EURÓPAI
BIZOTTSÁG

Brüsszel, 2019.10.30.
COM(2019) 552 final

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

A hatékony és valódi biztonsági unió megvalósításáról szóló huszadik eredményjelentés

I. BEVEZETÉS

A hatékony és valódi biztonsági unió megvalósításáról szóló huszadik eredményjelentés két fő pillér mentén vizsgálja az eddigi fejleményeket: a terrorizmus és a szervezett bűnözés elleni küzdelem, illetve az azokat támogató eszközök felszámolása; valamint e fenyegetésekkel szembeni védelmünk megerősítése és ellenálló képességünk kiépítése.

A Jean-Claude Juncker vezette Bizottság az első hivatali napjától kezdve kiemelt prioritásként kezelte a biztonságot. A 2015. áprilisi európai biztonsági stratéga[1] és a hatékony és valódi biztonsági unió előkészítéséről szóló 2016. áprilisi közlemény alapján[2], az EU összehangolt megközelítést alkalmazva reagált a sorozatos terrortámadásokra és egyéb növekvő biztonsági fenyegetésekre, és így komoly előrelépést tett kollektív biztonságunk megerősítése felé[3]. Egyre nyilvánvalóbbá vált, hogy a jelenlegi biztonsági kihívások – legyen szó terrorizmusról, szervezett bűnözésről, számítógépes támadásokról, dezinformációról vagy más számítógépes fenyegetésekről – közös veszélyt jelentenek. Csakis egymással együttműködve érhetünk el olyan mértékű kollektív biztonságot, amilyent a polgárok jogosan igényelnek és elvárnak. Ez a közös értelmezés képezte a hatékony és valódi biztonsági unió felé tett előrelépés alapját. A polgárok biztonságának megőrzésén dolgozó nemzeti hatóságok igényei alapján az uniós szintű támogatást olyan jogalkotási és operatív intézkedésekre összpontosítottuk, amelyek esetében az együttes fellépés hatással lehet a tagállamok biztonságára. Munkánkat az Európai Parlamenttel és a Tanáccsal szorosan együttműködve, a szélesebb nyilvánosság számára teljes mértékben átláthatóan végeztük. Ez a munka az alapvető jogok maradéktalan tiszteletben tartására épült, hiszen az Unió biztonsága kizárólag akkor garantálható, ha a polgárok biztosak lehetnek alapvető jogaik teljes körű tiszteletben tartása felől.

Az EU úgy **küzd a terrorizmus ellen**, hogy a robbanóanyagokhoz, tűzfegyverekhez és finanszírozási eszközökhöz való hozzáférést megnehezítő és a mozgásukat korlátozó új szabályokkal megszünteti a terroristák mozgásterét. Az EU fokozta az **információcserét** annak érdekében, hogy a meglévő információkat maximálisan kihasználva, valamint az információs hézagokat és a fehér foltokat megszüntetve pontos és teljes körű adatokhoz biztosítson hatékony hozzáférést a mindennapi végrehajtásban dolgozók, a rendőrök és a határőrök számára. A külső határok szilárd védelme a belső határellenőrzés nélküli szabad mozgást biztosító térség biztonságának egyik előfeltétele. 2019 márciusában az Európai Parlament és a Tanács megállapodásra jutott a tovább erősített és teljes mértékben felszerelt **Európai Határ- és Parti Őrségről**, és az új rendelet várhatóan 2019 december elején lép hatályba. Az EU platformot és finanszírozást biztosított a helyi közösségekben dolgozók számára a **radikalizálódás elleni küzdelemmel és az erőszakos szélsőségesség megelőzésével** kapcsolatos bevált gyakorlatok cseréjéhez, valamint új szabályokat javasol az online terrorista tartalmak hatékony eltávolítására. Az uniós támogatás hozzájárult ahhoz, hogy a nyilvános terek védelmének javítására, valamint a vegyi, biológiai, radiológiai és nukleáris biztonsági kockázatokkal szembeni felkészültség fokozására szolgáló cselekvési tervek segítségével **növeljék a városok támadásokkal szembeni ellenálló képességét**. Az EU úgy kezelte a **kiberbiztonsági és számítógépes fenyegetéseket**, hogy uniós kiberbiztonsági stratégiát hozott létre, ezzel kapcsolatos jogszabályokat fogadott el, továbbá választásaink hatékonyabb védelme érdekében szembeszállt a **dezinformációval**. Folytatódik

---

1 COM(2015) 185 final (2015.4.28.).
2 COM(2016) 230 final (2016.4.20.).
3 A hatékony és valódi biztonsági unió megvalósításáról szóló korábbi eredményjelentések tekintetében lásd: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

a **kritikus digitális infrastruktúránk biztonságának** erősítésére irányuló munka, beleértve az **5G hálózatok kiberbiztonságával** kapcsolatos, egész Európára kiterjedő, megerősített együttműködést.

Továbbra is akad bőven tennivaló. A németországi Hallében 2019. október 9-én egy zsinagóga ellen elkövetett támadás – amely során az elkövető két polgárt meggyilkolt, élőben közvetítve tette az interneten – sokkoló figyelmeztetés a jobboldali erőszakos szélsőségesség és az antiszemitizmus veszélyére. A támadás ismét ráirányította a figyelmet az internet terrorista propaganda céljára történő felhasználására, tehát arra, hogy **az online terrorista tartalmak törléséhez uniós szintű szabályokra van szükség**. A Bel- és Igazságügyi Tanács 2019. október 7–8-i ülésén megvitatta a jobboldali erőszakos szélsőségesség és terrorizmus kérdését, hangsúlyozva a további munka szükségességét, ideértve a jogellenes, jobboldali szélsőséges tartalmak online és offline terjedésének megakadályozását. Ugyanakkor a párizsi rendőrfőkapitányságon történt 2019. október 3-i merénylet, amely során három rendőrtiszt és egy polgári alkalmazott vesztette életét, azt mutatja, hogy a dzsihádista indíttatású terrorizmus továbbra is valós veszélyt jelent, és folytatni kell azokat a jelenleg is zajló erőfeszítéseket, amelyek a tagállamok e veszéllyel szembeni fellépésének támogatására irányulnak. Komoly hatást gyakorolhat Európa biztonságára, ha a nemrégiben bekövetkezett észak-szíriai események az ISIS/Dáis bebörtönzött tagjainak szökéséhez vezetnek. Fontos, hogy a tagállamok teljes mértékben kihasználják a meglévő információs rendszereket, hogy felderítsék és azonosítsák a külföldi terrorista harcosokat, amikor azok átlépik a külső határokat. Folyamatban van az arra irányuló munka is, hogy harctéri információkat használjanak a külföldi terrorista harcosok vád alá helyezéséhez.

Ez a jelentés bemutatja a hatékony és valódi biztonsági unió megvalósítására irányuló munka során a közelmúltban elért eredményeket, kiemelve azokat a területeket, ahol további lépésekre van szükség. Naprakész információkkal szolgál **az 5G hálózatok kiberbiztonsága** – különösen a 2019. október 9-én közzétett **uniós kockázatértékelési jelentés** – és **a dezinformáció elleni küzdelem** tekintetében elfogadott intézkedések végrehajtásáról.

Ez a jelentés elsősorban a biztonsági unió területén folytatott együttműködés **külső dimenziójára összpontosít**, ahol kétoldalú **terrorizmus elleni megállapodások** születtek Albániával és az Észak-macedón Köztársasággal, valamint előrehaladás történt az **utas-nyilvántartási adatok** cseréje tekintetében harmadik partnerországokkal folytatott együttműködés terén. Továbbá a Bizottság e jelentéssel együtt felhatalmazást kért az EU és **Új-Zéland** közötti, a személyes adatoknak a súlyos bűnözés és a terrorizmus elleni küzdelem céljából történő cseréjéről szóló megállapodásra irányuló tárgyalások megkezdésére.

II. A JOGALKOTÁSI PRIORITÁSOK TERÉN TETT ELŐRELÉPÉSEK

1. A radikalizálódás megelőzése az interneten és a közösségekben

A **radikalizálódás megelőzése** a terrorizmus jelentette fenyegetésre adott uniós válasz sarokköve. Ezzel függ össze, hogy a 21. századi terrorista tevékenységnek az internet lett az elsődleges színtere. A világszerte gyorsan növekvő dzsihádista és jobboldali erőszakos szélsőséges hálózatok fejlődését azok a felületek segítették elő, amelyeken a radikalizálódott egyének képesek kommunikálni és tartalmakat megosztani egymással. Ez az oka annak, hogy a Bizottság továbbra is kettős megközelítést alkalmaz az online radikalizálódással szemben, amelynek keretében a jogellenes online terrorista tartalmak eltávolítására irányuló, javasolt szabályok várhatóan megerősítik az online platformokkal kötött önkéntes partnerséget.

Ehhez elengedhetetlen **az online terrorista tartalmak terjesztésének megakadályozására irányuló jogalkotási javaslat**, amely olyan világos szabályokat és biztosítékokat tartalmaz, melyek kötelezővé tennék az internetes platformok számára, hogy az illetékes hatóságok indokolással ellátott kérésének kézhezvételét követően egy órán belül eltávolítsák a terrorista tartalmat, és a terrorista tartalomnak való kitettség szintjével arányos, proaktív intézkedéseket hozzanak[4]. Az Európai Parlament és a Tanács között folyamatban vannak az intézményközi tárgyalások, és 2019. október 17-én megtartották az első háromoldalú egyeztetést. Tekintettel az online terrorista tartalmak jelentette fenyegetésre, a Bizottság felkéri a társjogalkotókat, hogy 2019 végéig jussanak megállapodásra a javasolt jogszabályról.

A javasolt jogszabály kiegészíti az **uniós internetfórum** keretében az internetes ágazattal kialakított önkéntes partnerséget. A fórum 2015-ös létrehozása óta arra ösztönözte az internetes vállalkozásokat, hogy cselekvően lépjenek fel az online terrorista tartalmak azonosítása és eltávolítása érdekében, előkészítve ezáltal az ágazat által indított, „közös hasítófüggvény-adatbázisra”[5] vonatkozó kezdeményezést, és a terrorizmus elleni globális internetes fórum létrehozását. Az EU bűnüldözési ügynökségének (Europol) részét képező, a szélsőséges internetes tartalmakkal foglalkozó uniós egység jelentős szerepet játszott az internetes vállalkozásokkal való együttműködés megerősítésében, és hozzájárult az uniós internetfórum általános célkitűzéseihez. Az uniós internetfórum legutóbbi, 2019. október 7-i miniszteri ülésén az uniós tagállamok és az internetes vállalatok magas rangú képviselői elkötelezték magukat az úgynevezett **uniós válsághelyzeti protokoll** alapján történő együttműködés mellett. Az uniós válsághelyzeti protokoll meghatározza a megerősített együttműködés küszöbértékeit, és új módszereket alakít ki a válságreagálás megerősítése érdekében. Ez részét képezi a „Christchurchi cselekvési felhívás”[6] végrehajtására törekvő nemzetközi erőfeszítésnek, amelynek célja, hogy összehangolt és gyors reakciót biztosítva megfékezze a terrorista vagy erőszakos szélsőséges online tartalmak villámgyors terjedését

Az online radikalizálódással szembeni, említett intézkedéseken túl a Bizottság továbbra is támogatja **a radikalizálódás megelőzése és leküzdése érdekében** nemzeti és helyi szinten tett **gyakorlati jellegű** erőfeszítéseket. A radikalizálódással foglalkozó uniós információs hálózat keretében gyűjtött bőséges tapasztalatokra és szakismeretre építve az EU célzott támogatást nyújt a helyi szereplők – köztük a városok[7] – számára, valamint lehetőséget biztosít a szakemberek, kutatók és a politikai döntéshozók közötti eszmecserére. A hálózat például külön iránymutatást adott ki és munkaértekezleteket szervezett, hogy támogatást nyújtson a konfliktusövezetekből érkező gyermekekkel foglalkozó illetékes hatóságoknak[8]. A radikalizálódással foglalkozó uniós információs hálózat keretében végzett tevékenységek folytonosságának biztosítása érdekében a Bizottság elindította a 2020-tól kezdődő négyéves

---

4 COM(2018) 640 final (2018.9.12.).

5 Egy vállalkozásokból álló konzorcium által létrehozott olyan eszköz, amelynek célja az együttműködés megkönnyítése a terrorista tartalmak platformok közötti terjedésének megakadályozása érdekében.

6 A 2019. március 15-i christchurchi (Új-Zéland) támadásra válaszként Emmanuel Macron, francia elnök és Jacinda Ardern, Új-Zéland miniszterelnöke 2019. május 15-ére Párizsba hívták a világ vezetőit és az online platformokat, hogy útjára indítsák a „Christchurchi cselekvési felhívást”. Juncker elnök támogatta a felhívást, és bejelentette az uniós válsághelyzeti protokoll kidolgozását.

7 A városokkal folytatott biztonsági együttműködés tekintetében lásd még a felkészültségről és a védelemről, és különösen a nyilvános terek védelméről szóló V.2. szakaszt.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

időszakra vonatkozó, 61 millió EUR becsült összegű új keretszerződés megkötésére irányuló eljárást[9].

Az online terrorista tartalom jelentette fenyegetéssel szembeni fellépés érdekében a Bizottság a következőkre kéri fel az Európai Parlamentet és a Tanácsot:

- az év vége előtt zárják le tárgyalásokat az **online terrorista tartalom** terjesztésének megakadályozására irányuló jogalkotási javaslatról.

2. A biztonság, a határigazgatás és a migrációkezelés területén használt szilárdabb és intelligensebb információs rendszerek

Az EU fokozta az információcserét, ezáltal megkönnyítette a személyazonossággal való visszaélés leleplezését[10], megerősítette a határforgalom-ellenőrzést[11], korszerűsítette az egész Európára kiterjedő bűnüldözési adatbázisokat[12], megszüntette az információs hézagokat[13] és megerősítette az EU bűnüldözési ügynökségét, az Europolt[14]. Ebben központi szerepet játszik az **uniós információs rendszerek interoperabilitása**[15], ami a meglévő információk maximális kihasználását és a fehér foltok megszüntetését jelenti. A mindennapi végrehajtásban dolgozók igényeihez igazodó interoperabilitás eredményeként a bűnüldöző

9 A keretszerződés két részre oszlik: 29 000 000 EUR a radikalizálódással foglalkozó uniós információs hálózat tevékenységének a következő négy évben történő támogatását szolgálja, 32 000 000 EUR-t pedig a tagállamok, a nemzeti, regionális és helyi hatóságok és kiemelt harmadik országok hatékony radikalizálódás-kezelési kapacitásának erősítésére fordítanak, különösen hálózatépítési lehetőségek, célzott és igényvezérelt szolgáltatások biztosítása, valamint kutatás és elemzés formájában.

10 (EU) 2019/1157 rendelet (2019. június 20.) az uniós polgárok személyazonosító igazolványai és a szabad mozgás jogával élő uniós polgárok és azok családtagjai részére kiállított tartózkodási okmányok biztonságának megerősítéséről.

11 Minden polgárra kiterjedő szisztematikus ellenőrzések bevezetése a külső határokon a Schengeni Információs Rendszer használatával. Valamennyi schengeni állam, továbbá Románia, Bulgária, Horvátország és Ciprus is alkalmazza a releváns adatbázisok külső határokon történő rendszeres ellenőrzésére vonatkozó, 2017 áprilisában bevezetett szabályokat. E szabályok értelmében a szárazföldi vagy tengeri határokon átmeneti eltérések lehetségesek, de csak az uniós polgárok tekintetében, szem előtt tartva a forgalom áramlására gyakorolt aránytalan hatást. Mostanáig hat tagállam/schengeni társult ország (Horvátország, Finnország, Magyarország, Lettország, Norvégia és Szlovénia) jelentett be ilyen eltéréseket. A légi határok tekintetében 2019 áprilisában megszűnt a rendszeres ellenőrzésekre vonatkozó szabályoktól való eltérés lehetősége.

12 A megerősített Schengeni Információs Rendszer (az (EU) 2018/1860 rendelet (2018. november 28.), az (EU) 2018/1861 rendelet (2018. november 28.), az (EU) 2018/1862 rendelet (2018. november 28.)) és a harmadik országbeli állampolgárokra kiterjesztett Európai Bűnügyi Nyilvántartási Információs Rendszer (az (EU) 2019/816 rendelet (2019. április 17.)). A Schengeni Információs Rendszer megerősítése kiterjed arra az általános kötelezettségre, hogy a terrorizmussal kapcsolatos figyelmeztető jelzéseket be kell vinni a rendszerbe.

13 Az uniós határregisztrációs rendszer (az (EU) 2017/2226 rendelet (2017. november 30.)) és az Európai Utasinformációs és Engedélyezési Rendszer (az (EU) 2018/1240 rendelet (2018. szeptember 12.) és az (EU) 2018/1241 rendelet (2018. szeptember 12.)).

14 Az elmúlt években az Europol szerepe hatáskör és mélység tekintetében egyaránt jelentősen megerősödött. Az Europol-rendelet (az (EU) 2016/794 rendelet (2016. május 11.). 2016-os elfogadásával megerősítették az Ügynökséget. A tagállamok jelentősen növelték az Europollal és az Europolon keresztül megosztott információk mennyiségét. A Terrorizmus Elleni Küzdelem Európai Központjának létrehozása megerősítette az Europol elemzési képességeit a terrorizmussal kapcsolatos ügyekben. Az elmúlt években folyamatosan nőtt az Europol költségvetése, amely a 2014. évi 82 millió EUR-ról 2019-re 138 EUR-ra emelkedett. A 2020. évi költségvetésről folyamatban vannak a tárgyalások.

15 Az (EU) 2019/817 rendelet (2019. május 20.) és az (EU) 2019/818 rendelet (2019. május 20.).

szervek tagjai, a határőrök és a migrációs tisztviselők gyorsabb és rendszeresebb hozzáféréssel rendelkeznek majd az információkhoz, így az interoperabilitás elősegíti a belső biztonság és a határigazgatás javítását.

Az interoperabilitás és az azzal járó összes innováció azonban csak akkor fog a gyakorlatban is érzékelhető eredményt hozni a biztonság, a határigazgatás és a migrációkezelés terén, ha mindegyik tagállam maradéktalanul végrehajtja a vonatkozó jogszabályokat. Ez az oka annak, hogy az interoperabilitás **megvalósítása** politikai és technikai szinten egyaránt kiemelt prioritást képez a biztonsági unión belül. A Bizottság és a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökség (eu-LISA) – a tagállami koordinátorok hálózata segítségével, valamint a hatékony nyomonkövetési és koordinációs intézkedéseket lehetővé tévő teljesítménymérleg kidolgozása révén – szakértelemmel és a bevált gyakorlatok cseréjével támogatja a tagállamokat. Ahhoz, hogy 2020-ig megvalósuljon a biztonsági, határigazgatási és migrációkezelési uniós információs rendszerek közötti teljes körű interoperabilitás elérésének ambiciózus célkitűzése, kiemelten fontos az uniós ügynökségekkel, valamennyi tagállammal és a schengeni társult országokkal való szoros együttműködés.

Eddig az Európai Parlament és a Tanács még nem **fejezte be** az ezzel kapcsolatos **jogalkotási munkát**. Az összes függőben lévő jogalkotási javaslatra vonatkozó gyors megállapodás elengedhetetlen ahhoz, hogy teljes körűen és megfelelő időben megvalósítsák az interoperabilitást. Először is, az **Európai Utasinformációs és Engedélyezési Rendszer** technikai megvalósításának részeként a rendszer teljes körű kialakításához technikai módosításokat kell végrehajtani a vonatkozó rendeletekben[16]. A Bizottság felkéri az Európai Parlamentet, hogy gyorsítsa fel az említett technikai módosításokkal kapcsolatos munkáját annak érdekében, hogy mielőbb el lehessen kezdeni az intézményközi tárgyalásokat. Másrészt még mindig folynak intézményközi tárgyalások a meglévő **Vízuminformációs Rendszer** megerősítésére és korszerűsítésére irányuló 2018. májusi javaslatról[17]. A 2019. október 22-én lezajlott első háromoldalú egyeztetésre alapozva a Bizottság felkéri a két társjogalkotót, hogy mielőbb zárják le a tárgyalásokat. Harmadrészt, még mindig nem jött létre megállapodás arról a 2016. májusi bizottsági javaslatról, amely oly módon kívánja kibővíteni az **Eurodac**[18] hatályát, hogy ne csak a menedékkérők és az Unió külső határainak illegális átlépése során elfogott személyek ujjnyomatait és releváns adatait tárolja, hanem a jogellenesen tartózkodó harmadik országbeli állampolgárokét is. A javasolt módosítások emellett kiterjesztenék az EU területére szabálytalanul belépő személyek ujjnyomatainak és releváns adatainak a tárolási időtartamát. A Bizottság mindkét társjogalkotót felhívja arra, hogy jussanak gyors ütemben megállapodásra a javaslatokról.

A biztonsági, határigazgatási és migrációkezelési uniós információs rendszerek megerősítése érdekében a Bizottság a következőkre kéri fel az Európai Parlamentet és a Tanácsot:

- gyorsítsák fel a munkát annak érdekében, hogy mielőbb megállapodásra jussanak az **Európai Utasinformációs és Engedélyezési Rendszer** létrehozásához szükséges, javasolt technikai módosításokról.
- mielőbb folytassák le és zárják le a meglévő **Vízuminformációs Rendszer** megerősítését

[16] (EU) 2018/1240 rendelet (2018. szeptember 12.) és (EU) 2018/1241 rendelet (2018. szeptember 12.).
[17] COM(2018) 302 final (2018.5.16.).
[18] COM(2016) 272 final (2016.5.4.).

célzó javaslatról szóló tárgyalásokat.
- fogadják el az **Eurodacról** szóló jogalkotási javaslatot *(az együttes nyilatkozatban meghatározott prioritás).*

3. A terroristák mozgásterének megszüntetése

Az EU határozott lépéseket tett a terroristák mozgásterének megszüntetése érdekében azon új szabályok elfogadásával, amelyek megnehezítik a terroristák és más bűnözők számára a robbanóanyagokhoz[19], tűzfegyverekhez és finanszírozási eszközökhöz való hozzáférést[20], valamint korlátozzák azok mozgását[21].

A terrorizmusra adott igazságügyi válasz megerősítése érdekében az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (Eurojust) 2019. szeptember 1-jén létrehozta a **terrorizmus elleni küzdelem európai igazságügyi nyilvántartását**. A nyilvántartás igazságügyi információkat gyűjt majd annak érdekében, hogy kapcsolatokat állapítson meg a terrorista bűncselekmények gyanúsítottjai elleni eljárások között, és ily módon erősítse az ügyészek közötti koordinációt az esetleges határokon átnyúló vonatkozású terrorizmus elleni nyomozások során.

További erőfeszítésekre van azonban szükség a határokon átnyúló ügyekben folytatott vizsgálatok támogatása és megkönnyítése érdekében, különösen a bűnüldöző hatóságok **elektronikus bizonyítékokhoz való hozzáférése** tekintetében. Ami a nyomozások során felhasznált elektronikus bizonyítékok határon átnyúló hozzáférésének javítására irányuló 2018. áprilisi javaslatot[22] illeti, az Európai Parlamentnek még el kell fogadnia tárgyalási álláspontját, mielőtt megkezdődhetnének a társjogalkotók közötti tárgyalások. A Bizottság azt szorgalmazza, hogy az Európai Parlament tegyen előrelépést e jogalkotási javaslat tekintetében annak érdekében, hogy a társjogalkotók együttműködésével mielőbb el lehessen fogadni azt. A Bizottság **nemzetközi tárgyalásokat** is folytat az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférés javítása érdekében az uniós belső szabályokra vonatkozó, említett javaslata alapján. 2019. szeptember 25-én a Bizottság és az Egyesült Államok hatóságai megtartották **az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésről szóló EU–USA megállapodással** kapcsolatos hivatalos tárgyalások első fordulóját. A tervek szerint a következő fordulóra 2019. november 6-án kerül sor. **Az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményének második kiegészítő jegyzőkönyvéről** zajló tárgyalások keretében a Bizottság 2019 júliusában, szeptemberében és októberében három tárgyalási ülésszakon vett részt az Unió nevében. Bár e tárgyalások során érdemi előrelépés történt, még számos olyan fontos témáról megállapodásra kell jutni, amelyek kapcsán jelentős uniós érdekeltség nyilvánul meg, ilyenek például az adatvédelmi biztosítékok. A második kiegészítő jegyzőkönyvre vonatkozó tárgyalások 2019 novemberében és 2020 folyamán folytatódnak majd. Fontos a tárgyalások gyors lebonyolítása az elektronikus bizonyítékok megosztására vonatkozó nemzetközi együttműködés

[19] (EU) 2019/1148 rendelet (2019. június 20.) a robbanóanyag-prekurzorok forgalmazásáról és felhasználásáról. A rendelet 2019. július 31-én lépett hatályba, és alkalmazását a hatálybalépését követően 18 hónappal kell majd megkezdeni.

[20] (EU) 2019/1153 irányelv (2019. július 11.) a pénzügyi és egyéb információk bizonyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása céljából történő felhasználásának megkönnyítését szolgáló szabályok megállapításáról.

[21] Minden polgárra kiterjedő szisztematikus ellenőrzések bevezetése a külső határokon a Schengeni Információs Rendszer használatával.

[22] COM(2018) 225 final (2018.4.17.) és COM(2018) 226 final (2018.4.17.).

előmozdítása érdekében, biztosítva egyúttal az uniós jog és az azon alapuló tagállami kötelezettségek összeegyeztethetőségét, szem előtt tartva az uniós jog jövőbeli alakulását is.

Az Európai Parlament 2019. szeptember 19-én a pénzmosással kapcsolatban folyamatosan felmerülő aggályokra reflektálva elfogadta **a pénzmosás elleni uniós jogszabályok végrehajtásának állásáról szóló állásfoglalást**[23], amely a Bizottság által 2019. július 24-én elfogadott, négy jelentésből álló pénzmosás elleni csomagra[24] válaszol. Az Európai Parlament felhívta a tagállamokat, hogy gondoskodjanak a pénzmosás elleni irányelvek megfelelő és gyors végrehajtásáról. Az Európai Parlament felhívta továbbá a Bizottságot annak értékelésére, hogy egy pénzmosás elleni rendelet megfelelőbb lenne-e, mint egy irányelv, valamint hogy szükség van-e együttműködési és támogatási mechanizmusra a pénzügyi információs egységek támogatásához.

A bűnüldöző hatóságok elektronikus bizonyítékokhoz való hozzáférésének javítása érdekében a Bizottság a következőre kéri fel az Európai Parlamentet és a Tanácsot:

- jussanak mielőbb megállapodásra az **elektronikus bizonyítékokról** szóló jogalkotási javaslatokról *(az együttes nyilatkozatban meghatározott prioritás)*.

4. A kiberbiztonság megerősítése

A kiberbiztonság megerősítése a valódi és hatékony biztonsági unió megteremtésére irányuló munka egyik legfontosabb vetülete. Az Unió a 2017. évi uniós kiberbiztonsági stratégiát megvalósítva[25] az ellene irányuló támadások megnehezítésével és a helyreállítás felgyorsításával megerősítette ellenálló képességét, valamint fokozta az elrettentést azáltal, hogy – többek között a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete révén – növelte a támadók kézre kerítésének és megbüntetésének esélyét. Az Unió a kibervédelem terén is támogatja a tagállamokat az uniós kibervédelmi szakpolitikai keret megvalósításával.[26]

A kiberbiztonsági jogszabály[27] 2019. júniusi hatálybalépésével kezd formát ölteni **az uniós kiberbiztonsági tanúsítási keret**. A tanúsítás lényeges szerepet tölt be a digitális egységes piac szempontjából elengedhetetlenül fontos termékek és szolgáltatások iránti bizalomnak és azok biztonságának növelésében. A tanúsítási keret uniós szintű tanúsítási rendszereket biztosít majd átfogó szabályozás, műszaki követelmények, normák és eljárások formájában. Ebben két szakértői csoport vesz részt, nevezetesen a tagállami hatóságokat képviselő európai kiberbiztonsági tanúsítási csoport és az ágazat képviseletében az érdekelt felek kiberbiztonsági tanúsítási csoportja. Az utóbbi az információs és kommunikációs technológiai termékek és szolgáltatások keresleti és kínálati oldalát tömöríti, beleértve a kis- és középvállalkozásokat, digitális szolgáltatókat, európai és nemzetközi szabványügyi szerveket,

23 http://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_HU.html

24 Jelentés a határokon átnyúló tevékenységekhez kapcsolódó és a belső piacot érintő pénzmosási és terrorizmusfinanszírozási kockázatok értékeléséről (COM(2019) 370 (2019.7.24.)), Jelentés a tagállamok bankszámlákkal kapcsolatos nemzeti központi automatizált mechanizmusainak (központi nyilvántartások vagy központi elektronikus adat-visszanyerési rendszerek) összekapcsolásáról (COM(2019) 372 final (2019.7.24.)), Jelentés az uniós hitelintézeteket érintő közelmúltbeli állítólagos pénzmosási ügyek értékeléséről (COM(2019) 373 final (2019.7.24.)), Jelentés a pénzügyi információs egységek közötti együttműködés keretének értékeléséről (COM(2019) 371 final (2019.7.24.)).

25 JOIN(2017) 450 final (2017.9.13.).

26 A Tanács által 2018. november 19-én elfogadott uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat) (14413/18).

27 (EU) 2019/881 rendelet (2019. április 17.)

nemzeti akkreditáló testületeket, adatvédelmi felügyeleti hatóságokat és megfelelőségértékelő szervezeteket.

Az Európai Parlamentnek és a Tanácsnak időközben még meg kell állapodnia **az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra és a nemzeti koordinációs központok hálózatára** vonatkozó jogalkotási kezdeményezésről[28]. A javaslat célja, hogy megerősítse az Unió kiberbiztonsági kapacitását azáltal, hogy ösztönzi az európai technológiai és ipari kiberbiztonsági ökoszisztémát, valamint koordinálja és összevonja a kapcsolódó erőforrásokat. A Bizottság felkéri mindkét társjogalkotót, hogy a kiberbiztonság megerősítése érdekében ismét kezdjék meg és mielőbb zárják le az intézményközi tárgyalásokat e kiemelt kezdeményezésről.

A kiberbiztonság megerősítésére irányuló tevékenység a nemzeti és regionális szint támogatásra is kiterjed[29].

Az EU a rendszerekre és adatokra irányuló kiberfenyegetések mellett továbbra is fellép a **hibrid fenyegetésekkel** kapcsolatos összetett és sokrétű kihívásokkal szemben. A Tanácsban a hibrid fenyegetésekkel szembeni küzdelemmel foglalkozó horizontális munkacsoportot hoztak létre, hogy javítsák az EU és tagállamai hibrid fenyegetésekkel szembeni ellenálló képességét, és támogassák a társadalmak válsággal szembeni ellenálló képességének erősítését. A Bizottság és az Európai Külügyi Szolgálat támogatja ezeket az erőfeszítéseket a hibrid fenyegetésekkel szembeni fellépés 2016. évi közös kerete[30] és a reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítéséről szóló[31] 2018. évi közös közlemény alapján. Ezenfelül a Közös Kutatóközpont a hibrid fenyegetések jellemzésére szolgáló „koncepcionális keretmodellt” dolgoz ki azzal a céllal, hogy segítséget nyújtson a tagállamoknak és illetékes hatóságaiknak az általuk esetleg elszenvedett hibrid támadások típusának azonosításában. A modell azt vizsgálja, hogy egy adott (állami vagy nem állami) szereplő különféle (gazdasági, katonai, társadalmi, politikai) területeken milyen módon alkalmaz (a dezinformációtól a kémkedésig vagy a fizikai műveletekig terjedő) eszközöket ahhoz, hogy célkitűzések sorozatának elérése érdekében befolyásoljon egy célpontot.

A kiberbiztonság növelése érdekében a Bizottság a következőre kéri fel az Európai Parlamentet és a Tanácsot:

- gyors ütemben jussanak megállapodásra az **Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra és a nemzeti koordinációs központok hálózatára** vonatkozó jogalkotási javaslatról.

III. A DIGITÁLIS INFRASTRUKTÚRÁK BIZTONSÁGÁNAK JAVÍTÁSA

Az ötödik generációs (5G) hálózatok képezik majd a gerincét az egyre digitalizáltabb gazdaságoknak és társadalmaknak. Ezek a hálózatok több milliárd, egymással összekapcsolt tárgyra és rendszerre terjednek ki, többek között olyan kritikus fontosságú ágazatokban, mint az energiaipar, a közlekedés, a bankszektor és az egészségügy, továbbá érintik a bizalmas információkat továbbító ipari vezérlő- és az azokat támogató biztonsági rendszereket is. Ezért

[28] COM(2018) 630 final (2018.9.12.).

[29] A Bizottság támogatja például a Bretagne, Castilla y León, Észak-Rajna-Vesztfália, Közép-Finnország és Észtország részvételével kialakított régióközi innovációs partnerséget, amely az európai kiberbiztonsági értéklánc fejlesztésére irányul, a piaci hasznosításra és a méretarány növelésére helyezve a hangsúlyt.

[30] JOIN(2016) 18 final (2016.4.6.).

[31] JOIN(2018) 16 final (2018.6.13.).

alapvető fontosságú az 5G hálózatok kiberbiztonságának és ellenálló képességének biztosítása.

Összehangolt megközelítés részeként, a tagállamok – a Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség támogatásával – 2019. október 9-én közzétették **az 5G hálózatok összehangolt uniós kiberbiztonsági kockázatértékeléséről** szóló jelentést[32]. Ez a jelentős lépés beleilleszkedik a 2019. márciusi bizottsági ajánlás végrehajtásának folyamatába, amelynek célja, hogy Unió-szerte biztosítsa az 5G hálózatok magas szintű kiberbiztonságát[33]. A jelentés a tagállamok által készített nemzeti kiberbiztonsági kockázatértékelések eredményein alapul. Azonosítja a főbb fenyegetéseket és azok forrásait, a legérzékenyebb eszközöket, a főbb sebezhető pontokat (ideértve a technikai jellegű és az egyéb típusú sebezhetőségeket) és számos stratégiai kockázatot. Ez az értékelés szolgál alapul a nemzeti és európai szinten alkalmazható kockázatcsökkentő intézkedések meghatározásához.

A jelentés számos fontos **kiberbiztonsági kihívást** azonosít, amelyek valószínűsíthetően megjelennek vagy hangsúlyosabbá válnak az 5G hálózatokban. Ezek a kiberbiztonsági kihívások elsősorban az 5G technológia legfontosabb *innovációihoz* kapcsolódnak, különös tekintettel 5G-re épülő szoftverek, illetve a szolgáltatások és alkalmazások széles skálájának fontosságára, valamint a *beszállítóknak* az 5G hálózatok kiépítésében és üzemeltetésében játszott szerepére és az egyedi beszállítóktól való függés mértékére. Ez azt jelenti, hogy a szállítók termékei, szolgáltatásai és műveletei egyre inkább az 5G hálózatok „támadási felületének" részévé válnak. Ezen túlmenően különösen fontossá válik az egyedi beszállítók kockázati profilja, ideértve annak valószínűségét is, hogy a beszállítót egy nem uniós ország befolyásolja.

A 2019. márciusi bizottsági ajánlásban megállapított folyamattal összhangban a tagállamoknak 2019. december 31-ig el kell fogadniuk a feltárt kiberbiztonsági kockázatok nemzeti és uniós szinten történő kezelésére szolgáló **kockázatcsökkentő intézkedések készletét**. A Bizottság és az Európai Külügyi Szolgálat emellett folytatni fogja az 5G hálózatok kiberbiztonságáról és ellenálló képességéről a hasonlóan gondolkodó partnerekkel kialakított eszmecserét. Ezzel függ össze, hogy a Bizottság kapcsolatot tart a NATO-val az 5G hálózatok összehangolt uniós kiberbiztonsági kockázatértékelése tekintetében.

[32] Az 5G hálózatok összehangolt uniós kiberbiztonsági kockázatértékelését a kiberbiztonsági irányelv ((EU) 2016/1148 irányelv (2016. július 6.)) alapján létrehozott, az illetékes hatóságokat tömörítő együttműködési csoport – a Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség segítségével – készítette el: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019) 2355 final (2019.3.26.).

IV. A DEZINFORMÁCIÓ ELLENI KÜZDELEM ÉS A VÁLASZTÁSOK VÉDELME MÁS SZÁMÍTÓGÉPES FENYEGETÉSEKKEL SZEMBEN

Az EU – az európai értékek és az alapvető jogok teljes körű tiszteletben tartása mellett – kialakította **a dezinformációval szembeni összehangolt fellépés** keretét[34]. A dezinformációval szembeni cselekvési terv[35] keretében folytatódik dezinformáció játékterének leszűkítésére irányúló munka, többek között a választások integritásának védelme érdekében.

Ebben központi szerepet játszik az ágazattal kialakított együttműködés, amelyre az önszabályozás alapján 2018. októbertől alkalmazandó, az online platformokra és a reklámiparra vonatkozó, **a dezinformáció visszaszorítását célzó gyakorlati kódex** keretében kerül sor[36]. Az online platformok és a kódex más aláírói által benyújtott önértékelési jelentések alapján a Bizottság a kódex első éves működését követően értékelte annak hatékonyságát, és 2019. október 29-én a Bizottság nyilatkozatával együtt közzétette az értékelését.[37] A jelentések nagy vonalakban igazolják, hogy az aláíró felek komoly erőfeszítéseket tesznek kötelezettségvállalásaik teljesítésére.

A kódex aláírói eltérő sebességgel hoztak intézkedések a kódex öt kötelezettségvállalási pillérében, és ezek hatóköre is különböző. Általánosságban elmondható, hogy jelentősebb előrehaladás történt a 2019. évi európai választásokkal kapcsolatos kötelezettségvállalások tekintetében, nevezetesen a dezinformáció hirdetési és a bevételszerzési ösztönzőinek megszüntetése (1. pillér), a politikai és témafókuszú hirdetések átláthatóságának biztosítása (2. pillér), valamint a szolgáltatások hiteltelen beszámolókkal és magatartásokkal szembeni integritásának biztosítása (3. pillér) terén. Ezzel szemben kevesebb előrelépés történt vagy egyáltalán nem történt előrehaladás a fogyasztók helyzetének megerősítésére vonatkozó kötelezettségvállalások (4. pillér), valamint a kutatói közösség szerepének – többek között az adatállományokhoz releváns és a magánéletet tiszteletben tartó, kutatási célú hozzáférés platformok általi biztosítása révén történő – erősítésére irányuló kötelezettségvállalások (5. pillér) tekintetében. Különbségek vannak továbbá az egyes platformok által a kötelezettségvállalások teljesítése érdekében hozott intézkedések hatóköre tekintetében, valamint a tagállamok között az egyedi szakpolitikák alkalmazása terén. A Bizottság a dezinformációval szembeni fellépés fokozása érdekében továbbra is együttműködik a kódex aláíróival és egyéb érdekelt felekkel.

A dezinformációval szembeni cselekvési terv keretében Bizottság és a főképviselő – a tagállamokkal együttműködve – **riasztási rendszert** hozott létre a félretájékoztatási akciók kezelésére. A riasztási rendszer lehetővé tette az uniós intézmények és a tagállamok számára,

---

34 Lásd: Cselekvési terv a dezinformációval szemben (JOIN(2018) 36 final (2018.12.5.)).

35 JOIN(2019) 12 final (2019.6.14.).

36 A kódex keretében a Google, a Facebook, a Twitter és a Microsoft online platformok kötelezettséget vállaltak arra, hogy megakadályozzák szolgáltatásaik rossz szándékú szereplők általi manipulatív alkalmazását, rendelkeznek a politikai hirdetések átláthatóságáról és közzétételéről, valamint egyéb intézkedéseket hoznak az online ökoszisztéma átláthatóságának, elszámoltathatóságának és megbízhatóságának javítása érdekében. A reklámipart képviselő szakmai szövetségek ugyancsak kötelezettséget vállaltak arra, hogy együttműködnek a platformokkal annak érdekében, hogy javítsák a reklámok elhelyezésének ellenőrzését, és márkavédelmi eszközöket dolgoznak ki azzal a céllal, hogy korlátozzák a reklámok elhelyezését a dezinformációt terjesztő weboldalakon.

37 https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. A Google, a Facebook, a Twitter és a Microsoft mellett a kódex egyéb aláírói közé tartozik a Mozilla, a reklámipart képviselő hét európai szintű és nemzeti szintű szövetség, valamint az EDiMA, egy, az online ágazatban tevékenykedő platformokat és más technológiai vállalatokat képviselő európai szövetség.

hogy a 2019. évi európai parlamenti választásokat megelőzően megosszák egymással információikat és elemzéseiket, valamint összehangolják válaszlépéseiket. A választásokat követően ez a tevékenység még intenzívebbé vált: napi szinten folynak munkamegbeszélések, és a riasztási rendszer kapcsolattartói háromszor üléseztek különböző tagállamok szervezésében.

A dezinformáció azonosítására irányuló további gyakorlati lépést jelent a **stratégiai kommunikációs csoport** munkája, és különösen a keleti stratégiai kommunikációval foglalkozó munkacsoport tevékenysége. E munkacsoport működteti az „EUvsDisinfo" elnevezésű projektet, melynek célja a Kreml-párti dezinformáció figyelemmel kísérése, elemzése és megválaszolása[38]. 2019 eleje óta a 3 millió EUR-s első célzott költségvetés lehetővé tette e munka fokozását és az interneten, a műsorszolgáltatásban és a közösségi médiában jelenlévő Kreml-párti dezinformációnak az angoltól a szerbig és az arabig terjedő 19 nyelven történő figyelemmel kísérésére és elemzésére való kiterjesztését. A figyelemmel kísérési kapacitás javításának köszönhetően több mint kétszeresére nőtt a napvilágra hozott dezinformációs tevékenységek száma: 2019-ben mostanáig körülbelül 2 000 dezinformációs esetet tártak fel, szemben a 2018 azonos időszakában leleplezett 765 esettel. A keleti stratégiai kommunikációval foglalkozó munkacsoport alapvető szerepet játszott a 2019. évi európai parlamenti választásokat célzó, Kreml-párti dezinformáció figyelemmel kísérésében és leleplezésében. A kutatást egy olyan kampánnyal egészítették ki, amely felhívja a figyelmet a választási folyamatokba történő, világszerte tapasztalható beavatkozási kísérletekre. Az Európai Parlamenttel és a Bizottsággal szoros együttműködésben végzett tájékoztatási tevékenység eredményeként több mint 20 interjú jelent meg a médiában, és 300-at meghaladó számú újságíró kapcsolódott be a kampányba.

A Bizottság intézkedéseket hozott **az uniós intézményekkel és szakpolitikákkal kapcsolatos dezinformáció és tévhitek terjedésének korlátozása** érdekében is. Kommunikációs szakértőkből álló hálózatot hozott létre egy online portál segítségével, amely az uniós szakpolitikákról, valamint a dezinformációval kapcsolatos kihívásról és annak a társadalomra gyakorolt hatásáról szóló interaktív információs anyagokat kínál. Emellett az Európai Parlamenttel és az Európai Külügyi Szolgálattal együttműködésben a dezinformáció leküzdésére irányuló sorozatos közösségi média kampányokat[39] indított.

V. A BIZTONSÁGGAL KAPCSOLATOS TOVÁBBI KIEMELT KEZDEMÉNYEZÉSEK VÉGREHAJTÁSA

1. A biztonsági unió jogalkotási intézkedéseinek végrehajtása

A biztonsági unió keretében elfogadott intézkedések csak akkor hoznak optimális eredményt a biztonság tekintetében, ha minden tagállam gondoskodik azok mielőbbi és teljes körű végrehajtásáról. E célból a Bizottság tevékenyen támogatja a tagállamokat az uniós jogszabályok végrehajtásában, többek között finanszírozás és a bevált módszerek cseréjének elősegítése révén. A Bizottság teljes mértékben él a Szerződések által az uniós jog érvényesítéséhez ráruházott hatáskörökkel, ideértve megfelelő esetekben a kötelezettségszegési eljárást is.

[38] www.euvsdisinfo.eu

[39] https://europa.eu/euprotects/

Az uniós utas-nyilvántartási adatállományról szóló irányelv[40] átültetésének határideje 2018. május 25-én járt le. Eddig 25 tagállam jelentette be a teljes körű átültetést[41], ami jelentős előrelépést jelent 2018 júliusa óta, amikor a Bizottság 14 tagállam ellen indított kötelezettségszegési eljárást[42]. A 2018. július 19-én elindított, folyamatban lévő kötelezettségszegési eljárások ellenére két tagállam még nem jelentette be a teljes körű átültetést[43]. Ezzel párhuzamosan a Bizottság továbbra is támogatást nyújt minden tagállamnak az utas-nyilvántartási adatállomány kezelésére szolgáló saját rendszereik kialakításához, többek között az információk és bevált módszerek cseréjének elősegítésével.

A terrorizmus elleni küzdelemről szóló irányelv[44] átültetésének határideje 2018. szeptember 8-án járt le. Eddig 22 tagállam jelentette be a teljes kőrű átültetést, ami jelentős előrelépést jelent 2018 novembere óta, amikor a Bizottság 16 tagállam ellen indított kötelezettségszegési eljárást[45]. A folyamatban lévő kötelezettségszegési eljárások ellenére három tagállam még nem jelentette be a teljes körű átültetést[46]. 2019. július 25-én a Bizottság indokolással ellátott véleményt küldött két tagállamnak, amiért elmulasztották bejelenteni az irányelv teljes körű átültetését[47]. Erre válaszul mindkét tagállam bejelentette, hogy a jogalkotási munka még az idei év vége előtt befejeződik.

A fegyverek megszerzésének és tartásának ellenőrzéséről szóló irányelv[48] átültetésének határideje 2018. szeptember 14-én járt le. Eddig 13 tagállam jelentette be a teljes körű átültetést. A 2018. november 22-én elindított, folyamatban lévő kötelezettségszegési eljárások ellenére 15 tagállam még nem jelentette be a teljes körű átültetést[49]. 2019. július 25-én a Bizottság indokolással ellátott véleményt küldött 20 tagállamnak, amiért elmulasztották bejelenteni az irányelv teljes körű átültetését. Erre válaszul öt tagállam bejelentette az irányelv teljes körű átültetését[50].

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelv[51] átültetésének határideje 2018. május 6-án járt le. Eddig 25 tagállam jelentette be a teljes körű átültetést, ami jelentős előrelépést jelent 2018 júliusa óta, amikor a Bizottság 19 tagállam ellen indított

---

40 (EU) 2016/681 irányelv (2016. április 27.) Dánia nem vesz részt ennek az irányelvnek az elfogadásában, és az irányelv vagy annak alkalmazása rá nézve nem kötelező.

41 A teljes körű átültetés bejelentésére vonatkozó hivatkozások figyelembe veszik a tagállamok bejelentéseit, és nem érintik a bizottsági szolgálatok által végzett átültetési ellenőrzést (a 2019. október 17-én aktuális helyzet).

42 Lásd a hatékony és valódi biztonsági unió megvalósításáról szóló tizenhatodik eredményjelentést (COM(2018) 690 final (2018.10.10.)).

43 Szlovénia részleges átültetéséről tett bejelentést. Spanyolország nem tett bejelentést átültetésről (a 2019. október 17-én aktuális helyzet).

44 (EU) 2017/541 irányelv (2017. március 15.) Az irányelv az Egyesült Királyságban, Írországban és Dániában nem alkalmazandó.

45 Lásd a hatékony és valódi biztonsági unió megvalósításáról szóló tizenhetedik eredményjelentést (COM(2018) 845 final (2018.12.11.)).

46 Görögország és Luxemburg nem jelentette be a nemzeti végrehajtási intézkedéseket. A Lengyelország által bejelentett nemzeti intézkedések részleges átültetésnek felelnek meg (a 2019. október 17-én aktuális helyzet).

47 Görögország és Luxemburg.

48 (EU) 2017/853 irányelv (2019. október 17.).

49 Belgium, Csehország, Észtország, Lengyelország, Svédország, Szlovákia és az Egyesült Királyság az új rendelkezések egy részét átültető intézkedéseket jelentett be. Ciprus, Németország, Görögország, Spanyolország, Luxemburg, Magyarország, Románia és Szlovénia nem jelentett be átültető intézkedéseket (a 2019. október 17-én aktuális helyzet).

50 Finnország, Írország, Litvánia, Hollandia, Portugália (a 2019. október 17-én aktuális helyzet).

51 (EU) 2016/680 irányelv (2016. április 27.)

kötelezettségszegési eljárást[52]. A folyamatban lévő kötelezettségszegési eljárások ellenére három tagállam még nem jelentette be a teljes körű átültetést[53]. 2019. július 25-én a Bizottság úgy határozott, hogy két tagállammal szemben[54] az Európai Unió Bíróságához fordul az irányelv átültetésének elmulasztása miatt, valamint felszólító levelet küldött egy tagállamnak[55] az irányelv teljes körű átültetésének elmulasztása miatt[56].

A Bizottság értékeli **a negyedik pénzmosási irányelv**[57], átültetését, miközben azt is ellenőrzi, hogy a tagállamok végrehajtják-e a szabályokat. A tagállamoknak az irányelvet 2018. június 26-ig kellett átültetniük a nemzeti jogba. A Bizottság 21 tagállammal szemben fenntartja a kötelezettségszegési eljárást, mivel úgy értékelte, hogy a tagállamoktól érkezett bejelentések nem jelentik ezen irányelv teljes körű átültetését[58].

A Bizottság értékelte **a számítástechnikai bűnözéssel kapcsolatos irányelvek** átültetésének megfelelőségét. 2019 júliusában és októberében kötelezettségszegési eljárást indított 23 tagállam ellen, [59]mivel úgy értékelte, hogy az említett tagállamok által bejelentett nemzeti végrehajtási intézkedések nem jelentik **a gyermekek szexuális bántalmazásáról szóló irányelv**[60] helyes átültetését. A Bizottság 2019 júliusában és októberében hasonlóan kötelezettségszegési eljárást indított négy tagállam ellen[61], mivel úgy értékelte, hogy az említett tagállamok által bejelentett nemzeti végrehajtási intézkedések nem jelentik **az információs rendszerek elleni támadásokról szóló irányelv**[62] helyes átültetését.

A Bizottság felszólítja a tagállamokat, hogy sürgősen tegyék meg az alábbi irányelveknek a nemzeti jogba való átültetéséhez szükséges intézkedéseket, és ezeket jelentsék be a Bizottságnak:

- az **uniós utas-nyilvántartási adatállományról szóló irányelv**, amely tekintetében tagállamnak 1 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 1 tagállamnak pedig még teljes körűvé kell tennie az átültetésről szóló bejelentést[63];
- a **terrorizmus elleni küzdelemről szóló irányelv**, amely tekintetében 2 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 1 tagállamnak pedig még teljes körűvé kell tennie az átültetésről szóló bejelentést[64];

---

52 Lásd a hatékony és valódi biztonsági unió megvalósításáról szóló tizenhatodik eredményjelentést (COM(2018) 690 final (2018.10.10.)).

53 Szlovénia részleges átültetéséről tett bejelentést. Spanyolország nem tett bejelentést átültetésről. Bár Németország teljes átültetésről tett bejelentést, a Bizottság úgy ítéli meg, hogy ez az átültetés nem teljes körű (a 2019. október 17-én aktuális helyzet).

54 Görögország és Spanyolország.

55 Németország.

56 Görögország bejelentette a teljes körű átültetést, amelyet a Bizottság jelenleg értékel.

57 (EU) 2015/849 irányelv (2015. május 20.)

58 Belgium, Bulgária, Csehország, Dánia, Németország, Észtország, Írország, Franciaország, Olaszország, Ciprus, Lettország, Litvánia, Magyarország, Hollandia, Ausztria, Lengyelország, Románia, Szlovákia, Finnország, Svédország és az Egyesült Királyság (a 2019. október 17-én aktuális helyzet). Korábban az irányelvvel kapcsolatos 7 kötelezettségszegési eljárást lezártak.

59 Belgium, Bulgária, Csehország, Németország, Észtország, Görögország, Spanyolország, Franciaország, Horvátország, Olaszország, Lettország, Litvánia, Luxemburg, Magyarország, Málta, Ausztria, Lengyelország, Portugália, Románia, Szlovénia, Szlovákia, Finnország és Svédország.

60 2011/93/EU irányelv (2011. december 13.).

61 Bulgária, Olaszország, Portugália és Szlovénia.

62 2013/40/EU irányelv (2013. augusztus 12.).

63 Szlovénia részleges átültetéséről tett bejelentést. Spanyolország nem tett bejelentést átültetésről (a 2019. október 17-én aktuális helyzet).

- a **fegyverek megszerzésének és tartásának ellenőrzéséről szóló irányelv**, amely tekintetében 8 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 7 tagállamnak pedig még teljes körűvé kell tennie az átültetésről szóló bejelentést[65];
- a **bűnüldözésben érvényesítendő adatvédelemről szóló irányelv,** amely tekintetében 1 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 2 tagállamnak pedig még teljes körűvé kell tennie az átültetésről szóló bejelentést[66];
- a **negyedik pénzmosási irányelv**, amely tekintetében 21 tagállamnak kell még teljes körűvé tennie az átültetésről szóló bejelentést[67];
- a **gyermekek szexuális bántalmazásáról szóló irányelv,** amely tekintetében 23 tagállammal szemben indult kötelezettségszegési eljárás helytelen átültetés miatt[68];
- az **információs rendszerek elleni támadásokról szóló irányelv**, amely tekintetében 4 tagállammal szemben indult kötelezettségszegési eljárás helytelen átültetés miatt[69].

2. Felkészültség és védelem

A hatékony és valódi biztonsági unió megteremtésére irányuló munka egyik fontos eleme a biztonsági fenyegetésekkel szembeni ellenálló képesség megerősítése. A Bizottság támogatja a tagállamokat és a helyi hatóságokat a nyilvános terek védelmének megszilárdítása tekintetében, valamint a 2017. októberi cselekvési terv és az uniós városfejlesztési menetrend keretében létrejött, a nyilvános terek biztonságát szolgáló 2019. januári partnerség megvalósítása folyamán. Ez a munka azokat a városokat érinti, amelyek kapcsolatba léptek a Bizottsággal, és támogatást kértek a nyilvános terek védelme tekintetében előttük álló kihívások kezeléséhez.

A nyilvános terek biztonságának megerősítéséhez kulcsfontosságú a bevált módszerek helyi hatóságok és magánszolgáltatók közötti cseréje. Ez volt a központi téma a **Biztonság Európai Hetén**, amely 2019. október 14. és 18. között Nizzában (Franciaország) került megrendezésre „A terrorizmussal szemben szövetségre lépett városok védelme a városi területek biztonságának megszilárdítása során” elevezésű projekt keretében. Az Európa városaiból, a nemzeti hatóságoktól és kutatóintézetektől érkező 500 résztvevőt összekapcsoló rendezvény ráirányította a figyelmet az állami és magánszférában tevékenykedő összes érdekelt fél közötti szoros együttműködés fontosságára, és az új technológiák szerepére a városok hatékonyabb védelme terén. A nyilvános terek védelme ugyancsak téma volt a 2019. október 7. és 10. között Brüsszelben megrendezett **Régiók és Városok Európai Hete** alkalmával, ahol az egyik munkaértekezlet az uniós városfejlesztési menetrend keretén belül kialakított, a

---

64 Görögország és Luxemburg nem tett bejelentést az átültetésről. Lengyelország részleges átültetést jelentett be (a 2019. október 17-én aktuális helyzet).

65 Belgium, Csehország, Észtország, Lengyelország, Svédország, Szlovákia és az Egyesült Királyság az új rendelkezések egy részét átültető intézkedéseket jelentett be. Ciprus, Németország, Görögország, Spanyolország, Luxemburg, Magyarország, Románia és Szlovénia nem jelentett be átültető intézkedéseket (a 2019. október 17-én aktuális helyzet).

66 Szlovénia részleges átültetéséről tett bejelentést. Spanyolország nem tett bejelentést átültetésről. Bár Németország teljes átültetésről tett bejelentést, a Bizottság úgy ítéli meg, hogy ez az átültetés nem teljes körű (a 2019. október 17-én aktuális helyzet).

67 Belgium, Bulgária, Csehország, Dánia, Németország, Észtország, Írország, Franciaország, Olaszország, Ciprus, Lettország, Litvánia, Magyarország, Hollandia, Ausztria, Lengyelország, Románia, Szlovákia, Finnország, Svédország és az Egyesült Királyság (a 2019. október 17-én aktuális helyzet).

68 Belgium, Bulgária, Csehország, Németország, Észtország, Görögország, Spanyolország, Franciaország, Horvátország, Olaszország, Lettország, Litvánia, Luxemburg, Magyarország, Málta, Ausztria, Lengyelország, Portugália, Románia, Szlovénia, Szlovákia, Finnország és Svédország.

69 Bulgária, Olaszország, Portugália és Szlovénia.

nyilvános terek biztonságát szolgáló partnerségre vonatkozott. A rendezvény kiemelten foglalkozott a helyi hatóságoknak a biztonságpolitika területén betöltött szerepével, a nyilvános városi terek védelmével kapcsolatos fő biztonsági kihívások kezelésére szolgáló uniós szabályozással és finanszírozással, valamint olyan lényeges témákkal, mint az intelligens megoldások és technológiák révén megvalósuló innováció, ideértve a beépített biztonság fogalmát, valamint a megelőzés és a társadalmi befogadás. A Bizottság az Innovatív városfejlesztési tevékenységekre vonatkozó legutóbbi pályázati felhívásával – amelynek eredményeit 2019 augusztusában jelentették be – szintén hozzájárul a városok innovációjához ezeken a területeken. A kiválasztott projektek között szerepel, hogy három város (a görögországi Pireusz, a finnországi Tampere és az olaszországi Torinó) új megoldásokat tesztel majd a városi biztonság területén[70].

A Bizottság 2019. október 7-én találkozót szervezett a zsidó, muzulmán, keresztény és buddhista közösségek képviselőivel **az imahelyek hatékonyabb védelme** és a különböző vallási csoportok igényeinek feltérképezése céljából. A nyilvános terek védelmének javításáról szóló 2017. évi uniós cselekvési terv végrehajtásának keretébe illeszkedő találkozó azt mutatta, hogy a biztonsággal kapcsolatos tudatosság és felkészültség jelentősen eltér a különböző vallási közösségek között, ami rávilágít a bevált módszerek cseréjének fontosságára. A találkozó azt is nyilvánvalóvá tette, hogy az alapvető biztonsági intézkedések bevezetése és a biztonsággal kapcsolatos tudatosság fejlesztése nem összeegyeztethetetlen az imahelyek nyílt és hozzáférhető jellegének megőrzésével. A Bizottság elektronikus szakértői platformján egybegyűjti a bevált gyakorlatokat és figyelemfelkeltő anyagokat, és a nyilvános terek védelmére szolgáló köz- és magán fórumon felhívja a témára a tagállami biztonsági hatóságok figyelmét.

Egy további figyelmet igénylő sajátos terület a **drónok** által a kritikus infrastruktúrára és nyilvános terekre jelentett növekvő biztonsági fenyegetés. A Bizottság amellett, hogy – a személyzet nélküli légi járművek hasznos alkalmazási lehetőségeinek veszélyeztetése nélkül – kiegészíti a drónok személyzettel ellátott légi járművek által használt légtérben történő biztonságos üzemeltetésére vonatkozó közelmúltbeli uniós jogszabályt[71], támogatást nyújt a tagállamoknak a drónok rosszindulatú használatával kapcsolatos tendenciák nyomon követésében, a releváns kutatások finanszírozásában és az ellenintézkedések tesztelésének elősegítésében. A tapasztalatok és bevált gyakorlatok cseréje alapvető fontosságú, amint azt a 2019. október 17-én Brüsszelben megrendezett, a pilóta nélküli légijármű-rendszerek jelentette veszélyek leküzdésével foglalkozó magas szintű nemzetközi konferencia is igazolta. A Bizottság által szervezett, a tagállamok, a nemzetközi szervezetek, harmadik partnerországok, az iparág, a tudományos élet és a civil társadalom köréből érkező 250 résztvevőt egy asztalhoz ültető rendezvényen megvitatták a drónok jelentette biztonsági kihívásokat és kezelésük módozatait. A találkozó megmutatta, hogy szükség van a drónokkal kapcsolatos rendszeres kockázatértékelésekre, valamint a légiközlekedési és a bűnüldöző hatóságok közötti szoros együttműködésre a drónok biztonságos üzemeltetésére vonatkozó európai jogszabályok továbbfejlesztése során. Arra is szükség van, hogy összehangolt európai megközelítés révén tovább teszteljék a drónokkal szembeni ellenintézkedéseket. Ezenfelül egyetértés mutatkozott abban is, hogy a drónoknak biztonságosnak, megbízhatóan

[70] Az Innovatív városfejlesztési tevékenységek az Európai Regionális Fejlesztési Alapból társfinanszírozott eszközt alkotnak. További információkért lásd a következő honlapot: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

[71] A Bizottság (EU) 2019/947 végrehajtási rendelete (2019. május 24.) a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról.

működőnek és rosszindulatú célokra nehezen felhasználhatónak kell lenniük, továbbá hogy alapvető fontosságú a hatóságok és az iparág közötti szoros együttműködés.

3. Külső dimenzió

Mivel az Unió előtt álló biztonsági kockázatok többsége túllépi az uniós határokat és globális fenyegetést jelent, a partnerországokkal és szervezetekkel, valamint az érintett felekkel való együttműködés rendkívül lényeges a hatékony és valódi biztonsági unió kiépítése során.

Az információcsere központi szerepet játszik ebben az együttműködésben. A Bizottság e jelentéssel együtt ajánlást fogadott el a Tanács számára **a személyes adatoknak a súlyos bűnözés és a terrorizmus elleni küzdelem céljából történő**, az Europol és az illetékes új-zélandi hatóságok közöti **cseréjéről szóló EU–Új-Zéland megállapodásra** irányuló tárgyalások megkezdésére való felhatalmazásról. E megállapodások tovább erősítik majd az Europol azon képességét, hogy együttműködjön Új-Zélanddal az Europol célkitűzéseinek hatókörébe tartozó bűncselekmények megelőzése és leküzdése céljából. Bár az Europol és az új-zélandi rendőrség között 2019 áprilisában létrejött munkamegállapodás keretet biztosít a strukturált stratégiai szintű együttműködéshez, nem nyújt jogalapot a személyes adatok cseréjéhez. Az uniós jog és az alapvető jogok maradéktalan tiszteletben tartása mellett zajló személyesadat-csere elengedhetetlen a hatékony rendőrségi operatív együttműködéshez. Korábban a Bizottság a terrorizmus általi fenyegetettség, a migrációval kapcsolatos kihívások és az Europol operatív szükségletei alapján a közel-keleti/észak-afrikai régióban meghatározott nyolc olyan kiemelt országot, amelyekkel tárgyalásokat kell kezdeni.[72] Figyelembe véve az egész EU bűnüldöző hatóságainak operatív szükségleteit, valamint az e területen kialakítandó szorosabb együttműködés lehetséges előnyeit, amelyeket a 2019. márciusi christchurchi merénylet nyomon követése is beigazolt, a Bizottság úgy véli, hogy Új-Zélandot fel kell venni azon kiemelt országok közé, amelyekkel rövid távon tárgyalásokat kell kezdeni.

Az Unió harmadik országbeli partnerekkel folytatott biztonsági együttműködésének másik sarokköve az **utas-nyilvántartási adatok** továbbítása. 2019. szeptember 27-én a Bizottság ajánlást fogadott el a Tanács számára a terrorizmus és más súlyos nemzetközi bűncselekmények megelőzése és az ellenük való küzdelem céljából az utas-nyilvántartási adatoknak az adatvédelmi biztosítékok és az alapvető jogok maradéktalan tiszteletben tartása mellett történő továbbításáról szóló **EU–Japán** megállapodásra irányuló tárgyalások megkezdésére való felhatalmazásról[73]. A Tanács jelenleg munkacsoporti szinten vizsgálja az ajánlást, és a Bizottság felkéri a Tanácsot, hogy mielőbb fogadja el a Japánnal folytatandó tárgyalásokra vonatkozó megbízatást. Ha a 2020. évi olimpia idejére hatályba lépne a megállapodás, annak valódi biztonsági hozadéka lenne.

Globális szinten a Bizottság támogatja a **Nemzetközi Polgári Repülési Szervezet** munkáját, amely az utas-nyilvántartási adatok kezelésére vonatkozó szabvány kidolgozására irányul. Ez a 2396. ENSZ BT-határozatban szereplő azon felhívásnak tesz eleget, amely sürgeti az ENSZ valamennyi tagállamát, hogy fejlessze az utas-nyilvántartási adatok gyűjtésére, kezelésére és elemzésére való képességét. 2019. szeptember 13-án a Bizottság előterjesztette az EU által a

[72] Lásd a hatékony és valódi biztonsági unió megvalósításáról szóló tizenegyedik eredményjelentést (COM(2017) 608 final (2017.10.18.)). A kiemelt országok Algéria, Egyiptom, Izrael, Jordánia, Libanon, Marokkó, Tunézia és Törökország.

[73] COM(2019) 420 final (2019.9.27.).

Nemzetközi Polgári Repülési Szervezet Tanácsában az utasnyilvántartási adatokra vonatkozó szabványok és ajánlott eljárások tekintetében képviselendő álláspontról szóló tanácsi határozatra vonatkozó javaslatot[74]. A Tanács jelenleg munkacsoporti szinten vizsgálja az ajánlást, és a Bizottság sürgeti a tanácsi határozat mielőbbi elfogadását. Az Unió és tagállamainak álláspontját ismertette továbbá „Az utasnyilvántartási adatok gyűjtésére, felhasználására, kezelésére és védelmére vonatkozó szabványok és elvek" című tájékoztató dokumentum, amely a Nemzetközi Polgári Repülési Szervezet (ICAO) Közgyűlésének40. ülésszakán került benyújtásra.

Ami a **Kanadával megkötendő** új utas-nyilvántartási adatállományra vonatkozó megállapodásra irányuló munkát illeti, a Bizottság a megállapodás gyors véglegesítésére törekszik. Eközben az idén nyáron a Canberrába és Washingtonba tett 2019. augusztusi és szeptemberi látogatással elkezdődött az **Ausztráliával** megkötött utas-nyilvántartási adatállományra vonatkozó megállapodás közös felülvizsgálata és közös értékelése, valamint az **Egyesült Államokkal** megkötött utas-nyilvántartási adatállományra vonatkozó megállapodás közös értékelése. A Bizottság egy 2019. október 14-i zárt ülésen tájékoztatta az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottságát a Japánnal, Ausztráliával és Kanadával az utas-nyilvántartási adatok tekintetében végzett munka aktuális állásáról.

A terrorizmus elleni küzdelemről szóló, a **Nyugat-Balkánra** vonatkozó 2018. októberi közös cselekvési terv végrehajtása révén előrelépés történt a nyugat-balkáni partnerekkel folytatott biztonsági együttműködés terén is. Október 9-én a Bizottság két jogilag nem kötelező érvényű kétoldalú terrorizmus elleni megállapodást írt alá Albániával és az Észak-macedón Köztársasággal[75]. Ezek a megállapodások lefedik a közös cselekvési terv öt célkitűzését[76] és megjelölik a Bizottság által nyújtani kívánt támogatást, valamint meghatározzák a megfelelő partnerország hatóságai által meghozandó, testre szabott kiemelt intézkedéseket. A többi nyugat-balkáni partnerrel kötött hasonló megállapodások aláírására várhatóan az elkövetkező hetekben kerül sor. Ezen túlmenően a Bizottság 2019. október 7-én a Montenegró és az Európai Határ- és Partvédelmi Ügynökség közötti határigazgatási együttműködésről szóló megállapodást írt alá Montenegróval. Ez a megállapodás lehetővé teszi az Ügynökség számára, hogy segítséget nyújtson Montenegrónak az irreguláris migráció és a határon átnyúló bűnözés leküzdése céljából, ezáltal fokozva a biztonságot az EU külső határán.

A közös biztonsági fenyegetések kezelése terén a partnerországokkal folytatott együttműködés fokozása érdekében a Bizottság a következőkre kéri fel a Tanácsot:

- fogadja el a személyes adatoknak a súlyos bűnözés és a terrorizmus elleni küzdelem céljából történő cseréjéről szóló, az EU és **Új-Zéland** közötti megállapodásra irányuló tárgyalások megkezdésére vonatkozó felhatalmazást;
- fogadja el az utas-nyilvántartási adatok továbbításáról szóló, az EU és **Japán** közötti megállapodásra irányuló tárgyalások megkezdésére vonatkozó felhatalmazást;
- fogadja el **az EU által a Nemzetközi Polgári Repülési Szervezet Tanácsában** az

[74] COM(2019) 416 final (2019.9.13.).

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

[76] A közös cselekvési terv a következő öt célkitűzés mentén tervez intézkedéseket: a terrorizmus elleni harc szilárd keretének kialakítása; az erőszakos szélsőségesség hatékony megelőzése és az azzal szembeni fellépés; hatékony információcsere és operatív együttműködés; a pénzmosás és a terrorizmusfinanszírozás elleni küzdelmet szolgáló kapacitásépítés; a polgárok és az infrastruktúra védelmének megerősítése.

utasnyilvántartási adatokra vonatkozó szabványok és ajánlott eljárások tekintetében **képviselendő álláspontról szóló tanácsi határozatra** vonatkozó javaslatot.

VI. KÖVETKEZTETÉS

Ez a jelentés ismerteti a közös európai fenyegetések kezelése és a kollektív biztonságunk javítása érdekében az EU által meghozott intézkedések széles körét. Azon közös meggyőződéstől vezérelve, hogy napjaink biztonsági kihívásai az együttműködés és a harmadik országokkal közös munka révén kezelhetők a leghatékonyabban, a szereplők széles köre közötti szoros együttműködés, bizalomépítés, az erőforrások megosztása és a fenyegetésekkel szembeni közös fellépés alapján értünk el eredményeket a hatékony és valódi biztonsági unió felé történő előrehaladás során: mindez a városoktól és más helyi szereplőktől, a régiókon és nemzeti hatóságokon át egészen az uniós szinten eljáró Európai Parlamentig és Tanácsig átívelő valamennyi kormányzati szinten; a hatóságok, az uniós ügynökségek, a magánszféra szereplői és a civil társadalom bevonása mellett; valamint a különböző szakpolitikai területeken – például a közlekedéspolitika, a digitális egységes piac vagy a kohéziós politika területén – meglévő szakértelem, eszközök és források felhasználásával valósult meg. Ennek során a biztonsági unió keretében végzett munka beépült az alapvető jogok védelmébe, megóvta és előmozdította értékeinket.

Folytatni kell a hatékony és valódi biztonsági unió kialakítására irányuló munkát. Gyors megállapodásra van szükség a fontos, függőben lévő kezdeményezésekről, nevezetesen az alábbiakról: (1) az online terrorista tartalom eltávolításáról szóló jogalkotási javaslat, (2) a bűnüldöző hatóságok elektronikus bizonyítékokhoz való hozzáférésének javításáról szóló jogalkotási javaslat, (3) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozására irányuló jogalkotási javaslat, valamint (4) a biztonság, a határigazgatás és a migrációkezelés területén használt szilárdabb és intelligensebb információs rendszerekről szóló, függőben lévő jogalkotási javaslatok. Az elfogadott intézkedéseket és eszközöket a gyakorlatban is működőkő realitássá kell tenni azáltal, hogy minden tagállam kellő időben és maradéktalanul végrehajtja az uniós jogszabályokat, hogy hozzájussanak az azokból eredő összes biztonsági előnyhöz. Különösen lényeges, hogy minden tagállam végrehajtsa a biztonság, határigazgatás és migrációkezelés területén használt uniós információs rendszerek közötti interoperabilitásról szóló, közelmúltban elfogadott jogszabályt annak érdekében, hogy 2020-ig megvalósuljon a teljes körű interoperabilitás ambiciózus célkitűzése. Végezetül Európának éberen kell figyelnie a kialakuló és változó fenyegetéseket, és továbbra is együtt kell működnie a polgárok biztonságának fokozása érdekében.