



Estimado señor o señora,

Me pongo en contacto con usted para expresarle mi más profunda preocupación por la prevista Resolución del Consejo sobre la Encriptación [1] que ha sido publicada por la emisora austriaca ORF el 3 de noviembre de 2020. [2]

En el borrador de la resolución se pide que se busquen **soluciones técnicas que permitan a las autoridades nacionales romper la encriptación efectiva y segura de extremo a extremo en las comunicaciones privadas** a través de los servicios de mensajería. Se ha pedido a los gobiernos nacionales que envíen sus aportaciones antes del mediodía del jueves 12 de noviembre. Posteriormente, la Presidencia tiene la intención de presentar el texto al Comité Permanente de Cooperación Operativa en materia de Seguridad Interna (COSI) para su aprobación **el 19 de noviembre, con vistas a su presentación al COREPER II el 25 de noviembre, seguida de su adopción por el Consejo mediante procedimiento escrito.**

No existe una forma "equilibrada" de violar la seguridad de las comunicaciones en línea. Al contrario, es técnicamente imposible conceder acceso a las comunicaciones cifradas de forma segura sólo para fines "legales". En cuanto los servicios de mensajería permitan descifrar las comunicaciones privadas, por ejemplo mediante la implementación de puertas traseras o la provisión de claves maestras, la seguridad de las comunicaciones se romperá de una vez por todas, y no sólo para los fines "legítimos" previstos por los gobiernos nacionales. **Al romper la encriptación segura, se abrirá la puerta al espionaje masivo por parte de los servicios de inteligencia extranjeros y los grupos de crackers.** Cualquiera que sacrifique la encriptación segura para permitir la escucha, destruirá la protección de los secretos personales, los secretos de empresa y los de Estado. Como la encriptación garantiza evidentemente el ejercicio efectivo y la protección de las libertades de expresión y opinión, cualquier violación de la encriptación puede tener efectos perjudiciales sobre estos derechos fundamentales [3].

Como tal, contra lo que argumenta la Presidencia, **no hay un término medio entre la defensa de "los derechos fundamentales y la seguridad digital de los gobiernos, la industria y la sociedad" y la ruptura de la encriptación segura de extremo a extremo.**

Por lo tanto, apelo a su responsabilidad como representante de los servicios públicos para **defender y proteger el derecho fundamental a la privacidad, así como la seguridad de nuestra infraestructura de comunicaciones digitales**, salvaguardando nuestras comunicaciones privadas de la interferencia de terceros y de las autoridades nacionales, y rechazar la resolución propuesta.

Atentamente,

References:

[1] Council of the European Union: "Draft Resolution on Encryption - Security through encryption and security despite encryption", 06 November 2020, available at: 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, available at: <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, available at: <https://www.undocs.org/A/HRC/29/32>.