Az Európai Unió
Tanácsa

Brüsszel, 2020. november 24.
(OR. en)

13084/1/20
REV 1

LIMITE

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

FELJEGYZÉS

Küldi:	az elnökség
Címzett:	a delegációk
Előző dok. sz.:	12863/20
Tárgy:	A Tanács állásfoglalása a titkosításról – Biztonság titkosítással és biztonság a titkosítás ellenére

Mellékelten továbbítjuk a delegációknak a titkosításról szóló tanácsi állásfoglalást.

MELLÉKLET

A Tanács állásfoglalása a titkosításról
Biztonság titkosítással és biztonság a titkosítás ellenére

1. Preambulum: Biztonság titkosítással és biztonság a titkosítás ellenére

Az Európai Unió teljes mértékben támogatja az erős titkosítás fejlesztését, alkalmazását és használatát. Az Európai Unió hangsúlyozza, hogy az ezen állásfoglalással összefüggő tevékenységek során mind offline, mind online viszonylatban biztosítani kell az alapvető és az emberi jogok, valamint a jogállamiság teljes mértékben való tiszteletben tartását. A titkosítás nélkülözhetetlen eszközét képezi az alapvető jogok, valamint a kormányzat, az ipar és a társadalom digitális biztonsága védelmének. Az Európai Uniónak ugyanakkor biztosítania kell, hogy a biztonság és a büntető igazságszolgáltatás területén hatáskörrel rendelkező hatóságok, például a bűnüldöző és igazságügyi hatóságok mind online, mind offline gyakorolni tudják törvényes hatásköreiket a társadalom és a polgárok védelme érdekében.

Az Európai Tanács a 2020. október 1–2-i következtetéseiben (EUCO 13/20) megállapította, hogy *az EU fel fogja használni eszközeit és szabályozási hatásköreit a globális szabályok és normák alakításához való hozzájárulásra*. E következtetésekben az Európai Tanács azt is megállapította, hogy a Helyreállítási és Rezilienciaépítési Eszköz keretében rendelkezésre álló forrásokat olyan célok előmozdítására fogják felhasználni, mint például *az EU azon képességének javítása, hogy megvédje magát a kiberfenyegetésekkel szemben, biztonságos kommunikációs környezetet teremtsen különösen a kvantumtitkosítás révén, valamint hogy igazságszolgáltatási és bűnüldözési célokból biztosítsa az adatokhoz való hozzáférést*.

2. A titkosítás jelenlegi alkalmazása/állapota

A mai világban a titkosítási technológiát egyre szélesebb körben alkalmazzák, a köz- és a magánélet valamennyi területén. E technológia az egyének, a civil társadalom, a kritikus infrastruktúrák, a média és az újságírók, az ipar és a kormányzat védelmét szolgálja azáltal, hogy biztosítja a kommunikáció és a személyes adatok titkosságát, bizalmasságát, sértetlenségét és rendelkezésre állását: nyilvánvaló, hogy a titkosítási technológia alkalmazása valamennyi szereplő számára előnyös. A titkosításra az uniós adatvédelmi és kiberbiztonsági hatóságok olyan fontos eszközként tekintenek, amely hozzájárul többek között az EU-n kívülre továbbított személyes adatok védelméhez; ezen adattovábbítás feltétele, hogy a célország az uniós adatvédelemmel alapvetően egyenértékű adatvédelmet biztosítson, ami a Bíróság megállapítása szerint az ilyen adattovábbítás esetében jogi követelmény[1]. Egyfelől az elektronikus eszközöket és alkalmazásokat egyre inkább úgy programozzák, hogy a tárolt felhasználói adatokat alapértelmezetten titkosítva tárolják, másfelől egyre több kommunikációs csatornát és adattárolási szolgáltatást védenek végponttól végpontig terjedő (E2E) titkosítással is. Mindez a kommunikáció és az alkalmazások területén működő szereplők gyakorlatában is egyértelműen tükröződik: az azonnali üzenetküldő alkalmazások és az egyéb online platformok többsége esetében immár végponttól végpontig terjedő titkosítást alkalmaznak.

3. Kihívások a biztonság szavatolása terén

A „digitális élet” és a kibertér nemcsak nagy lehetőségeket nyújtanak, hanem jelentős kihívásokkal is járnak: a modern társadalmak digitalizációja bizonyos sebezhetőségeket eredményez, és a bűnözési célú visszaélés kockázatát hordozza. A bűnözők például a bűnelkövetéshez igénybe vehetnek könnyen megszerezhető, jogszerű célokra tervezett, kész titkosítási megoldásokat[2].

Ezzel párhuzamosan a bűnüldöző hatóságok számára egyre fontosabb az elektronikus bizonyítékokhoz való hozzáférés annak érdekében, hogy eredményesen tudjanak fellépni a terrorizmussal, a szervezett bűnözéssel, a gyermekek sérelmére elkövetett szexuális zaklatással (különösen annak online vonatkozásaival), valamint számos egyéb kiberbűncselekménnyel, illetve kibertérben elkövetett közönséges bűncselekménnyel szemben. Az illetékes hatóságok számára az elektronikus bizonyítékokhoz való hozzáférés elengedhetetlenül fontos lehet, méghozzá nem csupán a sikeres nyomozás és az elkövetők bíróság elé állítása, hanem az áldozatok védelme és a biztonság szavatolása szempontjából is.

---

[1] A Bíróság 2020. július 16-i ítélete, C-311/18. sz. Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems ügy, ECLI:EU:C:2020:559.

[2] iOCTA 2020, 25. o.

Bizonyos esetekben ugyanakkor a titkosítás rendkívüli módon megnehezíti vagy akár gyakorlatilag ellehetetleníti a kommunikációs tartalmak elektronikus bizonyíték felvétele céljából való elérését és elemzését, annak ellenére, hogy a hatóságoknak jogukban állna hozzáférni ezekhez az adatokhoz. Elengedhetetlen ezért, hogy a biztonsági és büntető igazságügyi hatóságoknak az aktuális technológiai környezettől függetlenül mindig módjukban álljon jogszerűen hozzáférni az ilyen adatokhoz feladataik ellátása keretében, törvényes felhatalmazásuknak megfelelően. A bűnüldözési jogköröket meghatározó jogszabályoknak minden esetben teljes mértékben tiszteletben kell tartaniuk a jogszerű eljárás követelményét és az egyéb biztosítékokat, csakúgy mint az alapvető jogokat, különösen a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot, valamint a személyes adatok védelméhez fűződő jogot.

4. A megfelelő egyensúly megteremtése

Biztosítani kell a „biztonság titkosítással és biztonság a titkosítás ellenére” elv maradéktalan érvényesülését. Az Európai Unió továbbra is támogatja az erős titkosítás alkalmazását. A titkosítás a digitalizációba vetett bizalomnak és az alapvető jogok védelmének az egyik alappillérét képezi, ezért azt terjeszteni és fejleszteni kell.

Rendkívül fontos, hogy titkosítással védjük a kommunikáció bizalmasságát és biztonságát, ugyanakkor fenntartsuk a jogállamiságot, valamint a biztonság és a büntető igazságszolgáltatás területén hatáskörrel rendelkező hatóságok lehetőségét arra, hogy a súlyos és/vagy szervezett bűnözés és a terrorizmus elleni – többek között a digitális világban folytatott – küzdelem során törvényes, egyértelműen meghatározott célokból hozzáférjenek a vonatkozó adatokhoz. Ezeket az érdekeket valamennyi meghozott intézkedés esetében gondosan egyensúlyba kell hozni a szükségesség, az arányosság és a szubszidiaritás elvével.

5. Összefogás a technológiai iparral

A haladás jegyében az Európai Unió aktív párbeszédre törekszik a technológiai iparral – bevonva a kutatási szereplőket és a tudományos köröket is –, az erős titkosítási technológiák folyamatos alkalmazásának és felhasználásának biztosítása érdekében. A kiberbiztonság garantálása mellett lehetővé kell tenni az illetékes hatóságok számára, hogy az alapvető jogok és a vonatkozó adatvédelmi jogszabályok teljes körű tiszteletben tartásával, jogszerűen és célzottan hozzáférjenek az adatokhoz. A titkosított adatokhoz való hozzáférésre szolgáló műszaki megoldásoknak meg kell felelniük a jogszerűség, az átláthatóság, a szükségesség és az arányosság elvének, beleértve a személyes adatok beépített és alapértelmezett védelmét is.

Mivel a kitűzött célok elérésének nincs egyetlen kizárólagosan helyes módja, a kormányzatoknak, az iparnak, a kutatásnak és a tudományos köröknek átlátható módon együtt kell működniük annak érdekében, hogy stratégiailag megteremtsék ezt az egyensúlyt.

6. Szabályozási keret

Tovább lehetne vizsgálni, hogy szükség van-e olyan uniós szintű szabályozási keret kidolgozására, amely lehetővé teszi az illetékes hatóságok számára operatív feladataik hatékony ellátását, ugyanakkor biztosítja a magánéletnek, az alapvető jogoknak és a kommunikáció biztonságának a védelmét.

A lehetséges technikai megoldásoknak lehetővé kell tenniük a hatóságok számára, hogy – a közös európai értékek tiszteletben tartása és az alapvető jogok védelme, valamint a titkosítás előnyeinek megőrzése mellett – gyakorolják vizsgálati hatásköreiket, amelyekre a nemzeti jogszabályok alapján az arányosság, a szükségesség és a bírósági felügyelet elve alkalmazandó. A lehetséges megoldásokat átlátható módon, a nemzeti és nemzetközi kommunikációs szolgáltatókkal és az egyéb érdekelt felekkel együttműködve kell kidolgozni. Az ilyen technikai megoldások és szabványok – és általában a technológia gyors fejlődése – szintén szükségessé tennék az illetékes hatóságok személyzete műszaki és operatív készségeinek és szakértelmének folyamatos javítását annak érdekében, hogy munkájuk során globális szinten hatékonyan tudják kezelni a digitalizáció jelentette kihívásokat.

7. Innovatív vizsgálati képességek

Végezetül rendkívül fontos az alábbiakra irányuló uniós szintű koordináció javítása:

1) valamennyi tagállam, valamint uniós intézmény és szerv erőfeszítéseinek egyesítése;

2) innovatív megközelítések meghatározása és kialakítása az új technológiák tekintetében;

3) megfelelő műszaki és operatív megoldások elemzése; valamint

4) személyre szabott, magas színvonalú képzés biztosítása.

A szolgáltatókkal, az egyéb érdekelt felekkel és valamennyi érintett illetékes hatósággal szoros együttműködésben műszaki és operatív megoldásokat kell kidolgozni a jogszerűség, a szükségesség és az arányosság elvére épülő szabályozási keret alapján, ugyanakkor a titkosított adatokhoz való hozzáférés biztosítására vonatkozóan nem célszerű egyetlen műszaki megoldást előírni.