Consiliul
Uniunii Europene

Bruxelles, 24 noiembrie 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

NOTĂ

Sursă:	Președinția
Destinatar:	Delegațiile
Nr. doc. ant.:	12863/20
Subiect:	Rezoluția Consiliului privind criptarea – Securitate prin criptare și securitate în pofida criptării

În anexă, se pune la dispoziția delegațiilor Rezoluția Consiliului privind criptarea.

ANEXĂ

Rezoluția Consiliului privind criptarea
Securitate prin criptare și securitate în pofida criptării

1. Preambul: Securitate prin criptare și securitate în pofida criptării

Uniunea Europeană sprijină pe deplin dezvoltarea, punerea în aplicare și utilizarea unei criptări solide. Uniunea Europeană subliniază necesitatea de a asigura respectarea deplină a drepturilor fundamentale și a drepturilor omului, precum și a statului de drept în toate acțiunile legate de prezenta rezoluție, atât online, cât și offline. Criptarea este un mijloc necesar de protejare a drepturilor fundamentale, precum și a securității digitale a guvernelor, industriei și societății. În același timp, Uniunea Europeană trebuie să asigure capacitatea autorităților competente în domeniul securității și justiției penale, cum ar fi autoritățile de aplicare a legii și autoritățile judiciare, de a își exercita competențele legale, atât online, cât și offline, protejând societățile și cetățenii noștri.

În conformitate cu concluziile Consiliului European din 1-2 octombrie 2020 (EUCO 13/20), „UE își va exploata instrumentele și competențele de reglementare pentru a contribui la conturarea normelor și standardelor globale”. S-a convenit ca fondurile din cadrul Mecanismului de redresare și reziliență să fie utilizate pentru a promova obiective precum „sporirea capacității UE de a se proteja împotriva amenințărilor cibernetice, de a oferi un mediu de comunicare securizat, în special prin intermediul criptării cuantice, și de a asigura accesul la date în scopuri judiciare și de asigurare a respectării legii”.

2. Utilizarea/situația actuală a criptării

În lumea de astăzi, tehnologia de criptare este utilizată din ce în ce mai mult în toate domeniile vieții publice și private. Este un mijloc de a proteja persoanele, societatea civilă, infrastructurile critice, mass-media și jurnaliștii, industria și guvernele prin asigurarea respectării vieții private și a confidențialității, precum și prin asigurarea integrității datelor și a disponibilității comunicațiilor și a datelor cu caracter personal: este evident că toate părțile beneficiază de pe urma tehnologiei de criptare. Autoritățile UE responsabile cu protecția datelor și cu securitatea cibernetică au identificat criptarea ca fiind un instrument important care contribuie, de exemplu, la protecția datelor cu caracter personal transferate în afara UE, dar care face obiectul cerinței unui nivel de protecție în esență echivalent, care, potrivit Curții de Justiție, este o cerință legală pentru transferurile de date[1]. Nu numai că dispozitivele electronice și aplicațiile sunt programate din ce în ce mai mult să cripteze implicit datele stocate ale utilizatorilor, ci și din ce în ce mai multe canale de comunicare și servicii de stocare a datelor sunt de asemenea securizate prin criptarea de la un capăt la altul (E2E). Acest lucru se reflectă pozitiv într-un răspuns din ce în ce mai pregnant din partea industriei comunicațiilor și aplicațiilor, în cadrul căreia majoritatea aplicațiilor de mesagerie instantanee și a altor platforme online au pus în aplicare, de asemenea, criptarea de la un capăt la altul.

3. Provocări pentru asigurarea securității

„Viața digitală” și spațiul cibernetic prezintă nu numai oportunități importante, ci și provocări considerabile: digitalizarea societăților moderne aduce cu sine anumite vulnerabilități și potențialul de exploatare în scopuri infracționale. Astfel, infractorii pot include în modurile lor de operare soluții de criptare ușor accesibile, gata de utilizare, concepute în scopuri legitime[2].

În același timp, autoritățile de aplicare a legii depind din ce în ce mai mult de accesul la probe electronice pentru a combate în mod eficace terorismul, criminalitatea organizată, abuzul sexual asupra copiilor (în special aspectele sale online), precum și o varietate de alte tipuri de criminalitate informatică și infracțiuni facilitate prin mijloace informatice. Pentru autoritățile competente, accesul la probele electronice poate fi esențial nu numai pentru desfășurarea cu succes a anchetelor și, prin urmare, pentru aducerea infractorilor în fața justiției, ci și pentru a proteja victimele și a contribui la asigurarea securității.

---

[1] Hotărârea din 16 iulie 2020 în cauza C-311/18, Comisarul pentru protecția datelor/Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

[2] IOCTA 2020, p. 25.

Cu toate acestea, există situații în care criptarea face ca accesul la conținutul comunicațiilor și analiza conținutului acestora în cadrul accesului la probele electronice să fie extrem de dificile sau practic imposibile, în pofida faptului că accesul la astfel de date ar fi legal. Prin urmare, independent de mediul tehnologic existent la un moment dat, este esențial să se mențină prerogativele autorităților competente în domeniul securității și justiției penale prin asigurarea accesului legal în vederea îndeplinirii atribuțiilor ce le revin, astfel cum este prevăzut și autorizat prin lege. Astfel de legi care prevăd competențe de asigurare a respectării legii trebuie să respecte întotdeauna pe deplin garanțiile procedurale și alte garanții, precum și drepturile fundamentale, în special dreptul la respectarea vieții private în ceea ce privește comunicațiile și dreptul la protecția datelor cu caracter personal.

4. Găsirea unui echilibru adecvat

Principiul securității prin criptare și al securității în pofida criptării trebuie să fie pe deplin respectat. Uniunea Europeană continuă să sprijine o criptare solidă. Criptarea este o ancoră de încredere în ceea ce privește digitalizarea și în ceea ce privește protecția drepturilor fundamentale și ar trebui promovată și dezvoltată.

Protecția caracterului privat și a securității comunicațiilor prin criptare și, în același timp, menținerea posibilității ca autoritățile competente din domeniul securității și justiției penale să aibă acces în mod legal la date relevante în scopuri legitime, clar definite, în combaterea criminalității grave și/sau organizate și a terorismului, inclusiv în lumea digitală, precum și respectarea statului de drept sunt extrem de importante. Orice acțiune întreprinsă trebuie să pună atent în balanță aceste interese cu principiile necesității, proporționalității și subsidiarității.

5. Unirea forțelor cu industria tehnologică

Avansând, Uniunea Europeană se străduiește să stabilească o discuție activă cu industria tehnologică, asociind în același timp cercetarea și mediul academic, pentru a asigura continuarea punerii în aplicare și a utilizării unei tehnologii solide de criptare. Autoritățile competente trebuie să poată avea acces la date în mod legal și bine direcționat, cu respectarea deplină a drepturilor fundamentale și a legilor relevante privind protecția datelor, menținând în același timp securitatea cibernetică. Soluțiile tehnice pentru obținerea accesului la date criptate trebuie să respecte principiile legalității, transparenței, necesității și proporționalității, inclusiv principiul protecției datelor cu caracter personal din faza de proiectare și în mod implicit.

Întrucât nu există o modalitate unică de atingere a obiectivelor stabilite, guvernele, industria, cercetarea și mediul academic trebuie să colaboreze în mod transparent pentru a crea în mod strategic acest echilibru.

6. Cadrul de reglementare

Ar putea fi evaluată în continuare necesitatea de a dezvolta un cadru de reglementare la nivelul UE care să le permită autorităților competente să își îndeplinească atribuțiile operaționale în mod eficace, protejând în același timp viața privată, drepturile fundamentale și securitatea comunicațiilor.

Soluțiile tehnice potențiale vor trebui să le permită autorităților să își utilizeze competențele de investigare care fac obiectul proporționalității, necesității și supravegherii judiciare în temeiul legislației lor naționale, respectând în același timp valorile europene comune și drepturile fundamentale și menținând avantajele criptării. Eventualele soluții ar trebui să fie elaborate într-un mod transparent, în cooperare cu furnizorii naționali și internaționali de servicii de comunicații și cu alte părți interesate relevante. Astfel de soluții și standarde tehnice, ca, de altfel, și dezvoltarea rapidă a tehnologiei în general ar necesita totodată îmbunătățirea continuă a competențelor tehnice și operaționale și a expertizei autorităților competente pentru a aborda în mod eficace provocările digitalizării în activitatea lor la scară mondială.

7. Capacități de investigare inovatoare

În cele din urmă, este extrem de important să se îmbunătățească coordonarea la nivelul UE care vizează:

1) combinarea eforturilor tuturor statelor membre și ale instituțiilor și organelor UE;

2) definirea și instituirea unor abordări inovatoare având în vedere noile tehnologii;

3) analizarea unor soluții tehnice și operaționale adecvate și

4) furnizarea unei formări adaptate de înaltă calitate.

Ar trebui să se elaboreze, în strânsă consultare cu furnizorii de servicii, cu alte părți interesate relevante și cu toate autoritățile competente relevante, soluții tehnice și operaționale ancorate într-un cadru de reglementare construit pe principiile legalității, necesității și proporționalității, deși nu ar trebui să existe o singură soluție tehnică prescrisă pentru a oferi acces la datele criptate.