Consiglio
dell'Unione europea

Bruxelles, 24 novembre 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

NOTA

Origine:	Presidenza
Destinatario:	Delegazioni
n. doc. prec.:	12863/20
Oggetto:	Risoluzione del Consiglio sulla crittografia - La sicurezza attraverso la crittografia e nonostante la crittografia

Si allega per le delegazioni la risoluzione del Consiglio sulla crittografia.

ALLEGATO

Risoluzione del Consiglio sulla crittografia
La sicurezza attraverso la crittografia e nonostante la crittografia

1. Preambolo: la sicurezza attraverso la crittografia e nonostante la crittografia

L'Unione europea sostiene pienamente lo sviluppo, l'attuazione e l'utilizzo di una crittografia forte. L'Unione europea sottolinea la necessità di garantire il pieno rispetto dei diritti fondamentali, dei diritti umani e dello Stato di diritto in tutte le azioni connesse alla presente risoluzione, sia online che offline. La crittografia è uno strumento necessario per tutelare i diritti fondamentali e la sicurezza digitale dei governi, dell'industria e della società. Nel contempo, l'Unione europea deve garantire che le autorità competenti nel settore della sicurezza e della giustizia penale, quali le autorità di contrasto e giudiziarie, siano in grado di esercitare i loro legittimi poteri, sia online che offline, proteggendo le nostre società e i nostri cittadini.

Secondo le conclusioni del Consiglio europeo del 1° e 2 ottobre 2020 (EUCO 13/20), *l'UE farà leva sui suoi strumenti e i suoi poteri normativi per contribuire a definire norme e regole globali.* È stato convenuto che i fondi a titolo del dispositivo per la ripresa e la resilienza sarebbero stati utilizzati per perseguire, tra gli altri, gli obiettivi di *potenziare la capacità dell'UE di proteggersi dalle minacce informatiche, provvedere a un ambiente di comunicazione sicuro, soprattutto attraverso la crittografia quantistica e garantire l'accesso ai dati a fini giudiziari e di contrasto*.

2. Utilizzo attuale/stato della crittografia

Nel mondo odierno la tecnologia crittografica è sempre più utilizzata in tutti i settori della vita pubblica e privata. Si tratta di un mezzo volto a proteggere le persone, la società civile, le infrastrutture critiche, i media e i giornalisti, l'industria e i governi, garantendo la privacy, la riservatezza, l'integrità dei dati e la disponibilità delle comunicazioni e dei dati personali: risulta evidente che tutte le parti beneficiano della tecnologia crittografica. La crittografia è riconosciuta dalle autorità dell'UE responsabili della protezione dei dati e della cibersicurezza come un importante strumento che contribuisce, ad esempio, alla protezione dei dati personali trasferiti al di fuori dell'UE, ma soggetti all'obbligo di un livello di protezione sostanzialmente equivalente che, a parere della Corte di giustizia, costituisce un requisito giuridico per i trasferimenti di dati [1]. Non solo le applicazioni e i dispositivi elettronici sono sempre più programmati per crittografare per default i dati archiviati degli utenti, ma sempre più canali di comunicazione e servizi di archiviazione dei dati sono anche protetti dalla crittografia end-to-end. Tale evoluzione trova un riscontro positivo nella crescente risposta dell'industria della comunicazione e delle applicazioni, in cui la maggior parte delle applicazioni di messaggistica istantanea e altre piattaforme online hanno ugualmente attuato la crittografia end-to-end.

3. Sfide da affrontare per garantire la sicurezza

La "vita digitale" e il ciberspazio presentano non solo grandi opportunità, ma anche notevoli sfide: la digitalizzazione delle società moderne comporta alcune vulnerabilità e un potenziale di sfruttamento a fini criminali. I criminali possono così includere nel loro *modus operandi* soluzioni crittografiche facilmente accessibili e standardizzate, che sono progettate per scopi legittimi[2].

Al tempo stesso le autorità di contrasto dipendono in misura crescente dall'accesso alle prove elettroniche per combattere efficacemente il terrorismo, la criminalità organizzata, gli abusi sessuali su minori (in particolare gli aspetti online) nonché una serie di altre forme di cibercriminalità e di reati favoriti dall'informatica. Per le autorità competenti, l'accesso alle prove elettroniche può essere fondamentale non solo per condurre indagini efficaci e assicurare in tal modo i criminali alla giustizia, ma anche per proteggere le vittime e contribuire a garantire la sicurezza.

---

[1] Sentenza del 16 luglio 2020 nella causa C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

[2] IOCTA 2020, pag. 25

Tuttavia vi sono casi in cui la crittografia rende estremamente difficile o praticamente impossibile l'accesso al contenuto delle comunicazioni e la sua analisi, nell'ambito dell'accesso alle prove elettroniche, nonostante che l'accesso a tali dati sia legittimo. A prescindere dall'attuale contesto tecnologico, risulta pertanto fondamentale preservare i poteri delle autorità competenti nel settore della sicurezza e della giustizia penale attraverso un accesso legittimo che consenta loro lo svolgimento dei compiti secondo quanto prescritto e autorizzato dalla legge. Tali leggi che prevedono poteri esecutivi devono sempre rispettare pienamente il giusto processo e altre garanzie nonché i diritti fondamentali, in particolare il diritto al rispetto della vita privata e del carattere privato delle comunicazioni e il diritto alla protezione dei dati personali.

4. Trovare un giusto equilibrio

Il principio della sicurezza attraverso la crittografia e nonostante la crittografia deve essere rispettato nella sua interezza. L'Unione europea continua a sostenere una crittografia forte. La crittografia funge da ancora della fiducia nella digitalizzazione e nella tutela dei diritti fondamentali e dovrebbe essere promossa e sviluppata.

È di fondamentale importanza tutelare il carattere privato e la sicurezza delle comunicazioni attraverso la crittografia e, nel contempo, preservare la possibilità per le autorità competenti nel settore della sicurezza e della giustizia penale di accedere legalmente ai dati pertinenti per scopi legittimi e chiaramente definiti, nell'ambito della lotta contro le forme gravi di criminalità e/o la criminalità organizzata e il terrorismo, anche nel mondo digitale, e nel rispetto dello Stato di diritto. Le azione intraprese devono rispettare attentamente l'equilibrio tra tali interessi e i principi di necessità, proporzionalità e sussidiarietà.

5. Cooperare con l'industria del settore tecnologico

Mentre compie passi in avanti, l'Unione europea si adopera per instaurare un dibattito attivo con l'industria del settore tecnologico, associando la ricerca e il mondo accademico, al fine di garantire il proseguimento dell'attuazione e dell'utilizzo di una tecnologia crittografica forte. Le autorità competenti devono essere in grado di accedere ai dati in modo legittimo e mirato, nel pieno rispetto dei diritti fondamentali e delle pertinenti leggi in materia di protezione dei dati, preservando nel contempo la cibersicurezza. Le soluzioni tecniche che consentono l'accesso ai dati crittografati devono rispettare i principi di legalità, trasparenza, necessità e proporzionalità, compresa la protezione dei dati personali sin dalla progettazione e per default.

Poiché non esiste un unico modo per conseguire gli obiettivi fissati, i governi, l'industria, la ricerca e il mondo accademico devono collaborare in modo trasparente per conseguire tale equilibrio in modo strategico.

6. Quadro normativo

Potrebbe essere esaminata ulteriormente la necessità di elaborare un quadro normativo in tutta l'UE, che consenta alle autorità competenti di svolgere efficacemente i loro compiti operativi, tutelando nel contempo la privacy, i diritti fondamentali e la sicurezza delle comunicazioni.

Le potenziali soluzioni tecniche dovranno consentire alle autorità di esercitare i loro poteri di indagine, che sono subordinati alla proporzionalità, alla necessità e al controllo giurisdizionale in virtù della legislazione nazionale di dette autorità, rispettando i valori comuni europei, tutelando i diritti fondamentali e preservando i vantaggi della crittografia. Le possibili soluzioni dovrebbero essere elaborate in modo trasparente, in cooperazione con i fornitori di servizi di comunicazione nazionali e internazionali nonché con le altre parti interessate. Tali soluzioni e norme tecniche, così come la rapida evoluzione della tecnologia in generale, richiederebbero inoltre il continuo miglioramento delle capacità e competenze tecniche e operative delle autorità competenti affinché affrontino efficacemente le sfide poste al loro lavoro dalla digitalizzazione su scala mondiale.

7. Capacità di indagine innovative

Infine, è di fondamentale importanza migliorare il coordinamento a livello dell'UE al fine di:

1) unire gli sforzi di tutti gli Stati membri, delle istituzioni e degli organi dell'UE;

2) definire e stabilire approcci innovativi in considerazione delle nuove tecnologie;

3) esaminare adeguate soluzioni tecniche e operative; e

4) fornire una formazione su misura e di alta qualità.

Le soluzioni tecniche e operative connesse a un quadro normativo basato sui principi di legalità, necessità e proporzionalità dovrebbero essere sviluppate in stretta consultazione con i fornitori di servizi, le altre parti interessate e tutte le pertinenti autorità competenti, sebbene non sia opportuno prescrivere un'unica soluzione tecnica per dare accesso ai dati crittografati.