvolgere un gruppo anche molto grande di persone e tutte contemporaneamente, non un unico destinatario. Quindi il periodo di conservazione dei contenuti deve estendersi fino a che tutti i partecipanti alla chat non avranno ricevuto il messaggio.
Nella sezione "In che modo e perché i tuoi dati vengono temporaneamente archiviati", sempre nelle FAQ di Google, scopriamo che il backend RCS di Google invia e archivia temporaneamente file come immagini, video, gif e adesivi con URL non decifrabili, generati in modo casuale. Questi URL non sono visibili a noi o alla persona che riceve il messaggio. Google blocca questo URL per impedire il collegamento tra il file ospitato ed il numero di telefono.
Non meno preoccupante sul piano degli adeguanti previsti dagli operatori mobili è la documentazione del traffico storico. Occorre subito dare avviso ai consulenti tecnici ed ai periti di parte che nelle cause in tribunale non troveranno più gli SMS che l'indagato invia o riceve nei tabulati di traffico telefonico, come avveniva fino ad oggi. Il nostro operatore mobile non avrà più visibilità dell'attività di invio e ricezione degli SMS se viene utilizzata la funzionalità di chat. Da una parte i clienti potranno aggirare così le tariffe commerciali che limitano ad un massimo prestabilito l'invio degli SMS, dall'altra parte questa funzionalità mette davvero in difficoltà le indagini elettroniche svolte su fatti accaduti nel passato. Anche su questo si auspica che gli operatori mobili trovino un adeguamento affinché queste informazioni non vadano perdute perché, in caso contrario, la soluzione alternativa rimane quella di contattare Google anche per lo storico degli SMS inviati e ricevuti dagli utenti degli operatori mobili italiani, con tutte le difficoltà che già conosciamo. ©