Martedì 6 Febbario 2024

Audizione informale del prof. Danilo Bazzanella nell'ambito dell'esame dello schema di decreto legislativo recante disposizioni correttive al decreto legislativo 8 novembre 2021, n. 207, di attuazione della direttiva (UE) 2018/1972, che modifica il decreto legislativo 1° agosto 2003, n. 259, recante il **codice delle comunicazioni elettroniche** (Atto n. 108).

Buongiorno,

sono il prof. Danilo Bazzanella, responsabile del gruppo di ricerca di Crittografia del Politecnico di Torino (CrypTO - https://crypto.polito.it) e componente del Senato Accademico del mio Ateneo. Oltre a insegnare nei corsi di Crittografia e di Blockchain nella Laurea Magistrale in Ingegneria Matematica e Informatica e nella nuova laurea magistrale in Cybersecurity, la mia attività di ricerca la crittografia e la matematica coinvolta nelle applicazioni crittografiche. Svolgo sia ricerca accademica di natura più teorica che attività di trasferimento tecnologico soprattutto a favore delle aziende del territorio piemontese.

Ringrazio l'onorevole presidente e gli onorevoli deputati per l'invito. È un piacere e un onore poter mettere la mia competenza al servizio della vostra attività.

Ho letto con attenzione lo schema di decreto legislativo riguardo le disposizioni correttive al Codice delle comunicazioni elettroniche.

Nel testo del decreto non ho identificato questioni dove la mia competenza tecnica possa essere rilevante, faccio però osservare che nel comma 6 dell'Art. 57, dedicato alle "prestazioni obbligatorie" per i soggetti autorizzati all'impianto ed esercizio di reti e servizi di comunicazione elettronica ad uso pubblico, si fa riferimento a un ulteriore decreto che deve precisare il "canone annuo forfettario per le prestazioni obbligatorie".

È riguardo a tale decreto che specifica il canone delle prestazioni obbligatorie che a mio parere si possono creare delle problematiche dovute alle caratteristiche dei metodi crittografici.

Andando nel dettaglio delle prestazioni obbligatorie c'è il rischio di richiedere prestazioni impossibili da effettuare per gli operatori delle telecomunicazioni, o possibili ma che possono rendere il servizio del tutto inefficiente o non sicuro per gli utenti.

È su questo punto che mi sentirei di fare le mie osservazioni tecniche, di natura crittografica.

Per loro natura i sistemi crittografici vengono costruiti in modo che la decifratura dei testi cifrati sia fattibile in un tempo ragionevole solo da chi possiede la relativa chiave segreta. Chi non possiede tale chiave per riuscire a decifrare i testi, anche con i più potenti calcolatori esistenti, impiegherebbe centinaia se non migliaia di anni di elaborazione. Quindi, di fatto, è impossibile decifrare i messaggi crittografati per chiunque non sia il legittimo destinatario del messaggio, cioè colui che conosce la chiave segreta.

Un operatore delle telecomunicazioni può sicuramente trovarsi nella situazione di trasmettere dei dati che contengono, anche a sua insaputa, dei messaggi cifrati con crittografia forte, quindi non decifrabile in nessun modo in tempi ragionevoli, e non è tecnicamente possibile che possa fornire il

testo in chiaro, anzi non è neppure in grado di capire se sta trasferendo un messaggio cifrato o una innocua serie di dati.

L'unica teorica soluzione sarebbe impedire l'utilizzo della crittografia forte da parte di tutti gli utenti, in modo che l'operatore delle telecomunicazioni possa sempre essere in grado di decifrare tutte le comunicazioni.

Questo però non è realizzabile, per motivi di sicurezza e tecnici:

- (di sicurezza) se non si utilizza la crittografia forte, non solo l'operatore delle telecomunicazioni può decifrare tutte le comunicazioni, ma anche tutti i malintenzionati, che per esempio potrebbero intercettare le comunicazioni degli utenti con la propria banca. Nel nostro mondo oramai così digitalizzato non possiamo fare a meno della crittografia.
- (tecnico) non sarebbe possibile verificare se un utente utilizza o meno la crittografia forte, perché è sostanzialmente impossibile distinguere messaggi cifrati con crittografia forte da innocue serie di dati.

Concluderei facendo una analogia che spero possa essere utile per inquadrare il problema. Dare l'obbligo agli operatori delle telecomunicazioni di decifrare tutti i messaggi che trasmettono, a prescindere dalla difficoltà o spesso l'impossibilità di tale operazione, sarebbe analogo a chiedere agli operatori telefonici di intercettare le comunicazioni telefoniche e tradurle in italiano prima di consegnarle all'autorità competente.

Consegnare le comunicazioni telefoniche è tecnicamente fattibile, tradurre qualsiasi dialogo telefonico in italiano sarebbe molto difficile se non sostanzialmente impossibile, oltre a esporre al rischio di errore. Analogamente si può certo chiedere a un operatore delle telecomunicazioni che fornisca tutti i dati che vengono trasmessi sulla propria rete, ma non la decifratura di tali dati.

Concludo quindi il mio intervento invitando a prestare attenzione all'elenco dettagliato delle prestazioni obbligatorie che si intende richiedere a un operatore delle telecomunicazioni, per evitare di inserire delle prestazioni che risultino molto difficili da eseguire o addirittura tecnicamente non eseguibili.

Grazie per l'attenzione.

Danilo Bazzanella
https://crypto.polito.it