



Brüsszel, 2017.1.25.  
COM(2017) 41 final

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI  
TANÁCSNAK ÉS A TANÁCSNAK**

**Negyedik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról**

## Negyedik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról

### I. BEVEZETÉS

A hatékony és valódi biztonsági unió megvalósításáról szóló negyedik havi jelentés két fő pillér mentén vizsgálja az eddigi fejleményeket: *a terrorizmus és a szervezett bűnözés elleni küzdelem, illetve az azokat támogató eszközök felszámolása; valamint az e fenyegetéssel szembeni védelmünk megerősítése és ellenállóképességünk kiépítése*. Ez a jelentés négy fő területre fókuszál; az információs rendszerekre és az interoperabilitásra, a puha célpontok védelmére, a kiberfenyegetésre és a nyomozások keretén belüli adatvédelemre.

A berlini karácsonyi vásár elleni decemberi támadás ismét rávilágított információs rendszereink súlyos gyengeségeire, amelyeket mindenekelőtt uniós szinten sürgősen kezelni kell annak elősegítése érdekében, hogy a nemzeti határvédelmi és bűnüldöző hatóságok a helyszínen hatékonyabban végezzék nehéz munkájukat. Sürgősen orvosolandó gyakorlati végrehajtási gyengeséget jelent, hogy a különböző információs rendszereket nem kapcsolták össze – lehetővé téve, hogy a támadók több személyazonosságot használva észrevétlenül mozogjanak akkor is, amikor átkelnek a határokon – továbbá, hogy a tagállamok ezt az információt nem töltik fel rutinszerűen az érintett uniós adatbázisokba. Ezenfelül további munkára van szükség a határokon foganatosított bűnüldözési intézkedések, valamint azon személyek visszatérése tekintetében, akiknek a menedékjog iránti kérelmét elutasították<sup>1</sup>.

Ami a puha célpontok védelmét illeti, a Bizottság fel fogja gyorsítani arra irányuló tevékenységét, hogy összefogja a tagállami szakértőket a bevált gyakorlatok megosztása és az egységes iránymutatások közös kidolgozása érdekében.

Az EU-t érő kiberfenyegetést jelentős médiafigyelem övezi, és ez a jelentés az e területen már folyamatban lévő különféle munkafolyamatokat tekinti át. Mindez kiterjed a megelőzés oldalára – az iparággal folytatott együttműködés keretében, amelynek célja a beépített biztonság előmozdítása és a hálózati és információs rendszerek biztonságáról szóló irányelv végrehajtása –, valamint a tagállamok, a nemzetközi szervezetek és a kibertámadások ellen azok bekövetkezésekor küzdő partnerek közötti együttműködés előmozdítása. Az elkövetkező hónapok folyamán a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője azonosítani fogja az ahhoz szükséges fellépéseket, hogy a 2013. évi uniós kiberbiztonsági stratégiára építve hatékony, uniós léptékű választ adjunk a szóban forgó fenyegetésekre.

A magánélet és a személyes adatok védelem lényeges alapvető jog, és így a valódi biztonsági unióra irányuló valamennyi intézkedés sarokkövét képezi. A 2016 áprilisában elfogadott, a rendőrségi és büntető igazságszolgáltatási területre vonatkozó adatvédelmi irányelv magas szintű közös adatvédelmi normát garantál, és ennél fogva elősegíti az érintett adatok zavartalan cseréjét a tagállamok bűnüldöző hatóságai között. A Bizottság adatvédelmi csomagja keretében az elektronikus hírközlési adatvédelmi irányelv felülvizsgálatát is elindította, hogy kiterjessze az irányelv hatályát valamennyi

---

<sup>1</sup> A Bizottság az elkövetkező hetekben fogja előterjeszteni a visszatérésről szóló felülvizsgált cselekvési tervet, lásd: A Bizottság jelentése az Európai Parlamentnek, az Európai Tanácsnak és a Tanácsnak az Európai Határ- és Parti Őrség működőképessé tételéről, COM(2017) 42.

elektronikus hírközlési szolgáltatóra, és összhangba hozza annak rendelkezéseit az általános adatvédelmi rendelettel. A javaslat célja az adatvédelem biztosítása az elektronikus hírközlési terén, azon indokok, így nemzetbiztonsági vagy nyomozási okok meghatározása mellett, amelyek alapján előírható az elektronikus hírközlési adatvédelmi rendelet hatályának korlátozása.

## II. AZ INFORMÁCIÓS RENDSZEREK ÉS AZ INTEROPERABILITÁS ERŐSÍTÉSE

Juncker elnök 2016. szeptemberi értékelő beszéde az Unió helyzetéről, valamint az Európai Tanács 2016. decemberi következtetései egyaránt rámutatnak, hogy milyen nagy jelentőséggel bír az információkezelés terén jelenleg fennálló hiányosságok orvoslása, illetve **a meglévő információs rendszerek interoperabilitásának és összekapcsoltságának** javítása. A közelmúltbeli események ismét rávilágítottak arra, hogy sürgősen össze kell kapcsolni a meglévő uniós adatbázisokat, nem utolsósorban azért, hogy a helyszínen dolgozó határőrizeti és bűnüldöző szerveket ellássák a személyazonossággal való visszaélés felderítéséhez szükséges eszközökkel. A 2016. decemberi berlini terrortámadás elkövetője például legalább 14 különböző személyazonosságot használt, és képes volt észrevétlenül mozogni a tagállamok között. Ahhoz, hogy lezárjuk ezt a lehetőséget a terroristák és a bűnözők előtt, elengedhetetlen, hogy a meglévő és a jövőbeni információs rendszerek lehetővé tegyék a biometrikus azonosítók alapján végzett, egyidejű lekérdezést.

A Bizottság 2016 áprilisában megindította az erre vonatkozó munkát „A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek” című javaslatával<sup>2</sup>, amely azonosította a meglévő rendszerek működésében és az EU adatgazdálkodási struktúrájában észlelhető hiányosságokat, valamint az abból adódó problémákat, hogy a meglévő rendszereket egyedileg tervezték meg, ahelyett hogy egymáshoz illesztették volna őket, aminek következtében eltérően szabályozott információs rendszerek összetett együttese és általános széttagoltság alakult ki. A Bizottság e folyamat keretében az uniós ügynökségekkel, a tagállamokkal és az érdekelt felekkel együttműködve létrehozta **az információs rendszerekkel és az interoperabilitással foglalkozó magas szintű szakértői csoportot**. Az elnök jelentése 2016. december 21-én ismertette a csoport **időközi megállapításait**<sup>3</sup>, amelyek között kiemelt javaslatként szerepel egy egységes keresőportál létrehozása, amely a bűnüldöző hatóságok és a határigazgatási szervek számára lehetővé tenné a meglévő uniós adatbázisok és információs rendszerek egyidejű lekérdezését. Az időközi jelentés hangsúlyozza továbbá az adatminőség fontosságát – ugyanis az információs rendszerek csupán annyira hatékonyak, amennyire a beléjük táplált adatok minősége és formátuma azt lehetővé teszi –, valamint ajánlásokat fogalmaz meg arra nézve, hogy automatizált adatminőség-ellenőrzés révén javítsák az uniós rendszerekben szereplő adatok minőségét.

A Bizottság gyorsan nyomon fogja követni az egységes keresőportál létrehozására vonatkozó javaslatot, és a nagyméretű IT-rendszerek operatív irányítását végző uniós

---

<sup>2</sup> „A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek” című közlemény, COM(2016) 205 final.

<sup>3</sup> <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1>

ügynökséggel, az eu-LISA-val együtt megkezdte az érintett meglévő uniós rendszerek egyidejű lekérdezését lehetővé tévő portállal kapcsolatos munkát. Célszerű, hogy júniusig elkészüljön egy erre vonatkozó tanulmány, amely alapul szolgál ahhoz, hogy az év vége előtt megtervezzék és teszteljék a portál prototípusát. A Bizottság úgy véli, hogy az Europolnak ezzel egyidejűleg folytatnia kell a munkáját egy olyan rendszerinterfészre vonatkozóan, amely lehetővé teszi a tagállamok határokon tevékenykedő tisztviselőinek, hogy a saját nemzeti rendszereik lekérdezésekor egyidejűleg automatikusan az Europol adatbázisokban is keressenek.

Az információs rendszerek interoperabilitására irányuló munka célja, hogy megszüntesse a határellenőrzés és -biztonság uniós adatgazdálkodási struktúrájának jelenlegi széttagoltságát és az ebből adódó hiányosságokat. Amennyiben az adatbázisok a személyazonossági adatok közös nyilvántartását használnák – amint azt a javasolt uniós határregisztrációs rendszer és a javasolt Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) esetében előirányozták –, egy személy csupán egyetlen személyazonossággal szerepelhetne a különböző adatbázisokban, ami megakadályozná különféle hamis személyazonosságok alkalmazását. A Bizottság első lépésként – a magas szintű szakértői munkacsoport időközi megállapításaiban javasoltaknak megfelelően – felkérte az eu-LISA-t, hogy elemezze a megosztott biometrikus megfeleltetési szolgáltatás megvalósításának technikai és operatív vonatkozásait. E szolgáltatás lehetővé tenné a biometrikus adatokat tartalmazó különböző adatbázisok lekérdezését, amely során napvilágra kerülhetnének a kérdéses személy által egy másik rendszerben használt hamis személyazonosságok. Ezen túlmenően a magas szintű szakértői munkacsoportnak most azt is meg kell vizsgálnia, hogy szükséges, műszakilag megvalósítható és arányos volna-e, ha más rendszerekre is kiterjesztenék a határregisztrációs rendszer és az ETIAS esetében előirányozott **közös személyazonosság-nyilvántartást**. A közös személyazonosság-nyilvántartás a biometrikus megfeleltetési szolgáltatásban tárolt biometrikus adatokon túl alfanumerikus személyazonossági adatokat is tartalmazhatna. A csoportnak 2017. április végéig kell előterjesztenie az erre vonatkozó megállapításait a zárójelentésében.

A közelmúltbeli biztonság események nyomatékossították annak szükségességét, hogy ismét megvizsgálják a tagállamok közötti **kötelező információmegosztás** kérdését. A **Schengeni Információs Rendszer** megerősítésére irányuló, 2016. decemberi bizottsági javaslat első alkalommal írja elő a tagállamok számára azt a kötelezettséget, hogy a terrorista bűncselekményekkel összefüggésben személyekre vonatkozó figyelmeztető jelzéseket kell kiadniuk. Fontos, hogy a társjogalkotók mostantól a javasolt intézkedések gyors elfogadásán dolgoznak. A Bizottság készen áll annak vizsgálatára, hogy más uniós adatbázisok esetében is célszerű volna-e bevezetni a kötelező információmegosztási kötelezettséget.

### III. A PUHA CÉLPONTOK VÉDELME A TERRORTÁMADÁSOKKAL SZEMBEN

Az Unión belüli legutóbbi merénylet, a berlini terrortámadás úgynevezett puha célpontok ellen irányult, amelyek általában olyan civilek által látogatott helyszínek, ahol sok ember gyűlik össze (pl. közterületek, kórházak, iskolák., stadionok, kulturális központok, kávéházak és vendéglők, bevásárlóközpontok és közlekedési csomópontok). E helyszínek jellegüknél fogva sebezhetőek és nehezen védhetőek, jellemző továbbá, hogy az ellenük intézett támadás nagy valószínűséggel tömeges pusztítást idéz elő. A fenti okokból e helyszínek a terroristák kedvelt célpontjai. A puha célpontok, így a közlekedés

elleni jövőbeni támadások veszélye továbbra is magas, amit a rendelkezésre álló elemzések, köztük az Europolnak a Dáís működésének változásáról szóló jelentése is megerősített<sup>4</sup>.

A 2015. évi európai biztonsági stratégia és a biztonsági unióról szóló 2016. évi közlemény kiemelte, hogy fokozni kell a biztonság erősítésére, valamint a puha célpontok védelmében mozgósítható innovatív felderítési eszközök és technológia alkalmazására irányuló munkát. A Bizottság azon dolgozik, hogy támogassa és ösztönözze a bevált gyakorlat tagállamok közötti megosztását a puha célpontok elleni támadások megelőzését és az azokra való reagálást szolgáló megfelelőbb eszközök kifejlesztése terén. E munka műveleti kézikönyvekben és útmutatókban öltött testet. A Bizottság jelenleg – a tagállami szakértőkkel szorosan együttműködve – fejleszti a különböző puha célpontokra (pl. bevásárlóközpontok, kórházak, sport és kulturális események) vonatkozó biztonsági eljárások és minták átfogó kézikönyvét. Az a cél, hogy a Bizottság 2017 elején a bevált tagállami módszerekre épülő, a puha célpontok védelmére vonatkozó iránymutatást adjon a tagállamoknak.

Ezzel egyidejűleg a Bizottság februárban megrendezi a puha célpontok védelmével foglalkozó nemzeti hatóságok első munkaértekezletét annak érdekében, hogy információkat cseréljenek és bevált gyakorlatokat dolgozzanak ki a puha célpontok védelme, a közrend és a közbiztonság összetett kérdésében. A Bizottság emellett a Belső Biztonsági Alap keretében finanszíroz egy, Belgium, Hollandia és Luxemburg részvételével zajló kísérleti projektet a különleges bűnüldözési beavatkozások olyan regionális kiválósági központjának létrehozása érdekében, amely képzést nyújt azoknak a rendőrtiszteknek, akik támadás esetén gyakran elsődleges beavatkozóként járnak el.

A puha célpontok elleni támadásokra való reagálás a Bizottság polgári védelmi tevékenységének alapvető elemét képezi. A Bizottság decemberben közölte, hogy a tagállamokkal karöltve milyen intézkedéseket szándékozik tenni annak érdekében, hogy védelmet nyújtson az uniós polgároknak és csökkentse a terrorista támadások nyomán közvetlenül keletkező sebezhetőségeket. A szóban forgó intézkedések erősíteni fogják az együttműködést a támadások következményeinek kezelésében résztvevő valamennyi szereplő között, a Bizottság pedig ígéretet tett arra, hogy támogatást nyújt a tagállami erőfeszítésekhez annak révén, hogy elősegíti a közös képzéseket és gyakorlatokat, valamint a meglévő fókuszpontok és szakértői csoportok közreműködésével folyamatos párbeszédet biztosít. A Bizottság támogatja továbbá a terrorista támadásokra való reagálást szolgáló speciális modulok kidolgozását az uniós polgári védelmi mechanizmus keretében, valamint a levont tanulságok megosztására és a tudatosság erősítésére irányuló kezdeményezéseket.

A Bizottság a tagállamokkal együtt azt is feltérképezi, hogy milyen uniós támogatás mobilizálásával segíthető az ellenállóképesség javítása és a biztonság megerősítése a potenciális puha célpontok környezetében. A tagállamok az Európai Beruházási Banktól (EBB) is igényelhetnének finanszírozást (beleértve az Európai Stratégiai Beruházási Alapot), összhangban az EU és az EBB csoport szakpolitikáival. A projekteket a jogszabályban meghatározott rendes döntéshozatali eljárás szerint bírálják el.

---

<sup>4</sup> Europol, *Changes in modus operandi of Islamic State (IS) revisited*, (Az Iszlám Állam működésében bekövetkezett változások ismételt vizsgálata), 2016. november, Europol Tájékoztató, elérhető a következő internetcímen: <https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited>

A Bizottság 2016. novemberében célzott munkaértekezletet szervezett a tömegközlekedési területek, például a repülőterek vagy pályaudvarok nyilvános részével kapcsolatos speciális puha célpontok tárgyában. Az eseményen az érdekelt felek széles köre hangsúlyozta, hogy egyensúlyt kell teremteni a biztonsági igények, az utasok kényelme és a közlekedés működése között. A következtetések kiemelték a nem csupán a személyzetre, hanem az utasokra is kiterjedő biztonsági kultúra kialakításának jelentőségét, a megfelelő ellenintézkedések meghatározásának alapjául szolgáló helyi kockázatértékelés fontosságát, valamint az összes résztvevő fél közötti fokozott párbeszéd szükségességét.

#### **IV. A KIBERFENYEGETÉSEK OKOZTA KIHÍVÁSSAL VALÓ SZEMBENÉZÉS**

A kiberbűnözés és a kibertámadások az Unió előtt álló alapvető kihívások, amelyek esetében az uniós szintű fellépés elősegítheti kollektív ellenállóképességünk erősítését. A kiberbiztonsági incidensek nap mint nap nagyon káros hatással vannak az emberek életére, és komoly gazdasági kárt okoznak az európai gazdaságnak és vállalkozásoknak. A kibertámadások a hibrid fenyegetések fontos elemei, amelyek időzítését pontosan összehangolják a fizikai fenyegetésekkel, például a terrorizmussal, és így pusztító hatást képesek kifejteni. Továbbá hozzájárulhatnak egy ország destabilizálásához vagy politikai intézményeinek és alapvető demokratikus folyamatainak ellehetetlenítéséhez. Mivel egyre nagyobb mértékben alkalmazunk online technológiákat, kritikus infrastruktúránk (a kórházaktól az atomerőművekig) egyre sebezhetőbbé válnak.

Az EU 2013-as kiberbiztonsági stratégiája a kiberbiztonsági kihívásokra vonatkozó alapvető szakpolitikai reagálás részét képezi. A központi intézkedés a tavaly júliusban elfogadott hálózat- és információbiztonsági irányelv<sup>5</sup>, amely megteremti a fokozott uniós szintű együttműködés és a kibertámadásokkal szembeni ellenállóképesség alapját annak révén, hogy támogatja a tagállamok közötti együttműködést és információcserét, valamint elősegíti a konkrét kiberbiztonsági incidensekkel kapcsolatos operatív együttműködést és a kockázatokkal kapcsolatos információk megosztását. A különböző ágazatokra kiterjedő és határokon átívelő következetes végrehajtás érdekében a Bizottság a tagállamok bevonásával februárban megtartja a hálózat- és információbiztonsággal foglalkozó együttműködési csoport első ülését.

A Bizottság és az EU főképviselője 2016 áprilisában elfogadták a hibrid fenyegetésekkel szembeni fellépés közös keretét<sup>6</sup>, amelyben 22 operatív fellépésre tettek javaslatot a tudatosság erősítése, az ellenállóképesség kiépítése, a válságreagálása javítása, valamint az EU és a NATO közötti együttműködés fokozása céljából. A Tanács felszólításának megfelelően a Bizottság és az EU főképviselője 2017. júliusig jelentést tesznek, hogy értékeljék az előrehaladást.

A Bizottság elősegíti és támogatja továbbá a technológiai innovációt, többek között azáltal, hogy felhasználja az uniós kutatási alapokat az új megoldások ösztönzésére és

---

<sup>5</sup> Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

<sup>6</sup> JOIN (2018)18.

olyan új technológiák létrehozására, amelyek elősegíthetik a kibertámadásokkal szembeni ellenállóképesség erősítését (pl. „beépített biztonsági” projektek). Tavaly nyáron a Bizottság 1,8 milliárd EUR összegű kiberbiztonsági köz-magán társulást indított az iparág részvételével<sup>7</sup>.

A közlekedés terén a digitalizálás fontos elősegítő tényezőjévé vált a napjaink közlekedési rendszere tekintetében olyannyira szükséges átalakításnak. A gyors ütemű digitalizálás sok előnnyel jár, ugyanakkor azonban sebezhetőbbé teszi a közlekedést a kiberbiztonsági kockázatok tekintetében. Számos intézkedés történt a fenyegetés különböző szinteken történő mérséklése érdekében, különösen a légi közlekedés terén, azonban a tengeri, folyami, vasúti és közúti közlekedés esetében is<sup>8</sup>. Most az jelenti a legfőbb kihívást, hogy tovább pontosítsák, harmonizálják és kiegészítsék a kibertámadásokkal szembeni ellenállóképesség eltérő vonatkozásainak erősítésében résztvevő különféle érdekelt tevékenységét.

Általánosabb szempontból és tekintettel a fenyegetés gyorsan változó jellegére, a Bizottság és az EU főképviselője a 2013-as uniós kiberbiztonsági stratégiát alapul véve az elkövetkező hónapok folyamán azonosítja a szóban forgó fenyegetésekkel kapcsolatos hatékony uniós szintű reagáláshoz szükséges intézkedéseket.

## V. A SZEMÉLYES ADATOK VÉDELME A HATÉKONY NYOMOZÁSOK ELŐSEGÍTÉSE MELLETT

A rendőrségi és büntető igazságszolgáltatási területre vonatkozó adatvédelmi irányelv<sup>9</sup> a terrorizmus és a súlyos bűnözés elleni küzdelem egyik építőeleme. A tagállami bűnüldöző hatóságok az irányelvben lefektetett közös adatvédelmi normák alapján zavartalanul kicserélhetik a vonatkozó adatokat, miközben a bűncselekmények áldozatainak, tanúinak és gyanúsítottainak adatai megfelelő védelmet élveznek.

Ezenfelül a Bizottság január 11-én elfogadta a (2002/58/EK irányelvet felváltó) **elektronikus hírközlési adatvédelmi rendelet** tervezetét<sup>10</sup> annak érdekében, hogy a 2015. áprilisi európai digitális egységes piaci stratégiában meghatározottaknak

<sup>7</sup> A kibertámadásokkal szembeni ellenálló képességről szóló 2016. évi közleményben – COM(2016) 410 final – tett bejelentés.

<sup>8</sup> Példaként szolgálnak a nemzetközi iránymutatások, például a Nemzetközi Tengerészeti Szervezet által kidolgozott vagy az EU és az USA együttes kezdeményezésére a Nemzetközi Polgári Repülési Szervezet egy közelmúltban elfogadott állásfoglalása keretében létrehozott dokumentum; az incidensek bejelentése, amelyek segítségével az Európai Repülésbiztonsági Ügynökség reaktívabb működési módot alakít ki, valamint a kidolgozás alatt lévő új rendszerekben, például a SESAR közös vállalkozás európai légiforgalmi szolgáltatási főtervében alkalmazandó beépített kiberbiztonság.

<sup>9</sup> Az Európai Parlament és a Tanács(EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről. Az irányelv 2016. május 5. óta van hatályban, és a tagállamoknak 2018. május 6-ig kell átültetniük. A Bizottság a tagállamok közreműködésével szakértői csoportot hozott létre a rendőrségi irányelv átültetésével kapcsolatos álláspontok kicserélésére.

<sup>10</sup> Az adatvédelemről és az elektronikus kommunikációkról szóló rendelet, COM(2017) 10.

megfelelően gondoskodjon az egyének és a vállalatok kommunikációjának magas szintű titkosságáról, valamint az összes piaci szereplőre érvényes egyenlő versenyfeltételekről. A felülvizsgált elektronikus hírközlési adatvédelmi rendelet a jelenlegi irányelvhez hasonlóan különös szabályokat állapít meg az általános adatvédelmi rendelethez<sup>11</sup> képest, valamint meghatározza a magánélet és a személyes adatok védelmére vonatkozó keretet az elektronikus hírközlési ágazatban.

E felülvizsgálat révén az összes elektronikus hírközlési adat bizalmasnak/tiszteletben tartandónak tekinthető, még akkor is, ha a kommunikáció kiegészítő jellegű – akár hagyományos távközlési szolgáltatások, akár olyan, azokkal funkcionálisan egyenértékű hálózatszemleges online (OTT) szolgáltatások (pl. Skype és WhatsApp) keretében zajlik, amelyeket sok felhasználó a szokásos távközlési szolgáltatók alternatívájaként használ<sup>12</sup>. A szolgáltatókat terhelő kötelezettségek köre – az ügyfelek adatvédelmi döntéseinek az adatok felhasználása, tárolása és felhasználása során történő tiszteletben tartása mellett – magában foglalja az EU-n kívül letelepedett szolgáltatók azon kötelezettségét, hogy képviselőt nevezzenek ki valamely tagállamban. Ez arra is lehetőséget nyújt a tagállamoknak, hogy elősegítsék a bűnüldözést, valamint az igazságügyi hatóságoknak az elektronikus bizonyítékokhoz való hozzáférés érdekében a szolgáltatókkal folytatott együttműködését (lásd alább).

A jelenlegi elektronikus adatvédelmi szabályokhoz hasonlóan az elektronikus hírközlési adatvédelmi rendeletjavaslat<sup>13</sup> 11. cikkében előírt kivétel lesz irányadó a bűnüldözési és igazságügyi hatóságoknak a nyomozáshoz szükséges, fontos elektronikus információkhoz való hozzáférésre nézve. E rendelkezés lehetővé teszi, hogy az uniós vagy a nemzeti jogban korlátozzák a kommunikáció titkosságát, amennyiben ez szükséges és arányos a nemzetbiztonság, a védelem, a közbiztonság megóvása, valamint a bűncselekmények megelőzése, nyomozása, kivizsgálása, illetve büntetőeljárás alá vonása, vagy a büntetőjogi szankciók végrehajtása érdekében. Ez a rendelkezés kiváltképpen lényeges az **adatmegőrzésre** vonatkozó nemzeti szabályok tekintetében (azaz amikor arra kötelezik a távközlési szolgáltatókat, hogy egy konkrét időszakra őrizzék meg a kommunikációt esetleges bűnüldözési hozzáférés céljából) azt követően, hogy az Európai Unió Bírósága (EUB) 2014-ben megsemmisítette az adatmegőrzési irányelvet<sup>14</sup>. Azóta nem létezik adatmegőrzésre vonatkozó uniós jogi eszköz, és egyes tagállamok saját nemzeti adatmegőrzési törvényt fogadtak el. A svéd és a brit adatmegőrzési törvényt megtámadták az EUB előtt, amely a *Tele2* ügyben december 21-én hozta meg ítéletét<sup>15</sup>. Az EUB megállapította, hogy összeegyeztethetetlen az uniós

---

<sup>11</sup> Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet), amely 2018. május 25-től válik alkalmazandóvá.

<sup>12</sup> Ez következik a Bizottság által 2016. szeptember 14-én előterjesztett, az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló irányelvben (a távközlési csomag) elfogadott megközelítésből, COM(2016) 590 final.

<sup>13</sup> Lás a 11. cikk (1) bekezdését, az „adatmegőrzési rendelkezést”, amely nem változott az elektronikus hírközlési adatvédelmi irányelv 15. cikkéhez képest, és összhangban áll az általános adatvédelmi rendelet követelményeivel. Az ilyen korlátozásnak tiszteletben kell tartania az alapvető jogok lényegi tartalmát, valamint szükségesnek, megfelelőnek és arányosnak kell lennie.

<sup>14</sup> Az EUB C-293/12. és C-594/12. sz., *Digital Rights Ireland* egyesített ügyekben hozott 2014. április 8-i ítélete.

<sup>15</sup> Az EUB C-203/15. és C-698/15. sz., *Tele2* ügyben hozott 2016. december 21-i ítélete.



joggal az a nemzeti jogszabály, amely a bűnözés elleni küzdelem érdekében előírja az előfizetők és a felhasználók valamennyi forgalmi és a helymeghatározó adatának általános és válogatás nélküli megőrzését az összes hírközlési eszköz esetében. Az ítélet hatásainak elemzése folyamatban van, és a Bizottság iránymutatást fog kidolgozni arra nézve, hogy a nemzeti adatmegőrzési törvényeket miképp lehet az ítéletnek megfelelően kialakítani.

A bűncselekmények digitális nyomokat hagynak, amelyek bizonyítékként szolgálhatnak a bírósági eljárás folyamán; a gyanúsítottak közötti elektronikus kommunikáció gyakran az egyetlen bizonyíték, amit a bűnüldöző hatóságok és az ügyészek be tudnak szerezni. Az **elektronikus bizonyítékokhoz** való hozzáférés megszerzése azonban – különösen ha külföldön vagy felhőben tárolják azokat – műszaki és jogi szempontból egyaránt bonyolult, és gyakran eljárásjogilag is terhes folyamat, ami hátráltatja a nyomozók gyors előrehaladás iránti igényét. E nehézségek kezelése érdekében a Bizottság jelenleg olyan megoldásokat mérlegel, amelyek lehetővé teszik, hogy a nyomozók hozzájussanak a határon túli elektronikus bizonyítékokhoz, ideértve a kölcsönös jogsegély hatékonyságának fokozását és az internetszolgáltatókkal való közvetlen együttműködés lehetőségeinek feltárását, valamint hogy javaslatot tegyen a kibertérben lévő joghatóság meghatározására és érvényesítésére, maradéktalan összhangban az alkalmazandó adatvédelmi szabályokkal.<sup>16</sup> A Bizottság 2016. december 9-én jelentést tett a Bel- és Igazságügyi Tanácsnak az elért előrehaladásról<sup>17</sup>.

Egy átfogó (és még jelenleg is folyamatban lévő) szakértői konzultációs eljárás lehetővé tette a Bizottság számára, hogy meghatározza az elektronikus bizonyítékokhoz való hozzáférés által felvetett különféle, gyakran összetett problémákat, és jobban megértse a tagállamok jelenlegi szabályait és gyakorlatait, valamint azonosítsa a lehetséges szakpolitikai alternatívákat. Az eredményjelentés áttekintést ad azokról az elképzelésekről, amelyek az információgyűjtés és a szakértői folyamat során addig felmerültek, valamint azokról, amelyeket a Bizottság – az érdekeltekkel konzultálva – az elkövetkező hónapok során fog tovább vizsgálni. A Bizottság 2017-ben egy kezdeményezést fog előterjeszteni a munkaprogramjában bejelentetteknek megfelelően.

## VI. KÖVETKEZTETÉS

A március 1-jén esedékes következő jelentés lehetőséget ad a végrehajtás előrehaladásának felülvizsgálatára az említett és egyéb fontos munkaterületeken.

---

<sup>16</sup> Amint arra kötelezettséget vállalt az európai biztonsági stratégiában, COM(2015) 185 final, és „Az európai biztonsági stratégia megvalósítása a terrorizmus elleni küzdelem és a hatékony és valódi biztonsági unió előkészítésének érdekében” című bizottsági közleményben, COM(2016) 230 final.

<sup>17</sup> A büntető igazságszolgáltatás kibertérben való érvényesítésének javításáról szóló 2016. június 9-i következtetéseiben a Tanács felszólította a Bizottságot, hogy hozzon konkrét intézkedéseket, dolgozzon ki közös uniós megközelítést, és 2017. júniusig mutassa be az eredményeket.