Gentile Signore o Signora,

mi rivolgo a voi per esprimere le mie più profonde preoccupazioni in merito alla prevista risoluzione del Consiglio sulla crittografia[1] pubblicata dall'emittente austriaca ORF il 3 novembre 2020.[2]

La bozza di risoluzione **richiede soluzioni tecniche che consentano alle autorità nazionali di porre fine alla crittografia efficace e sicura end-to-end sui servizi di messaggistica privata**. I governi nazionali sono stati invitati a presentare il loro contributo entro giovedì 12 novembre a mezzogiorno. Successivamente, la Presidenza intende presentare il testo al Comitato permanente per la cooperazione operativa in materia di sicurezza interna (COSI) per l'approvazione il **19 novembre, in vista di un'ulteriore presentazione al COREPER II il 25 novembre, seguita dall'adozione da parte del Consiglio mediante procedura scritta**.

Non esiste un modo "equilibrato" di violare la sicurezza delle comunicazioni online, anzi, è tecnicamente impossibile concedere l'accesso a comunicazioni criptate in modo sicuro solo per scopi "leciti". Non appena i servizi di messaggistica consentiranno la decodifica delle comunicazioni private, ad esempio attraverso l'implementazione di backdoor o la fornitura di chiavi master, la sicurezza delle comunicazioni sarà infranta una volta per tutte - e non solo per gli scopi "legittimi" previsti dai governi nazionali. **Una volta che la crittografia sicura sarà infranta, si aprirà la porta allo spionaggio di massa da parte di servizi segreti stranieri e gruppi di hacker**. Chiunque sacrifichi la crittografia sicura per consentire le intercettazioni distruggerà la protezione dei segreti personali, dei segreti industriali e dei segreti di stato. Poiché la crittografia assicura evidentemente l'esercizio effettivo e la protezione della libertà di espressione e di opinione, qualsiasi violazione della crittografia può avere effetti negativi su questi diritti fondamentali[3].

In quanto tale, contrariamente a quanto sostenuto dalla Presidenza, **non esiste una via di mezzo tra la difesa dei "diritti fondamentali e la sicurezza digitale dei governi, dell'industria e della società" e la violazione della crittografia sicura end-to-end**.

Pertanto, faccio appello alla Sua responsabilità in quanto rappresentante dei servizi pubblici di **tutelare il diritto fondamentale alla privacy e alla sicurezza delle nostre infrastrutture di comunicazione digitale**, salvaguardando le nostre comunicazioni private da interferenze di terzi e delle autorità nazionali e respingendo la risoluzione proposta.

Cordiali saluti,

Riferimenti

[1] Consiglio dell'Unione Europea: "Progetto di risoluzione sulla crittografia -Sicurezza tramite crittografia e sicurezza nonostante la crittografia", 06 novembre 2020, disponibile al link: https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf

[2] Moechel, Erich: "Auf den Terroranschlag folgt EU-Verschlüsselungsverbot", ORF-Online, 08 November 2020, disponibile al link: https://fm4.orf.at/stories/3008930

[3] Davide Kaye: "Report of the UN-Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye", presented to the United Nations Human Rights Council, Twenty-Ninth Session on 22 May 2015, disponibile al link: https://www.undocs.org/A/HRC/29/32