Az Európai Unió
Tanácsa

Brüsszel, 2025. március 13.
(OR. en)

15941/2/24
REV 2

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

FELJEGYZÉS

Küldi:	az elnökség
Címzett:	a delegációk
Előző dok. sz.:	11281/24
Tárgy:	A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport zárójelentése

A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport társelnökei nevében az elnökség mellékelten továbbítja a delegációk részére a magas szintű munkacsoport zárójelentését.

Ez a felülvizsgált változat tükrözi a nyelvi felülvizsgálat során végrehajtott szerkesztési változtatásokat.

MELLÉKLET

A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport zárójelentése

2024. november 15.

Az alábbiakban kifejtettek kizárólag a magas szintű munkacsoportban részt vevő szakértők véleményét tükrözik, és nem tekintendők az Európai Bizottság vagy a Tanács hivatalos álláspontja kifejezésének.

A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport ajánlásainak végrehajtása során teljeskörűen tiszteletben kell tartani a tagállami hatásköröket. Az ajánlások kizárólag a bűnüldözési tevékenységekre, valamint az igazságügyi célokra használt kereskedelmi eszközökre alkalmazandók, és nem érintik a tagállamoknak a nemzetbiztonsággal kapcsolatos kizárólagos felelősségét. A szuverén eszközök, valamint a kizárólag nemzetbiztonsági célokra használt és/vagy kifejlesztett eszközök ezért nem tartoznak ezen ajánlások hatálya alá.

Tartalom

Összefoglaló

Az Európai Unió egy, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséget alkot, amelyben tiszteletben tartják az alapvető jogokat, valamint a tagállamok eltérő jogrendszereit és jogi hagyományait. Az EU magas szintű biztonságot[1] törekszik biztosítani olyan intézkedések révén, amelyek célja a bűnözés megelőzése és üldözése, illetve a bűnüldöző, igazságügyi és más illetékes hatóságok közötti koordináció és együttműködés megkönnyítése.

A technológiai fejlődés, valamint társadalmaink digitalizációja jelentősen megváltoztatta a polgárok mindennapi életét, a bűnüldöző és az igazságügyi hatóságokat pedig új kihívások elé állította a magas szintű biztonság biztosítása terén, nemzeti és uniós szinten egyaránt. A jelenlegi digitális korban szinte minden bűnügyi nyomozásnak van digitális eleme. Ez a szempont a hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport 2023. áprilisi keretdokumentumában is megjelenik:

> A technológiákkal és eszközökkel […] bűncselekmények céljából is visszaélnek. E fejlemények nyomán egyre nagyobb kihívást jelent a hatékony bűnüldözés fenntartása az EU-ban a közbiztonság védelme, valamint a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása, továbbá az áldozatok igazságszolgáltatással és kártérítéssel kapcsolatos jogos elvárásainak való megfelelés céljából. Ha nem lépünk fel a megfelelő módon ezzel a tendenciával szemben, fennáll annak a valós veszélye, hogy az lehetőséget nyújt a bűnözők számára a „sötétben” rejtőzködésre […]. Ez komoly fenyegetést jelent az egyének és a társadalom biztonságára nézve, és végső soron akadályozhatja az állam azon pozitív kötelezettségének teljesítését, hogy továbbra is biztosítsa a jogállamiságot és a társadalom demokratikus működését[2].

[1] E dokumentum alkalmazásában a „biztonság” a bűnözés elleni küzdelmet, illetve a közbiztonságot fenyegető veszélyek megelőzését jelenti.

[2] 8281/23, 2023. április 13.

Az Európai Unió Alapjogi Chartája garantálja a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való jogot, valamint a személyes adatok védelméhez való jogot. A közlések titkossága – függetlenül attól, hogy írásban vagy telefonon közölt információkról van-e szó – a demokratikus társadalmak egyik fő vívmánya, amely biztosítja, hogy sem az állam, sem magánszereplők ne avatkozhassanak be az emberek véleménynyilvánítási szabadságába, és lehetővé teszi egy virágzó civil társadalom létrehozását. E jogok gyakorlása jogi keretek között korlátozható, különösen a nemzetbiztonság, a nemzetvédelem vagy a közbiztonság védelmét célzó intézkedésekkel összefüggésben, valamint a bűncselekményeknek, illetve az elektronikus hírközlési rendszerek jogosulatlan használatának a megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása érdekében, amennyiben az ilyen intézkedések egy demokratikus társadalomban szükségesnek, megfelelőnek és arányosnak minősülnek. Ezért a bűnüldöző és igazságügyi hatóságok megnyithatnak és olvashatnak írásbeli közléseket, lehallgathatnak telefonhívásokat és belehallgathatnak beszélgetésekbe, feltéve hogy az szükségesnek, arányosnak és indokoltnak minősül, és hogy az ilyen intézkedések összhangban vannak az alkalmazandó jogi rendelkezésekkel, továbbá azokat az alapvető jogok kellő tiszteletben tartásával hajtják végre. Erre a technológiai fejleményektől függetlenül valamennyi illetékes hatóság számára lehetőséget kell biztosítani. A személyközi kommunikáció új formáinak az elmúlt években tapasztalt elterjedése azzal jár, hogy a társadalom egészének új realitásokhoz kell alkalmazkodnia. Fenn kell tartanunk a polgárok közötti kommunikáció védelmét, ugyanakkor azt is biztosítanunk kell, hogy a bűnüldöző és az igazságügyi hatóságok továbbra is eleget tudjanak tenni a polgárok védelmére vonatkozó kötelezettségüknek a súlyos és szervezett bűnözés, valamint a terrorizmus megelőzése és az azok elleni küzdelem révén. Sürgősen alkalmazkodnunk kell, és a szakértők haladéktalan cselekvésre szólítják fel a politikai döntéshozókat, mivel a bűnüldöző hatóságok már most sem tudnak lépést tartani a technológiai fejlődéssel, ami közvetlenül befolyásolja a polgárok jogainak védelmére való képességüket.

A bel- és igazságügyi miniszterek a 2023. január 26-i nem hivatalos ülésükön megvitatták, hogy a technológiai fejlemények milyen kihívások elé állítják a bűnüldözést a digitális korban. Ezenkívül aggodalmukat fejezték ki amiatt, hogy az alkalmazandó szabályok és azok értelmezése az ítélkezési gyakorlatban, továbbá a gyakorlati és az operatív akadályok egyre nehezebbé teszik a bűnüldöző hatóságok számára munkájuk elvégzését, különösen a bűncselekmények nyomozásához és a vádeljárás lefolytatásához szükséges adatok megőrzése és az azokhoz való hozzáférés terén[3].

[3] Lásd a 2023. március 23-i 7184/1/23 REV 1 dokumentumot és a tagállamok abban foglalt észrevételeit.

E megbeszélést követően a Tanács jóváhagyta egy olyan csoport létrehozását, amelynek feladata, hogy kidolgozzon egy stratégiai szempontú, előretekintő jövőképet arra vonatkozóan, hogy az igazságügyi és bűnüldöző hatóságok a digitális korban miként tudnak hatékonyan és jogszerűen hozzáférni az adatokhoz, az elektronikus bizonyítékokhoz és az információkhoz: ennek nyomán létrejött **a hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport**[4].

A magas szintű munkacsoport célja az volt, hogy megoldásokat találjon a következő kihívásra: annak érdekében, hogy az EU-ban élő valamennyi személy számára biztosítani lehessen a magas szintű biztonságot, lehetővé kell tenni az adatokhoz való jogszerű hozzáférést, ugyanakkor hatékony és időtálló megoldások révén biztosítani kell az alapvető jogok tiszteletben tartását, beleértve a magánélet tiszteletben tartásához és az adatvédelemhez való jogot, továbbá a magas szintű kiberbiztonságot.

A magas szintű munkacsoport munkájának fő eredményét jelentő **42 ajánlás**[5] olyan időszakban született, amikor az online elszámoltathatóság egyre inkább elvárás. Az ajánlások a jelenlegi kihívások mellett a technológiai fejlődés tükrében várható jövőbeli kihívásokra is kiterjednek, céljuk pedig, hogy lehetővé tegyék egy olyan átfogó uniós megközelítés kialakítását, amely a hatékony bűnügyi nyomozások és vádeljárások biztosítását szolgálja. Az ajánlások a következő három témakör köré szerveződnek: **kapacitásépítés; az iparral való együttműködés és szabványosítás; valamint jogalkotási intézkedések.** Kiemelik azokat a kihívásokat, amelyekkel a bűnüldöző szervek szembesülnek a bűnügyi nyomozások során az olvasható formátumú adatokhoz való hozzáférés terén a harmonizált adatmegőrzési kötelezettségek hiánya és az uniós ítélkezési gyakorlatból fakadó szigorú követelmények, a végponttól végpontig terjedő titkosítás egyre gyakoribb használata, valamint egyes nem hagyományos hírközlési szolgáltatók részéről az együttműködés hiánya miatt. A magas szintű munkacsoport üdvözli az elektronikus bizonyítékokra vonatkozó szabályokat, az ajánlásokban azonban rávilágít azok korlátaira a titkosítás jelentette kihívások kezelése terén, és szorosabb együttműködést szorgalmaz a bűnüldöző és igazságügyi hatóságok, valamint a szolgáltatók között a tartós párbeszéd előmozdítása és az operatív, technikai és üzleti igények kölcsönös megértése, továbbá a titkosított adatokhoz való hozzáféréssel kapcsolatos nehézségek leküzdése érdekében. A szakértők szerint a bűnüldöző szervek és a szolgáltatók közötti szorosabb együttműködés bizonyos mértékben javítani fogja a helyzetet, az időtálló megoldáshoz azonban arra is szükség van, hogy jogszabályok révén érvényesítsék a szolgáltatók együttműködési kötelezettségeit, anélkül, hogy az általánosságban vagy szisztematikusan gyengítené a titkosítást a szolgáltatás felhasználói számára.

---

4 A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport – Európai Bizottság (europa.eu).

5 A magas szintű munkacsoport ajánlásai.

A Tanács 2024. június 13-án **véleménycserét tartott** a magas szintű munkacsoport ajánlásairól, széles körben üdvözölte a magas szintű munkacsoport szakértői által végzett munkát, és kiemelte, hogy fel kell gyorsítani a hatékony bűnüldözést szolgáló adathozzáféréssel kapcsolatos munkát[6]. A belügyminiszterek a következő prioritásokat határozták meg: 1. harmonizált uniós jogi keret létrehozása a bűnüldözési célú adatmegőrzésre vonatkozóan; 2. a személyközi elektronikus hírközlési adatokhoz való hatékony hozzáférésre vonatkozó szabályok megállapítása; valamint 3. jogi és technikai szempontból megfelelő megoldások kidolgozása arra vonatkozóan, hogy egyedi esetekben, bírósági végzés alapján miként lehet hozzáférni titkosított elektronikus hírközlési adatokhoz a súlyos és szervezett bűnözés, valamint a terrorizmus megelőzése, kivizsgálása és büntetőeljárás alá vonása céljából.

A miniszterek emellett szorgalmazták, hogy az EU gyakoroljon erősebb hatást a protokollok és technológiák szabványosítására, és alkalmazzon összehangolt megközelítést a digitális kriminalisztikai eszközök és eljárások tanúsítása terén. Végezetül pedig hangsúlyozták annak jelentőségét, hogy készüljön olyan ütemterv az ajánlások végrehajtására vonatkozóan, amely az átlátható ütemezést, valamint a megvalósíthatóság és a megfelelő pénzügyi források értékelését is tartalmazza. Az egyes ajánlások végrehajtásának koordinációját is fontosnak tartották.

E zárójelentés célja, hogy részletesen ismertesse a szakértők által azonosított kihívásokat, és felvázolja a munka folytatásának és **az ajánlások gyakorlati átültetésének** lehetőségeit. Felvázol a szakértők által felvetett több kulcsfontosságú kérdést, amelyekre a magas szintű munkacsoport megbízatásával összhangban három munkafolyamat épült.

Először is, a **digitális kriminalisztika** terén kulcsfontosságú az adatokhoz való hozzáférés ahhoz, hogy a bűnüldöző szervek összegyűjthessék és elemezhessék az elektronikus eszközökből származó bizonyítékokat. Ezek az adatok megbízható információkat szolgáltatnak a bűnözői tevékenységekről, valamint a bűncselekmények elkövetőinek azonosításához is. Bizonyos technológiák, például a titkosítás gyors fejlődése és széles körű használata szükségessé teszi a bűnüldöző hatóságok számára az erőforrások, a készségek és a műszaki megoldások javítását a titkosított adatokhoz való hozzáféréssel összefüggésben. E tekintetben és a kereskedelmi megoldások alkalmazása tekintetében támogatást nyújthat a határokon átnyúló hatékony együttműködés a szakértelem megosztása, szabványosított eszközök és eljárások kifejlesztése, valamint az erőforrások összevonása révén. A szakértők azonban egyetértettek abban, hogy a kapacitásépítés önmagában nem elég a bűnüldözési képességek javításához. Egyes szakértők úgy vélték, hogy az olvasható formátumú adatokhoz való hozzáférés egyértelműen szabályozott körülmények között történő lehetővé tétele fenntarthatóbb hosszú távú megoldást jelentene.

[6] 11281/24, 2024. június 21.

Másodszor, ahhoz, hogy a bűnüldöző szervek hatékonyan ki tudják vizsgálni a bűncselekményeket és le tudják folytatni a vádeljárást, az **adatmegőrzés** harmonizált és következetes jogi szabályozására van szükség, az alapvető jogok teljes körű tiszteletben tartása mellett. A technológiák gyors fejlődése nyomán egyre nagyobb a jelentősége annak, hogy a bűnüldöző szervek időben hozzáférjenek a szolgáltatók által tárolt releváns adatokhoz. Különösen a szolgáltatók által tárolt hírközlési metaadatokhoz való hozzáférés elengedhetetlen a gyanúsítottak azonosításához és tevékenységeik megértéséhez, és bebizonyosodott, hogy ez fontos szerepet játszik a nyomozások előbbrevitelében.

Harmadszor, a **jogszerű lehallgatás** alapvetően fontos a szervezett bűnözéssel és a terrorista csoportokkal kapcsolatos hatékony nyomozáshoz és a vádeljárás lefolytatásához. Lehetővé teszi a hatóságok számára, hogy bírósági határozat alapján és az alapvető jogok maradéktalan tiszteletben tartása mellett kérjék a szolgáltatóktól, hogy bocsássák rendelkezésre a kommunikáció tartalmát, amely felbecsülhetetlen információt nyújt a bűnözői tevékenységekről. Tekintettel a hagyományos hírközlési szolgáltatók felől az Európai Elektronikus Hírközlési Kódex (EEHK)[7] szerinti over-the-top (OTT) szolgáltatások felé való elmozdulásra, valamint arra, hogy a bűnözők egyre inkább a végponttól végpontig terjedően titkosított platformokat veszik igénybe[8], a kommunikációs adatokhoz való valós idejű, jogszerű hozzáféréshez fel kell mérni, hogy milyen egyértelmű szabályok szükségesek a bűnüldöző hatóságok és a technológiai vállalatok közötti együttműködésre vonatkozóan, valamint megerősített uniós szintű együttműködésre van szükség a határokon átnyúló megkeresések megkönnyítése érdekében.

Az ajánlások, valamint e zárójelentés tartalma **kizárólag a magas szintű munkacsoport szakértőinek elvárásait és kéréseit** tükrözi.

E jelentés benyújtásával **a magas szintű munkacsoport befejezte munkáját**, és felkéri a Bizottságot, a tagállamokat, az Európai Parlamentet és valamennyi érdekelt felet, hogy a hatékony bűnüldözést szolgáló adathozzáférés kérdésének kezelésére irányuló intézkedések kidolgozása során merítsenek ihletet az ajánlásokból és a jelentésből. Ezen intézkedésekhez olyan erőteljes narratívának kell társulnia, amely hangsúlyozza, hogy sürgősen jelentős lépéseket kell tenni az adatokhoz való hatékony és jogszerű hozzáférés biztosítása érdekében. A szakértők arra ösztönzik az összes uniós intézményt és szervet, hogy haladéktalanul vigyék tovább ezt a munkát, külön ütemtervben meghatározott konkrét kezdeményezések végrehajtása révén.

---

[7] Az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, 2018. december 11-i (EU) 2018/1972 európai parlamenti és tanácsi irányelv kiterjeszti a jogi keretnek a hagyományos hírközlési szolgáltatásokra alkalmazandó részét azokra a vállalkozásokra is, amelyek internetalapú szolgáltatásokat kínálnak olyan távközlési infrastruktúrán keresztül, amelynek nem tulajdonosai vagy kezelői, ideértve a számfüggetlen személyközi hírközlési szolgáltatásokat is (NI-ICS).

[8] Europol: Az internetes szervezett bűnözés általi fenyegetettség értékelése (IOCTA), 2024.

Jogszerű hozzáférés: a legfőbb kihívások

Az elmúlt években számos területen javultak a képességeink a bűnözés elleni küzdelem és az EU biztonságának megőrzése területén. Hatékonyabbá vált a bűnüldözési és igazságügyi együttműködés, új jogszabályokat és eszközöket vezettek be a súlyos és szervezett bűnözés elleni küzdelem érdekében, és megerősítették a migránscsempészés, az emberkereskedelem, a tűzfegyver- és kábítószer-kereskedelem, a korrupció és más súlyos bűncselekmények elleni küzdelemre irányuló közös erőfeszítéseket.

A bűnüldöző hatóságok azonban nap mint nap új kihívásokkal szembesülnek polgáraink biztonságának megőrzése terén, különös tekintettel a társadalmunk digitalizációja által előidézett kihívásokra.

A digitális technológiák megváltoztatják az életünket – azt, ahogy kommunikálunk, ahogy éljük a mindennapjainkat, ahogy dolgozunk stb. –, és ezen átalakulás társadalmi vonatkozásai mélyrehatóak. A digitalizáció potenciális megoldást nyújthat számos olyan kihívásra, amellyel Európa és az európaiak szembesülnek, és rengeteg lehetőséget kínál: a munkahelyteremtésre, az oktatás előmozdítására, a versenyképesség és az innováció fellendítésére, az éghajlatváltozás elleni küzdelemre, a zöld átállás megkönnyítésére, és még sorolhatnánk.

Ugyanakkor a digitalizáció megteremti annak feltételeit is, hogy a bűnözők kihasználják a technológiai fejlődést bűncselekmények elkövetésére, mind az online, mind az offline térben. A titkosított készülékeket és alkalmazásokat, az új hírközlési szolgáltatókat, a virtuális magánhálózatokat (VPN) stb. úgy alakították ki, hogy azok védjék a jogszerű felhasználók magánéletét. Ezek azonban hatékony eszközül szolgálnak a bűnözők számára személyazonosságuk elrejtéséhez, jogellenes termékeik és szolgáltatásaik forgalmazásához, a fizetések közvetítéséhez, valamint tevékenységeik és kommunikációjuk elfedéséhez, sikeresen elkerülve ezáltal a felderítést, a nyomozást és a büntetőeljárást. Amellett, hogy léteznek olyan eszközök és szolgáltatások, amelyeket kifejezetten jogellenes tevékenységek végzése céljára alakítottak ki, illetve használnak, bizonyított, hogy a bűnözők egyre inkább kihasználják a jogszerű elektronikus hírközlési szolgáltatások által rendelkezésre bocsátott, a magánélet védelmét szolgáló intézkedéseket. ***A bűnüldöző hatóságok e tekintetben gyakran lemaradnak a bűnözőkhöz képest, mivel nem rendelkeznek megfelelő személyzettel, eszközökkel és forrásokkal ahhoz, hogy eredményesen kezeljék e kihívást***. E fejlemények eredményeként az utóbbi években már az jelenti az egyik legfőbb kihívást a bűnügyi nyomozások és a büntetőeljárások számára, hogy bűnüldözési céllal hozzá lehessen férni az adatokhoz. Mindazonáltal figyelemreméltó sikerekről is be tudunk számolni: a bűnüldöző hatóságoknak például sikerült felszámolniuk olyan bűnügyi jellegű titkosított kommunikációs hálózatokat, mint az EncroChat és a SkyECC, és továbbra is folytatnak olyan műveleteket, mint a „Desert Light”, amelynek során 2022 novemberében lebuktattak egy kokainkereskedőkből álló „szuperkartellt”. Az Europol visszafejtési platformja az elmúlt néhány évben számos magas szintű nyomozást támogatott, hozzájárulva ezzel a terrorizmus, valamint a súlyos és szervezett bűnözés elleni sikeres bűnüldözési intézkedésekhez.

E sikertörténetek mögött azonban számos olyan eset sorakozik, amikor késedelmes és sikertelen a nyomozás, mivel – a gyakorlati szakemberek beszámolói szerint – folyamatosan nehézségekbe ütköznek az operatív igények időben történő kielégítése kapcsán.

A jogszerű hozzáférés révén a hatóságok képessé válnak arra, hogy célzottan nyomon kövessék és lehallgassák a bűnözői célú kommunikációt, valamint megzavarják a bűnözők tevékenységét, ez pedig megnehezíti a technológia bűnözői célú felhasználását. Ezzel szemben szilárd jogi keret és megfelelő források nélkül a bűnüldöző hatóságok továbbra is leküzdhetetlen nehézségekkel fognak szembenézni, és fennáll annak a kockázata, hogy nem lehet hozzáférni kritikus bizonyítékokhoz, számos különböző okból.

- A bűnüldözési célú adatmegőrzési szabályok következetlensége és nem megfelelő volta miatt **az adatok nem mindig állnak rendelkezésre**, különösen ha törölték őket. Ez a hiányosság súlyosan akadályozza a súlyos és szervezett bűnözéssel kapcsolatos nyomozásokat. Konkrétabban, a SIRIUS projekt keretében 2023-ban végzett felmérésben[9] a megkérdezett nyomozók közel fele a harmonizált adatmegőrzési szabályozás hiányát említette elsődleges akadályként. Harmonizált szabályok nélkül fennáll a veszélye annak, hogy döntő fontosságú adatok nem érhetők el, ami aláássa a bűnözés elleni hatékony küzdelem jegyében tett erőfeszítéseket.
- **Az adatokat nem lehet visszanyerni**, különösen akkor, ha az eszközből való kinyerés sikertelen. A szükséges készségek, a megfelelő eszközök és a készülékek gyártóival való elégséges együttműködés hiánya nehézkessé, költségessé és időigényessé teszi a digitális kriminalisztikát, sőt, akár el is lehetetleníti azt. Ez a jelentős hiányosság akadályozza a nyomozások eredményességét. Fejlett kriminalisztikai képességek és készségek híján, valamint az iparral való, illetve a nemzeti hatóságok közötti együttműködés javítása nélkül döntő fontosságú digitális bizonyítékok maradnak elérhetetlenek, ami súlyosan gátolja a bűnüldözési erőfeszítéseket.
- A titkosítás miatt **az adatok nem mindig olvashatók**. Manapság számos szolgáltatás használ végponttól végpontig terjedő titkosítást a közlések titkosságának, a magánélet védelmének és a kiberbiztonságnak a megóvása érdekében, de ez rendkívül megnehezítheti a bűnüldöző szervek számára a kommunikációs adatokhoz való hozzáférést. Ez azt jelenti, hogy még ha az adatokat jogszerűen le is hallgatják, azokat gyakran lehetetlen dekódolni. Ezen adatok olvasásának képessége nélkül fontos bizonyítékok maradnak rejtve, ami nagyban megnehezíti a bűncselekmények nyomozását.

[9] SIRIUS Határokon átnyúló hozzáférés az elektronikus bizonyítékokhoz (SIRIUS projekt), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Az adatok nem mindig elemezhetők**, például mivel a technológia és/vagy az emberi erőforrások nem mindig állnak rendelkezésre adatok nagy mennyiségének a megszűrésére vagy a lefoglalt adatok hatékony módon történő, és egyúttal az EU alapvető értékeivel, valamint az EU és a tagállamok jogi kereteivel összeegyeztethető szűrésére és elemzésére.

- **Az adatok nem szerezhetők be** a joghatóságok közötti kollízió miatt. Az adatok gyakran átlépik a nemzetközi határokat, ami bonyolult joghatósági kihívásokat teremt. Az adatokhoz való hozzáférésre vonatkozó jogszabályok és szabályozások eltérnek a különböző országok között, ami megnehezíti a külföldön tárolt adatok beszerzését. Az elektronikus bizonyítékokról szóló új uniós rendelet és irányelv fontos lépést jelent ennek megkönnyítése felé, de még sok a tennivaló ezen intézkedések teljes körű végrehajtásához – márpedig a teljes körű végrehajtás nélkül továbbra is jelentős kihívást jelent a bűnüldözés számára a más országokból származó kulcsfontosságú adatokhoz való hozzáférés.

Ezek olyan kihívások, melyekkel a bűnüldöző hatóságok nap mint nap szembesülnek.

A bűnözők folyamatosan úgy alakítják a magatartásukat, hogy elkerüljék a felderítést. A rendelkezésre álló statisztikák[10] azt mutatják, hogy a bűnözők egyre inkább olyan platformokra térnek át, melyek legálisak, és végponttól végpontig terjedő titkosítást alkalmaznak. Ha azonban ott hatékony ellenintézkedéseket vezetnek be, valószínűleg ismét áttérnek más kommunikációs csatornákra. Ezért rendkívül fontos, hogy a bűnüldöző szervek – valamennyi érintett közösség szakértőinek támogatásával – képesek legyenek figyelemmel kísérni a technológiai fejlődést és előre jelezni a bűnözői magatartás változásait, például a 6G-hez, a dolgok internetéhez és a műholdas kommunikációhoz kapcsolódóan. Ezen túlmenően fenn kell tartani azokat a kapacitásokat, amelyek lehetővé tették a kifejezetten bűnözési célú hírközlési szolgáltatások (pl. EncroChat, Ghost ECC) elleni sikeres műveleteket, és hozzá kell igazítani azokat a hasonló jövőbeli kihívásokhoz.

[10] Europol IOCTA 2024.

Egyre nagyobb szükség van arra, hogy a bűnüldöző szervek jogszerűen hozzá tudjanak férni a digitális információkhoz. Mivel a bűnözők egyre nagyobb mértékben támaszkodnak online szolgáltatásokra, az online szolgáltatókhoz intézett adatkikérések száma is emelkedik: 2017 és 2022 között háromszorosára nőtt az ilyen megkeresések száma[11]. A kommunikációs adatok (a metaadatok és a tartalmi adatok egyaránt) kulcsfontosságúak számos bűnügyi nyomozáshoz. Úgy tekinthető, hogy a digitális bizonyítékokhoz való hozzáférés a nyomozások 85 %-ában kulcsszerepet játszik[12]. Az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférésre vonatkozó új szabályoknak köszönhetően az illetékes hatóságok jobban hozzá tudnak majd férni ezekhez az adatokhoz. Ezek a szabályok azonban csak akkor működhetnek, ha az adatok olvasható formátumban állnak rendelkezésre. Hasonlóképpen, a lefoglalt eszközökben tárolt adatokhoz való hozzáférés és a kommunikáció jogszerű lehallgatása továbbra is rendkívül nagy kihívás marad mind jogi, mind gyakorlati szempontból. Ami a határokon átnyúló ügyekben az átvitel alatt lévő adatok hatékony lehallgatását illeti, a tagállamok igazságügyi együttműködés iránt folyamodhatnak a kölcsönös jogsegélyről szóló egyezmény[13] és az európai nyomozási határozat[14] alapján; ezeket a jogi eszközöket azonban leginkább a fizikai bizonyítékok cseréjét szem előtt tartva alakították ki, és hatékonyságuk a technológiai fejlődéssel összefüggésben korlátozott mértékű lehet.

A jogszerű hozzáférést a nemzeti, az uniós és a nemzetközi jogban rögzített ***szigorú feltételekhez kell kötni***, és átlátható, elszámoltatható eljárások keretében kell szabályozni e hozzáférést, többek között meg kell akadályozni az üzleti titkok jogosulatlan felfedését, jogszerű felfedés esetén pedig biztosítani kell, hogy azok bizalmas jellegének megőrzése érdekében megfelelő intézkedéseket hozzanak.

A jogszerű hozzáférést illetően teljes mértékben tiszteletben kell tartani a szükségesség és az arányosság elvét, és azt szükség esetén bíróság vagy független hatóság általi jóváhagyáshoz kell kötni. Az adatokhoz való hozzáférést szilárd magánélet-védelmi és kiberbiztonsági intézkedésekkel (pl. titkosítás, tűzfalak, a vírusok és rosszindulatú szoftverek elleni védelem) kell ellensúlyozni. Annak biztosítása, hogy az adatokhoz való hozzáférés a nyomozás céljából szükséges mértékre korlátozódjon, segít megvédeni az egyéni felhasználók magánéletét.

---

11 SIRIUS projekt.

12 A Bizottság hatásvizsgálata az elektronikus bizonyítékokról szóló rendeletre és az elektronikus bizonyítékokról szóló irányelvre irányuló javaslatokról (2018. április 17.).

13 Kölcsönös jogsegély – Az Európa Tanács előírásai – PC-OC (coe.int) (MLA - Council of Europe standards - PC-OC (coe.int)).

14 https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32014L0041.

Bár az adatokhoz való bűnüldözési célú jogszerű hozzáférés az alapja annak, hogy polgáraink számára a lehető legmagasabb szintű biztonságot garantáljuk, ez nem mehet az alapvető jogoknak vagy a rendszerek és termékek kiberbiztonságának a rovására. Nem szabad kompromisszumot kötni egyrészről az emberek személyi sérthetetlenségének és biztonságának védelme, másrészről a jogaik védelme között; olyan egyensúlyt kell találni, amely biztosítja, hogy egyiknek a védelme se sértse a másikét. Az EU-nak és a tagállamoknak egyaránt kötelessége biztosítani, hogy a polgárok az alapvető jogaik magas szintű védelmében részesüljenek, és biztonságban érezzék magukat a mindennapi életük során. A technológiai fejlődés nem teremthet biztonságos terepet a bűnözők számára: amennyiben alapos gyanú merül fel arra vonatkozóan, hogy bűncselekményt követtek el vagy készülnek elkövetni, a bűnüldöző szerveknek hozzáféréssel kell rendelkezniük azokhoz az eszközökhöz, amelyek lehetővé teszik számukra a releváns adatokhoz való hozzáférést.

Az emberi jogok európai egyezménye, a nemzeti alkotmányok és az Európai Unió Alapjogi Chartája egyaránt elismeri, hogy mindenkinek joga van a magánélethez, és hogy ebbe beletartozik a személyes kommunikáció is. Az Európai Unió Alapjogi Chartája emellett az adatvédelemhez való jogot is rögzíti. A magánélethez való jog és a személyes adatok védelméhez való jog nem abszolút jogok, hanem azokat a társadalomban betöltött szerepükkel összefüggésben kell vizsgálni[15]. A hatóságok nem avatkozhatnak be e jogok gyakorlásába***, kivéve, ha az ilyen beavatkozás összhangban van a törvénnyel, tiszteletben tartja a jogok lényegét, valamint egy demokratikus társadalomban szükséges és arányos intézkedés.*** E feltételek teljesülése esetén a magánélethez és a személyes adatok védelméhez való jog korlátozható, többek között a nemzetbiztonság és a közbiztonság, valamint a bűncselekmények megelőzése, nyomozása, felderítése és büntetőeljárás alá vonása érdekében.

Döntő fontosságú az erős elszámoltathatóság. Demokratikus társadalmainkban a jogalkotók felelőssége, hogy megteremtsék az ilyen elszámoltathatóság feltételeit, biztosítva a magánélet és a biztonság magas szintjét. ***A magánélet védelme és a biztonság nem zárja ki egymást***.

Az innováció és az erős kiberbiztonság előmozdítása érdekében az indokolt esetekben biztosított jogszerű hozzáférést szolgáló megoldásokat az összes érdekelt féllel – többek között az iparral – együttműködve kell kidolgozni. ***Ezeket a megoldásokat az összes lényeges igény és követelmény kellő figyelembevételével kell megtervezni, és nem engedhető meg, hogy azokról kizárólag a technológiai vállalatok döntsenek***.

[15] 2024. április 30-i *La Quadrature du Net és társai* ítélet, C-470/21, EU:C:2024:370, 70. pont.

A további lépések megtétele előtt technikai értékeléseket kell végezni annak érdekében, hogy el lehessen oszlatni a kiberbiztonsági szakértők egy részének azzal kapcsolatos aggályait, hogy bonyolult feladat a jogszerű hozzáférés biztosítása az erős kiberbiztonság fenntartása mellett. ***A termékek és szolgáltatások kiberbiztonságának biztosítása és az adatokhoz való jogszerű hozzáférés egyaránt jogi kötelezettségekből ered, és a kettőnek tudnia kell együtt léteznie***. A jogszerű hozzáférésre vonatkozó követelményeket az összes érdekelt fél (beleértve az ipar képviselőit, az adatvédelmi és kiberbiztonsági szakértőket, valamint a bűnüldözési szakembereket) által kidolgozott, a vonatkozó jogi követelményeket tükröző egyértelmű szabványok és megfelelően kiértékelt lehetséges megoldások alapján kell végrehajtani, biztosítva ezáltal, hogy a jogszerű hozzáférés ne veszélyeztesse a termékek és szolgáltatások biztonságát.

Számos vállalat és szolgáltató vonakodik együttműködni a bűnüldöző szervekkel az önkéntes intézkedésekkel kapcsolatos jogbizonytalanság miatt, illetve tartva attól, hogy felhasználóiknál ez visszatetszést válthat ki. Ez a vonakodás akadályozza a nyomozásokat. Ezenkívül az a vélekedés, hogy a felhasználók a magánélet védelmét a közbiztonság fölé helyezik, azt eredményezheti, hogy az ágazati szereplők vonakodnak kommunikációs csatornákat nyitni a bűnüldöző hatóságokkal és kialakítani a jogszerű hozzáférést garantáló, megfelelő mechanizmusokat. E probléma kezeléséhez egyértelmű jogi keretre van szükség az adatokhoz való jogszerű hozzáféréssel kapcsolatban. A jelenleg hatályos jogszabályi környezetben jelentős akadályok nehezítik az ilyen hozzáférés biztosítását, különösen önkéntes alapon.

A vállalatok és a bűnüldöző szervek közötti együttműködés nem felel meg a céljának és rosszul működik, ezért további, egyértelmű szabályokra van szükség. ***Egyértelmű és érvényesíthető jogi kötelezettségek hiányában gyakran előfordul, hogy a vállalatok nem tudnak segítséget nyújtani a bűnüldöző szerveknek az adatokhoz való hozzáférésben***.

A jogszerű hozzáférést biztosító hatékony megoldások hiányában ***gyakran a sérülékenységen alapuló megoldásokat tekintik az egyetlen lehetőségnek***.

Amikor a lehallgatott adatokat (és adott esetben a valamilyen készülékből kinyert egyéb adatokat) magánvállalatok által tervezett eszközökkel dolgozzák fel, a nemzeti hatóságoknak – függetlenül attól, hogy a szóban forgó vállalatok milyen biztosítékokat nyújtanak – nincs valós rálátásuk arra, hogy milyen adatokat és hogyan szűrtek meg, és kénytelenek kizárólag azokra a tanúsítványokra támaszkodni, amelyeket a lehallgatási szolgáltatást nyújtó vállalatok székhelye szerinti ország kormánya állít ki. Ezt a problémát tovább súlyosbítja az, hogy az eszközök/szolgáltatások hatékonyságának megőrzése érdekében titokban kell tartani a kiaknázott sérülékenységet. Ez a probléma különösen akkor ad okot aggodalomra, ha a szolgáltató székhelye az EU-n kívül található.

Végül, de nem utolsósorban az intruzív nyomozási technikákkal kapcsolatos szolgáltatásokat nyújtó magánvállalatoknak az az érdekük, hogy maximalizálják a nyereségüket, és ezért előfordulhat, hogy úgy döntenek, hogy eszközeiket olyan rezsimek részére értékesítik, amelyek nem demokratikusak (ahogyan az a Hacking Team botrány esetében is történt[16]).

Másfelől viszont az adatokhoz való hozzáféréssel kapcsolatos kihívások arra ***ösztönözhetik a bűnüldöző szerveket, hogy intruzívabb nyomozási intézkedéseket alkalmazzanak***. Ilyen esetekben a bűnüldöző hatóságok kénytelenek olyan intézkedésekhez folyamodni, amelyek jobban beavatkoznak a magánéletbe, például fizikai megfigyeléshez a földrajzi helymeghatározási adatokhoz való hozzáférés helyett vagy házkutatáshoz a jogszerű lehallgatás helyett.

Ha a bűnüldöző hatóságok nem tudnak hozzáférni az adatokhoz, az az igazságszolgáltatási rendszerbe vetett közbizalom jelentős megrendüléséhez vezethet. Ha a nyomozások késedelmesek vagy sérül az integritásuk, a polgárok úgy érzékelhetik, hogy a rendszer nem vezet eredményekre. Ez a bizalomvesztés alááshatja a közrendet, és csökkentheti a nyilvánosság hajlandóságát arra, hogy segítse a bűnüldözési erőfeszítéseket.

Végső soron ***a jogszerű hozzáférés lehetővé teszi a bűnüldöző szervek számára, hogy bizonyítékokat gyűjtsenek annak érdekében, hogy igazságot szolgáltassanak az áldozatoknak, és megvédjék őket a további sérelmekkel szemben***. Az adatok fontos nyomot szolgáltathatnak mindenféle – akár offline, akár online elkövetett – bűncselekmény feltárásához és büntetőeljárás alá vonásához. A digitális technológiákkal, szolgáltatásokkal és kommunikációval való, bűnözők által elkövetett visszaélések következtében az egyének az internetes megfélemlítés súlyos formáinak, személyazonosság-lopásnak, csalásnak stb. lehetnek kitéve. Ezek a tapasztalatok súlyos érzelmi és mentális következményekkel járhatnak a sértettekre nézve, tovább súlyosbítva a már meglévő egyenlőtlenségeket és sebezhetőségeket.

---

[16] Lásd: https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

Minden bűnügyi nyomozás során szükség van bizonyítékra az elkövető azonosításához vagy a felelősségének bizonyításához a bíró előtt. Emellett a bizonyíték abban is segíthet, hogy felmentsenek egy olyan személyt, akit tévesen vádoltak meg. Ha a nyomozók és ügyészek nem tudnak hozzáférni a szükséges információkhoz, előfordulhat, hogy nem tudnak előbbre jutni a nyomozásban, és nem tudják azonosítani az elkövetőt, ami további szenvedést és pénzügyi veszteséget okoz a sértettnek, és rombolja az igazságszolgáltatási rendszerbe vetett bizalmat. A hagyományos fizikai bizonyítékok önmagukban nem mindig elegendőek a kapcsolatok felfedéséhez és a nyomra bukkanáshoz. ***A bűnüldözésnek és az igazságszolgáltatásnak készen kell állnia a digitális kor kihívásaira. Csak így lesznek képesek megvédeni társadalmainkat és gazdaságainkat*** a kibertámadásokból és hibrid fenyegetésekből, valamint a szervezett bűnözésből eredő növekvő fenyegetésekkel szemben.

Összegezve, ha a bűnüldöző hatóságok nem tudnak hatékonyan hozzáférni az adatokhoz, jelentősen gyengül az a képességük, hogy garantálják a biztonságot és elfogják a legsúlyosabb bűncselekmények elkövetőit. ***A bűnüldözés számára biztosítani kell az adatokhoz való jogszerű, szigorúan ellenőrzött hatékony hozzáférést, szilárd adatvédelmi és kiberbiztonsági garanciák mellett, nevezetesen a bűncselekmények megelőzése, felderítése, nyomozása és büntetőeljárás alá vonása érdekében, lehetővé téve ezzel számukra a biztonság garantálását, az uniós polgárok számára pedig azt, hogy biztonságban éljék az életüket, és igazságot szolgáltassanak a számukra a sérelmükre elkövetett bűncselekményekért***.

I. fejezet: Digitális kriminalisztika

MIK A NEHÉZSÉGEK?

A digitális kriminalisztika fogalma az elektronikus eszközökön bármilyen digitális formában tárolt digitális bizonyítékok (kommunikációs metaadatok és tartalmi adatok) gyűjtését, elemzését és megőrzését jelenti, beleértve a számítógépes merevlemezekből, mobiltelefonokból, intelligens készülékekből, járműnavigációs rendszerekből, elektronikus ajtózárakból, a felhőben tárolt adatokból és egyéb digitális eszközökből származó információkat.

Mivel a kommunikációs adatokhoz való hozzáférés egyre több nehézséggel jár, a bűnügyi nyomozások során egyre nagyobb a jelentősége a lefoglalt eszközökből (vagy csatlakoztatott eszközök hálózataiból) történő információkinyerésnek. Az eszközökben tárolt inaktív adatokhoz való hozzáférés jobb minőségű információkkal szolgálhat a bűnüldöző szervek számára például a szervezett bűnözői csoportok tagjainak személyazonosságáról, mint más technikák, például a jogszerű lehallgatás. Egyes szakértők azzal érvelnek, hogy nem lehet előre tudni, hogy mely adatok fontosak egy adott nyomozásban: a nyomozás előrehaladtával létfontosságúnak bizonyulhatnak olyan információk is, amelyek kezdetben esetleg lényegtelennek tűntek. Az egy adott eszközben található valamennyi adathoz való hozzáférés fontos lehet a gyanúsított ártatlanságának megerősítése és a vádlott jogainak védelme szempontjából is[17]. Ezenkívül a nyomozási módszereknek mindig arányosaknak kell lenniük.

Az **erőforrások** és képességek krónikus **hiányát**, amellyel a bűnüldöző hatóságok ezen a területen küzdenek, súlyosbítja az új technológiák (pl. új típusú eszközök, a dolgok internete és a felhőalapú számítástechnika) bevezetése, amelyek új készségeket és eszközöket igényelnek. Jóllehet a tagállami ügynökségekben és intézményekben már jelentős szakértelem áll rendelkezésre a digitális kriminalisztika területén, ez a tudás szétaprózódott, és nem alakultak ki egyértelmű mechanizmusok a képességek megosztására és terjesztésére, ami azt jelenti, hogy a meglévő tudás továbbra is az egyes intézményeken belül marad.

[17] Egy szakértő megemlített egy olyan esetet, amelyben az eszköztevékenység elemzése döntő szerepet játszott annak bizonyításában, hogy a gyanúsított nem lehetett érintett a gyilkosságban.

A **digitális kriminalisztikai laboratóriumok összehasonlítható kapacitásainak hiánya**, valamint a **szabványosított kriminalisztikai eljárások**, továbbá **a digitális kriminalisztikai szakértők készségeinek és szakértelmének elismerését** lehetővé tevő mechanizmusok általános hiánya miatt akadályokba ütközhet a határokon átnyúló együttműködés.

A magas szintű munkacsoport szakértőinek álláspontja egyértelmű: a bűnüldöző hatóságok számára az egyik legfőbb kihívást az jelenti, hogy az eszközökön alapértelmezett beállítás az adatok **titkosítása**. A modern eszközök bizonyos típusain tárolt adatokhoz, melyeket kriptochipekkel[18] vagy erős titkosítási algoritmusokkal és összetett jelszavakkal védenek, nem tudnak hozzáférni a bűnüldöző hatóságok, még a leghatékonyabb visszafejtési platformok használatával sem. A titkosításra, valamint egyéb kiberbiztonsági és adatvédelmi intézkedésekre szükség van az információs rendszerek, valamint a kommunikációs és személyes adatok védelméhez, de ezek az intézkedések – és különösen az alapértelmezett titkosítás egyre gyakoribb használata – rontja a bűnüldöző szervek azon képességét, hogy bizonyítékokat gyűjtsenek.

A tagállamok korlátozott **szakértelemmel és képességekkel** rendelkeznek ezen a területen: szinte mindegyikük arról számol be, hogy nem állnak a rendelkezésükre a szakemberek igényeit kielégítő technikai megoldások, és túlnyomó többségük úgy véli, hogy készségeik és pénzügyi lehetőségeik elégtelenek. A bűnüldöző hatóságok azon képessége, hogy a lefoglalt eszközökön tárolt információkat visszafejtsék, tagállamonként jelentősen eltér: a sikerességi arány a 15–20 %-tól a több mint kétharmadig terjed. Ahol meg is vannak a képességek, azok általában hatástalanok, ha erős jelszavakkal védett adatokat vagy speciális, titkosított konténerekben őrzött fájlokat kellene visszafejteni. Még ha sikeres is a visszafejtés, az gyakran nem történik meg időben. A visszafejtő berendezések drágák és rendkívül specifikusak, a hardver pedig kapacitásigényes.

A bűnüldöző szervek digitális kriminalisztikai részlegeinek többsége kereskedelmi forgalomban kapható megoldásokra támaszkodik az eszközökben található adatokhoz való hozzáférés terén, ami további kihívásokat vet fel: ezek a megoldások nehezen tudnak lépést tartani a technológiai fejlődéssel, és gyorsan elavulttá válnak; a licencek magas költsége jelentősen visszafogja a jogosult felhasználók számát; továbbá az ilyen megoldásokat gyakorta Európán kívül fejlesztik ki, és előfordulhat, hogy azok nem igazán felelnek meg az uniós bűnüldöző hatóságok igényeinek, vagy nem teljesítik az uniós digitális kriminalisztikára irányadó elszámoltathatósági normákat.

[18] Például az újabb Apple laptopokban található T2 biztonsági chip.

A bűnüldöző hatóságoknak gyakran nincs más lehetőségük, mint hogy kihasználják a **sérülékenységeket** annak érdekében, hogy hozzáférést szerezzenek az eszközök visszafejtő kulcsaihoz. Az e megközelítésen alapuló nyomozási technikákat azonban össze kell egyeztetni a kiberrezilienciáról szóló rendeletben rögzített azon célkitűzéssel, hogy biztonságosabb hardverekről és szoftverekről kell gondoskodni; az ilyen technikák nem szándékolt következményeit enyhítené a sérülékenységek kezelésére és felfedésére szolgáló rendszerek megléte. A szakértők alternatív megoldásokat is fontolóra vettek, például a gyanúsítottak kötelezését arra, hogy adják át a nyomozó hatóságoknak a szóban forgó eszközökhöz való hozzáféréshez szükséges elemeket (pl. jelszavakat). Az ilyen esetekben alkalmazandó nemzeti jogi keretek jelentős mértékben eltérnek egymástól, és csak három tagállam jelezte, hogy országukban konkrét jogszabályi rendelkezések kötelezik a gyanúsítottat arra, hogy adja meg a hozzáférést a titkosítási kulcsokhoz vagy a visszafejtett adatokhoz[19]. Egyes tagállamok arra kötelezik a gyanúsítottakat, hogy bocsássanak rendelkezésre bizonyos biometrikus adatokat (pl. ujjlenyomatot), ezáltal biztosítva hozzáférést az adott eszközhöz; más esetekben a gyanúsítottaknak fel kell fedniük a jelszavukat. Általánosságban elmondható, hogy ez a terület további értékelésre szorul.

A fentiekben megjelölt nehézségek némelyike esetleg enyhíthető **a tagállamok kapacitásainak közös felhasználásúvá tételével**, a nemzetbiztonsággal kapcsolatos kizárólagos hatáskörük tiszteletben tartása mellett. Ez a megoldás azonban továbbra sem kap figyelmet, néha a jogi korlátok miatt (hét tagállamban megszorítások vonatkoznak az eszközök megosztására, öt tagállamnak pedig a más tagállamok által megosztott eszközök használatával kapcsolatban kell megszorításokat betartania), tágabban tekintve azonban annak okán, hogy nincsenek bevett mechanizmusok az eszközök megosztására vagy a licencek közös beszerzésére.

Régebben a bűnüldöző hatóságok egyértelmű **kommunikációs csatornákat tartottak fenn a gyártókkal, a szolgáltatókkal és a beszállítókkal**. Ez lehetővé tette számukra, hogy együttműködési protokollokat dolgozzanak ki, amelyek segítették az újonnan bevezetett technológiai fejlesztések jobb megértését, és ennek következtében megkönnyítették a bűnüldözési intézkedéseket, miközben biztosították a kiberbiztonságot is. Tekintettel az új technológiák bevezetésének és az új vállalatok piacra lépésének ütemére, a feltételek megváltoztak, és az iparral való együttműködés már nem áll fenn.

A megfelelő szabványok elfogadása lehetővé tenné a termékprotokollok és a műszaki architektúra oly módon történő alakítását, hogy a bűnüldöző szervek aggályait és a műszaki követelményeket már korai szakaszban figyelembe lehessen venni. **A bűnüldöző szervek érintett szabványügyi testületekben való részvételének** mértéke azonban nem elégséges, ami befolyásolja a jövőbeli technológiai szabványok kidolgozásában való valódi részvételre való képességüket.

---

[19] Eurojust Kiberbűnözési Igazságügyi Figyelő (Eurojust Cybercrime Judicial Monitor) (4. szám), 2018. december, 34. o., https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

LEHETSÉGES MEGOLDÁSOK

I. A digitális kriminalisztikai eszközök területén a kapacitás növelése érdekében fokozni és észszerűsíteni kell az erőfeszítéseket

A tagállamok már rendelkeznek a digitális kriminalisztika elvégzéséhez szükséges szakértelemmel és kapacitással; technikai megoldásaik megosztásával és közös felhasználásúvá tételével azonban az érintett nemzeti intézmények és hatóságok hasznosíthatják más ügynökségek tapasztalatait, és jelentős méretgazdaságosságot érhetnek el, csökkentve ezáltal a szükséges pénzügyi források nagyságát. A tagállamok e célból további megoldásokat tárhatnak fel, mind a digitális kriminalisztikai eszközök, mind a képzés és a készségfejlesztés területén.

1. ajánláscsoport

A digitális kriminalisztika területén az együttműködés fokozása és az erősebb kollektív kapacitás kiépítése érdekében a szakértők a következőket javasolják:

1. *a meglévő digitális kriminalisztikai hálózatok feltérképezése és összekapcsolása, valamint egy titkárság létrehozása [1. ajánlás];*
2. *a tudás hozzáférhetőbbé tétele és terjesztése a szakértők körében [1. ajánlás];*
3. *a tudás egybegyűjtésére szolgáló mechanizmusok átgondolása [2. ajánlás];*
4. *a kutatás-fejlesztés finanszírozásának növelése, és a teljesítendő eredmények egyértelmű megjelölése [4. ajánlás];*
5. *az Europol-eszköztár népszerűsítése az eszközök megosztásának központi platformjaként [4. ajánlás];*
6. *a megoldások és a digitális kriminalisztikai eszközök tagállamok közötti megosztásának megkönnyítése bizalmi környezetben (a nemzeti szabályok figyelembevétele mellett) [2. ajánlás];*
7. *a digitális kriminalisztikai eszközökre vonatkozó licencek közös beszerzésére szolgáló, uniós szintű mechanizmus kidolgozása, hogy a licenceket a tagállamok megoszthassák egymással [3. ajánlás];*
8. *a digitális kriminalisztikai eszközök gyártóival és fejlesztőivel való együttműködés előmozdítása a bűnüldöző hatóságok által ezen eszközök használatával megszerzett adatok struktúrájának és formátumának észszerűsítése céljából, ideális esetben közösen elfogadott szabványok alapján [12. ajánlás];*
9. *a kereskedelmi forgalomban lévő digitális kriminalisztikai eszközök értékelésére és – adott esetben – tanúsítására szolgáló uniós szintű mechanizmus/rendszer kialakítása, szem előtt tartva a nyomozásokra és a büntetőeljárásokra esetlegesen gyakorolt potenciális negatív hatásokat, mint például szükségtelen terhek bevezetését [5. ajánlás].*

Több szervezet, hálózat, szövetség és projekt is létezik, amelyek összefogják a gyakorló szakembereket és a partnerek különböző kategóriáit, hogy növeljék az uniós bűnüldöző szervek kapacitását a digitális nyomozások területén:

- az *Igazságügyi Szakértői Intézetek Európai Hálózata* (ENFSI)[20] a legfőbb olyan európai hálózat, amely a digitális kriminalisztikával foglalkozik (más területek mellett); 39 országból 73 tagja van, és ezek a tagok különböző munkacsoportokban vesznek részt – ilyen például az igazságügyi információs technológiával és a digitális képalkotással foglalkozó munkacsoport;
- *a Kiberbűnözés Elleni Technológiafejlesztés Európai Szövetsége* (EACTDA)[21] számos tagállam bűnüldöző hatóságait, kutatási és technológiai szervezeteit, ipari partnereit és a tudományos élet képviselőit tömöríti azzal a céllal, hogy megkönnyítse a biztonsági kutatási projektek eredményeinek gyakorlati alkalmazását, valamint hogy az uniós közbiztonsági szervezetek számára olyan szoftvereszközökkel szolgáljon, melyek teljes körű tesztelésen estek át és működésre készek, mégpedig licencköltségek nélkül, hozzáférést biztosítva a forráskódhoz;
- az Európai Csalás Elleni Hivatal (OLAF) 2007 óta külön *digitális kriminalisztikai és elemzői képzést (DFAT)* kínál a nemzeti bűnüldöző hatóságok részére, különös hangsúlyt helyezve az Európai Unió pénzügyi érdekeit sértő csalásra, korrupcióra és egyéb jogellenes tevékenységekre; évente mintegy 175 digitális kriminalisztikai szakértő részesül képzésben, aminek eredményeként fokozatosan kiépül a bűncselekmények ezen területét illetően képzett szilárd közösség;
- más projektek, mint például a *CYCLOPES*[22] és az *I-LEAD*[23], bár nem állandó struktúrák, szakértőket tömörítenek, és releváns hiányelemzést végeznek.

A meglévő állandó hálózatok azonban nem fogják össze az uniós bűnüldöző hatóságok digitális kriminalisztikai egységeit, valamint a velük szorosan együttműködő szervezeteket (például a Dublini Egyetem [UCD] Kiberbiztonsággal és a kiberbűncselekmények nyomozásával foglalkozó központját vagy a kiberbűnözéssel foglalkozó litván képzési, kutatási és oktatási kiválósági központot).

---

20 https://enfsi.eu/.
21 https://www.eactda.eu/index.html.
22 https://www.cyclopes-project.eu/.
23 https://cordis.europa.eu/project/id/740685/en

Az Europol (különösen az Europol Innovációs Labor a Kiberbűnözés Elleni Európai Központtal együtt) bizonyos mértékben már együttműködik a fent felsorolt valamennyi hálózattal, és bebizonyosodott, hogy képes összefogni jelentős számú gyakorló szakembert, például az Európai Innovációs Klíringtestület (EuCB) központi csoportjai keretében, vagy az *Igazságügyi szakértői fórum*[24] megszervezésével, illetve azáltal, hogy segít kapcsolatot teremteni a szakértők és a megfelelő partnerek között, például a *Kiberinnovációs fórumon*[25] keresztül.

Az Europol emellett olyan kész infrastruktúrát is kínál – az Europol szakértői platformot (EPE) –, amely lehetővé teszi a szakértők közötti együttműködést és tudásmegosztást konkrét témákban.

Fő intézkedés: A magas szintű munkacsoport szakértői az Europol digitális kriminalisztikai képességeinek megerősítését szorgalmazzák

Szereplők: Europol, Európai Bizottság, tagállamok	*Időkeret: 2028*	*Költségvetés: megvitatására a későbbiekben kerülhet sor, a következő MFF-ről még folyamatban lévő megbeszélések eredményétől függően*

- Az Európai Bizottság számára készített politikai iránymutatás (2024–2029) értelmében az Europolt jelentős mértékben meg fogják erősíteni; a magas szintű munkacsoport szakértői azt szorgalmazzák, hogy ennek részeként fokozzák az Europol arra irányuló kapacitását, hogy segíteni tudjon a tagállamoknak **az erőforrások, az ismeretek és a szakértelem egybegyűjtésében, valamint a megoldások és a digitális kriminalisztikai eszközök megosztásában**, bizalmi környezetben. Ez alól ki kell zárni a szuverén eszközöket és a kizárólag nemzetbiztonsági célokra használt és/vagy kifejlesztett eszközöket.

- A magas szintű munkacsoport szakértői szorgalmazzák, hogy az Europol **vállalja a központi platform szerepét** az e területen releváns műveleti szakértelemhez való hozzáférés tekintetében, és lehetőség szerint **hozzon létre egy, a SIRIUS-hoz hasonló projektet a digitális kriminalisztika területén** a tudás és a szakértelem megosztásának, valamint a bevált gyakorlatok cseréjének megkönnyítése érdekében.

- A magas szintű munkacsoport szakértői felkérik az Europolt, hogy – az EuCB iránymutatása mellett és más érintett ügynökségek hozzájárulásának figyelembevételével – vállaljon nagyobb szerepet az olyan **szervezetek és projektek koordinálásában**, amelyek a digitális kriminalisztika területén uniós szinten hozzájárulnak a tudás-előállításhoz.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference
[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024

Számos olyan pénzügyi eszköz létezik, amelyet igénybe lehet venni a kutatás és az eszközfejlesztés támogatására a digitális kriminalisztika területén.

- A *Belső Biztonsági Alap (BBA)* keretében az Európai Bizottság rendszeres időközönként tesz közzé nyílt pályázati felhívásokat a kiberbűnözés és a digitális nyomozások területén. A meglehetősen szűk költségvetés ellenére (a jelenlegi MFF-ben hozzávetőleg 15 millió EUR-t különítettek el ezekre az intézkedésekre), az e felhívások nyomán kiválasztott projektek célzottnak és sikeresnek bizonyultak.

  A BBA költségvetésének mintegy kétharmadát megosztott irányítás keretében osztják el, és a tagállamok választják ki, hogy mely projekteket finanszírozzák, és ők vállalnak felelősséget a napi irányításért. Így tehát a tagállamoknak lehetőségük van arra, hogy nemzeti programjaik keretében digitális kriminalisztikával kapcsolatos projekteket támogassanak.

- A *Horizont Európa keretprogramnak a társadalmat szolgáló polgári biztonság klasztere* hét évre 1,596 milliárd EUR összköltségvetéssel rendelkezik, célja pedig, hogy a napjainkban végbemenő példa nélküli átalakulások, valamint a növekvő globális kölcsönös függőségek és fenyegetések közepette elősegítse a biztonságos európai társadalmak kialakulását, a szabadság és a jogérvényesülés európai kultúrájának megerősítésével egyidejűleg. Az elmúlt években számos idevágó kutatási projekt részesült innen támogatásban, például a FORMOBILE[26] és az EXFILES[27], amelyek segítették a gyakorló szakembereket mindennapi tevékenységeikben.

- A *Digitális Európa program* az a fő uniós finanszírozási eszköz, amelynek a célja az EU digitális infrastruktúrájának különböző kezdeményezések révén történő fejlesztése. A program, amelynek teljes költségvetése a 2021–2027-es időszakra 7,5 milliárd EUR, jelentős forrásokat különít el kifejezetten a kiberbiztonságra, és a digitális kriminalisztikára is kiterjed.

[26] FORMOBILE – A mobiltelefontól a bíróságig – Teljes FORenzikus nyomozási lánc a MOBILeszközökre fókuszálva: https://cordis.europa.eu/project/id/832800.

[27] EXFILES – Európa felveszi a harcot a bűnözéssel és a terrorizmussal szemben: https://exfiles.eu/.

Az Europol visszafejtési platformja a BBA egyik vezérprojektje. A platform – melyet 2020-ban hozott létre az Europol az Európai Bizottság Közös Kutatóközpontjával (JRC) szoros együttműködésben – segítséget nyújt a nemzeti bűnüldöző hatóságoknak azáltal, hogy visszafejti digitális bizonyítékaikat. Célja, hogy fenntartható megoldást kínáljon a bűnüldöző hatóságok számára, hozzáférést biztosítva azokhoz a technikai és informatikai erőforrásokhoz, melyekre szükségük van. Az elmúlt néhány évben számos komoly ügyben igénybe vették a platformot, és ezek közel felében döntő eredményeket értek el, ami több sikertörténethez vezetett. 2023-ban a platform 37 nyomozást támogatott sikeresen (gyermekek szexuális kizsákmányolása, terrorizmus, kiberbűnözés, szervezett bűnözés, kábítószer-csempészet és csalás ügyében, valamint nagy horderejű pénzügyi nyomozásokat), többek között olyan kiemelt fontosságú nyomozásokat is, mint a SkyECC és az Encrochat ügyében folytatottak. A platform a bűnüldöző hatóságok alapvető eszközévé vált, de nem elegendő ahhoz, hogy megoldja az uniós hatóságok által a visszafejtés terén tapasztalt összes nehézséget.

Fő intézkedés: A magas szintű munkacsoport szakértői szorgalmazzák az EU visszafejtési képességei használatának továbbfejlesztését és előmozdítását

Szereplők: Európai Bizottság, Europol	*Időkeret: 2028*	*Költségvetés: a tagállamok által meghatározandó (pl. a BBA nemzeti programok keretében)*

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy célzott finanszírozás (például a Belső Biztonsági Alap nemzeti programjai keretében) és a bevált gyakorlatok cseréje révén támogassa a nemzeti hatóságok képességét arra, hogy jó minőségű háttérinformációkat gyűjtsenek, hogy ezáltal hozzá tudjanak járulni az Europol visszafejtési platformja hatékonyságának növeléséhez; mindeközben tiszteletben kell tartani a tagállamok nemzetbiztonsággal kapcsolatos kizárólagos hatáskörét.

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy támogassa az Europol arra irányuló beruházásait, hogy fenntartsa a technikai képességeket és fokozza a visszafejtési képességeket, lépést tartson a technológiai fejlődéssel és figyelembe vegye a kvantumkriptográfiai kutatás fejleményeit.

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy pénzügyileg támogassa a tagállamokat a **nemzeti és regionális visszafejtési képességek** fejlesztésében, az Europol erőfeszítéseinek kiegészítése érdekében.

A meglévő uniós finanszírozási programok jelentős támogatást kínálnak a bűnüldözés számára. E lehetőségeket tovább lehetne észszerűsíteni, aminek köszönhetően jobban hozzá tudnának járulni a digitális kriminalisztikai részlegek kapacitásainak javításához, valamint a vevőfogvatartásnak és annak csökkentéséhez, hogy a bűnüldöző szervek az EU-n kívül kifejlesztett „fekete doboz” jellegű eszközökre támaszkodjanak (ezek olyan adatkezelő eszközök, amelyeknek a működését nem tudják megbízható hatóságok ellenőrizni).

A tevékenységi ciklus különböző lépésekből áll: kutatás, fejlesztés, alkalmazás; ezek mind szükségesek ahhoz, hogy az eredmények kézzelfogható hozzáadott értékkel szolgáljanak a bűnüldöző hatóságok számára. Ezeket a lépéseket különböző rendszerek támogatják. Az uniós szinten rendelkezésre álló lehetőségek teljes körű kihasználása érdekében a nemzeti közigazgatásoknak, bűnüldöző hatóságoknak és gyakorlati szakembereknek tisztában kell lenniük az egyes konkrét programok és mechanizmusok funkcióival és célkitűzéseivel.

A Horizont Európa számos sikeres projektet támogatott, a bűnüldözési szakemberek aktív részvételével. A Horizont Európa azonban kutatási program, és ehhez kell igazítani az arra vonatkozó elvárásokat, hogy a kifejlesztett eszközök mennyire állnak készen az operatív alkalmazásra.

A BBA által finanszírozott és az EACTDA által bonyolított *Tools4LEAs* projekt célja, hogy megkönnyítse a biztonsággal kapcsolatos kutatási projektek eredményeinek alkalmazását, valamint hogy az uniós közbiztonsági szervezetek számára olyan szoftvereszközökkel szolgáljon, melyek teljes körű tesztelésen estek át és működésre készek, mégpedig licenckőltségek nélkül, hozzáférést biztosítva a forráskódhoz. A *Tools4LEAs* projekt a legalkalmasabb arra, hogy a kutatási projektek eredményeire építve elősegítse az operatív eszközök megvalósítását. Az Europol részt vesz a *Tools4LEAs* projektben, és irányítja annak munkáját, közösen minden olyan végfelhasználóval, amely tagja az EACTDA-nak.

Az EuCB a tagállamok több mint 15 központi csoportját hozta létre az új technológiák kiaknázása és innovatív eszközök közös megalkotása érdekében. A tagállamok az EuCB központi csoportjait arra használták fel, hogy azok keretében koordinálják a Belső Biztonsági Alapból nyújtott, vissza nem térítendő támogatásokból finanszírozott innovatív eszközök, például a MARIT-D, a ProfID és keresőrobotok fejlesztésének egy részét. A központi csoportok ideális keretet jelentenek ahhoz, hogy a tagállamok koordinálják a digitális nyomozási eszközök közös megalkotását.

A *BBA keretében kiírt* célzott *pályázati felhívások* révén az Európai Bizottság továbbra is finanszíroz olyan projekteket, amelyek már jelentősen hozzájárultak az operatív intézkedések sikeréhez. A CERBERUS projekt például az EncroChat rendszer sérülékenységeit azonosította be, aminek köszönhetően a francia csendőrség – a holland nemzeti igazságügyi intézet és a Dublini Egyetem (UCD) támogatásával – felszámolta azt. A FREETOOL projekt[28] pedig, amelyet az UCD Kiberbiztonsággal és a kiberbűncselekmények nyomozásával foglalkozó központja irányít, lehetővé tette egy sor ingyenes, a kiberbűncselekmények nyomozását segítő eszköz[29] kifejlesztését, amelyeket kifejezetten arra alakítottak ki, hogy megfeleljenek a digitális nyomozások és elemzések támasztotta konkrét bűnüldözési követelményeknek. Ezeket az eszközöket a bűnüldöző szervekkel partnerségben fejlesztették ki, és azok szabadon hozzáférhetők a bűnüldöző közösség számára. A több tucat joghatóságból kikerülő több mint 100 bűnüldöző hatósághoz tartozó 3000 felhasználó iratkozott fel az eszközökhöz való hozzáférésre, amelyeket több bűnüldöző hatóság szervezeti szinten is bevezetett, és nagy horderejű nyomozások során is használták azokat. A *Jogérvényesülés program* a büntetőügyekben folytatott igazságügyi együttműködésre is kiterjed, és előmozdíthatná a digitális nyomozási eszközök használatával kapcsolatos, határokon átnyúló együttműködést is.

[28] https://www.ucd.ie/cci/projects/freetool/.

[29] Az eszközök bevethetők a nyomozás különböző szakaszaiban, úgymint: keresést megelőző, nyílt forrásból származó értékelt felderítési információ (OSINT) gyűjtése; előadat-kriminalisztika; memóriaelemzés; keresést követő OSINT és online források megőrzése; fájlok/artefaktumok automatizált visszanyerése; igazságügyi szakértői jelentés; médiatartalmak feldolgozása; valamint artefaktumok földrajzi helymeghatározása.

Létrehozása óta az *Europol-eszköztár* (ETR) egyre bővült, és mára több mint 40 fejlett eszközt foglal magában, amelyek közvetlen hozzáférést biztosítanak az európai bűnüldöző szervek számára a legkorszerűbb technológiákhoz. Az eszköztár minden hónapban új eszközökkel gazdagodik, és ha az Unióban dolgozó szakemberek valamilyen szoftvert keresnek a nyomozásaik előbbre viteléhez, ez jelenti számukra az elsődleges forrást. Az ETR-nek jelenleg több mint 270 000 felhasználója van, és több mint 780 000 letöltést végeztek az itt elérhető különböző eszközökből. Az eszközöket a nemzeti nyomozó egységek széles körben használták számos művelet támogatására, többek között a bűnözés különböző területein, például az emberkereskedelem, a súlyos és szervezett bűnözés, a kiberbűnözés és a gyermekek online szexuális bántalmazása területén. Az ETR közvetlen hasznosítási lehetőséget kínál az olyan, uniós finanszírozású projektek számára, amelyek konkrét és kiforrott eredményeket kínálnak, és amelyek alkotói hajlandók licenciába adni azokat az Europolnak, amely aztán terjeszti azokat az összes európai bűnüldöző hatóság körében. Az INSPECTr, a Tools4LEAs és a FORMOBILE projekt kiválasztott partnerei már megosztottak eszközöket az ETR-ben. Az Europol egyeztetést folytat az Európai Unió Bűnüldözési Képzési Ügynökségével (CEPOL) annak érdekében, hogy felhasználói képzést szervezzen az ETR eszközeiről.

Emellett a Digitális Európa program várhatóan jobban elő fogja mozdítani a kiberbiztonság és a kiberbűnözés elleni küzdelem közötti szinergiákat és kiegészítő jelleget, mivel e két terület gyakran ugyanazokra a digitális kriminalisztikai eszközökre és technikákra támaszkodik.

Jelenleg nincs olyan mechanizmus, amely annak biztosítását szolgálná, hogy a digitális kriminalisztikai eszközök megfeleljenek az EU-ban irányadó elszámoltathatósági és kriminalisztikai normáknak. Az erre szolgáló mechanizmus keretében elő kellene írni, hogy technikai értékelés készüljön az ilyen eszközökről annak biztosítása érdekében, hogy azok teljes mértékben megfeleljenek az arányosság követelményének (azaz az eszköz bizonyítottan csak a megcélzott információkhoz engedjen hozzáférést, és ezáltal az elemzés kizárólag a szükséges mértékre korlátozódjon), maradéktalanul átláthatók legyenek és tiszteletben tartsák a vádlott jogait (azaz az eszköz bizonyítottan hiteles és pontos információkat nyerjen vissza, ezáltal nyújtva biztosítékot a védőügyvédek és a bíróságon tanúvallomást tevő független igazságügyi szakértők számára), továbbá maradéktalanul megfeleljen egyéb jogi követelményeknek is (pl. a mesterséges intelligenciáról szóló rendeletnek való megfelelés). Ezáltal nőne a bizonyítékok megbízhatóságába vetett hit a bíróságokon, nemzeti szinten és határokon átnyúlóan is, ami megerősítené a határokon átnyúló együttműködést is.

Fő intézkedés: A magas szintű munkacsoport szakértői célzott finanszírozást szorgalmaznak a digitális kriminalisztikai eszközök kutatására, fejlesztésére és alkalmazására irányuló projektek számára

Szereplők: Európai Bizottság, Europol, tagállamok, EACTDA, ENFSI	*Időkeret: 2024-től*	*Költségvetés:*

- A magas szintű munkacsoport szakértői felkérik a tagállamokat, hogy **a BBA nemzeti programjuk keretében finanszírozott digitális kriminalisztikai projekteket integrálják a meglévő mechanizmusokba** (pl. EMPACT) vagy hálózatokba (pl. ECTEG, EACTDA) annak érdekében, hogy hasznosítani lehessen más tagállamok gyakorló szakembereinek tapasztalatait, és ezzel egyidejűleg elő lehessen mozdítani az eredmények más bűnüldöző hatóságok általi terjesztését és alkalmazását.

- A magas szintű munkacsoport szakértői üdvözlik az Európai Bizottság arra irányuló jelenlegi erőfeszítéseit, hogy a digitális kriminalisztikai eszközök kutatása, fejlesztése és alkalmazása támogatásban részesüljön a megfelelő pénzügyi programok – **Horizont Európa**, **Digitális Európa** és a **BBA** – keretében elérhető finanszírozás révén. A BBA keretében az Európai Bizottság – a rendelkezésre álló forrásoktól függően – kétévente **nyílt pályázati felhívásokat** fog közzétenni a kiberbűnözés és a digitális nyomozások területén.

- A magas szintű munkacsoport szakértői üdvözlik az Európai Bizottság arra irányuló erőfeszítéseit, hogy a BBA keretében finanszírozásban részesüljön az **EACTDA** annak érdekében, hogy az olyan szoftvereszközökkel szolgáljon az uniós közbiztonsági szervezetek számára, melyek teljes körű tesztelésen estek át és működésre készek, mégpedig licenckköltségek nélkül, hozzáférést biztosítva a forráskódhoz.

- A magas szintű munkacsoport szakértői üdvözlik az Európai Bizottság arra irányuló jelenlegi erőfeszítéseit, hogy a finanszírozási lehetőségek keretében előmozdítsa az **Europol-eszköztár** használatát, mely az eszközök terjesztésének központi platformjaként szolgál; arra ösztönzik az **Europol Innovációs Labort**, hogy folytassa az azt célzó erőfeszítéseit, hogy megbízható, biztonságos, ingyenes, könnyen telepíthető és skálázható nyomozási eszközök álljanak az uniós bűnüldöző szervek rendelkezésére.

- A magas szintű munkacsoport szakértői szorgalmazzák a kereskedelmi forgalomban lévő digitális kriminalisztikai eszközök uniós szintű **értékelésére és adott esetben tanúsítására szolgáló rendszerek létrehozásának** további megfontolását. Ez történhetne például az **Igazságügyi Szakértői Intézetek Európai Hálózatának keretében**.

A digitális kriminalisztikai eszközök licencei drágák, és egyes bűnüldöző hatóságok számára néha megfizethetetlenek. A licencek közös beszerzése, amelyeket aztán különböző tagállamok hatóságai megoszthatnak egymással, alacsonyabb árak elérését teheti lehetővé.

A Horizont Európa keretében finanszírozott *iProcureNet* projekt[30] kidolgozott egy módszertant a közös közbeszerzésre a biztonság területén, valamint hálózatba szervezte a tagállami közbeszerzési hatóságokat. Összetételére és munkaszervezésére tekintettel *a belső biztonság európai innovációs központja* alkalmas lenne arra, hogy kísérő szerepben segítse a közös igények tagállamok általi meghatározását, és megállapítsa, hogy mely eszközök lennének a leghasznosabbak, feltéve, hogy a központon belül létrejönne egy digitális kriminalisztikával foglalkozó külön munkafolyamat.

A digitális kriminalisztikai eszközök amellett, hogy költségesek, további problémákat is felvetnek. Például előfordulhat, hogy az ezen eszközök által visszanyert adatok struktúrája olyan, vagy olyan formátumban vannak megjelenítve, hogy az nem felel meg a további feldolgozásra (pl. adatelemzés vagy -megosztás) használt meglévő belföldi információs rendszerek jellemzőinek. Ezért meg kell határozni, hogy a tagállamok milyen közös követelményeket állítanak a digitális kriminalisztikai eszközök segítségével megszerzett adatok struktúrájára és formátumára vonatkozóan. Ennek alapján a tagállami hatóságok abban a helyzetben lennének, hogy – például a fent vázolt közös közbeszerzési eljárások keretében – megbeszéléseket folytassanak a digitális kriminalisztikai eszközök szolgáltatóival annak érdekében, hogy az általuk támasztott követelményeket kellően figyelembe tudják azok venni.

Fő intézkedés: A magas szintű munkacsoport szakértői hangsúlyozzák, hogy a digitális kriminalisztikai eszközök beszerzése során jobb ár-érték arányt kell elérni

Szereplők: Tagállamok, Európai Bizottság, a belső biztonság európai innovációs központja, Europol	*Időkeret: 2025-től (közös közbeszerzés)*	*Költségvetés: n. a.*

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy:
  - támogassa a tagállamokat a hatékony nyomozásokhoz leginkább szükséges **digitális kriminalisztikai eszközök azonosításában** (lehetőség szerint a belső biztonság európai innovációs központja keretében);
  - támogassa **az operatív egységek és** az iProcureNet által tömörített **közbeszerzési hatóságok kapcsolattartói közötti együttműködést**;
  - indítson **kísérleti projektet a digitális kriminalisztikai eszközök licenceinek közös beszerzésére**.
- A magas szintű munkacsoport szakértői úgy vélik, hogy az **Europol** megfelelő helyzetben van ahhoz, hogy segítsen a tagállamoknak a digitális kriminalisztikai eszközök segítségével **megszerzett adatok struktúrájára és formátumára vonatkozó közös követelmények** meghatározásában, valamint hogy ennek alapján előmozdítsa az érintett nemzeti hatóságok és szakértők közötti együttműködést annak érdekében, hogy azok kapcsolatba léphessenek ezen eszközök előállítóival és fejlesztőivel a célból, hogy megállapodjanak a szabványokról, továbbá hogy a tagállamok által támasztott követelményeket figyelembe lehessen venni.

[30] https://www.iprocurenet.eu/.

II. Kapacitások cseréje és érzékeny eszközök megosztása

Jelenleg a bűnüldöző hatóságok számára továbbra is az jelenti a legfőbb lehetőséget a titkosított tartalomhoz való hozzáférésre, ha kiaknázzák a sérülékenységeket annak érdekében, hogy hozzáférést szerezzenek az eszközök visszafejtő kulcsaihoz, mivel csak korlátozottan állnak rendelkezésre visszafejtési képességek (pl. az Europol visszafejtési platformja), és nincs tényleges együttműködés az ágazattal, illetve külön jogi keret sem szabályozza a digitális eszközökön található információkhoz való jogszerű hozzáférést.

Még ha e feltételek (egy része) bizonyos mértékig fenn is áll, valószínű, hogy a bűnözők külön erre a célra szolgáló titkosított eszközökre támaszkodnak az információk vagy a jogellenes tartalmak elrejtése érdekében. Ennélfogva a belátható jövőben továbbra is szükség lesz arra, hogy a bűnüldöző hatóságok érzékeny eszközöket[31] és kapacitásokat használjanak és esetleg megosszanak.

2. ajánláscsoport

Az érzékeny eszközök megosztása és a kapcsolódó kapacitások felelős kezelése érdekében a szakértők a következőket ajánlják:

1. *olyan mechanizmusok létrehozásának megfontolása, amelyek biztosítják, hogy az érzékeny eszközöket a nemzeti szabályok teljes körű tiszteletben tartása mellett lehessen megosztani [1. ajánlás];*

2. *az olyan kapacitások cseréjére irányuló külön folyamat kialakítása, amelyek potenciálisan kiterjednek a sérülékenységek kiaknázására, ami lehetővé tenné a tudás és az erőforrások egybegyűjtését annak biztosítása mellett, hogy tiszteletben tartják az információk bizalmas jellegét és érzékenységét [6. ajánlás];*

3. *a bűnüldöző hatóságok által kiaknázott sérülékenységek kezelésére és felfedésére vonatkozó európai megközelítés kialakításának esetleges megfontolása, a meglévő bevált gyakorlatok alapján [2. ajánlás].*

Az Európai Bizottság a Horizont Európa és a BBA révén támogatott olyan projekteket (*EXFILES* és *ForRES*[32]), amelyek kifejezetten a sérülékenységekre és a szoftverek kiaknázására irányulnak, és amelyek olyan eszközökkel és protokollokkal szolgálnak a bűnüldözési szakemberek számára, amelyek alkalmasak a gyors és következetes adatkinyerésre az összes vonatkozó jogi rendelkezés egyidejű betartása mellett.

---

31 „Érzékeny eszközök” alatt a digitális kriminalisztikai eszközöket és a taktikai lehallgatási eszközöket értjük.

32 https://forres.eu.

Az érzékeny eszközök és a kapcsolódó kapacitások megbízható európai partnerek közötti megosztása megkönnyíti az operatív együttműködést, lehetővé teszi a tudás közös felhasználásúvá tételét, és méretgazdaságosságot teremt, csökkentve a szükséges erőforrások nagyságát.

Bár a nyomozások szempontjából néha még mindig kulcsfontosságú a sérülékenységek kiaknázása, azt rendkívül körültekintően kell kezelni, a vonatkozó nemzeti jogi kerettel összhangban, mivel az kedvezőtlenül befolyásolja a hardverek és szoftverek biztonsági státuszát.

Fő intézkedés: A magas szintű munkacsoport szakértői szorgalmazzák az érzékeny eszközök megosztásának és a kapcsolódó kapacitások felelős kezelésének a támogatását

Szereplők: Tagállamok, Európai Bizottság | *Időkeret: 2024-től* | *Költségvetés: n. a.*

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy továbbra is támogassa – a megfelelő finanszírozási programokon keresztül – az érzékeny eszközök (mind a digitális kriminalisztikai eszközök, mind a taktikai lehallgatási eszközök) megosztására és az erőforrások összevonására irányuló projekteket; a Bizottság támogathatná **egy olyan transznacionális platform létrehozását is, amely az ismeretek strukturálását és megosztását szolgálná**.
- A magas szintű munkacsoport szakértői felkérik az Európai Bizottság Közös Kutatóközpontját, hogy vizsgálja meg annak megvalósíthatóságát, hogy a meglévő bevált gyakorlatokra építve kidolgozásra kerüljön a bűnüldöző hatóságok által kiaknázott **sérülékenységek kezelésére és felfedésére vonatkozó európai megközelítés**.

III. A digitális kriminalisztika területén a készségek fejlesztésére és a szakértelem bővítésére irányuló kollektív beruházások

A bűnüldöző szervek személyzete érintett tagjainak képzésben kell részesülniük a nyomozásaik során alkalmazandó nyomozási eszközök és technikák használatáról, és szakértelmüket tanúsítani kell. A szükséges és dokumentált kompetenciáiknak tükrözniük kell a feladatkörüket, és ki kell terjedniük legalább a mobileszközökkel kapcsolatos általános (eszközfüggetlen) digitális kriminalisztikára, a bizonyítékok felügyeleti láncával kapcsolatos kérdéskörökre, valamint a megszerzés, az elemzés, a jelentéstétel és a bíróság előtti bemutatás típusaira vonatkozó alapismeretekre. A dokumentációban fel kell tüntetni, hogy ezeket a kompetenciákat képzés útján vagy a munkájuk során szerezték-e meg.

3. ajánláscsoport

A digitális kriminalisztika területén a készségek és szakértelem – ideértve a visszafejtést és a szabványosítást is – fejlesztésének támogatása érdekében a szakértők a következőket ajánlják:

1. *a szakértők képzési lehetőségeinek számszerű növelése [7. ajánlás];*
2. *a digitális kriminalisztikai szakértők uniós szintű tanúsítási rendszerének létrehozása a részükre nyújtott szakmai képzés minőségének és egységességének biztosítása érdekében [7. ajánlás];*
3. *beruházás a szabványosítással kapcsolatos technikai készségek terén mutatkozó hiányosságok pótlása céljából, valamint a tudatosság növelése a tudományos élet képviselőivel és más érintett intézményekkel kötött megállapodások révén [8. ajánlás].*

A CEPOL számos idevágó témában tart tanfolyamokat[33]. A Kiberbűnözés Elleni Európai Képzési és Oktatási Csoport (ECTEG)[34] tanfolyamokat dolgoz ki a kiberbűnözésről és a digitális kriminalisztikáról, és azokat ingyenesen a CEPOL és a nemzeti bűnüldöző hatóságok rendelkezésére bocsátja.

Az ECTEG kidolgozta a *Decrypt* projektet, amely képzési anyagot biztosít az uniós tagállamok bűnüldöző hatóságai számára, melynek segítségével fejleszthetik jogszerű visszafejtési képességeiket a titkosított bizonyítékok jogszerű kezelésére irányuló kifinomult stratégiák révén. A Decrypt-et a CEPOL, valamint a nemzeti egységek is telepíthetik, a JRC által rendelkezésre bocsátott infrastruktúra felhasználásával.

---

[33] Digitális kriminalisztikai nyomozói képzés, mobil kriminalisztika, élőadat-kriminalisztika és Mac kriminalisztika.

[34] Az ECTEG nonprofit szervezet, amely 20 európai ország 30 bűnüldöző hatóságát, nemzetközi testületeket és a tudományos élet képviselőit tömöríti. A BBA támogatásával az ECTEG képzési erőforrásokat, megoldásokat és anyagokat dolgoz ki, népszerűsít és oszt meg. Lásd: https://www.ecteg.eu/.

Ugyanilyen fontos, hogy az elsődleges beavatkozók is rendelkezzenek a digitális kriminalisztikával kapcsolatos alapkészségekkel. Egyéb projektek mellett az ECTEG létrehozta az *eFirst* képzést („Educating law enforcement first responders on cyber-essentials” – Oktatás a bűnüldöző szervek elsődleges beavatkozói számára a kiberbűnözés elleni fellépés alapjairól). Az eFirst online, saját ütemben elvégezhető képzési modul, amelyet olyan rendőröknek szántak, akik a terepen dolgoznak (járőrök, helyszínelők, házkutatást végzők), vagy akiknek a feladata a sértettek első panasztételének felvétele. Alapismereteket nyújt a kiberbűnözésről és a digitális kriminalisztikáról. Alapul szolgálhat a rendőrségi akadémiákon tartott személyes képzésekhez is.

A szakértői profilok tanúsítása biztosítja, hogy minden személy rendelkezzen a szükséges ismeretekkel és készségekkel. Arra motiválja a szakembereket, hogy fejlesszék készségeiket, és naprakészek legyenek a szakterületüket érintő fejleményekkel kapcsolatban, emellett támogatja a szakmai előmenetelt és a személyes elismerést is. Ennek eredményeként pedig javul a munka minősége és pontossága. Ezenkívül a személyes tanúsítás révén:

- világosan és átláthatóan részletezni lehet a digitális kriminalisztikai szakértők készségeit és kompetenciáit, lehetővé téve a gyakorló szakemberek és az egységek vezetői számára annak azonosítását, hogy kire van szükségük ahhoz, hogy teljesüljenek az adott feladat hatékony ellátásához szükséges követelmények;

- könnyebbé válhat a nemzeti, regionális és uniós szintű képzések kidolgozása, valamint az vezérfonalként szolgálhat azok megszervezéséhez; az összes uniós tagállamra kiterjedő, összehasonlítható rendőrségi képzés biztosítja, hogy minden rendőr egységes szintű ismeretekhez és készségekhez férjen hozzá, függetlenül attól, hogy melyik országhoz tartoznak;

- javítható a bírósági eljárások átláthatósága;

- erősödhet a nyomozók és a többi szereplő közötti bizalom, ami fokozhatja a nemzeti bűnüldöző hatóságok közötti nemzetközi együttműködést.

A CEPOL megkezdte a rendfenntartás *ágazati képesítési keretrendszerének* kidolgozását, amely a határokon átnyúló együttműködésre összpontosít. E modell gyakorlati megvalósításához alapul szolgálhat az a munka, melyet az ECTEG végzett el a digitális kriminalisztikai szakértők tanúsítása terén *a kiberbűnözésre vonatkozó globális tanúsítási projekt*[35] keretében.

Mind az ECTEG, mind az EACTDA arra fordítja erőforrásai egy részét, hogy támogassa *az érintett bűnüldözési szakemberek szabványosítási folyamatokban való hatékony részvételét*, például azáltal, hogy elősegíti a szükséges készségek elsajátítását.

Fő intézkedés: A magas szintű munkacsoport szakértői a szakmai készségek javítását és a profilok tanúsítását szorgalmazzák

Szereplők: CEPOL, ECTEG	*Időkeret: az intézkedések folyamatban vannak; a digitális kriminalisztikai szakértők tanúsítási rendszerének 2026-ig kell létrejönnie*	*Költségvetés:*

- A magas szintű munkacsoport szakértői felkérik a CEPOL-t, hogy továbbra is **tartson** képzéseket (különös tekintettel az oktatók képzésére).
- A magas szintű munkacsoport szakértői felkérik az ECTEG-et, hogy folytassa a digitális kriminalisztikai tanfolyamok **kidolgozását, naprakésszé tételét és kísérleti jellegű megtartását** szakértők és elsődleges beavatkozók számára, különös hangsúlyt helyezve a visszafejtésre.
- A magas szintű munkacsoport szakértői üdvözlik, hogy a Bizottság jelenleg is támogatja az ECTEG-et (a BBA keretében meghirdetett nyílt pályázati felhívások útján), valamint a tanfolyamok **kihelyezését** regionális szintre.
- A magas szintű munkacsoport felkéri az ECTEG-et, hogy folytassa annak a lehetőségnek a feltérképezését, hogy uniós szintű tanúsítási rendszert vezessenek be a digitális kriminalisztikai szakértők számára, a CEPOL-t pedig arra, hogy a rendfenntartás **ágazati képesítési keretrendszerével** és a **kiberbűnözésre vonatkozó globális tanúsítási projekttel** kapcsolatos munkájukra építve a lehető legnagyobb mértékben járuljon hozzá ehhez az erőfeszítéshez.
- A magas szintű munkacsoport felkéri az ECTEG-et, hogy továbbra is segítse elő, hogy az érintett gyakorló szakemberek megszerezzék **a szabványosítási folyamatokkal kapcsolatos kompetenciákat és szakértelmet**.

[35] https://www.ecteg.eu/running/gcc/.

IV. A jogszerű hozzáférés megkönnyítése

A beépített jogszerű hozzáférést szabályozó normák nélkül a bűnüldöző hatóságoknak egyre gyakrabban kell ahhoz folyamodniuk, hogy kiaknázzák a sérülékenységeket annak érdekében, hogy hozzáférést szerezzenek azokhoz a lefoglalt eszközökhöz, amelyeken az információk titkosítással védettek. Amellett azonban, hogy ez a módszer előbbre lendítheti a nyomozásokat, magas pénzügyi költségekkel jár. Ezért át kell gondolni a lehetséges alternatívákat.

4. ajánláscsoport

Az érintett ágazati partnerekkel való együttműködés mechanizmusainak kialakítása, valamint annak a lehetőségnek a vizsgálata érdekében, hogy – az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatával összhangban – kötelező erejű normákat írjanak elő és közelítsék a jogszabályokat a jogszerű hozzáférés területén, a szakértők a következőket javasolják:

1. *az azzal kapcsolatos eszközök, bevált gyakorlatok és ismeretek megosztására szolgáló platform létrehozása (SIRIUS vagy azzal egyenértékű platform), hogy a terméktulajdonosok, a gyártók és a hardvergyártók hogyan biztosíthatnak hozzáférést az adatokhoz [11. ajánlás];*

2. *bűnüldözési kapcsolattartó pontok létesítésének feltérképezése a digitális hardver- és szoftvergyártók körében [11. ajánlás];*

3. *a tagállamok hatályos jogszabályainak átfogó feltérképezése és az azokat ismertető uniós kézikönyv kidolgozása a digitális hardver- és szoftvergyártók azzal kapcsolatos jogi felelősségének részletes taglalása érdekében, hogy eleget tegyenek a bűnüldöző szervektől érkező adatigényléseknek, figyelembe véve azokat a konkrét forgatókönyveket és követelményeket, amelyek esetében a vállalatok kötelesek hozzáférést adni az eszközökhöz [25. ajánlás];*

4. *kutatócsoport létrehozása a digitális készülékekre vonatkozó beépített jogszerű hozzáféréssel (beleértve a titkosított adatokhoz való hozzáféréssel) kapcsolatos kötelezettségek műszaki megvalósíthatóságának értékelésére; e hozzáférési kötelezettségeket úgy kell megállapítani, hogy fennmaradjon és ne csorbuljon a készülékek biztonsága és az információk védelme valamennyi felhasználó számára, valamint hogy e hozzáférési kötelezettségek ne gyengítsék és ne ássák alá a hírközlés biztonságát [26. ajánlás];*

5. *a fent említett feltérképezéstől függően kötelező érvényű ipari szabványok kidolgozása az EU-ban forgalomba hozott eszközökre vonatkozóan, a jogszerű hozzáférés integrálása és az e területre vonatkozó jogszabályok közelítésének előmozdítása érdekében [25. ajánlás].*

A bűnüldöző szervek iparral való jelenlegi együttműködése nem vezet konkrét eredményekre; a bűnüldöző hatóságok eszközökhöz és alkalmazásokhoz való jogszerű hozzáférését célzó útvonalak kialakítása érdekében meg kell erősíteni az iparral folytatott együttműködést. Például a videokamerás megfigyelés felvételei esetében a bűnüldöző hatóságok egyre gyakrabban szembesülnek olyan titkosított fájlokkal, amelyeket nem lehet automatikus szoftverrel elemezni, különösen akkor, ha nagy mennyiségű videofelvételről van szó.

Elméletileg a bűnüldöző hatóságok támogatást kérhetnek az eszközgyártóktól, amelyek megadhatják a szoftverük forráskódját annak érdekében, hogy megkönnyítsék a titkosítatlan tartalmi adatokhoz való hozzáférést, vagy pedig rendelkezésre bocsáthatják a bűnügyi nyomozások során fellelt berendezések műszaki dokumentációját.

Az Europol megfelelő helyzetben lenne ahhoz, hogy összegyűjtse a bevált gyakorlatokat (például bűnüldözési kapcsolattartó pontok létrehozásával) és az azzal kapcsolatos ismereteket, hogy a terméktulajdonosok, a gyártók és a hardvergyártók hogyan könnyíthetnék meg a hozzáférést, és ezeket az ismereteket aztán elérhetővé tehetné az összes bűnüldöző hatóság részére a SIRIUS-on (vagy egy azzal egyenértékű platformon) keresztül.

Ezzel párhuzamosan a nyomozások hatékonyságának növelése és ezzel egyidejűleg az ágazati szereplők közötti egyenlő versenyfeltételek biztosítása érdekében olyan átláthatóbb megoldásokat kell fontolóra venni, amelyek lehetővé teszik a lefoglalt eszközökön lévő titkosítatlan adatokhoz való hozzáférést, a kiberbiztonság megőrzése és a magánélet védelme mellett.

A szakértők sürgetik az Európai Bizottságot, hogy a jogszerű hozzáférésre vonatkozó bűnüldözési követelmények részletes elemzése alapján dolgozzon ki egy *technológiai ütemtervet*[36], amely egy helyen tartalmazza a technológiai, kiberbiztonsági, adatvédelmi, szabványosítási és biztonsági szakértők által végzendő intézkedéseket, és biztosítja a megfelelő koordinációt.

E technológiai ütemterv egyik fő intézkedése annak értékelése lenne, hogy *technikailag megvalósítható-e* a digitális fájlokhoz és eszközökhöz való, *beépített jogszerű hozzáférés kötelezettsége* (ideértve a titkosított adatokhoz és a titkosított CCTV-felvételekhez való hozzáférést is)[37], szigorú kiberbiztonsági biztosítékok szavatolása mellett, a hírközlés biztonságának gyengítése vagy aláásása nélkül. Ezt az értékelést az összes érdekelt fél bevonásával végeznék el.

---

[36] A jelentés több helyen és fejezetben is egyetlen konkrét „technológiai ütemtervre” hivatkozik.

[37] Lásd: A titkosítással kapcsolatos szakpolitikai párbeszéd előbbre vitele – Carnegie Alapítvány a Nemzetközi Békéért (Moving the Encryption Policy Conversation Forward’ - Carnegie Endowment for International Peace) - https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Amennyiben ezen értékelés megerősítené, hogy a fenti feltételeknek megfelelő, beépített jogszerű hozzáférés kötelezettsége megvalósítható, a technológiai ütemtervnek meg kell határoznia *a szabványügyi testületekkel való* tartós, hosszú távú *együttműködés* folyamatát is. A bűnüldöző szervek e szabványosítási folyamatban való részvételét az Europol koordinálhatná az EACTDA támogatásával.

A digitális hardver- és szoftvergyártóknak a bűnüldöző hatóságoktól érkező adatigénylések teljesítésével kapcsolatos felelősségét meghatározó meglévő tagállami jogi keretek feltérképezése alapján fel lehetne mérni, hogy szükség van-e *jogszabályokra, illetve iránymutatásokra és ajánlásokra* [az e területre vonatkozó jogszabályok közelítésének előmozdítása érdekében].

Fő intézkedés: A magas szintű munkacsoport szakértői szorgalmazzák az iparral való együttműködés fokozását, az érintett szabványokra való hivatkozások fokozottabb említését a közelgő uniós kezdeményezésekben, valamint a jogszerű hozzáférésre vonatkozó jogszabályok közelítését az EUB és az Emberi Jogok Európai Bírósága ítélkezési gyakorlatával összhangban

Szereplők: Europol; Európai Bizottság *Időkeret: 2025-től* *Költségvetés: n. a.*

- A magas szintű munkacsoport szakértői felkérik az **Európai Bizottságot**, hogy dolgozzon ki célzott **technológiai ütemtervet** a digitális eszközökhöz való jogszerű hozzáférés lehetőségeinek feltérképezése céljából.
- A magas szintű munkacsoport szakértői felkérik az **Europolt**, hogy gyűjtse össze a bevált gyakorlatokat és az azzal kapcsolatos ismereteket, hogy a terméktulajdonosok, a gyártók és a hardvergyártók hogyan könnyíthetnék meg a hozzáférést, és ezeket az ismereteket aztán tegye elérhetővé az összes bűnüldöző hatóság részére a **SIRIUS**-on (vagy egy azzal egyenértékű platformon) keresztül.

II. fejezet: Adatmegőrzés

MIK A NEHÉZSÉGEK?

A múltban az összegyűjtött bizonyítékok elsődleges formája a fizikai bizonyíték volt, manapság viszont a hírközlési szolgáltatók hatalmas mennyiségű potenciális bizonyítékot tárolnak metaadatok formájában. Bár a bűnügyi nyomozások során nem a digitális adatok jelentik az egyetlen szükséges bizonyítékot, ez a típusú bizonyíték szinte valamennyi nyomozás során kritikus fontosságú – különösen azon gyanúsítottak vagy célszemélyek személyazonosságának megállapítása szempontjából, akik releváns információkkal rendelkezhetnek –, függetlenül attól, hogy ezen adatok a fizikai vagy a digitális világban elkövetett bűncselekményekhez kapcsolódnak-e. Különösen ez utóbbit illetően gyakran a hírközlési metaadatok (nevezetesen az IP-címek és a portszámok) képezhetik az egyetlen módját a gyanúsítottak azonosításának[38].

Ezért ahhoz, hogy a bűnüldözés képes legyen a digitális korban elkövetett bűncselekmények nyomozására, a digitális bizonyítékokat olvasható formátumban kell rendelkezésre bocsátani, és azoknak szükség esetén hozzáférhetőknek kell lenniük, kellően tiszteletben tartva a büntetőeljárásokra vonatkozó megfelelő biztosítékokat, az eljárási jogokat, valamint a magánélet és az adatok védelmét. Az adatok megőrizhetők üzleti (például számlázási) vagy bűnüldözési célból. Az adatmegőrzés segíthet annak biztosításában, hogy az adatok rendelkezésre álljanak, és az illetékes hatóságok hozzáférhessenek azokhoz a bűnügyi nyomozások és a büntetőeljárások keretében. A szolgáltatók által megőrzött adatok döntő fontosságúak lehetnek a bűnözés elleni hatékony küzdelem szempontjából, és ezen adatok megőrzése előfeltétele annak, hogy a bűnüldöző szervek később hozzá tudjanak férni azokhoz, valamint annak, hogy a bűnüldöző hatóságok le tudják folytatni a nyomozásokat[39]. Ugyanakkor az elektronikus hírközlési adatvédelmi irányelvben[40] és az általános adatvédelmi rendeletben (GDPR)[41] meghatározott adattakarékossági elv előírja, hogy a szolgáltatók csak addig tárolhatják (vagy más módon kezelhetik) a forgalmi adatokat, amíg az magához a kommunikációhoz, a számlázáshoz vagy – bizonyos esetekben – az elektronikus hírközlési szolgáltatások értékesítéséhez szükséges. Minden egyéb adattárolást az elektronikus hírközlési adatvédelmi irányelv 15. cikkében meghatározott követelményeknek megfelelő jogi keretnek kell szabályoznia. Ez a rendszer azt tükrözi, hogy egyensúlyt kell teremteni a magánélethez és az adatvédelemhez való alapvető jogok, valamint a bűnüldözési intézkedések céljai között.

---

38 A szakértők több példát is megvitattak a digitális adatok nyomozásokban való relevanciájával és az adatkikérések számával kapcsolatban. Az egyik szakértő szerint az elmúlt öt évben a terrorizmussal vagy a szervezett bűnözéssel kapcsolatos valamennyi nyomozás során felhasználtak szolgáltatóktól kikért adatokat. 2023-ban az egyik tagállamban több mint 1 300 000 számot kértek ki gazdasági szereplőktől a büntetőeljárások során történő azonosítás céljából, és az igazságszolgáltatási rendszer később csaknem mindegyiküket validálta.

39 E dokumentum alkalmazásában az „adatokhoz való hozzáférés” alatt a bűnüldözés számára, előzetes bírói engedélyhez kötöttség esetén ilyen engedély alapján, nyomozási célokra, eseti alapon biztosított hozzáférés értendő.

40 2002/58/EK irányelv, 6. cikk.

41 (EU) 2016/679 rendelet, 5. cikk (1) bekezdés c) pont.

Jelenleg nincs olyan uniós jogszabály, amely szabályozná az adatmegőrzést. Az EUB 2014-ben megsemmisítette az uniós adatmegőrzési irányelvet[42], felhívva a figyelmet arra, hogy a szolgáltatók által eredetileg gyűjtött adatok bűnüldözési célból történő [általános és különbségtétel nélküli] tárolása jelentős mértékben sérti a magánélethez és az adatvédelemhez való alapvető jogot[43]. Ennek eredményeként a nemzeti jogi keretek olyan változásokon mentek keresztül, amelyek nyomán jelentős különbségek keletkeztek az EU-ban[44]: míg egyes tagállamokban még mindig vannak olyan szabályok, amelyek arra kötelezik a hírközlési szolgáltatókat, hogy bűnüldözési célból őrizzenek meg bizonyos kategóriákba tartozó adatokat, más tagállamok változtatásokat hajtottak végre annak érdekében, hogy teljesítsék a forgalmi adatok célzott megőrzésére vonatkozó, az ítélkezési gyakorlatban javasolt kritériumot;[45] mások pedig – szintén a nemzeti bíróságok későbbi ítéletei miatt – nem rendelkeznek a bűnüldözési célú adatmegőrzésre vonatkozó külön szabályokkal, és kizárólag a vállalatok által üzleti célból megőrzött adatokra támaszkodnak. Az ilyen adatokhoz való hozzáférés feltételei az alkalmazandó nemzeti jogi kerettől és az adatok típusától (előfizetői, forgalmi vagy tartalmi adatok) függenek. A koherens és harmonizált uniós adatmegőrzési kötelezettségeknek ez a hiánya azt eredményezi, hogy a tagállamok között eltérések mutatkoznak a különböző típusú metaadatok szolgáltatók általi megőrzését (és annak időtartamát) szabályozó követelmények terén.

---

42 2006/24/EK irányelv. Az irányelv arra kötelezte az uniós tagállamokat, hogy fogadjanak el intézkedéseket annak biztosítására, hogy az elektronikus hírközlési szolgáltatásokat és hálózatokat nyújtó szolgáltatók hat hónaptól két évig terjedő időtartamra őrizzék meg a forgalmi és helymeghatározó adatokat, továbbá az előfizető vagy a nyilvántartott felhasználó azonosításához szükséges kapcsolódó adatokat annak érdekében, hogy az illetékes hatóságok hozzá tudjanak férni azokhoz a nemzeti jogszabályokban meghatározott súlyos bűncselekmények nyomozása, felderítése és büntetőeljárás alá vonása céljából.

43 A vonatkozó ítélkezési gyakorlat áttekintését lásd: A nemzeti adatmegőrzési kötelezettségek jövője – Hogyan kell nemzeti szinten alkalmazni a Digital Rights Ireland ügyben hozott ítéletet? (The future of national data retention obligations – How to apply Digital Rights Ireland at national level?) – European Law Blog (Európai jogi blog), V. Franssen; Az adatmegőrzés újrakalibrálása az EU-ban (Recalibrating Data Retention in the EU)– eucrim; az Eurojust/EJCN 2024. évi jelentése. Az Európai Unió Bírósága ítélkezési gyakorlatának hatása a nemzeti adatmegőrzési rendszerekre és az EU-n belüli igazságügyi együttműködésre (The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU); Kiberbűnözési Igazságügyi Figyelő – 6. szám; Kiberbűnözési Igazságügyi Figyelő – 9. szám.

44 A tagállamok eltérő válaszokat adtak az adatmegőrzési irányelv megsemmisítésére, és a nemzeti szinten kezdeményezett intézkedések nyomán megnőtt a nemzeti adatmegőrzési rendszerek sokfélesége. Az Eurojust/EJCN 2024. évi adatmegőrzési jelentése szerint a 2018–2022-es időszakban 12 ország módosította a jogszabályait. A válaszadók arról számoltak be, hogy ezek a módosítások közvetlen következményei az EUB következő ügyeinek: a C-746/18. sz. *Prokuratuur* ügy, valamint a C-511/18., C-512/18. és C-520/18. sz. *La Quadrature du Net és társai* egyesített ügyek. A 27 tagállamból 23 rendelkezik adatmegőrzési szabályokkal; hét tagállam vezetett már be célzott adatmegőrzési szabályokat. A kérdés áttekintését lásd: A Bizottság tanulmánya az elektronikus hírközlés nem tartalmi adatainak bűnüldözési célú megőrzéséről (Commission Study on the retention of electronic communications non-content data for law enforcement purposes), 2020, 39. o.

45 A Bíróság több ítéletben dolgozta ki a forgalmi és helymeghatározó adatok célzott megőrzésének fogalmát, és úgy határozott, hogy az adatok megőrzése összeegyeztethető lehet az uniós jogszabályokkal, amennyiben az az adatok konkrét, célzott körére irányul, és meghatározott célokból történik. Azonban az adatok ilyen célzott körének meghatározásához a Bíróság által javasolt kritériumok gyakorlati alkalmazása nehézségekbe és kihívásokba ütközött azon tagállamok felsőbíróságain, amelyek azt megkísérelték.

Azon tagállamokban, amelyek nem írnak elő adatmegőrzési kötelezettséget, nehéz vagy néha lehetetlen azonosítani a gyanúsítottakat vagy az olyan személyeket, akik egy bűnügyi nyomozás során releváns információval rendelkezhetnek („célszemély”)[46]. Az elektronikus bizonyítékokra vonatkozó új szabályok hozzáadott értékét a hatálybalépésüket követően az is növelné, ha adatmegőrzési kötelezettségekkel egészülnének ki, ellenkező esetben ugyanis nincs garancia arra, hogy a megőrzésre vagy közlésre kötelező európai határozatok hatálya alá tartozó információk (ide tartoznak a forgalmi adatok, a kizárólag a felhasználó azonosítása céljából kikért adatok és az előfizetői adatok) rendelkezésre fognak állni.

A jelenlegi körülmények egyaránt érintik a **bűnüldöző szerveket** és a **hírközlési szolgáltatókat**, de ami a legfontosabb, **hatással vannak a polgárokra és az áldozatokra** is, akik számára nem biztosítható az igazságszolgáltatáshoz való jog, ha a nyomozás elindításakor az adatokat már törölték, vagy pedig nem őrizték meg azokat[47].

I. Az egyes tagállamok joghatósága alá tartozó kérdések

Azokban a tagállamokban, **ahol nincsenek konkrét kötelezettségek** a bűnüldözési célú adatmegőrzésre vonatkozóan, a nyomozások – az esetlegesen rendelkezésre álló egyéb bizonyítékok mellett – a vállalatok által üzleti és kereskedelmi célból tárolt adatokra támaszkodnak. A kereskedelmi adatok a szolgáltatók belső politikáinak hatálya alá tartoznak: a vállalatok a forgalmi adatokat különböző időszakokra (pl. körülbelül 6 hónapra) tárolják, a helymeghatározó adatokat pedig – amelyek általában nem bírnak üzleti jelentőséggel – gyakran még rövidebb ideig. A kisvállalkozások gyakran egyáltalán nem, vagy csak nagyon rövid ideig tárolják az előfizetői vagy a hírközlési metaadatokat. Ennek eredményeként a nyomozások gyakran versenyfutást jelentenek az idővel, mivel a nyomozóknak azonosítaniuk kell az adatszolgáltatót, és a vonatkozó szabályokkal összhangban, még az adatok törlése előtt továbbítaniuk kell a megkeresést, ami néha csupán napok vagy órák kérdése. Egyes esetekben a vállalatok nem nyújtanak tájékoztatást az általuk kezelt és tárolt konkrét adatokról, ami megnehezíti az illetékes hatóságok számára, hogy célzott megkereséseket nyújtsanak be, amikor adatokra van szükségük. Egyes tárhelyszolgáltatások lehetővé teszik a felhasználók számára, hogy fiktív adatok felhasználásával béreljenek szervertárhelyet, ami azt jelenti, hogy még ha tárolnak is felhasználói adatokat, azok nem megbízhatók[48].

---

[46] Példákért lásd: Háttérdokumentum – Az adatokhoz való hozzáféréssel kapcsolatban a bűnüldözés előtt álló operatív kihívások (Background document Operational challenges faced by law enforcement related to access to data) – A hatékony bűnüldözést szolgáló adathozzáféréssel foglalkozó magas szintű munkacsoport első plenáris ülésére benyújtott hozzájárulás, 4. o.

[47] A polgárokra és az áldozatokra gyakorolt hatással kapcsolatban lásd: *Dwyer kontra Commissioner of An Garda Siochána* – [2020] IESC 4 (2020.2.24.), és különösen annak 9. pontja.

[48] https://en.wikipedia.org/wiki/Bulletproof_hosting.

A legtöbb tagállamban **érvényben vannak adatmegőrzésre** vonatkozó jogszabályok. Azonban, mint ahogy azt már fentebb ismertettük, néhány nemzeti jogszabály módosult az EUB ítéletei nyomán, az adatmegőrzési irányelv érvénytelenítését követően. A tagállamok eltérő válaszokat adtak az ítéletekre, így változatos jogi környezet alakult ki. Egyes tagállamok arra irányuló erőfeszítéseket tettek, hogy bevezessenek egy célzott adatmegőrzési formát, amit az EUB az egyik lehetséges megoldásként javasolt az adatmegőrzés kapcsán. A magas szintű munkacsoport szakértői azonban hangsúlyozták, hogy e kritériumok végrehajtása jogi és technikai kérdéseket vet fel a megvalósíthatóságukat illetően[49], a szolgáltatók pedig bírálták a célzott megőrzés technikai végrehajtásával kapcsolatos költségeket, és nagyobb általánosságban a jogszabályok gyakori változását. Egy nemzeti szinten felmerült másik fontos jogi kérdés az, hogy a nemzeti jogszabályok a legtöbb esetben nem terjednek ki az OTT-szolgáltatásokra. Az OTT-szolgáltatások konkrét esetét a lenti 1.3. pont tárgyalja részletesebben.

II. Határokon átnyúló vonatkozású nehézségek az EU-ban

Adatmegőrzéssel kapcsolatos nehézségek a határokon átnyúló megkeresésekkel kapcsolatban is felmerülnek, nevezetesen amikor az illetékes hatóság egy másik tagállamban székhellyel rendelkező szolgáltatótól kér adatokat. Előfordulhat, hogy a határokon átnyúló megkereséseket magukban foglaló esetekben a fogadó ország hatóságai (az adatok vagy a vonatkozó jogszabályok hiánya miatt) nem tudnak teljesíteni egy másik ország által kibocsátott megkeresést.

A metaadatok megőrzésére vonatkozó harmonizált uniós szintű kötelezettségek hiánya akadályozza a tagállamok bűnüldöző szerveit abban, hogy **adatokat kérjenek** más tagállamokban székhellyel rendelkező szolgáltatóktól. Még ha nemzeti szinten léteznek is adatmegőrzési rendszerek, az adatmegőrzési időszakok vonatkozásában nincs összhang a nemzeti rendszerek között, és az egyes tagállamok között jelentős eltérések tapasztalhatók[50].

---

[49] Bár az EUB némi iránymutatással és példákkal szolgál arra vonatkozóan, hogy hogyan kell értelmezni a forgalmi adatok **célzott megőrzését**, az ítélkezési gyakorlat csak iránymutatásokkal szolgálhat, és nem elég konkrét ahhoz, hogy részletesen kifejtse az összes adatkategória megőrzésének lehetséges korlátait. Ennek következtében az elmúlt években a Bíróság elé terjesztettek több, az adatmegőrzési szabályokkal szembeni ügyet, a tagállamok pedig nincsenek abban a helyzetben, hogy jogbiztonságot nyújtsanak.

[50] Az adatoktól és a bűncselekmény típusától függően a metaadatok megőrzésének időtartama 6 és 72 hónap között változhat. Az Eurojust/EJCN 2024. évi adatmegőrzési jelentésében a válaszadók jelezték, hogy a megőrzött adatok hiánya, a megőrizhető adatkategóriákra vonatkozó korlátozások és a rövid(ebb) adatmegőrzési időtartamok miatt kevesebb adat állt rendelkezésre. Az, hogy nem állnak rendelkezésre adatok, következésképpen befolyásolja a hatóságok azon képességét is, hogy végrehajtsák az európai nyomozási határozatokat és a kölcsönös jogsegély iránti megkereséseket.

Hasonlóképpen, uniós szinten nem létezik harmonizált megközelítés a megőrzendő **adatok meghatározására** vonatkozóan sem[51]. A nemzeti jogszabályok különböző kategóriájú adatok különböző célokból való (adók, auditok, bűnüldözés) megőrzésére kötelezhetik a szolgáltatókat. Abban is eltérhetnek egymástól, hogy ezt milyen szintű részletességgel teszik: egyes jogszabályok részletes felsorolást tartalmaznak a megőrzendő nem tartalmi adatokról, míg mások lazábban határozzák meg a nem tartalmi adatokat[52]. A szolgáltatók emellett az általuk kínált szolgáltatástól, valamint az üzleti és kereskedelmi igényeiktől függően is különböző típusú adatokat tárolnak különböző időtartamokra. Ez rendkívül változatos környezetet eredményez, ahol nem csupán a tagállamok között, de az egyes szolgáltatások között is jelentős eltérések vannak.

Ezek az eltérések a tagállamok között a megőrzött adatokhoz való hozzáférés tekintetében fennálló különbségek miatt is fontosak: egyes tagállamok bírói engedélyt írnak elő a metaadatok bizonyos típusaihoz való hozzáférés tekintetében, mások viszont nem. A szolgáltatók arról számolnak be, hogy az adatok közlésére alkalmazandó szabályokkal kapcsolatos jogbizonytalanság az egyik oka a késedelmeknek, valamint annak, hogy nem teljesítik a bűnüldöző szervek megkereséseit.

---

[51] Az adatmegőrzésről szóló bizottsági tanulmányban foglaltak szerint (48. o.): Bizonyos típusú információkat minden tagállam előfizetői vagy forgalmi adatként sorol be, nincs azonban egyetértés a következő adatpontok besorolását illetően: IP-címek, SIM-kártya-számok, eszközazonosító számok (pl. IMSI, IMEI), valamint a dinamikus IP-címek portszámai. Egyes tagállamok (EE, FR, IE) ezeket az adatpontokat előfizetői adatoknak, míg mások (DE, ES, IT, PL, SI) forgalmi adatoknak tekintik.

[52] Az egyes tagállamokban megőrzött adatok áttekintéséért lásd az adatmegőrzésről szóló bizottsági tanulmány III. mellékletét.

Az illetékes hatóságoknak meg kell felelniük egyrészt a kért adatokat birtokló szolgáltatóra alkalmazandó nemzeti szabályozásoknak, másrészt pedig a maguk a szolgáltatók által meghatározott egyedi követelményeknek is. A SIRIUS 2022. évi éves jelentésében[53] foglaltak szerint a szolgáltatók előírhatják a külön erre a célra létrehozott portálok használatát, vagy a megkeresések meghatározott formanyomtatványokon vagy nyelveken történő benyújtását. Megkövetelhetik továbbá az ügy jellegéről történő tájékoztatást, a megkeresés nemzeti jogalapjára való egyértelmű hivatkozást vagy szűk időkeretek megadását a kért adatokkal kapcsolatban. Bár e kérdések közül néhányra megoldást nyújt majd az elektronikus bizonyítékokról szóló csomag 2026-ig sorra kerülő végrehajtása, a magas szintű munkacsoport szakértői hangsúlyozták, hogy koherenciára van szükség e szabályok, illetve az adatmegőrzésre vonatkozó bármilyen esetleges harmonizált keret között. Az Európai Távközlési Szabványügyi Intézet (ETSI) kidolgozott ugyan szabványokat a számfüggő személyközi hírközlési szolgáltatásokkal (hagyományos távközlés) kapcsolatos metaadatok iránti megkeresések formátumára vonatkozóan, a szolgáltatók azonban nem alkalmazzák ezeket következetesen a tagállamokban. Az OTT[54]-szolgáltatók által a bűnüldöző hatóságoknak történő adattovábbításra vonatkozó szabványok kidolgozása még folyamatban van, és nem került sor azok teljes körű végrehajtására. Ezenkívül a szolgáltatók szabadon dönthetnek arról, hogy milyen formában gyűjtik és tárolják a felhasználói adatokat, ami azt eredményezi, hogy a szakemberek nagyon eltérő formában kapnak nyers adatokat; ez jelentős terhet ró a bűnüldözésre, amely számára előnyös lenne a megkeresések benyújtására, valamint a megkeresésekre adott válaszok és az adatok küldésére és fogadására vonatkozó eljárások, **hírközlési rendszerek és formátumok** észszerűsítése. A szabványosított hírközlési rendszerek és formátumok egyúttal a megkeresések feldolgozásával járó költségeket is csökkentenék a vállalatok számára.

Azt követően, hogy a bűnüldöző szervek jogszerűen hozzáfértek az adatokhoz, képesnek kell lenniük kiaknázni azokat; az adatoknak ezért **olvashatóknak** kell lenniük. A szolgáltatók azonban egyre gyakrabban kínálnak olyan szolgáltatásokat, amelyek lehetővé teszik a forgalmi adatok végponttól végpontig terjedő titkosítását, és amikor ezeket az adatokat kérésre a bűnüldöző és az igazságügyi hatóságok rendelkezésére bocsátják, azokat gyakran ilyen titkosított formában adják át.

---

53 sirius-eu-digital-evidence-situation-report-2022, 14. o.

54 E jelentésben az „over-the-top (OTT) hírközlési szolgáltatások” olyan alkalmazásokat és szolgáltatásokat jelölnek, amelyek kommunikációs és médiaszolgáltatásokat (például üzenetküldést, valamint hang- és videohívásokat) nyújtanak az interneten a hagyományos távközlési szolgáltatók (távközlési vállalatok) bevonása vagy ellenőrzése nélkül. Az OTT hírközlési szolgáltatások közé többek között a következők tartoznak: üzenetküldő alkalmazások, például a WhatsApp, a Telegram, a Facebook Messenger; hang- és videohívásokat biztosító szolgáltatások, például a Skype, a Zoom, a Google Meet, a Viber; valamint közösségimédia-platformok, például az Instagram és a Snapchat (üzenetküldés és médiamegosztás).

Végezetül e status quo másik érzékelhető következménye annak kockázatához kapcsolódik, hogy a bűnüldöző szervek **bizonyítékait** bíróság előtt **megtámadhatják**[55]. Az EUB egyértelművé tette, hogy az adatmegőrzéssel szerzett bizonyítékok elfogadhatósága a nemzeti jog hatálya alá tartozik[56], az egyenértékűség és a tényleges érvényesülés elvére is figyelemmel[57]; a nemzeti adatmegőrzési rendszerek közötti különbségek következésképpen hatással lehetnek a bizonyítékok elfogadhatóságára a határokon átnyúló eljárásokban[58].

[55] Lásd az Eurojust/EJCN 2024. évi adatmegőrzési jelentésének „A bizonyítékok gyűjtése és elfogadhatósága” (Collection and admissibility of evidence) című fejezetét.

[56] A Bíróság 2020. október 6-i ítélete, La Quadrature du Net és társai, C-511/18, ECLI:EU:C:2020:791, 222–228. pont; 2022. április 5-i ítélet, Commissioner of An Garda Síochána és társai, C-140/20, ECLI:EU:C:2022:258, 127. pont.

[57] Ugyanott, 223. pont: „…azzal a feltétellel [...], hogy e szabályok nem lehetnek kedvezőtlenebbek a hasonló jellegű belső jogi helyzetekre vonatkozókhoz képest (az egyenértékűség elve), és nem tehetik gyakorlatilag lehetetlenné vagy rendkívül nehézzé az uniós jog által biztosított jogok gyakorlását (a tényleges érvényesülés elve)”.

[58] Több bírósági ügyben is vitatták a nem tartalmi adatok bizonyítékként való elfogadhatóságát. Ezek összefoglalóját lásd az adatmegőrzésről szóló bizottsági tanulmány 41. oldalán.

III. Az OTT- és más szolgáltatókkal kapcsolatos nehézségek

Míg a fenti kérdések az elektronikus hírközlési szolgáltatásokat nyújtó valamennyi szolgáltatót érintik, az OTT-szolgáltatók esetében az adatokhoz való jogszerű hozzáférés terén további kihívások merülnek fel a bűnüldöző hatóságok számára. Nemzeti és uniós szinten is megfigyelhető, hogy az OTT-szolgáltatók gyakran úgy vélik, hogy rájuk nem alkalmazandók a hagyományos hírközlési szolgáltatókra vonatkozó kötelezettségek. Az OTT-szolgáltatók az EEHK hatálya alá tartoznak ugyan, viszont az a tény, hogy gyakran az EU-n kívüli székhellyel rendelkeznek, és nem vonatkoznak rájuk engedélyezési rendszerek (azaz előfordulhat, hogy csak általános felhatalmazások hatálya alá tartoznak) és szankciók, bizonytalansághoz vezet az adatmegőrzési kötelezettségeiket illetően – meghatározott adattípusokat is beleértve –, és megnehezíti a megfelelés kikényszerítését. Ezen túlmenően, a hagyományos hírközlési szolgáltatók a legtöbb esetben üzleti célból megőriznek bizonyos, a felhasználók azonosítását lehetővé tévő adatokat (például IP-számokat a portszámmal és az időtartománnyal együtt), ez viszont nem igaz az **OTT-szolgáltatókra**, amelyek csupán a kereskedelmi céljaikhoz szükséges nem tartalmi adatokat őrzik meg, és egyes esetekben azokat is csak rövid ideig[59]. Az OTT-szolgáltatók nem őriznek meg semmilyen dinamikus IP-címhez kapcsolódó nem tartalmi adatot (portszám és időtartomány). Ez megnehezítheti vagy akár lehetetlenné is teheti az olyan, egyre szélesebb körben használt rendszereken folytatott kommunikáció metaadatainak visszanyerését, mint például a WhatsApp vagy a Telegram. Ahogyan már említettük, a megőrzött adatok típusai a nyújtott szolgáltatástól függően is változnak. Míg a szolgáltatók egyes esetekben iránymutatásokat adnak ki, amelyekben ismertetik az általuk megőrzött adattípusokat[60], más esetekben az OTT-szolgáltatók nem tesznek közzé ilyen információt. Ez párosulva azzal, hogy a szolgáltatókra nem vonatkoznak **kötelezettségek** az általuk üzleti célból előállított, kezelt és tárolt adatok típusainak **átláthatóságára** vonatkozóan, gyakran problémákat okoz a bűnüldöző hatóságok számára, amikor megpróbálják azonosítani, hogy a szolgáltatók megőriztek-e adatokat, ki milyen adatokat tárol és milyen típusú adatkészleteket lehet kikérni, és végső soron amikor megkereséseket küldenek a szolgáltatóknak.

---

[59] Ez különösen igaz a kis szolgáltatók esetében. Az adatmegőrzésről szóló bizottsági tanulmány (103. oldal) szerint az IP-címeket átlagosan 30 napig őrzik meg.

[60] Lásd például itt: law-enforcement-guidelines-outside-us.pdf (apple.com).

Ugyanakkor a szolgáltatókhoz beérkező megkeresések növekvő mennyisége[61] azzal együtt, hogy nagy méretű adatkészleteket kell feldolgozniuk, hozzájárul ahhoz, hogy egyes megkeresések esetében késedelemre vagy elutasításra kerül sor[62]. A szolgáltatóknak az üzleti modelljükkel kapcsolatos konkrét döntéseiből eredő okok mellett ez betudható még annak is, hogy **korlátozott számú együttműködési mechanizmus** áll rendelkezésre egyrészt a bűnüldöző és az igazságügyi hatóságok, másrészt pedig a magánvállalatok között.

Végezetül, még ha nem is tartoznak az EEHK hírközlési szolgáltatókra vonatkozó fogalommeghatározásának hatálya alá, egyes kialakulóban lévő technológiák és más digitális szereplők (például autógyártók és a nagy nyelvi modellre (LLM) épülő MI-rendszerek) olyan kommunikációs metaadatokat állítanak elő és kezelnek, amelyek információkkal szolgálhatnak bűnözői tevékenységekről. Annak ellenére, hogy ezek a szolgáltatások egyre nagyobb mennyiségű adatot kezelnek, jelenleg nem vonatkoznak rájuk adatmegőrzési kötelezettségek.

LEHETSÉGES MEGOLDÁSOK

I. A hírközlési szolgáltatók és a gyakorló szakemberek közötti együttműködés megerősítése

Egy olyan környezetben, ahol a harmonizált szabályok hiánya akadályozza az elektronikus bizonyítékok gyűjtését, a bűnüldöző hatóságoknak gyakran a szolgáltatókkal való **önkéntes együttműködésre** kell támaszkodniuk a nyomozások lefolytatása során. Ez a megoldás segítséget jelentett bizonyos kiemelt jelentőségű nyomozásokban[63], ugyanakkor jogbizonytalanság jellemzi, és nem mindig kivitelezhető: az önkéntes együttműködés a szolgáltató típusától és méretétől függ, a kisebbek ugyanis – a nagyobbaktól eltérően – gyakran nagyon rövid ideig őrzik meg az adatokat, vagy nem rendelkeznek az ahhoz szükséges erőforrásokkal, hogy válaszoljanak a bűnüldöző hatóságok megkereséseire[64].

---

61 A SIRIUS 2023. évi éves jelentése szerint a szolgáltatókhoz benyújtott adatigénylések száma évről évre folyamatosan növekszik (lásd a 66. és azt követő oldalakat).

62 A SIRIUS 2023. évi éves jelentése (61. lábjegyzet) áttekintést nyújt az elektronikus bizonyítékok iránti megkeresések késedelmének/elutasításának fő okairól (lásd a 68. és azt követő oldalakat).

63 Lásd a SIRIUS 2023. évi éves jelentésének (61. lábjegyzet) 19. oldalán szereplő példákat.

64 A SIRIUS 2023. évi éves jelentése (61. lábjegyzet) (79. o.) szerint az önkéntes együttműködés keretében benyújtott megkeresések nagy száma kihívást jelent a szolgáltatók számára, és ajánlott, hogy a szolgáltatók részt vegyenek a SIRIUS nemzetközi rendezvényein annak érdekében, hogy a kisebb online szolgáltatók támaszkodhassanak a SIRIUS-projekt keretében a hatóságokkal való együttműködés terén szerzett szakértelemre annak érdekében, hogy jobban megértsék ezt a kérdést, strukturálják a hatóságok megkereséseire való válaszadással kapcsolatos politikájukat, és gondoskodjanak arról, hogy fel legyenek készülve a közelgő jogalkotási fejleményekre.

Az iparral való partnerségeket és együttműködést **egyértelmű jogi kerettel** kell alátámasztani, amely minden olyan életképes megoldás alapvető eleme, amely lehetővé teszi a bűnüldöző és az igazságügyi hatóságok számára az elektronikus bizonyítékokhoz való jogszerű hozzáféréssel kapcsolatos nehézségek leküzdését. Amellett, hogy mindkét fél eleget tesz a jogi kötelezettségeinek, az is fontos, hogy állandó és bizalomra épülő kapcsolat alakuljon ki a bűnüldözési szakemberek és a szolgáltatók között, hogy megértsék egymás szükségleteit, és közösen működőképes megoldásokat tudjanak kidolgozni. A magánszektorral való **együttműködést szolgáló** stabil **mechanizmusokra** van szükség egyrészt a szolgáltatók által előállított és tárolt adatok és a megőrzési idejük **átláthatóságának növelése** érdekében, másrészt pedig annak céljából, hogy biztosítani lehessen a megőrzendő és hozzáférhetővé teendő **adatok harmonizált kategorizálását**, ki lehessen alakítani az adatigénylés **szabványosított formátumait**, valamint létre lehessen hozni az illetékes hatóságok és a szolgáltatók közötti közvetlen információcsere **biztonságos csatornáit**.

Az ilyen együttműködés megerősítésére több lehetőséget is meg lehet vizsgálni, amelyek közül néhány kötelező erejű (kemény jogi), míg mások puha jogi megoldásokat tartalmaznak. Az e szakaszban felsorolt megoldások némelyikét a II. szakaszban említett hatásvizsgálat keretében meg kellene vizsgálni, majd adott esetben azt követően jogszabályban meghatározni.

5. ajánláscsoport

Annak biztosítása érdekében, hogy az illetékes hatóságok a megfelelő adatbirtokosok azonosítása révén képesek legyenek releváns adatokat keresni, hogy a szolgáltatók szabványosított formátumban kapják meg az ilyen megkereséseket, és hogy a határokon átnyúló együttműködést ne akadályozzák kollíziók, a szakértők a következőket ajánlják:

1. *a bűnüldözési szakemberek és a szolgáltatók közötti együttműködés kialakítása és megerősítése az információcsere, a kapacitásépítés és a képzés támogatása, valamint az együttműködés elveinek és módozatainak meghatározása érdekében [13. ajánlás], például egy olyan koordinációs központ létrehozása révén, amely lehetővé teszi az illetékes hatóságok számára az érintett szolgáltatók azonosítását és a jogszerű megkeresések célzottabb kibocsátását [18. ajánlás]. Ennek végrehajtására a következőképpen kerülhetne sor:*

    a. *a meglévő uniós szintű struktúrákra – például a SIRIUS-ra, az Európai Igazságügyi Hálózatra (EIH)/a számítástechnikai bűnözés elleni európai igazságügyi hálózatra (EJCN) és az uniós internetfórumra – építve;*

    b. *egyetértési megállapodások révén, az egyes tagállamokban nemzeti szinten kialakult bevált gyakorlatok felhasználásával [14. ajánlás];*

2. *az elektronikus hírközlési szolgáltatásokat és egyéb hírközlési szolgáltatásokat nyújtó szolgáltatókra vonatkozó átláthatósági szabályok előmozdítása az általuk az üzleti tevékenységük során kezelt, előállított vagy tárolt adatok tekintetében, valamint a bűnüldöző hatóságoknak a rendelkezésre álló adatokról való tájékoztatását illetően – a nyomozás titkosságával kapcsolatos korlátok figyelembevétele mellett –, a szolgáltatókkal kötött együttműködési megállapodások vagy szükség esetén kötelezettségek megállapítása révén [17. ajánlás, 16. ajánlás];*

3. *elfogadott szabványokon alapuló egyszerűsített eljárások és formátumok kidolgozása annak érdekében, hogy a szolgáltatókhoz intézett megkeresések benyújtására és a válaszok fogadására strukturált módon kerülhessen sor [15. ajánlás], valamint a platformokon belül egyedüli kapcsolattartó pontok kijelölésének előmozdítása az illetékes hatóságoktól érkező megkeresések kezelése és a velük való kapcsolattartás céljából [36. ajánlás];*

4. *olyan mechanizmusok létrehozása, amelyek biztosítják, hogy a határokon átnyúló megkereséseket hatékonyan, az esetleges ütközéseket elkerülve, célzottan továbbítsák a szolgáltatóknak, ihletet merítve az elektronikus bizonyítékokra vonatkozó mechanizmusokból, valamint annak biztosítása, hogy e mechanizmusok összhangban legyenek az elektronikus bizonyítékokról szóló rendeletben megállapított szabályokkal [19. ajánlás].*

Jelenleg rendelkezésre állnak olyan uniós struktúrák, amelyek lehetővé teszik az érintett szereplők számára, hogy megismerkedjenek az eszközökkel és a bevált gyakorlatokkal. A SIRIUS-projekt a bűnüldöző hatóságok, az igazságügyi hatóságok és a szolgáltatók együttes bevonásával elősegítheti a szolgáltatók birtokában lévő felhasználói adatokkal kapcsolatos megkeresésekre vonatkozó ismeretek és eszközök cseréjét[65], és – különösen a SIRIUS egyedüli kapcsolattartó pontjai meglévő hálózatának köszönhetően – platformként szolgálhat a megkereső hatóságok és a szolgáltatók közötti közvetlen kapcsolat kialakításához[66]. A SIRIUS a jogi eszközök, az ítélkezési gyakorlat, a formátumok stb. **központi adattáraként** szolgálhatna, hasonlóan az elektronikus bizonyítékok határokon átnyúló megosztásához[67].

Az **uniós internetfórum**[68] – mint a tagállamok, az internetes ágazat és más partnerek már meglévő, együttműködésen alapuló környezete – olyan platformként szolgálhatna, ahol uniós szinten közvetlen kapcsolatokat és bizalmat lehetne kialakítani az érintett szereplők között a digitális adatokhoz való hozzáféréssel kapcsolatos tevékenységek terén. Hozzájárulhatna a szolgáltatók és az adatkezelők által gyűjtött és kezelt adatok **nyílt katalógusának** létrehozásához és naprakészen tartásához, amely központi kezelését esetleg a SIRIUS végezhetné. Ez a katalógus csökkentené az átláthatóság jelenlegi hiányát, és egyértelműbbé tenné a bűnüldöző és igazságügyi hatóságok számára, hogy milyen adatokat kérhetnek, valamint koordinációs központként szolgálna annak azonosítása kapcsán, hogy kinek kell címezni a megkeresést. Ezen túlmenően abban az esetben, ha jogi kötelezettségeket rónak a szolgáltatókra, a katalógus hozzáadott értéket biztosítana annak nyomon követésében és értékelésében, hogy a szolgáltatók teljesítik-e az átláthatósági kötelezettségeket az általuk tárolt vagy más módon kezelt adattípusok tekintetében.

---

65 A SIRIUS egyedüli kapcsolattartó pontjainak a jogszerű adatigénylések szakértőiből álló hálózata előmozdítja a bevált gyakorlatokat, és arra ösztönzi az országokat, hogy hozzák létre a saját egyedüli kapcsolattartó pontjaikat. Az egyedüli kapcsolattartó pontok olyan kijelölt személyek, egységek vagy intézmények, amelyek a kormányzati hatóságok szolgáltatóknak címzett megkereséseit központilag kezelik, felülvizsgálják, majd benyújtják. Jelenleg 25 ország 36 bűnüldöző hatósága képezi részét ennek a hálózatnak.

66 A SIRIUS-projekt kapcsolatfelvételi pontként szolgál az elektronikus adatoknak más joghatóságokban székhellyel rendelkező szolgáltatóktól történő beszerzése tekintetében. A SIRIUS a bűnüldöző és az igazságügyi közösségek számára korlátozott hozzáférésű platformot biztosít az ismeretek és a bevált gyakorlatok megosztására. A SIRIUS-projekt több mint 1000 vállalat kapcsolattartási adatait tartalmazó naprakész adattárat gondoz, amely a kisebb, nehezen megtalálható vagy néha elérhetetlen szolgáltatókra összpontosít. Az illetékes hatóságok ezért egyetlen tranzakció keretében több címet is lehívhatnak, ami segít nekik abban, hogy hatékonyabban kezeljenek nagy mennyiségű összetett információt. SIRIUS-projekt | Europol (europa.eu).

67 A SIRIUS egy uniós finanszírozású projekt, amely a bűnügyi nyomozások és a büntetőeljárások keretében segíti a bűnüldöző és igazságügyi hatóságokat az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférésben. Az Europol és az Eurojust által az EIH-val szoros partnerségben végrehajtott SIRIUS-projekt központi referenciaként szolgál az EU-ban az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáféréssel kapcsolatos ismeretek megosztása tekintetében. SIRIUS-projekt | Europol (europa.eu).

68 Európai uniós internetfórum – Európai Bizottság (europa.eu).

Az elektronikus bizonyítékokról szóló csomaggal való szinergiák kiaknázása költségeket és erőforrásokat takarítana meg, és hozzájárulna az elektronikus bizonyítékokra vonatkozó jogszabályok teljes körű végrehajtásához. Például a bűnüldöző hatóságok arra való ösztönzését, hogy hozzanak létre a (határokon átnyúló) adatszolgáltatás iránti megkeresések tekintetében egyedüli kapcsolattartó pontként eljáró egységeket vagy bővítsék azok kapacitását, ki lehetne terjeszteni a nemzeti szinten benyújtott megkeresésekre, vagy pedig a nyomozók és az elsődleges beavatkozók számára nyújtandó képzési programok biztosítására vonatkozó követelményre. Hasonlóképpen, az elektronikus bizonyítékokról szóló csomag végrehajtásával összefüggésben jelenleg folyamatban lévő, az illetékes hatóságok és a szolgáltatók közötti közvetlen információcserét lehetővé tevő **digitális platform** létrehozására irányuló erőfeszítéseket meg lehetne ismételni a nemzeti jogszabályok alapján megőrzött kommunikációs metaadatok tekintetében.

A tagállamok fontolóra vehetik **egyetértési megállapodások** létrehozását annak eszközeként, hogy a nemzeti jogszabályok működésének támogatása érdekében előmozdítsák az együttműködést és közös értelmezést alakítsanak ki a szolgáltatók, a kormány és a bűnüldöző hatóságok között. A néhány tagállamban látható pozitív példák inspirációként szolgálhatnak a megállapodásoknak az összes érintett szereplő (vállalatok, ügynökségek stb.) bevonásával történő strukturálásához, annak biztosítása érdekében, hogy azok az együttműködés valamennyi releváns aspektusára kiterjedjenek (egyedüli kapcsolattartó pontok kijelölése a szolgáltatók és a bűnüldöző hatóságok számára, technikai igények, a szolgáltatandó adatok kategóriáinak közös meghatározása, közös eljárások, a megkeresések szabványosított mintájának kidolgozása, adatbiztonsági és adattakarékossági intézkedések stb.)[69]. A fent vázoltak szerint a szolgáltatóktól (köztük az OTT-szolgáltatóktól) történő adatgyűjtésre és az illetékes hatóságoktól érkező adatigénylésekre vonatkozó **szabványosított protokollok** mind a bűnüldöző hatóságok, mind a szolgáltatók számára előnyösek lennének, mely utóbbiak automatizált mechanizmusokat hozhatnának létre a válaszadásra, költségeket és időt takarítva meg ezzel. Bár a követelmények tekintetében vannak különbségek (az elektronikus bizonyítékokkal kapcsolatos kereten alapuló) **nemzeti** és **határokon átnyúló megkeresések** között, a munkafolyamatokat és az adatigénylési csatornákat mindazonáltal ki lehetne dolgozni, mivel a szabványosítás a kért/kapott adatok formátumára vonatkozik. A szabványügyi testületek – mint például az ETSI – a legalkalmasabbak arra, hogy kidolgozzák ezeket a szabványosított formátumokat. A tagállamok bűnüldözési szakértői azonban eddig csak korlátozott mértékben vettek részt ezekben a folyamatokban. Ezért az Europol és a Bizottság által vezetett, **a belső biztonsággal kapcsolatos szabványosítással foglalkozó** meglévő **uniós munkacsoport** koordinálhatná és ösztönözhetné a tagállamok részvételét az ilyen fórumokon. A munka során építeni lehetne az ETSI által kidolgozott meglévő szabványokra, amelyeket ki lehetne terjeszteni más adatkategóriákra is[70].

---

[69] Írország 2024. április 6-i egyetértési megállapodásának célja a távközlésről (adatok megőrzéséről) szóló (módosított) 2011. évi törvény alkalmazásának támogatása. Az Igazságügyi Minisztérium kinevezett egy független elnököt, meghatározta a feladatokat, és meghívta a bűnüldöző szervek és a szolgáltatók képviselőit.

[70] TS 102 657: Megőrzött adatok kezelése; Átviteli interfész a megőrzött adatoknak, valamint a megőrzött adatok kategóriáinak a kikéréséhez és átadásához (előfizető, felhasználás, berendezés, hálózati elem és számlázási adatok); TS 103 120: A parancsokkal kapcsolatos információkra vonatkozó interfész (elektronikus interfészt határoz meg két rendszer között a szükséges jogszerű intézkedések meghatározásával és irányításával kapcsolatos biztonságos információcsere céljából; jellemzően jogszerű lehallgatáshoz használják, de a megőrzött adatok tekintetében is felhasználható; jellemzően egyrészt a szolgáltató, másrészt a jogszerű intézkedés kérelmezésére jogosult kormány vagy bűnüldöző hatóság között használják); TS 103 705: A jogszerű közlésre szolgáló adatstruktúrák (fejlesztés alatt; csak adatstruktúrák, nincs átviteli interfész, nincs előre meghatározott faszerkezet, a szolgáltató által meghatározott típusok és információk).

Fő intézkedés: a magas szintű munkacsoport szakértői az együttműködés előmozdítását és közös értelmezés kialakítását szorgalmazzák a szolgáltatók, a kormány és a bűnüldöző hatóságok között

Szereplők: Európai Bizottság, tagállamok, Europol (SIRIUS), Eurojust, uniós internetfórum	*Időkeret: még meghatározandó*

- A magas szintű munkacsoport szakértői felkérik az **Európai Bizottságot**, az **Europolt** és a **tagállamokat**, hogy értékeljék a bűnüldöző hatóságok és a magánvállalatok közötti együttműködés előmozdításának és javításának módjait, támogatva az állandó párbeszédet és az operatív, technikai és üzleti igények kölcsönös megértését. A II. szakaszban említett hatásvizsgálattal összefüggésben a magas szintű munkacsoport szakértői arra is felkérik a Bizottságot, hogy fontolja meg az adatgyűjtés átláthatóságára vonatkozó konkrét kötelezettségek és állandó együttműködési struktúrák kidolgozását.

- A magas szintű munkacsoport szakértői felkérik az **Európai Bizottságot**, az **Europolt** és az **Eurojustot**, hogy hozzanak létre az egyrészt a bűnüldöző hatóságok és az igazságszolgáltatás, másrészt pedig a hírközlési szolgáltatók közötti információcserét lehetővé tévő új platformokat, illetve ösztönözzék a már meglévő ilyen platformok használatát, annak céljából, hogy összeállítsák a hírközlési szolgáltatók és az adatkezelők által az üzleti tevékenységük során előállított és tárolt adatok katalógusát, melynek kezelését a SIRIUS végzi majd.

- A magas szintű munkacsoport szakértői felkérik a **tagállamokat**, hogy vizsgálják meg annak lehetőségét, hogy szolgáltatók, kormányok és bűnüldöző hatóságok részvételével olyan együttműködési megállapodásokat és/vagy egyetértési megállapodásokat kössenek, amelyek célja, hogy az elvek és a szabványos eljárások közösen történő meghatározása révén támogassák a nemzeti jogszabályok működését.

- A magas szintű munkacsoport szakértői felkérik az **Europolt** és az **Európai Bizottságot**, hogy vegyék igénybe a belső biztonsággal kapcsolatos szabványosítással foglalkozó meglévő munkacsoportot ahhoz, hogy elősegítsék a tagállamok részvételét a szabványosítási fórumokon annak érdekében, hogy azok részt tudjanak venni a vonatkozó szabványok meghatározásában és együtt kialakítsák a szolgáltatókkal való együttműködésre vonatkozó eljárásokat részletező protokollokat.

- A magas szintű munkacsoport szakértői felkérik az **Európai Bizottságot**, az **Europolt**, az **Eurojustot/EIH-t** és a **tagállamokat**, hogy használják ki az olyan eszközökkel való szinergiákat, mint például az elektronikus bizonyítékokról szóló csomag, arra, hogy kiépítsék vagy beszerezzék a szükséges eszközöket, például azáltal, hogy kiterjesztik a fejlesztés alatt álló digitális platformok alkalmazását, hogy azok felhasználhatók legyenek a megkeresések benyújtására szolgáló portálként.

II. A metaadatok hírközlési szolgáltatók általi megőrzésére és az illetékes hatóságok általi hozzáférésre vonatkozó minimumszabályok harmonizálása

A szakértők nagyrészt egyetértenek abban, hogy szükség van a metaadatok bűnüldözési célú megőrzését szabályozó harmonizált uniós keretre. Ez szabványosított megoldásokat biztosítana, valamint egyértelmű és érvényesíthető kötelezettségeket írna elő a hírközlési szolgáltatók és az adatkezelők számára azzal kapcsolatban, hogy mikor és hogyan kell megőrizni adatokat, és hogy milyen körülmények között kell hozzáférést biztosítani a megőrzött adatokhoz. Ez a keret a megőrzésre és a hozzáférésre vonatkozó egyértelmű szabályok meghatározásával egyrészt azt a célt szolgálná, hogy egyértelmű biztosítékokat nyújtson az alapvető jogok és az alapvető érdekek tekintetében, figyelembe véve az alkalmazandó ítélkezési gyakorlatban foglaltakat, másrészt pedig hogy egyértelművé tegye a hírközlési szolgáltatókra alkalmazandó, az adatok bűnüldözési célú megőrzésére és megosztására vonatkozó szabályokat. Ezen túlmenően az adatok megőrzésének biztosításával ez a keret támogatná az elektronikus bizonyítékokról szóló csomag teljes körű végrehajtását.

6. ajánláscsoport

Annak biztosítása érdekében, hogy a bűncselekmények nyomozásához és büntetőeljárás alá vonásához szükséges digitális bizonyítékok rendelkezésre álljanak, továbbá hogy a tagállamok között ne legyen széttagoltság a megőrzésre vonatkozó szabályok és az alapvető jogokkal – különösen a magánélet és az adatok védelmével, a véleménynyilvánítás szabadságával és a védelemhez való joggal, így többek között a tisztességes eljáráshoz való joggal – kapcsolatos biztosítékok tekintetében, valamint hogy garantált legyen a jogbiztonság egyrészt az illetékes hatóságok, másrészt pedig az elektronikus és egyéb hírközlési szolgáltatók számára, a szakértők a következőket javasolják:

1. *a metaadatok kategóriáinak meghatározása a felhasználás célja alapján (a célszemély azonosítása, lokalizálása, online tevékenységének megállapítása, illetve értékelése) [28. ajánlás], annak biztosítása érdekében, hogy az elektronikus hírközlési szolgáltatásokat és egyéb hírközlési szolgáltatásokat nyújtó szolgáltatók megőrizzenek legalább a célszemély azonosításához elegendő adatot [27. ajánlás v. pontja];*
2. *az említett adatok minimális megőrzési időtartamának meghatározása;*
3. *a megőrzött adatokhoz való hozzáférés feltételeinek kialakítása [27. ajánlás iv. pontja], amelyek az adatkategóriától, a bűncselekmény kategóriájától (pl. kizárólag az interneten elkövetett bűncselekmények) vagy az áldozatokat fenyegető veszélytől függően eltérnek egymástól [29. ajánlás];*
4. *az ilyen jogi, szabályozási és technikai rendelkezések oly módon történő kialakítása, hogy azok biztosítsák a célszemélyek alapvető jogainak és szabadságainak teljes körű tiszteletben tartását, valamint azt, hogy e jogok bármilyen korlátozása szükséges és arányos legyen [27. ajánlás vi. pontja];*
5. *annak biztosítása, hogy ugyanazok a szabályok, kötelezettségek és biztosítékok vonatkozzanak a hagyományos hírközlési szolgáltatókra, az OTT-szolgáltatásokra és minden más olyan meglévő vagy jövőbeli szolgáltatóra, amely adatokat állít elő és kezel [27. ajánlás i. és ii. pontja];*
6. *annak biztosítása, hogy a kereskedelmi és üzleti célból megőrzött felhasználói adatok a megfelelő biztosítékok mellett ténylegesen hozzáférhetők legyenek a bűnüldöző szervek számára (31. ajánlás), és hogy az illetékes hatóságok el tudják olvasni a szolgáltatóktól jogszerűen kapott adatokat [27. ajánlás iii. pontja];*
7. *annak biztosítása, hogy a tagállamok szankciókat tudjanak érvényesíteni azokkal az elektronikus és egyéb hírközlési szolgáltatókkal szemben, amelyek nem tanúsítanak együttműködést az adatok megőrzésével és benyújtásával kapcsolatban, például közigazgatási szankciók alkalmazása vagy az uniós piacon való működésre vonatkozó képességük korlátozása révén [30. ajánlás].*

Ami a **metaadatok megőrzését** illeti, különbséget kell tenni az egyes adatkategóriák között, megkülönböztetve egymástól a célszemély azonosításához szükséges adatokat (előfizetői adatok[71] és a forráskommunikáció IP-címei[72]) és a forgalmi[73] és helymeghatározó adatokat[74], és az egyes kategóriák esetében eltérő megőrzési időtartamokat és biztosítékokat kell előírni. Az adatokhoz való hozzáférés szakaszában is annak biztosítása a cél, hogy a meghozandó intézkedések magánéletbe való beavatkozásának mértéke egyensúlyban legyen a nyomozás tárgyát képező bűncselekmény súlyosságával. A közelmúltbeli ítélkezési gyakorlattal[75] összhangban meg lehetne vizsgálni az általános adatmegőrzésre vonatkozó olyan minimumkövetelmények bevezetésének lehetőségét, amelyek elegendők lennének annak szavatolásához, hogy bármely felhasználót egyértelműen azonosítani lehessen. A forgalmi és a helymeghatározó adatok esetében meg kell vizsgálni szigorúbb kiegészítő kritériumok alkalmazását.

Annak érdekében, hogy ezt a keretet a lehető leginkább időtálló és **technológiasemleges** módon lehessen kialakítani, a megőrzendő adatok kategorizálását előretekintő megközelítés alapján kell meghatározni, beleértve például az adatok funkciói alapján meghatározott általános adatkészleteket (a kommunikáció forrásának vagy céljának egyedi azonosítását lehetővé tevő adatok, a kommunikáció forrása helyének azonosítását lehetővé tevő adatok stb.), a meglévő adattípusok listájával (IP-cím, IMEI stb.) együtt. Ez a keret lehetővé tenné annak megfelelő értékelését, hogy az egyes adatkategóriák milyen mértékű beavatkozással járnak, és ennélfogva milyen biztosítékokra van szükség.

---

71 A kis szolgáltatókkal kapcsolatos néhány kivételtől eltekintve üzleti célból általában már megőrzik a felhasználói adatokat. Ilyen esetben – és az arányos biztosítékok sérelme nélkül – ezeket az adatokat a bűnüldöző szervek rendelkezésére kell bocsátani.

72 Az ítélkezési gyakorlat a közérdek védelme érdekében lehetővé teszi az elektronikus hírközlési rendszerek felhasználóinak személyazonosságára vonatkozó adatok általános és különbségtétel nélküli megőrzését, valamint a nemzetbiztonság védelme, a súlyos bűncselekmények elleni küzdelem és a közbiztonságot érintő súlyos fenyegetettség megelőzése érdekében az IP- címek általános és különbségtétel nélküli megőrzését (2020. október 6-i ítélet, *La Quadrature du Net és társai*, C-511/18., C-512/18. és C-520/18. sz. egyesített ügyek, illetve 2024. április 30-i ítélet, *La Quadrature du Net és társai*, C-470/21 [„Hadopi”], ECLI:EU:C:2024:370).

73 „Forgalmi adat”: egy közlésnek az elektronikus hírközlő hálózaton keresztül történő továbbítása vagy erre vonatkozó számlázás céljából kezelt minden adat (a 2002/58/EK irányelv 2. cikke).

74 „Helymeghatározó adat”: egy nyilvánosan elérhető elektronikus hírközlési szolgáltatás felhasználója végberendezésének földrajzi helyzetét jelző, az elektronikus hírközlő hálózatban kezelt minden adat (a 2002/58/EK irányelv 2. cikke); a felhasználó berendezésének helymeghatározó adatait a 2002/58/EK irányelv 9. cikkében meghatározott, forgalmi adatokon kívüli helymeghatározó adatoknak kell tekinteni.

75 A Hadopi-ítélet.

Amint azt a szakértők és a közelmúltbeli ítélkezési gyakorlat[76] meghatározták, az adatmegőrzési kötelezettségeknek **az adatokhoz való hozzáférésre vonatkozó** szigorú **követelményekkel** való kombinálása további biztosítékokat nyújtana az alapvető jogok, és különösen a magánélet és az adatok védelme tekintetében. Ezért a magas szintű munkacsoport szakértői megvitatták, hogy szükség van-e eltérő hozzáférési szabályok kialakítására például a következőktől függően: a bűncselekmény típusa és súlyossága, a bűncselekmény által az áldozatokra jelentett veszély mértéke, a hozzáférés célja és az adatokhoz való hozzáférés tekintetében illetékes hatóságok. Ezt a megközelítést hasznos módszernek tekintették az olyan bűncselekmények nyomozására és büntetőeljárás alá vonására vonatkozó konkrét szabályok meghatározásához is, amelyek esetében a nyomozás különösen nagy kihívást jelent, mint például a kizárólag az interneten elkövetett bűncselekmények, ahol a digitális bizonyíték jelenti az egyetlen rendelkezésre álló bizonyítékot.

Az adatokhoz való jogszerű hozzáférést követően a megkereső hatóságoknak el kell tudniuk olvasni azokat. A szolgáltatóknak ezért az adatokat **érthető formátumban** kell rendelkezésre bocsátaniuk. A szolgáltatók gyakran végponttól végpontig terjedő titkosított szolgáltatásokat[77] kínálnak a forgalmi és az előfizetői adatok tekintetében, és nem fejtik vissza ezeket az adatokat, amikor megosztják azokat az illetékes hatóságokkal. A magas szintű munkacsoport szakértői úgy vélték, hogy az adatmegőrzési rendszereknek kötelezettségeket kellene tartalmazniuk a szolgáltatók számára arra vonatkozóan, hogy titkosítatlan adatokat bocsássanak rendelkezésre, ugyanakkor biztosítsák az erős kiberbiztonságot, valamint az adatok és a magánélet védelmére vonatkozó jogszabályoknak való teljes körű megfelelést anélkül, hogy veszélyeztetnék a titkosítást.

A meghatározott adatkategóriák megőrzésére vonatkozó minimumkövetelményeknek minden elektronikus hírközlési szolgáltatást nyújtó (jelenlegi vagy jövőbeli) gazdasági szereplőre vonatkozniuk kellene (és végrehajthatóknak kellene lenniük) annak érdekében, hogy az adatmegőrzési keret most és a jövőben is hatékony legyen. A jövőbeli technológiai fejlődés figyelembevétele érdekében az adatmegőrzési kötelezettségek hatálya alá tartozó szervezetek körébe kell tartozniuk a távközlési szolgáltatóknak, az OTT-szolgáltatóknak és más olyan üzemeltetőknek, amelyek a szolgáltatásukat igénybe vevő konkrét természetes vagy jogi személlyel kapcsolatos adatokat gyűjtenek, például autógyártóknak vagy LLM-re épülő MI-rendszereknek. E kötelezettségeknek végrehajthatóknak, és a szolgáltatók tekintetében elszámoltathatóknak kell lenniük; ez számos megoldás segítségével elérhető, amelyek magukban foglalhatnak piaci akadályokat (működési engedélyek) és közigazgatási szankciókat.

---

[76] A közelmúltbeli Hadopi-ügyben a Bíróság arra a következtetésre jutott, hogy a magánélet védelme a megőrzés és a hozzáférés kombinálásával biztosítható.

[77] Lásd az I. szakaszt.

Minden lehetséges jövőbeli uniós keret alapvető elemét képezi egy olyan rendszer, amely végrehajtható szankciókat tartalmaz a nem együttműködő szolgáltatókra és a jogellenes szolgáltatások számára tárhelyet biztosító szolgáltatókra vonatkozóan. Tekintettel az e konkrét aspektus és a jogszerű lehallgatással összefüggésben megvitatott lehetséges megoldások közötti interakcióra, a szankciókról a jogszerű lehallgatásról szóló következő ülésen kell majd megbeszéléseket folytatni.

Míg a legtöbb szolgáltató esetében az adatok megőrzésére és rendelkezésre bocsátására vonatkozó kötelezettségek teljesítéséhez főként technikai megvalósításra lenne szükség (azaz az üzleti célból gyűjtött vagy kezelt adatoknak az illetékes hatóságok számára történő rendelkezésre bocsátására), ez alapértelmezés szerint elvégzendő felhasználói regisztrációs eljárások előírását eredményezné azon szolgáltatók esetében, amelyek jelenleg nem regisztrálják a felhasználóikat, mert erre üzleti szempontból nincs szükségük (mint például az OTT-szolgáltatók). A magas szintű munkacsoport szakértői pozitívnak ítélték az ilyen jellegű kötelezettségeket az arról folytatott megbeszélések keretében, hogy növelni kell a szolgáltatók azzal kapcsolatos **átláthatóságát és elszámoltathatóságát**, hogy milyen adatokat gyűjtenek és tárolnak, és mennyi ideig. Az egyéb jogi eszközök (GDPR) alapján történő kategorizálás tekintetében meglévő kötelezettségek betekintést nyújthatnak az e szolgáltatók által kezelt adatokba.

Fő intézkedés: A magas szintű munkacsoport szakértői új uniós adatmegőrzési és -hozzáférési keretet szorgalmaznak

Szereplők: Európai Bizottság, Tanács, Európai Parlament

Időkeret: 2025–2026

- A magas szintű munkacsoport szakértői sürgetik az **Európai Bizottságot**, hogy indítsa el a hatásvizsgálatra irányuló eljárást annak értékelése céljából, hogy milyen különböző módokon lehetne növelni az illetékes hatóságok arra vonatkozó kapacitását, hogy a hírközlési szolgáltatók által előállított és tárolt múltbeli metaadatokhoz való hozzáférés révén biztosítsák a bűncselekmények hatékony nyomozását és büntetőeljárás alá vonását. A hatásvizsgálatnak ki kell továbbá terjednie a szubszidiaritással kapcsolatos követelményekre, az alapvető jogokra és a belső piacra gyakorolt hatásra, valamint az egyéb hatályos jogi eszközökkel való kapcsolatra is. Ennek egy, a rendes jogalkotási eljárás keretében elfogadandó jogalkotási javaslat alapjául kell szolgálnia.

III. fejezet: Jogszerű lehallgatás

MIK A NEHÉZSÉGEK?

„A kommunikáció jogszerű lehallgatása” azt jelenti, hogy egy harmadik fél – hatóság vagy jogszabály alapján felhatalmazott más szervezet – leplezett hozzáférést szerez valamely gyanús kommunikációból származó adatokhoz. Míg a múltban a jogszerű lehallgatás főként a telefonhívásokra vonatkozott, a hagyományos hanghívásokról az üzenetküldő szolgáltatásokra és az egyéb elektronikus hírközlési formákra való áttérés növekvő mértéke új kihívásokat teremtett.

Az EEHK felismerte ezt az áttérést, és kiterjesztette a jogi keretnek a hagyományos hírközlési szolgáltatásokra alkalmazandó részét azokra a vállalkozásokra is, amelyek internetalapú szolgáltatásokat kínálnak olyan távközlési infrastruktúrán keresztül, amelynek nem tulajdonosai vagy kezelői, ideértve a számfüggetlen személyközi hírközlési szolgáltatásokat is (NI-ICS). A gyakorlatban ez azt jelenti, hogy a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatókra potenciálisan ugyanaz a jogi keret vonatkozhat, mint a hagyományos távközlési szolgáltatókra, a jogszerű lehallgatás tekintetében is. A tagállamok előírhatják, hogy az üzemeltetők – a közlés bizalmasságára vonatkozó rendelkezéseket és az alóli kivételeket tartalmazó (EU) 2016/679 rendelettel és 2002/58/EK irányelvvel összhangban – tegyék lehetővé az elektronikus hírközlésnek az illetékes nemzeti hatóságok általi jogszerű lehallgatását. Az EEHK szerinti általános felhatalmazási rendszer keretében a tagállamok újra megállapíthatják ezt a követelményt.

A jogszerű hozzáférésnek nem kell hálózati szintűnek lennie – ahogyan az a hagyományos telefonhívások és szöveges üzenetek (SMS) esetében volt –, hanem az korlátozódhat a felhasználó készülékére (mielőtt az információt elküldik) vagy a címzett szintjére (pl. amikor az üzeneteket a felhőben tárolják). E jelentés keretében a jogszerű lehallgatás e három felhasználási esetre terjed ki, és olyan adatokra vonatkozik, amelyekhez valós időben vagy kis időeltolódással fértek hozzá.

Fontos különbséget tenni **a hírközlési szolgáltató által alkalmazott** lehallgatási technológiák és a bűnüldöző hatóságok által önállóan bevethető technológiák között. A „jogszerű lehallgatásnak” az ETSI-szabványokban rögzített fogalommeghatározása csak az előbbi technológiákra terjed ki [e jelentésben erre mint „**szolgáltató-alapú lehallgatásra**” hivatkozunk], amelyhez szükség van arra, hogy a hírközlési szolgáltató olyan műszaki rendszereket telepítsen, amelyek a lehallgatott adatokat összegyűjtik, és a megkereső hatóságok részére továbbítják. Az utóbbi technológiák [melyekre e jelentésben mint „**taktikai lehallgatásra**” hivatkozunk] olyan eszközöket foglalnak magukban, amelyeket nem szükséges állandó jelleggel, fizikailag telepíteni a hálózatra, mint például az IMSI-gyűjtő berendezések[78] vagy az okostelefonokon található adatok lehallgatására szolgáló szoftverek. Az említett felhasználási esetek eltérő mértékű beavatkozással és eltérő jellegű kihívásokkal járnak, és nem ugyanazon jogi szabályozás hatálya alá tartoznak.

Bár a hagyományos távközlés jogszerű lehallgatása számos nyomozásban továbbra is alapvető fontosságú eszközt jelent[79], ezen intézkedés eredményessége drasztikusan csökkent, mivel a távközlési szolgáltatásokat manapság többnyire más szereplők nyújtják: különböző források szerint jelenleg az összes mobilüzenet mintegy 97%-át olyan üzenetküldő alkalmazásokon keresztül küldik, mint a WhatsApp, a Facebook Messenger és a WeChat, míg a hagyományos SMS- és MMS-üzenetek csak körülbelül 3%-át teszik ki az üzeneteknek. Ezenkívül 2023-ban az OTT-kommunikáció több mint 90%-át végponttól végpontig terjedő titkosított szolgáltatásokon keresztül bonyolították le[80].

A szakértők egyetértenek abban, hogy a következő tendenciák voltak megfigyelhetők: először a bűnözők a hagyományos hírközlési szolgáltatók felől kezdtek áttérni a széles körben elterjedt OTT-szolgáltatásokra; aztán a legfajsúlyosabb bűnözői körök fokozatosan kezdtek olyan bűnözői hálózatokat használni, amelyeket kifejezetten erre a célra alakítottak ki (például Encrochat és Sky ECC); 2020 óta pedig – miután a legnagyobb titkosított bűnözői kommunikációs hálózatokat felszámolták – sokan közülük úgy döntöttek, hogy visszatérnek a hétköznapi, végponttól végpontig terjedő titkosítással védett OTT-szolgáltatásokra.

---

78 Az IMSI-gyűjtő berendezések olyan megfigyelési eszközök, amelyek bázisállomásokat utánozva lehallgatják a mobiltelefon-jeleket, és így fogják be a nemzetközi mobil-előfizetői azonosító (IMSI) számokat és a kommunikációs adatokat.

79 Az elmúlt években Európában jelentősen és folyamatosan nőtt a jogszerű lehallgatás iránti megkeresések száma. A megkeresések különösen nagy számáról számolt be például Németország, Franciaország és az Egyesült Királyság, ezen belül Németországban kiugróan megnőtt az ilyen megkeresések száma. 2023-ban például a Deutsche Telekom több mint 31 000 lehallgatás iránti megkeresést kapott, szemben azzal, hogy ez a szám 2022-ben 26 000 körül volt (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Források: Comparitech és Statista.

Ebben a környezetben a hírközlési szolgáltatók olyan mértékű kihívásokkal szembesülnek a jogszerű lehallgatás iránti megkeresések megválaszolása tekintetében, hogy alig tudnak megfelelni a jogszerű lehallgatásra vonatkozóan a Számítástechnikai Bűnözésről szóló Budapesti Egyezményben meghatározott alapvető követelményeknek[81]. Következésképpen a hagyományos jogszerű lehallgatás operatív értéke gyakran csupán taktikai információkra korlátozódik, például annak meghatározására, hogy egy készülék bekapcsolt vagy kikapcsolt állapotban van-e, hogy hol található a hálózati antenna, vagy hogy ki kivel áll kapcsolatban; az OTT-szolgáltatókon keresztül továbbított tartalmi adatok jogszerű lehallgatása azonban az esetek többségében nem lehetséges.

Mindezek következtében a bűnüldöző hatóságok gyakran nem tudnak hozzáférni a célba vett kommunikációhoz és kiolvasni annak tartalmát[82], vagy akár nem is jönnek rá, hogy valós időben ki használ egy adott internetszolgáltatást, és nem tudják szűrni a releváns információkat. Az, hogy az átvitel alatt lévő adatokhoz való hozzáférés terén ilyen jelentős kiesés figyelhető meg, több módon is érinti a nyomozásokat:

- komoly nehézségekbe ütközik a bűncselekmények megelőzése, a bűnszervezetek feltérképezése és az online vagy offline elkövetett büntetendő cselekmények attribúciója;
- a bűnüldöző hatóságok egyre gyakrabban használnak úgynevezett különleges technikákat[83], amelyek gyakran nagyobb beavatkozással járnak és sokkal veszélyesebbek a rendőrök számára, például amikor az igazságügyi hatóság a célponthoz közeli kamerák vagy mikrofonok telepítését írja elő;
- a bűnüldöző hatóságok egyre gyakrabban használnak olyan nyomozási technikákat, amelyek kevésbé célzottak: a kommunikáció tartalmához vagy a pontos földrajzi helymeghatározási adatokhoz való hozzáférés híján a nyomozóknak gyakran az **összes** olyan személyre kiterjedő nyomozást kell folytatniuk, aki kapcsolatban áll a büntetendő cselekmény elkövetésével gyanúsított személlyel.

Mindezek fényében a magas szintű munkacsoport szakértői négy fő kategóriába sorolták a kihívásokat.

---

81 https://rm.coe.int/1680081561 [20. és 21. cikk]

82 Egy szakértő jelezte, hogy az esetek 99%-ában nem állnak rendelkezésre tartalmi adatok jogszerű lehallgatás útján.

83 Az úgynevezett különleges technikák taktikai eszközök széles skáláját foglalják magukban, amelyek segítségével kamerákon, mikrofonokon, a készülékekhez való távoli hozzáférésen vagy GPS-nyomkövetőkön stb. keresztül információk nyerhetők az érintett célpontról.

I. A kommunikáció nem hagyományos hírközlési szolgáltatókon keresztül folytatott jogszerű lehallgatása

A jogszerű lehallgatást a tagállamok többsége valamilyen formában szabályozza, arra kötelezve a hírközlési szolgáltatókat, hogy telepítsenek lehallgatási képességeket[84]. Jóllehet a jogszerű lehallgatást elrendelő határozatok kibocsátásának feltételei országonként jelentősen eltérnek, az üzemeltetőkre vonatkozó kötelezettségek gyakran hasonlóak[85]: képesnek kell lenniük arra, hogy belföldön hézagok nélkül lehallgassák a meghatározott célponttól származó valamennyi releváns kommunikációt, és biztosítaniuk kell a lehallgatott adatok gyűjtéséhez és a bűnüldöző szerveknek történő továbbításához szükséges infrastruktúrát.

Azokban az esetekben, amikor a távközlési hálózat üzemeltetői (olyan hírközlési szolgáltatók, amelyek a hálózat tulajdonosai és hozzáféréssel rendelkeznek a hálózat infrastruktúrájához) biztosítják a hírközlési szolgáltatásokat is (telefonhívásokat, SMS-eket stb.), többségében képesek teljesíteni a jogszerű lehallgatási kötelezettségeket[86]. A legtöbb esetben az ETSI-szabványokra támaszkodnak, és szakosodott technológiai szolgáltatókat vesznek igénybe saját korlátaik figyelembevétele érdekében, ideértve a költséghatékonyságot, a hálózati infrastruktúrára gyakorolt minimális hatást, az interoperabilitást, a megbízhatóságot és a biztonságot.

Az OTT-szolgáltatások esetében bonyolultabb a helyzet: a jogszerű lehallgatást vagy a távközlési hálózat üzemeltetője, vagy a szolgáltatást nyújtó OTT-szolgáltató végezheti.

Ha az OTT-szolgáltatásokon keresztül zajló kommunikáció lehallgatását a távközlési hálózat szintjén végzik, annak gyakran korlátozott mértékű az eredményessége. Először is előfordulhat, hogy a távközlési hálózat üzemeltetője nem tudja azonosítani a célpont kommunikációját (pl. nyilvános wifi-kapcsolat esetén). Emellett az OTT-szolgáltatások gyakran használnak olyan védett protokollokat, amelyeket jogszerű lehallgatási rendszerekkel kell dekódolni, ami növeli a folyamat költségeit, hosszát és összetettségét. Végezetül, a végponttól végpontig terjedő titkosítás OTT szolgáltatók általi használata rendkívül megnehezíti a tartalomadatokhoz való hozzáférést, és a metaadatokhoz való hozzáférést is egyre gyakrabban akadályozza, mivel az országok túlnyomó többsége úgy tekinti, hogy – a Budapesti Egyezménnyel összhangban – a távközlési hálózatok üzemeltetőinek azon kötelezettsége, hogy titkosítatlan információkkal szolgáljanak, megszűnik, ha egy harmadik fél titkosítást alkalmaz.

---

84 Lásd: „*Lawful interception – A market access barrier in the European Union*" (Jogszerű lehallgatás – a piacra jutást gátló akadály az Európai Unióban), Vadim Doronin, in: *Computer Law & Security Review* 51 (2023) 105867.

85 Bár vannak különbségek a tartalmi, illetve a nem tartalmi adatokkal kapcsolatos kötelezettségek terén.

86 Bár az olyan jellemzők, mint a home routing, a hálózatszeletelés vagy az RCS-szolgáltatások, gátolhatják a távközlési hálózatok üzemeltetőit abban, hogy teljesíteni tudják kötelezettségeiket (lásd a technológiai kihívásokról szóló szakaszt).

Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (1) bekezdése hivatkozik az „elektronikus hírközlési szolgáltatásoknak” az EEHK szerinti fogalommeghatározására, amely 2018 óta tartalmazza a számfüggetlen személyközi hírközlési szolgáltatásokat is (NI-ICS). Ez viszont azt jelenti, hogy az elektronikus hírközlési szolgáltatások ma már szélesebb körű fogalma (az elektronikus hírközlési adatvédelmi irányelv elfogadásakor alkalmazott fogalomhoz képest) lehetővé teszi a tagállamok számára, hogy közvetlenül az OTT-szolgáltatókhoz forduljanak a jogszerű lehallgatás elvégzése céljából[87]. A tagállamok eddig változó mértékben éltek ezzel a lehetőséggel: egyes tagállamok hasonló kötelezettségeket állapítottak meg az elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók valamennyi típusa számára, beleértve az OTT-szolgáltatókat is, míg mások kizárják az OTT-szolgáltatókat[88]. **A gyakorlatban az figyelhető meg, hogy a széles körben elterjedt OTT-szolgáltatások – a meglévő kötelezettségektől függetlenül – nem alakították ki azokat a technikai mechanizmusokat, amelyek szükségesek lennének az uniós tagállamok hatóságaitól érkező, jogszerű lehallgatás iránti megkeresések megválaszolásához**, elsősorban jogi okokból[89].

Ezzel szemben az Egyesült Királyság – a nyomozati jogkörökről szóló törvény (*Investigatory Powers Act*) alapján – létrehozta az OTT-kommunikáció jogszerű lehallgatásának keretét, amely az Egyesült Királyság és az Egyesült Államok közötti adathozzáférési megállapodás elfogadásának köszönhetően az USA-ban letelepedett OTT-szolgáltatásokra is alkalmazandó. Az Egyesült Királyság illetékes hatóságai szerint ez lényeges különbséget jelent a bűnmegelőzés és a nyomozások terén.

Végezetül, a nemzeti hatóságok szakértői egyértelművé tették, hogy a sérülékenységek kiaknázásán alapuló taktikai lehallgatás nem hatékony és nem is kívánatos alternatívája az OTT-szolgáltatókra alkalmazandó, érvényesíthető jogszerű lehallgatási szabályoknak, és annak – az arányosság biztosítása érdekében – konkrét, meghatározott esetekre kell korlátozódnia, a nemzeti jogban meghatározott erős garanciák mellett.

---

87 Bár még viták folynak az alkalmazhatóság pontos hatályáról, és az értelmezések tagállamonként eltérőek.

88 Lásd: „*Lawful interception – A market access barrier in the European Union*” (Jogszerű lehallgatás – a piacra jutást gátló akadály az Európai Unióban), Vadim Doronin, in: *Computer Law & Security Review* 51 (2023) 105867.

89 Ezt nem támasztják alá statisztikák, mivel a nemzeti hatóságok nagyon ritkán küldenek jogszerű lehallgatás iránti megkereséseket az OTT-szolgáltatóknak, mivel tisztában vannak azzal, hogy az valószínűleg nem vezet eredményre.

II. Határokon átnyúló megkeresések

Az OTT-szolgáltatókhoz és – kisebb mértékben – a hagyományos hírközlési szolgáltatókhoz intézett, határokon átnyúló jogszerű lehallgatás iránti megkeresések számos kihívást jelentenek a bűnüldöző hatóságok számára.

Ami a hagyományos hírközlési szolgáltatókat illeti, a hatóságok elsősorban szervezési nehézségekkel küzdenek. Először is, a nemzetközi együttműködési eszközök – nevezetesen a kölcsönös jogsegély mechanizmusai – kivitelezhetetlennek bizonyulhatnak olyan sürgős lehallgatások esetében, amelyeket engedélyeztetni kell, és órákon – nem pedig napokon vagy heteken belül – kell elvégezni[90]. Ennek oka az ahhoz szükséges lépések száma, hogy mind a megkereső, mind a megkeresett tagállamban biztosított legyen a jogszabályoknak való megfelelés. Az általános megítélés szerint a kölcsönös jogsegély folyamata nem hatékony és nehézkes, ha a jogszerű lehallgatásra alkalmazzák. Az EU-n belüli hagyományos kölcsönös jogsegély iránti eljárásokat felváltotta a 2017 óta alkalmazott európai nyomozási határozat (ENYH)[91], amelynek keretében szigorú határidőket[92] állapítottak meg a kért bizonyítékok összegyűjtésére, korlátozták a megkeresések elutasításának lehetséges okait, és egységes formanyomtatványt vezettek be a hatóságok számára, amelyen segítséget kérhetnek a bizonyítékok keresése során. Továbbá, amennyiben a lehallgatás elvégzéséhez nincs szükség technikai segítségre attól a tagállamtól, ahol a lehallgatás célszemélye tartózkodik, az adott tagállamot egységes formanyomtatványon értesítik a lehallgatásról, és az 96 órán belül kifogást emelhet ellene. A C-670/22. sz., mérföldkőnek számító ügyben az EUB a „titkos távközlési információgyűjtés” tág fogalmát alkalmazta, megállapítva, hogy a végberendezésekhez való, valamely internetalapú távközlési szolgáltatás forgalmi, helymeghatározó és kommunikációs adatainak megszerzésére irányuló leplezett hozzáférés „titkos távközlési információgyűjtésnek” minősül. A szakértők mindazonáltal úgy vélik, hogy az ENYH bevezetésével elért jelentős javulás nem elég ahhoz, hogy ki lehessen elégíteni a mozgásban lévő adatokhoz való gyors és harmonizált, határokon átnyúló hozzáférés iránti igényt.

Emellett a tagállami hatóságok arról számoltak be, hogy a meglévő műszaki architektúra gyakran nem alkalmas arra, hogy az egyik tagállamban elvégzett jogszerű lehallgatás során szerzett adatokat közel valós időben egy másik tagállamnak továbbítsák. Egyes esetekben, amikor idevágó szervezeti protokollok vannak érvényben, a továbbítandó adatok mennyisége egyszerűen meghaladja a biztonságos kommunikációs csatornákon keresztül elérhető sávszélesség kapacitását.

---

90 A szakértők említettek olyan eseteket, amikor az ügy lezárult még azelőtt, hogy a határokon átnyúló jogszerű lehallgatást ténylegesen végrehajtották volna, vagy olyan eseteket is, amikor a kölcsönös jogsegéllyel kapcsolatos ügyhátralék több mint 8 hónapot ölelt fel.

91 DK és IE kivételével, ahol az ENYH nem alkalmazandó.

92 30 nap az ENYH elismerésére és további 90 nap a végrehajtására.

Az OTT-kommunikáció lehallgatása összetett joghatósági kérdéseket vet fel a telefonbeszélgetések lehallgatásához képest, mely utóbbi esetében a szolgáltatók jól meghatározott földrajzi területen kínálják szolgáltatásaikat. A hagyományos távközlési szolgáltatások egy konkrét fizikai hálózati infrastruktúrához vannak kötve, ami biztosítja, hogy a szolgáltató rendelkezik létesítményekkel és jogi jelenléttel abban az országban, ahol a lehallgatásra sor kerül. Ez a helyhez kötöttség csökkenti az EU-n belüli jogi konfliktusok kockázatát, és leegyszerűsíti a megfelelést.

Ezzel szemben az OTT-szolgáltatások esetében előfordulhat, hogy a megkereső hatóság, a lehallgatás célpontja, a fizikai végrehajtás helye és a vállalkozás székhelye több különböző joghatóságban található. Az e joghatóságokban fennálló jogi keretek közötti kölcsönhatás kollízióhoz vezethet[93].

A rendőri és igazságügyi hatóságok számára teljesen egyértelmű, hogy a jogszerű lehallgatás iránti megkereséseknek a nemzetközi eszközökön keresztül való bonyolítása a gyakorlatban nem életképes megoldás. Ha a bűnüldöző hatóságok megkerülik a kölcsönös jogsegély folyamatát, és ehelyett – a nemzeti joguk alapján – közvetlenül a szolgáltatóknak kézbesítik a határozatokat, az OTT-szolgáltatók, mint például a Microsoft, a META vagy a Google egymásnak ellentmondó jogi követelményekkel szembesülhetnek. Például sok esetben előfordul, hogy a megkereső tagállamban olyan szabályok vannak érvényben a jogszerű hozzáférésre vonatkozóan, amelyek ellentétesek az ír joggal[94], amely pedig több nagy OTT-szolgáltatóra nézve az irányadó jog, mivel Írországban van a székhelyük, de emellett még a szolgáltatásnyújtás helye szerinti tagállamok nemzeti jogának hatálya alá is tartozhatnak.

Közös intézkedésekkel, valamint a jogszerű lehallgatásra vonatkozó szabályok uniós szintű, bizonyos fokú harmonizációjával esetleg hatékonyan megoldhatók ezek a kihívások, megkönnyítendő és felgyorsítandó a jogszerű lehallgatás iránti, határokon átnyúló megkereséseket. Ez előfeltétele lenne egyéb szervezeti és technikai jellegű kihívások kezelésének, amelyekre akkor lehet megoldást találni, ha egyértelmű, végrehajtható szabályok vannak érvényben.

---

93 Lásd: A bűnüldöző szervek általi lehallgatással kapcsolatos aggályok az EEHK keretében (*„LE interception concerns under the EECC”*), Microsoft, 2020. január.

94 Az ír jog tiltja az OTT-szolgáltatók számára az élő lehallgatást.

III. Technológia

A jogi megfontolásoktól függetlenül, a kommunikációs technológiák fejlődése befolyásolja a bűnüldöző hatóságok arra irányuló technikai képességét, hogy lehallgassák a közvetlenül a hírközlési szolgáltatók vagy OTT-szolgáltatók által nyújtott szolgáltatások igénybevételével folytatott kommunikációt.

A hagyományos hírközlési szolgáltatók esetében a jogszerű lehallgatási képességeket a technológiaszolgáltatók általában az ETSI-szabványokra alapozva fejlesztik ki, és azok a 3GPP[95] részét képezik. Ebből következően a jól felszerelt rendőri szolgálatok képesek kielégítően elvégezni a hagyományos kommunikáció – hang- és SMS-üzenetek – lehallgatását, és potenciálisan lehallgathatják az említett szolgáltatók hálózatain nyújtott szolgáltatások igénybevételével folytatott internetalapú kommunikációt is.

Ugyanakkor a kommunikációs infrastruktúrák fokozódó összetettsége és az 5G-s protokollok – mint például a virtualizáció, a hálózatszeletelés, a pereminformatika és a magánélet védelmét megerősítő funkciók – új technológiai kihívások elé állítják a hagyományos szolgáltatókat[96]. A magas szintű munkacsoport szakértői különösen a home routinggal[97] és az RCS-szolgáltatásokkal[98] összefüggő kihívásokat emelték ki.

A jövőre előretekintve, az 5G-vel kapcsolatos tapasztalatok alapján, a magas szintű munkacsoport szakértői szerint kihívásokra kell számítanunk a 6G jövőbeli (2030 utánra tervezett) bevezetésével összefüggésben is, mivel az újabb lépést fog jelenteni a magánélet védelmét megerősítő funkciók tekintetében[99] – valószínűleg sztenderd jellemzőként magában foglalva a végponttól végpontig terjedő titkosítást –, mindez pedig megnehezítheti majd a lehallgatásokat. Ezzel egyidejűleg az új kommunikációs technológiák – mint például a dolgok internete és a műholdas kommunikáció –, valamint a kvantuminformatika fejlődése[100] újabb kihívásokat hoznak majd magukkal.

---

95 A Harmadik Generációs Partnerségi Projekt, amely megalapozta az olyan kommunikációs technológiák fejlesztését, mint például az 5G, a dolgok internete és a mobil széles sávú szolgáltatások.

96 Lásd: „*Law enforcement and judicial aspects related to 5G*” (Az 5G-vel kapcsolatos bűnüldözési és igazságügyi szempontok), a terrorizmus elleni küzdelem uniós koordinátora, 2019, https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol – Position paper on Home routing.pdf (Állásfoglalás a home routingról) (europa.eu).

98 Az RCS protokoll lehetővé teszi csoportos csevegések, videók, hang és nagy felbontású képek átvitelét; gyakran használják SMS helyett. A protokoll alkalmazásától függően az RCS-üzenetek jogszerű lehallgatása lehetetlennek bizonyulhat, ez pedig jelentős hatással van a bűnüldözésre (2023-ban több, mint 1 milliárd aktív RCS-felhasználó volt).

99 Lásd: 6G roadmap (6G-ütemterv): https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf.

100 *The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement* (A második kvantumforradalom: a kvantuminformatika és a kvantumtechnológiák hatása a bűnüldözésre) | Europol (europa.eu).

Végezetül, a magas szintű munkacsoport szakértői kiemelték, hogy a bűnüldöző hatóságok számára az egyik legnagyobb technikai nehézséget a végponttól végpontig terjedő titkosítás jelenti, különösen az OTT-kommunikáció esetében, ahol a kommunikáció több mint 80 %-a végponttól végpontig terjedő titkosítást alkalmazó szolgáltatások révén történik (élő kommunikáció és biztonsági tárhely), ami megakadályozza, hogy a nyomozók hozzáférjenek a kommunikáció tartalmához. A szakértők ugyanakkor egyetértenek abban, hogy a végponttól végpontig terjedő titkosítás olyan, hathatós biztonsági intézkedésnek tekinthető, amely hatékonyan védi a polgárokat a bűnözés különböző formáival szemben. A végponttól végpontig terjedő titkosítás biztosítja, hogy csak a kommunikációt folytató felhasználók férhessenek hozzá az üzeneteik tartalmához, és ezáltal hatékony védelmet nyújt a jogszerűtlen lehallgatással, az adatlopással, az államilag támogatott kémkedéssel, valamint a hekkerek, kiberbűnözők vagy akár maguk a szolgáltatók általi jogosulatlan hozzáférés más formáival szemben.

Azok a kihívások, amelyekkel a bűnüldöző hatóságok a bűnözők és terroristák végponttól végpontig terjedő titkosítás alkalmazásával történő kommunikációjának nyomon követése során szembesülnek, nehezen számszerűsíthetők. Ennek az az oka, hogy a bűnüldöző hatóságok gyakran úgy döntenek, hogy nem szánnak időt és erőforrásokat az elektronikus megfigyelést engedélyező bírósági határozatok beszerzésére olyan platformok esetében, amelyekről ismert, hogy alapértelmezetten végponttól végpontig terjedő titkosítást alkalmaznak[101]; ezért az olyan, ténylegesen benyújtott, tartalmi adatokra irányuló jogszerű lehallgatás iráni megkeresések száma, amelyek esetében a lehallgatás a végponttól végpontig terjedő titkosítás miatt nem végezhető el, nagyon alacsony és nem mutat valós képet. A megfigyelési képesség ebből következő hiányossága olyan, számottevő „holtteret” és sérülékenységet jelent a bűnüldöző hatóságok számára, amelynek a bűnözők és a terroristák teljes mértékben tudatában vannak, és amelyet aktívan ki is használnak, amint ezt az EncroChat[102] és a Sky ECC ügy is mutatta. Ezek az ügyek több ezer letartóztatást – többek között számos, nagy horderejű bűncselekményekben érintett bűnöző letartóztatását – eredményezték Európa-szerte. Erre a problémára mások mellett az európai rendőrségi vezetők[103] és a G7-ek[104] is több nyilatkozatukban felhívták a figyelmet. Annak szemléltetésére, hogy a tartalmi adatokhoz való hozzáférés emiatti ellehetetlenülése milyen következményekkel jár, a szakértők számos ismert példát soroltak fel – többek között terrorizmussal[105], kábítószer-kereskedelemmel[106] és szexuális kényszerítéssel[107] kapcsolatos ügyeket –, amelyek során a titkosítás alkalmazása jelentős mértékben akadályozta a bűnüldöző hatóságok azon képességét, hogy súlyos és szervezett bűncselekményeket akadályozzanak meg, illetve felvegyék a küzdelmet azok ellen.

A bűnüldöző hatóságok képviselői olyan megközelítést részesítenének előnyben, amely előírná a vállalatok számára, hogy – szigorú feltételek mellett – biztosítsák a bűnüldöző hatóságok hozzáférését a titkosítatlan adatokhoz. Ugyanakkor meg kell jegyezni azt is, hogy a kiberbiztonsági szakértők aggályokat vetettek fel azzal kapcsolatban, hogy az ilyen megoldások aláásnák a kiberbiztonságot. Néhány bűnüldözési szakértő jelezte, hogy egyes esetekben a titkosítást úgy hajtották végre, hogy az összeegyeztethető volt mind a kiberbiztonsággal, mind pedig annak szükségességével, hogy fenn kell tartani bizonyos szolgáltatásokat, például az operációs rendszerek frissítéseit, a tartalmak (pl. e-mailek vagy webes munkamenetek) kiberbiztonsági célú szkennelését vagy a kulcsfontosságú helyreállítási mechanizmusokat, amennyiben a felhasználó kéri ezt a funkciót.

---

101 Manpearl, 2017.

102 Az EncroChat és a Sky ECC ügyről lásd bővebben: Europol és Eurojust – „*Third Report of the Observatory Function on Encryption*” (A megfigyelőközponti funkció harmadik jelentése a titkosításról), 2021. június.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version .

105 2017 márciusában az 52 éves Kálid Maszúd iszlamista indítékú terrortámadást hajtott végre London központjában. A támadásban hat személy életét vesztette, és huszonkilencen sérültek meg. Noha az incidensről beszámoló jelentések arra engedtek következtetni, hogy Maszúd egyedül tervezte meg és hajtotta végre a támadást, később megállapítást nyert, hogy néhány perccel a támadás elkövetése előtt egy „Dzsihád” című PDF-dokumentumot küldött számos ismerősének WhatsAppon és iMessage-en. E két szolgáltatás alapértelmezetten végponttól végpontig terjedő titkosítást alkalmazott, és alkalmaz jelenleg is. Források: Max Hill: „*The Westminster Bridge Terrorist Attack*” (A Westminster hídi terrortámadás) (London: The Stationery Office, 2018); BBC News: „*WhatsApp Must Not Be a »Place for Terrorists to Hide«*” (A WhatsApp nem lehet a terroristák „búvóhelye”), 2017. március 26.

106 A szakértők olyan, nagy horderejű, kábítószer-kereskedelemmel kapcsolatos ügyeket említettek meg, amelyekben mindaddig lehetetlen volt előrelépést elérni, amíg a hatóságoknak nem sikerült hozzáférést szerezniük az EncroChaten és a Sky ECC-n keresztül folytatott titkosított kommunikációhoz.

107 Egy egyesült királysági, nagy horderejű ügyben a szexuális kényszerítéssel kapcsolatban folytatott rendőrségi nyomozást hátráltatta, hogy a gyanúsítottak WhatsAppon kommunikáltak, és a végponttól végpontig terjedő titkosítás megnehezítette a kulcsfontosságú bizonyítékokhoz való hozzáférést. Mivel a bűnüldöző hatóságok a felhasználók hozzájárulása nélkül nem tudták visszafejteni a WhatsApp-üzeneteket, ez akadályozta a nyomozást.

Ennek alapján a bűnüldözési szakértők egyetértettek abban, hogy a titkosítással összefüggő kihívások olyan többdimenziós megközelítést tesznek szükségessé, amely egyensúlyt teremt a magánélethez való jog, a biztonság és annak szükségessége között, hogy a bűnüldöző hatóságok hozzá tudjanak férni az adatokhoz a bűnözés elleni küzdelem, valamint az emberek életének, testi épségének és magántulajdonának védelme érdekében. Nem valószínű, hogy egyetlen megoldással kezelni lehetne minden releváns aggályt, a különböző megközelítések kombinációja azonban segíthet enyhíteni a problémát.

IV. Bűnözői jellegű hírközlési szolgáltatók

A bűnözők a végponttól végpontig terjedő titkosítást alkalmazó, általánosan elterjedt platformokat is használják kommunikációjuk elrejtésére; ugyanakkor dönthetnek úgy is, hogy a kifejezetten bűnözői tevékenységek céljára kialakított biztonságos kommunikációs csatornákat veszik igénybe (a továbbiakban: „CCC-k”, ami a „bűnözői kommunikációs csatornák” [*criminal communication channels*] rövidítése)[108]. Az EncroChat és a Sky ECC egyaránt jól ismert CCC-k, amelyek a bűnözői tevékenységek elrejtésére kialakított, végponttól végpontig terjedő titkosítást alkalmazó, beépített üzenetküldő szolgáltatással együtt értékesítettek telefonokat, amelyeket a dark weben reklámoztak. 2020-ban és 2021-ben mindkét platformot felszámolták, mégpedig azoknak a nemzetközi közös bűnüldözési műveleteknek köszönhetően, amelyek rávilágítottak e platformoknak a szervezett bűnözésben való széles körű részvételére. Számos hasonló platform, például a Phantom Secure[109] és az Exclu[110] felszámolására is sor került, ugyanakkor sok kisebb platform még mindig működik, és ezek biztonságos helyszíneket biztosítanak a bűnözői információcsere számára. Ebben a fragmentált környezetben alapvető fontosságú, hogy a bűnüldöző hatóságok képesek legyenek felismerni a CCC-ket, nyomon követni és megakadályozni a tevékenységüket, felszámolni őket, és bíróság elé állítani a bűnözőket.

[108] https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf

[109] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

[110] *New strike against encrypted criminal communications with dismantling of Exclu tool* (Az Exclu felszámolása újabb csapás a titkosított bűnügyi kommunikáció ellen) | Eurojust | Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (europa.eu)

Az ebbe a típusba tartozó, tisztességtelen hírközlési szolgáltatók esetében a szolgáltató által végzett lehallgatás nem jöhet szóba, ezért a bűnüldöző hatóságoknak releváns taktikai lehallgatási képességekre – eszközökre és szakértelemre – van szükségük a felhasználóknak a titkosítás ellenére történő célzott nyomon követéséhez. A bűnüldözési szakértők hangsúlyozták, hogy az ilyen technikák fejlesztéséhez és használatához jelentős kihívások, kockázatok és korlátok kapcsolódnak, tekintettel arra, hogy azok arányossága nem garantálható, ezért helyénvaló az alkalmazásukat a legnagyobb horderejű esetekre korlátozni. A nemzeti hatóságok a kapacitásuktól és a jogi keretüktől függően különböző megközelítéseket alkalmaznak, amelyek magukban foglalhatnak saját fejlesztésű, harmadik felektől vásárolt, illetve szolgáltatásként üzemeltetett eszközöket; függetlenül attól, hogy melyik lehetőséget alkalmazzák, a szakértők egyetértenek abban, hogy az ilyen eszközök használatához garanciákra és biztosítékokra van szükség. Ide tartozhat annak átgondolása, hogy miként javítható az eszközök felügyelete, értékelése és tanúsítása, valamint a sérülékenységek kezelésére vonatkozó szilárd keret kialakítása, teljes mértékben tiszteletben tartva ugyanakkor a tagállamok büntetőügyekben fennálló eljárási autonómiáját és a nemzetbiztonsággal kapcsolatos kizárólagos hatáskörüket.

A nyomozó hatóságok jogi kihívásokkal is szembesülnek; ilyenek például az elsősorban (mivel minden adatforgalom titkosított) bűnözői célú szolgáltatásokat kínáló hírközlési szolgáltatók és tárhelyszolgáltatások tevékenységeinek bűncselekménnyé nyilvánításával kapcsolatos nehézségek, márpedig első lépésként erre van szükség ahhoz, hogy sor kerülhessen bírósági vagy közigazgatási intézkedések meghozatalára. Ezen túlmenően a tagállamok számára lehetővé kell tenni, hogy szankciókat szabjanak ki a CCC-kre annak érdekében, hogy korlátozni vagy blokkolni tudják az ilyen szolgáltatásokhoz való hozzáférést az EU-ban, és ezáltal ellehetetlenítsék azok bűnözői üzleti modelljének működését. Ez akkor válhat majd szükségessé, ha és amikor a jogszerű lehallgatási kötelezettségek alkalmazandók lesznek az OTT-szolgáltatások esetében – mégpedig annak megakadályozása érdekében, hogy a bűnözők újból visszatérjenek a tisztességtelen hírközlési szolgáltatókhoz.

Végül meg kell említeni, hogy bíróság előtt támadják olyan ügyek különböző aspektusait, mint az EncroChat és a Sky ECC ellen indított ügyek. Az EU-n belül jelentős eltérések vannak a más tagállamban lehallgatott adatok bizonyítékként való felhasználására vonatkozó követelmények között, ami jogbizonytalanságot eredményez az olyan, hasonló műveletek esetében, amelyeket egy tagállam hajt végre, de potenciálisan sok tagállamra hatással lehetnek.

LEHETSÉGES MEGOLDÁSOK

I. A jogszerű lehallgatás iránti megkeresések végrehajthatóvá tétele valamennyi típusú elektronikus hírközlési szolgáltató esetében

Az EU-ban a jogszerű lehallgatási képességek a hagyományos hírközlési szolgáltatókra korlátozódnak, ám a legtöbb kommunikáció jelenleg nem hagyományos hírközlési szolgáltatókon keresztül történik[111]. Függetlenül attól, hogy a hírközlési szolgáltatást az infrastruktúra tulajdonosa nyújtja-e vagy sem, a bűnüldöző hatóságoknak egyformán képeseknek kell lenniük arra, hogy jogszerűen lehallgassák a célszemélyeket. Az olyan alternatív megoldások, mint például a számfüggetlen személyközi hírközlési szolgáltatásoknak és más hírközlési szolgáltatásoknak kizárólag a távközlési hálózat szintjén történő jogszerű lehallgatása, a számfüggetlen személyközi hírközlési szolgáltatók jogszerű lehallgatásának lefolytatására vonatkozó nemzetközi együttműködési eszközök igénybevétele, vagy a taktikai lehallgatás széles körű alkalmazása, nem működőképesek[112].

A fentiek alapján a magas szintű munkacsoport szakértői elsőrendű fontosságúnak tartják annak biztosítását, hogy a rendelkezésre álló adatok jogszerű lehallgatására vonatkozó kötelezettségek egyformán alkalmazandók és végrehajthatók legyenek a hagyományos és a nem hagyományos hírközlési szolgáltatók tekintetében is. E kötelezettségek harmonizációjának lehetővé kell tennie a határokon átnyúló megkeresések teljesítésével kapcsolatos nehézségek leküzdését.

E cél elérése érdekében és az EU-n belüli, a jogszerű lehallgatásra vonatkozó szabályok közelítése és harmonizációja felé való fokozatos elmozdulás céljából a magas szintű munkacsoport szakértői fokozatos megközelítést javasolnak: először is uniós szinten meg kell állapodni a strukturálásra vonatkozó elvekről (1. lépés); ezt követően a Bizottságnak támogatnia kell ezen elvek végrehajtását (2. lépés); végül pedig, további értékelés alapján, ezen elvek jogi eszközben történő kodifikálására is sor kerülhet (3. lépés).

---

111 Az Egyesült Királyságban 2022-ben elküldött SMS-ek és MMS-ek száma 36 milliárd volt, az online üzenetek száma ugyanakkor 1,3 billió (*WhatsAppening in the world of online communications?* (Mi történik az online kommunikáció világában?- Ofcom).

112 Lásd a kihívásokról szóló részt.

1. lépés: Megállapodás a közös alapelvekről

Először is közös értelmezést kell kialakítani arra vonatkozóan, hogy az elektronikus hírközlési szolgáltatások mely kategóriáira vonatkozhatnak a jogszerű lehallgatásra irányuló belföldi kötelezettségek az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet szabályainak megfelelően.

Másodszor, megállapodásra kell jutni a magas szintű operatív követelményekről, és ennek keretében egyértelműen meg kell határozni, hogy a nemzeti hatóságok mit várnak el a jogszerű lehallgatás tekintetében, és ahhoz milyen biztosítékoknak kell kapcsolódniuk. Megállapítást nyert, hogy a bűnüldözési követelmények meghatározásához jó alapként szolgál a LEON[113]. Ezt a dokumentumot olyan követelményekkel kell kiegészíteni, amelyek például az arányosságra, a felügyeletre és az átláthatóságra vonatkoznak, lehetőség szerint különbséget téve a tartalmi és a nem tartalmi adatokra alkalmazandó szabályok között, teljes mértékben tiszteletben tartva a kiberbiztonságot, az adatvédelmet és a magánélet védelmét, ugyanakkor nem veszélyeztetve a titkosítást. Egy kiberszakértőket, a magánélet védelmével foglalkozó szakértőket, illetve bűnüldözési szakértőket is magában foglaló ad hoc szakértői csoport esetleges létrehozása biztosíthatná a követelmények szükség szerinti aktualizálását, lehetőség szerint az Europol belső biztonsággal kapcsolatos szabványosítással foglalkozó munkacsoportjának – a továbbiakban is folytatandó – munkájára építve.

Harmadszor, egyértelműen meg kell határozni az illetékesség fogalmát annak az OTT-szolgáltatásokra való alkalmazhatósága tekintetében, figyelembe véve a nemzeti hatóságok közötti, illetve – ami a legfontosabb – a nemzeti hatóságok és az OTT-szolgáltatók közötti eltérő értelmezéseket. Egyértelművé kell tenni például az olyan esetekre vonatkozó szabályokat, amikor a célpont holléte bizonytalan. Iránymutatásra van szükség azzal kapcsolatban is, hogy ki értékelheti a megkeresés jogszerűségét, például a szolgáltatók ebben az összefüggésben betöltött szerepét illetően. Végül, de nem utolsósorban, bár az eddig hozott bírósági ítéletek túlnyomó többsége megerősítette az EncroChat és a Sky ECC elleni eljárási cselekmények jogszerűségét, még folyamatban van számos olyan bírósági ügy[114], amely jelentős hatással lehet a nagy horderejű bűncselekményekben érintett bűnözők elítélésére. Ezért szükség lehet a taktikai lehallgatási intézkedésekből származó bizonyítékok tagállamok közötti elfogadhatóságának, az ítéletek és bírósági határozatok kölcsönös elismerésének, valamint a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésnek a megkönnyítésére.

---

[113] A LEON (*Law Enforcement – Operational Needs for Lawful Access to Communications*) (Bűnüldözés – A kommunikációhoz való jogszerű hozzáférés iránti operatív szükségletek) a svéd bűnüldöző hatóságok által az uniós tagállamok, Észak-Amerika és Ausztrália bűnüldöző hatóságainak képviselőivel szoros együttműködésben végzett munka eredménye. Célja a kommunikációs tartalmakhoz, az ilyen tartalmakra vonatkozó adatokhoz és az előfizetői információkhoz való jogszerű hozzáférés iránti bűnüldözési szükségletek azonosítása és leírása. Lásd: „*Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications* (LEON)" (A Tanács elnökségének közleménye a kommunikációhoz való jogszerű hozzáférés iránti bűnüldözési operatív szükségletekről), 6050/23, 2023. február 16.

[114] Lásd a T-1180/23. sz., a T-148/24. sz., a T-167/24. sz., a T-484/24. sz. és a T-560/24. sz. ügyet.

7. ajánláscsoport

Annak érdekében, hogy uniós szinten megállapodás szülessen a rendelkezésre álló adatok jogszerű lehallgatásának közös elveiről, amelyek az elektronikus hírközlési szolgáltatók valamennyi típusára alkalmazandók, a szakértők a következőket javasolják:

1. *a jogszerű lehallgatás fogalmának és hatályának pontosítása a hatályos uniós jogi aktusokkal és más releváns európai és nemzetközi eszközökkel – például a Számítástechnikai Bűnözésről szóló Egyezménnyel (Budapesti Egyezmény) – összhangban [38. ajánlás];*

2. *a LEON dokumentum inspirációs forrásként való felhasználása a közös operatív követelmények meghatározásához [21. ajánlás];*

3. *a szükséges biztosítékok meghatározása [17. ajánlás, 41. ajánlás];*

4. *a kiberbiztonsági perspektíva figyelembevétele oly módon, hogy egyetlen intézkedés se eredményezhessen olyan kötelezettséget a szolgáltatók számára, hogy IKT-rendszereiket olyan módon kelljen kiigazítaniuk, amely negatívan befolyásolná a felhasználóik kiberbiztonságát [41. ajánlás];*

5. *az adatokkal kapcsolatos illetékesség fogalmának egyértelművé tétele az esetleges kollíziók kezelése érdekében [39. ajánlás], valamint olyan uniós szintű minimumszabályok elfogadásának előmozdítása, amelyek adott esetben lehetővé teszik a taktikai lehallgatási intézkedésekből származó bizonyítékok tagállamok közötti elfogadhatóságát, olyan mértékben, amennyiben ez az ítéletek és bírósági határozatok kölcsönös elismerésének, valamint a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésnek a megkönnyítéséhez szükséges [42. ajánlás].*

Meg kell fontolni, hogy mi a legjobb megközelítés a 7. ajánláscsoportban említett közös elvek összeállítására és elfogadására, valamint az ezen elvek megosztását szolgáló legmegfelelőbb eszköz meghatározására vonatkozóan. Visszatekintve, a jogszerű lehallgatásról szóló 1995. január 17-i tanácsi állásfoglalás[115] fontos szerepet játszott a jogszerű lehallgatási megoldások harmonizációjának elősegítésében, mivel referenciaként szolgált az ETSI által a jogszerű lehallgatásra vonatkozóan kidolgozott szabványokhoz. Egy ehhez hasonló megközelítés szintén előnyös lehet, esetleg bizottsági vagy tanácsi ajánlás formájában.

[115] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104

Fő intézkedés: A magas szintű munkacsoport szakértői felkérik az EU-t, hogy 2025-ben adjon ki ajánlást az adatokhoz való valós idejű hozzáférésről

Időkeret: 2025 *Költségvetés: még meghatározandó*

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy adjon ki ajánlást, amely egyértelműen meghatározza az elektronikus hírközlési szolgáltatók vonatkozásában a jogszerű lehallgatás fogalmát[116], és részletezi a rendelkezésre álló nem tartalmi és tartalmi adatok jogszerű lehallgatására esetlegesen alkalmazandó különböző követelményeket, a kiberbiztonságnak, az adatvédelemnek és a magánélet védelmének a teljes körű tiszteletben tartása mellett, a titkosítás veszélyeztetése nélkül, a LEON dokumentumban meghatározott közös operatív követelményekre építve.

2. lépés: Uniós támogatás nyújtása az egyenlő versenyfeltételek biztosítása és a határokon átnyúló együttműködés fokozása érdekében

Az uniós szintű technikai, jogi és szervezeti harmonizáció alapját az 1. lépésben meghatározott közös elvek adnák. Konkrét eredményekké való átalakításukhoz a Bizottság általi koordináció és pénzügyi támogatás szükséges. Ez magában foglalná egy külön eljárás kialakítását, a meglévő munkacsoportok igénybevételét és szükség esetén újak létrehozását, az érintett érdekelt felekkel – köztük az OTT-szolgáltatókkal és az ágazat képviselőivel – való koordináció biztosítását, az érintett szervek, nevezetesen a Tanács és az Európai Parlament számára történő jelentéstételt, valamint a nyilvánosság számára az átláthatóság biztosítását. Magában foglalhatná továbbá célzott tanulmányok finanszírozását, akár közvetlenül, akár releváns – például az érintett ügynökségekkel vagy tudományos partnerekkel kialakított – partnerségeken keresztül.

[116] A szolgáltató által végzett lehallgatásra korlátozva, a fentiekben meghatározottak szerint.

A magas szintű munkacsoport szakértői ezenkívül hangsúlyozták, hogy a fent vázolt munka elvégzése mellett sürgősen javítani kell a határokon átnyúló jogszerű lehallgatás iránti, a jelenlegi keret alapján benyújtott megkeresések hatékonyságát. Ez a célkitűzés a következőket foglalná magában:

- az ENYH[117] jelenlegi korlátainak értékelése és a működési hatékonyság javítására irányuló munka,
- a jogszerű lehallgatás révén gyűjtött bizonyítékok határokon átnyúló cseréjével kapcsolatos technikai és szervezeti korlátok kezelése, ami pedig további munkát igényelne a következőkkel kapcsolatban:
    - a probléma feltérképezése (milyen korlátok vannak, mely tagállamok tapasztalják azokat, stb.),
    - az adatstruktúrák, a bizalmi mechanizmusok és az adatszűrés szabványosítása a nem releváns adatok továbbításának elkerülése, valamint a célhoz kötöttség, az arányosság és az adattakarékosság adatvédelmi elveinek tiszteletben tartása érdekében,
    - a határokon átnyúló továbbítási eszközök kialakítása és kapacitása,
    - a kapcsolódó finanszírozási rendszerek azonosítása,
- a határokon átnyúló jogszerű lehallgatás iránti megkeresések egyszerűsítése egyablakos ügyintézési pontok kijelölése és azok személyzetének képzése révén, az egyablakos ügyintézési pontok és a digitális bizonyítékokhoz való hozzáférés terén végzett átfogó munkával összehangolva, kiemelt szerepet biztosítva a SIRIUS projektnek,
- adott esetben a tagállamok és az Egyesült Államok közötti kétoldalú megállapodások előmozdítása, ami előfeltétel annak megkönnyítéséhez, hogy a nemzeti hatóságok közvetlenül fordulhassanak megkereséseikkel a leggyakoribb OTT-szolgáltatókhoz, ugyanis az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésről szóló, jelenleg tárgyalás alatt álló EU–USA megállapodás hatálya – a tárgyalási irányelvek értelmében – nem fog kiterjedni a jogszerű lehallgatásra, ez pedig azt jelenti, hogy egyedi megállapodásokra lesz szükség a kollíziók kezeléséhez.

---

[117] A büntetőügyekben kibocsátott európai nyomozási határozatról (ENYH) szóló, 2014. április 3-i 2014/41/EU európai parlamenti és tanácsi irányelv „távközlés”-re utal; ezt a legtöbb tagállam azonban tágabban értelmezte – az EEHK aktualizálásával összhangban –, ezért fontolóra lehetne venni és tovább lehetne vizsgálni, hogy szükség van-e az ENYH módosítására e tekintetben.

Végezetül, a szakértők olyan intézkedések megfontolását tartják szükségesnek, amelyek fokozhatnák a nemzeti hatóságok által a nem együttműködő elektronikus hírközlési szolgáltatásokkal szemben hozott intézkedések visszatartó erejét. A szakértők külön kiemelték, hogy értékelni kell a lehetséges műszaki megoldások megvalósíthatóságát és arányosságát.

8. ajánláscsoport

Annak biztosítása érdekében, hogy az elektronikus hírközlési szolgáltatók széles köre – beleértve az OTT-szolgáltatókat is – a nemzeti jogszabályokban meghatározottak szerint reagáljon a jogszerű lehallgatás iránti megkeresésekre, a szakértők a következőket javasolják:

1. *az 1.1. ajánlásban meghatározott elvek végrehajtásának támogatása koordináció és finanszírozás révén;*

2. *annak megvizsgálása, hogy az ENYH hogyan tudná jobban támogatni a határokon átnyúló jogszerű lehallgatás iránti megkereséseket, például a jogbiztonság javítása, a határozatokra való válaszadás határidejének lerövidítése és az ENYH egységes használatának előmozdítása révén [40. ajánlás];*

3. *olyan mechanizmusok (interoperabilitás és kiberbiztonság) és infrastruktúrák (sávszélesség és méretezhetőség) kiépítése, amelyek összeegyeztethetők a nagy adatkészletek valós idejű, határokon átnyúló továbbításával [9. ajánlás];*

4. *az egyablakos ügyintézési pontok kijelölésének előmozdítása az EU-ban a hatóságoktól érkező megkeresések kezelése és a hatóságokkal való kapcsolattartás céljából, a jogszerű lehallgatással kapcsolatos kötelezettségek teljesítésének elősegítése és a határokon átnyúló megkeresések hatékony célzására irányuló mechanizmusok kialakítása érdekében [19. és 36. ajánlás];*

5. *az adatokhoz való valós idejű hozzáférésre vonatkozó kétoldalú megállapodások kidolgozásának előmozdítása harmadik országokkal, mindenekelőtt az Egyesült Államokkal [38.4. ajánlás].*

A jogszerű lehallgatásról szóló uniós ajánlás hatékony végrehajtását több tevékenység révén lehetne támogatni.

Fő intézkedés: A magas szintű munkacsoport szakértői felkérik a Bizottságot, hogy biztosítson megfelelő koordinációt és finanszírozást a jogszerű lehallgatásról szóló uniós ajánlás végrehajtásához

- A magas szintű munkacsoport szakértői felkérik a Bizottságot, hogy terjesszen elő egyértelmű tervet a jogszerű lehallgatásról szóló uniós ajánlás végrehajtásának támogatására, figyelembe véve a pénzügyi tervezési szempontokat is.

3. lépés: Egy, a jogszerű lehallgatásra vonatkozó jogi eszköz esetleges kidolgozásának megvizsgálása

A koordináció önmagában nem feltétlenül elégséges a harmonizáció megkívánt szintjének eléréséhez, még akkor sem, ha azt a meglévő jogi eszközök hatékonyabbá tételét célzó intézkedések egészítik ki. Új szabályokra lehet szükség a megkeresések végrehajthatóságának és a jogbiztonságnak a garantálása, a kollíziók megszüntetése, valamint a megfelelőségi és jogszerűségi ellenőrzésekhez kapcsolódó adminisztratív terhek csökkentése érdekében. Ezen túlmenően, a jogszerű lehallgatásra vonatkozó szabályok közötti, az EU-n belüli különbségek miatt megterhelő követelmények vonatkoznak a szabályozás hatálya alá tartozó szervezetekre, például az OTT-szolgáltatókra, ez pedig a piacra jutást gátló akadályokat jelenthet a hírközlési szolgáltatók számára[118]. E tekintetben a rendelkezésre álló adatok jogszerű lehallgatására vonatkozó, harmonizált uniós szabályok elfogadása elősegítené Európa jövőbeli digitális infrastruktúrájának kiépítését, előnyben részesítve egy olyan modellt, amelyben a távközlési infrastruktúra potenciálisan az egész kontinensre kiterjedő lefedettséget kínál[119].

Az internetes kommunikációra való átállás erőteljes ösztönzőt jelent arra vonatkozóan, hogy uniós szintű, harmonizált hozzáférési szabályokat határozzunk meg; mindazonáltal gondosan meg kell vizsgálni egy esetleges jogi eszköz elfogadhatóságát, megvalósíthatóságát, valamint az ágazatra, a kiberbiztonságra és a biztonságra gyakorolt hatását, figyelembe véve az egyes tagállamoknak a jogszerű lehallgatással kapcsolatos jogi szabályozása közötti jelenlegi különbségeket. A magas szintű munkacsoport szakértői hangsúlyozták, hogy az említett esetleges jogi eszköznek: i. meg kell felelnie az 1.1. ajánlásban meghatározott elveknek; ii. teljes mértékben figyelembe kell vennie az alapvető jogokkal kapcsolatos szempontokat, valamint az államok szuverenitását a büntetőügyek és a nemzetbiztonság tekintetében; továbbá iii. az elektronikus bizonyítékokról szóló csomaggal kapcsolatban végzett munka eredményein kell alapulnia.

A magas szintű munkacsoport szakértői egyetértettek abban, hogy minden olyan kezdeményezésnek, amely a jogszerű lehallgatásra vonatkozó szabályok alkalmazásának valamennyi típusú elektronikus hírközlési szolgáltatás tekintetében történő szorgalmazására vagy kötelezővé tételére irányulna, egyértelmű és érvényesíthető keretet kell magában foglalnia a jogellenesen működő és/vagy a bűnüldöző hatóságokkal való együttműködés bármely formáját megtagadó **hírközlési szolgáltatókkal szembeni fellépéshez**. Egy ilyen keret hiányában veszélybe kerülne a szabályok betartása, a bűnözők pedig tömegesen helyeznék át a kommunikációjukat a szabályokat be nem tartó szolgáltatókhoz. Bármely ezzel kapcsolatos jövőbeli uniós kezdeményezésnek különbséget kell tennie a jogi kötelezettségeiket nem teljesítő OTT-szolgáltatók, illetve az olyan elektronikus hírközlési szolgáltatók között, amelyek kifejezetten a bűnözői tevékenységekre szabott szolgáltatásokat kínálnak. Emellett pedig minden kezdeményezésnek figyelembe kell vennie az uniós vívmányokat is, különösen a digitális szolgáltatásokról szóló rendeletet.

---

118 Lásd: „*Lawful interception – A market access barrier in the European Union*” (Jogszerű lehallgatás – a piacra jutást gátló akadály az Európai Unióban), Vadim Doronin, in: *Computer Law & Security Review* 51 (2023) 105867.

119 *White Paper – How to master Europe's digital infrastructure needs*? (Fehér könyv – Hogyan lehet megfelelni Európa digitális infrastrukturális igényeinek?) | *Shaping Europe's digital future* (Európa digitális jövőjének alakítása) (europa.eu)

Egy ilyen kezdeményezés akár közigazgatási vagy bírósági intézkedéseket is magában foglalhat. A magas szintű munkacsoport szakértői e kérdés mélyreható vizsgálatát szorgalmazták; ennek során figyelembe kell venni mind az alapvető jogokkal és a kiberbiztonsággal kapcsolatos aggályokat, mind pedig a kapcsolódó összetett technológiai kihívásokat.

9. ajánláscsoport

A szakértők azt javasolják, hogy – további elemzés és hatásvizsgálat nyomán – kerüljön sor ***egy bűnüldözési célú, a jogszerű lehallgatásra vonatkozó („puha" jogi eszközökből vagy kötelező erejű jogi eszközökből álló) uniós eszköz kidolgozására****, amely végrehajtható kötelezettségeket állapítana meg az EU-ban elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók számára. A szakértők javaslata szerint az említett lehetséges jogi eszköznek: [38. ajánlás]*

1. *követnie kell a 7. ajánláscsoportban megállapított elveket;*
2. *technológiasemlegesnek kell lennie [21. ajánlás];*
3. *támogatnia kell a nem együttműködő elektronikus hírközlési szolgáltatásokkal szembeni büntetőjogi intézkedések – ideértve a szabadságvesztést is – uniós szintű harmonizációját [34. ajánlás];*
4. *teljes mértékben figyelembe kell vennie az alapvető jogokkal kapcsolatos szempontokat, valamint az államok szuverenitását a büntetőügyek és a nemzetbiztonság tekintetében [38. ajánlás];*
5. *az elektronikus bizonyítékokra vonatkozó szabályok elfogadásával kapcsolatban végzett munka eredményein kell alapulnia [a 38. ajánlás iv. pontja];*
6. *köteleznie kell a szolgáltatókat arra, hogy szolgáltatásaik bizonyos funkcióit be- vagy kikapcsolják azzal a céllal, hogy egy esetleges parancs kézhezvételét követően információkat szerezzenek (például tárolják egy adott felhasználó földrajzi helymeghatározási adatait azt követően, hogy az adott személy tekintetében jogszerű megkeresés történt) [32. ajánlás];*
7. *olyan mechanizmusokat kell magában foglalnia, amelyek biztosítják egyrészről azt, hogy a tagállamok a digitális szolgáltatásokról szóló rendelet szabályaival összhangban és lehetőség szerint azokra építve érvényesíteni tudják a nem együttműködő elektronikus hírközlési szolgáltatásokkal szembeni szankciókat (közigazgatási vagy büntetőjogi intézkedéseket, attól függően, hogy a szolgáltató pusztán nem együttműködő, vagy pedig bűncselekmény jellegű szolgáltatást nyújt), másrészről azt, hogy az említett szankciók visszatartó erővel bírjanak e szervezetek számára [33. ajánlás].*

A jogszerű lehallgatásról szóló uniós ajánlásban meghatározott elvek érvényesítése fontos lépés lenne a jogszerű lehallgatásra vonatkozó harmonizáltabb és végrehajthatóbb szabályok rendelkezésre állása felé. Mindazonáltal továbbra is szükség lehet egy jogi eszközre is, a jogbiztonság javítása és annak biztosítása érdekében, hogy a jogszerű lehallgatás végrehajtása során valamennyi érintett elektronikus hírközlési szolgáltatás tekintetében meglegyenek a szükséges biztosítékok, továbbá annak biztosítása érdekében, hogy azokat az elektronikus hírközlési szolgáltatásokat, amelyek nem hajlandóak a tagállamok által megállapított szabályok érvényesítésére, kötelezzék erre.

Fő intézkedés: A magas szintű munkacsoport szakértői felkérik a Bizottságot, hogy vizsgálja meg a bűnüldözési célú jogszerű lehallgatásra vonatkozó jogszabályi keret továbbfejlesztését

- A magas szintű munkacsoport szakértői felkérik az Európai Bizottságot, hogy – egy esetleges hatásvizsgálatot megelőzően – vizsgálja meg egy, a jogszerű lehallgatásra vonatkozó uniós jogi eszköz kidolgozásának lehetőségét, az elektronikus bizonyítékokról szóló uniós rendelet és irányelv előkészítése során végzett munkára építve és a lehetséges technológiasemleges megoldások azonosítására összpontosítva.

II. A technológiai kihívások kezelése

Számos olyan kihívás, amellyel a bűnüldöző hatóságoknak szembe kell nézniük az adatokhoz való hozzáféréssel kapcsolatban, a technológiai fejlődés előrejelzésének és az ahhoz való alkalmazkodásnak a nehézségéből fakad. Ennek az az oka, hogy – más ágazatok, például a védelem vagy az űrágazat szereplőivel ellentétben – a bűnüldöző hatóságok nem rendelkeznek az ehhez szükséges erőforrásokkal vagy nem tartanak fenn szoros kapcsolatot az ágazattal ennek érdekében, és nem is megszokott dolog számukra, hogy ezt meg kell tenniük. A belső biztonság területén működő szereplők sok esetben reaktív módon próbálják meg pótolni a technológiai hiányosságokat, vagy – még gyakrabban – megpróbálják a szükségleteiket a rendelkezésre álló és megfizethető, készen kapható technológiával kielégíteni. A reaktív megközelítésről a proaktívabb megközelítésre való áttérés előmozdítása érdekében a technológiai kihívásokat strukturált, előretekintő és multidiszciplináris módon kell kezelni, a következő két fő prioritást tartva szem előtt: a nemzeti hatóságok szempontjából alapvető fontosságú annak biztosítása, hogy a bűnüldöző hatóságok hozzájuthassanak a rendelkezésre álló, átvitel alatt lévő adatok megszerzéséhez és feldolgozásához szükséges megfelelő kapacitásokhoz; a szolgáltatók és a technológiaszolgáltatók számára pedig alapvető fontosságú, hogy teljesíteni tudják az adatokhoz való hozzáféréssel, a magánélet védelmével és a kiberbiztonsággal kapcsolatos kötelezettségeiket, ugyanakkor az érdekeik védelme is biztosított legyen.

A szakértők ezért a technológiai kihívások előrejelzését javasolják olyan átfogó és előretekintő politika keretében, amely **a jogszerű hozzáférésre vonatkozó technológiai ütemterven** alapul, és amely meghatározza a célkitűzéseket, valamint a célkitűzések eléréséhez szükséges, megfelelő finanszírozással ellátott kerettevékenységeket.

A kapacitásépítést illetően, habár a kihívások eltérőek, a szakértők által javasolt megközelítés gyakran hasonló a digitális kriminalisztika, az adatmegőrzés és a jogszerű lehallgatás esetében[120], és ugyanazokra az ajánlásokra épül; ide tartozik az elérendő célokra alapozott tervezés a finanszírozási lehetőségek célzott felhasználása érdekében, az ágazati szereplőknek és a kulcsfontosságú érdekelt feleknek – például a belső biztonság európai innovációs központjának – a szorosabb bevonásával.

A bűnüldözési szakértők azonban különösen kiemeltek két, kifejezetten a jogszerű lehallgatáshoz kapcsolódó elemet.

- A metaadatok – például a helymeghatározási adatok, a hívásnyilvántartások és az e-mail-fejlécek – fokozott felhasználása révén több nyomozati bizonyíték válik megszerezhetővé. **Ahogy egyre több eszköz csatlakozik az internethez, a generált adatok mennyisége növekedni fog, és ez több lehetőséget kínál a viselkedési minták azonosítására.** A szakértők hangsúlyozták, hogy **a metaadatok fokozott** – például a mesterséges intelligencia segítségével történő – **felhasználásával** kapcsolatban további kutatásra és innovációra, valamint ezek eredményeinek kiterjedtebb gyakorlati hasznosítására van szükség, a tartalmi adatokhoz való hozzáférési lehetőség hiánya enyhítésének egyik módjaként. Ugyanakkor megemlítették azokat a magánélet védelmével kapcsolatos kockázatokat is, amelyek a személyes metaadat-tömegek mesterséges intelligencián alapuló kiterjedt feldolgozásával járnak, és amelyeket egyensúlyba kell hozni a tartalmi adatok célzott kiaknázásával. A bűnüldözési szakértők azonban egyértelműen jelezték, hogy a metaadatok önmagukban nem helyettesíthetik teljes mértékben a kommunikációs tartalom bizonyító erejét a szándék bizonyításában.
- Amikor a bűnözők végponttól végpontig terjedő titkosítást alkalmazó, célzott kommunikációs platformokat vesznek igénybe, a bűnüldöző hatóságoknak a **sérülékenységek** kiaknázásán alapuló taktikai megoldásokat kell alkalmazniuk a gyanúsítottak kommunikációjához való hozzáférés érdekében. Számos bűnüldöző hatóság már olyan jogi keret alapján működik, amely lehetővé teszi a kommunikációs végpontokon történő lehallgatást, és rendelkezik is az ehhez szükséges technológiával, és e tekintetben még további előrelépésre van szükség. Ez magában foglalhatja az EU-ban készült eszközök fejlesztésének támogatását, valamint annak lehetővé tételét, hogy a bűnüldöző hatóságok beszerezzék és a meglévő jogi kerettel összhangban használják azokat.

  A bűnüldözési szakértők ugyanakkor megjegyezték, hogy e módszer alkalmazását mint a bizonyítékgyűjtés elsődleges eszközét, nem helyénvaló bővíteni, mivel a taktikai lehallgatás nem problémamentes, és az arányossága nem garantálható. Például joghatósági kérdések merülhetnek fel a célpont holléte alapján. Továbbá, az olyan sérülékenységek kiaknázása, amelyek nem hozhatók nyilvánosságra, mindenképpen ellentmond az alapvető kiberbiztonsági elveknek.

[120] Lásd részletesen a digitális kriminalisztikáról szóló fejezetben.

Ami a beépített jogszerű hozzáférést illeti, a bűnüldözési szakértők óvatos megközelítést javasoltak, mivel az ágazati szereplőket nem lehet felkérni arra, hogy a szolgáltatás valamennyi felhasználóját érintően, általánosan vagy rendszerszintűen építsenek be olyan rendszereket, amelyek valószínűleg gyengítik a titkosítást; a jogszerű hozzáférésnek célzottnak, az egyes kommunikációkra eseti alapon vonatkozónak kell lennie. A szakértők egyetértettek az általános célkitűzés fontosságával, de hangsúlyozták, hogy fokozatosan kell előrehaladni, és be kell vonni az érdekelt felek valamennyi érintett kategóriáját, beleértve a technológiai, kiberbiztonsági és adatvédelmi szakértőket is, figyelembe véve a lehetséges kockázatokat és a nyilvános vita érzékeny jellegét. Erőteljesen tanácsolták különösen a tényeken alapuló megközelítés alkalmazását, valamint az olyan műszaki megoldások rendelkezésre állásának gondos értékelését, amelyek nem gyengítik a kommunikáció kiberbiztonságát, illetve nem befolyásolják hátrányosan a szolgáltatók kiberbiztonságát.

10. ajánláscsoport

A jogszerű lehallgatás technológiai kihívásainak kezelése érdekében a szakértők ***a jogszerű hozzáférésre vonatkozó technológiai ütemterv***[121] *kidolgozását javasolják, amelynek különösen:*

1. *össze kell fognia a technológiai, kiberbiztonsági, adatvédelmi, szabványosítási és biztonsági szakértőket, és biztosítania kell a megfelelő koordinációt, potenciálisan egy állandó struktúra révén [22. ajánlás];*
2. *támogatnia kell az adatgyűjtésre és az adatokhoz való hozzáférésre szolgáló eszközökre – többek között a visszafejtési képességekre, valamint a mesterséges intelligencián alapuló adatelemzési kapacitásokra – irányuló kutatást és fejlesztést, valamint ezen eszközök elterjedését*[122] *[4. ajánlás];*
3. *támogatnia kell a szabványosítás olyan, koordinált megközelítését, amely adott esetben figyelembe veszi az adatokhoz való jogszerű hozzáféréssel kapcsolatos szükségleteket, továbbá [15., 16. és 20. ajánlás]:*
    a. *támogatja valamennyi érintett közösség gyakorló szakembereinek részvételét a vonatkozó szabványügyi csoportokban;*
    b. *megfelelő szabványosítási intézkedéseket kapcsol a jövőbeli kezdeményezésekhez (a technológiasemleges megközelítés előmozdítása érdekében);*
    c. *kiterjed valamennyi kommunikációs technológiára, a dolgok internetére (ideértve például a hálózatba kapcsolt autókat) és a konnektivitás minden formájára (ideértve például a műholdas kommunikációt);*
4. *fokoznia kell az ágazattal való uniós koordinációt az olyan helyzetek kezelése érdekében, amikor léteznek technológiai megoldások, de azokat nem alkalmazzák; ilyen esetekben*[123] *egyértelmű iránymutatásra és uniós szinten elősegített párbeszédre van szükség [24. ajánlás];*
5. *minden releváns technológia tekintetében a bűnüldöző hatóságok által jelzett igényeknek megfelelően kell biztosítania a beépített jogszerű hozzáférést, garantálva ugyanakkor az erőteljes biztonságot és kiberbiztonságot, valamint a jogszerű hozzáférésre vonatkozó jogi kötelezettségek teljesítését [22. ajánlás];*
6. *teljeskörűen kezelnie kell a titkosítással összefüggő kihívásokat, a következők révén:*
    a. *annak biztosítása, hogy az esetleges új kötelezettségek és/vagy szabványok sem közvetlenül, sem közvetve ne eredményezzenek olyan kötelezettségeket a szolgáltatók számára, amelyek következtében a végponttól végpontig terjedő titkosítás általános veszélyeztetése vagy gyengítése miatt csökken a kommunikáció biztonsága [23. ajánlás];*
    b. *annak biztosítása, hogy a beépített jogszerű hozzáférés ne gyakoroljon negatív hatást az érintett hardver- vagy szoftverarchitektúrák biztonsági helyzetére [23. ajánlás];*
    c. *törekvés egy olyan módszertan kialakítására – koordinált módon, uniós finanszírozás igénybevételével –, amely célzott jogszerű hozzáférés kidolgozására, kezelésére és alkalmazására irányul az olyan esetek kezelése érdekében, amikor az adatokhoz való hozzáférés nem lehetséges az elektronikus hírközlési szolgáltatásokkal való együttműködés révén [10. ajánlás].*

---

121 A technológiai ütemtervnek a következő három munkafolyamatra kell kiterjednie: digitális kriminalisztika, adatmegőrzés és jogszerű lehallgatás.

122 Ez az ajánlás az eszközön tárolt adatokhoz való hozzáférésre is vonatkozik (lásd a digitális kriminalisztikáról szóló részt), de a felhasználás esetei némileg eltérnek egymástól.

123 Például amikor a home routingra vonatkozó megállapodások vagy az RCS-szolgáltatás konkrét megvalósítási módjai nem teszik lehetővé a jogszerű lehallgatást.

Bár a magas szintű munkacsoport szakértői által javasolt egyes kezdeményezések részben már léteznek, nagy szükség van arra, hogy a technológiai ütemterv strukturáltabb formában határozza meg a jogszerű hozzáférésre vonatkozó közép- és hosszú távú technológiai politikát, konkrét célok kitűzése révén, valamint egy kapcsolódó nyomonkövetési eszközzel együtt. Ennek a megközelítésnek nemcsak az átvitel alatt lévő adatokhoz való hozzáférésre kell kiterjednie, hanem a digitális kriminalisztikára és az adatmegőrzésre is.

A technológiai ütemtervnek előretekintőnek és végrehajthatónak kell lennie, a kiemelt témákra kell összpontosítania, és illeszkednie kell az EU digitális stratégiájához. Be kell vonnia – szoros partnerség révén – az érdekelt felek valamennyi érintett kategóriáját, különösen az uniós intézményeket, szerveket és ügynökségeket, a nemzeti hatóságokat, minden érintett terület tudományos szakembereit, az ágazati szereplőket és a nem kormányzati szervezeteket, és egyértelmű irányítással kell rendelkeznie.

Fő intézkedés: A magas szintű munkacsoport szakértői sürgetik a Bizottságot, hogy terjesszen elő és hajtson végre az adatokhoz való hozzáférésre vonatkozó technológiai ütemtervet

- A magas szintű munkacsoport szakértői felhívják az Európai Bizottságot, hogy terjesszen elő és hajtson végre olyan technológiai ütemtervet, amely a titkosítással kapcsolatos kihívásokra összpontosít, és kiterjed minden releváns szempontra, ideértve a technológiai, piaci, kiberbiztonsági, alapjogi, szabványosítási, bűnüldözési és a kutatással kapcsolatos szempontokat. A technológiai ütemtervnek 2025-ben el kell készülnie, és a tagállamoktól, valamint az uniós intézményektől, szervektől és ügynökségektől származó – többek között a kiberbiztonsággal, az adatvédelemmel és a magánélet védelmével kapcsolatos – releváns szakértelem összességére kell épülnie.