EURÓPAI
BIZOTTSÁG

Brüsszel, 2019.7.24.
COM(2019) 353 final

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

Tizenkilencedik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról

I. BEVEZETÉS

A hatékony és valódi biztonsági unió megvalósításáról szóló tizenkilencedik jelentés 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.

„Az európaiak joggal várják el, hogy az Unió garantálja biztonságukat. A Jean-Claude Juncker vezette Bizottság az első hivatali napjától kezdve kiemelt prioritásként kezeli a biztonságot. Az Európai Tanács a 2019–2024-es időszakra szóló új stratégiai menetrendjében az Unió négy fő prioritása között első helyen szerepel „a polgárok és a szabadságok védelmére" vonatkozó célkitűzés[1]. Az Európai Tanács emellett kijelentette, hogy az eddigi eredményekre építve tovább fogja fokozni a terrorizmus és a határokon átnyúló bűnözés elleni küzdelmet, ennek érdekében pedig – többek között – javítani fogja az együttműködést és az információmegosztást, és tovább fogja fejleszteni a közös eszközöket.

Az Európai Parlament, a Tanács és a Bizottság közötti szoros együttműködésnek köszönhetően az EU jelentős előrelépést tett a hatékony és valódi biztonsági unió megteremtésére irányuló közös erőfeszítések terén: számos kiemelt jogalkotási kezdeményezést vezetett be és nem jogalkotási kezdeményezések széles körét valósította meg annak érdekében, hogy támogassa a tagállamokat és fokozza valamennyi polgár biztonságát[2]. Az Unió határozott lépéseket tett a terroristák mozgásterének megszüntetése érdekében, hogy ne álljanak rendelkezésükre olyan az eszközök, amelyekkel támadásokat képesek végrehajtani, és e célból tilalmat vezetett be bizonyos tűzfegyverek megszerzésére és használatára vonatkozóan, továbbá korlátozta a pénzügyi forrásokhoz való hozzáférés lehetőségeit. Az EU emellett megerősítette a tagállamok közötti információmegosztást, valamint megszüntette az információs hézagokat és a fehér foltokat, miközben fellépett a radikalizálódással szemben, intézkedéseket hozott az európaiak online védelme érdekében, megszilárdította az Unió külső határainak igazgatását, továbbá megerősítette a biztonság területén folytatott nemzetközi együttműködést.

Van azonban még több olyan kiemelt kezdeményezés a biztonsági unióra vonatkozóan, amelyet még nem fogadtak el a társjogalkotók. Az Európai Parlament 9. jogalkotási ciklusának 2019. július 2-i megkezdését követően e jelentés:

- meghatározza, hogy mely területeken kell intézkedéseket tenniük a társjogalkotóknak a közvetlen fenyegetések kezelése érdekében. Különösen sürgős feladat fellépni **a terrorista propaganda és az online radikalizálódás elleni küzdelem** terén.
- meghatározza, hogy melyek azok a biztonsági unióra vonatkozó, elfogadásra váró kiemelt kezdeményezések, amelyek vonatkozásában a társjogalkotók további lépéseire van szükség, hogy fokozzuk a **kiberbiztonságot**, elősegítsük az **elektronikus bizonyítékokhoz** való hozzáférést, valamint sikeresen lezárjuk a biztonság, a határigazgatás és a migrációkezelés területén használt információs rendszerek szilárdabbá és intelligensebbé tételére irányuló munkát.
- a tagállamok által 2019. július 15-ig benyújtott nemzeti kockázatértékelésekre alapozva tájékoztatást nyújt **az 5G hálózatok biztonságának** értékelése és megerősítése érdekében 2019 márciusában megkezdett sürgős együttes munka jelenlegi állásáról;
- foglalkozik a Bizottság által a **pénzmosás elleni küzdelemre** vonatkozóan 2019. július 24-én elfogadott négy jelentéssel, amelyek elemzik a pénzmosással kapcsolatos jelenlegi kockázatokat és sebezhető pontokat, valamint értékelik, hogy a vonatkozó uniós szabályozási

[1] https://www.consilium.europa.eu/media/39917/a-new-strategic-agenda-2019-2024-hu.pdf

[2] Az intézkedésekről áttekintést nyújt a „Biztonsági unió – a védelmet nyújtó Európa" című tájékoztató (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_hu.pdf), valamint a hatékony és valódi biztonsági unió megvalósításáról szóló tizennyolcadik eredményjelentés (COM(2019) 145 final, 2019. március 20.).

keretet hogyan alkalmazzák jelenleg a magán- és az állami szektorban;

- beszámol a biztonsági unióra vonatkozó jogalkotási intézkedések végrehajtása terén 2019 márciusa óta megvalósított előrelépésről[3] – e tekintetben elsődleges prioritást élvez, hogy a tagállamok mielőbb teljes körűen megvalósítsák az információs rendszerek interoperabilitását;
- számot ad a dezinformációval szembeni fellépés terén és a választások kiberalkalmas fenyegetésekkel szembeni védelme érdekében tett folyamatos erőfeszítésekről, a biztonsági fenyegetésekkel szembeni felkészültség és védelem javítására irányuló munkáról, valamint a nemzetközi partnerekkel a biztonsági kérdésekben folytatott együttműködésről.

II. A JOGALKOTÁSI PRIORITÁSOK TERÉN TETT ELŐRELÉPÉSEK

1. A radikalizálódás megelőzése az interneten és a közösségekben

A terrorizmusra való uniós reagálás központi eleme a radikalizálódás megelőzése, mind az interneten, mind pedig közösségeinkben.

Az új-zélandi Christchurch városában 2019. március 15-én elkövetett rettenetes merénylet sokkoló figyelmeztetés, hogy milyen módon használhatják fel az internetet a terroristák a céljaik megvalósítására, függetlenül attól, hogy a dzsihádizmus, a szélsőjobboldali vagy más szélsőséges ideológiák motiválják őket. A christchurchi merénylet élő videóközvetítésének az online platformokon való széles körű és gyors terjedése rámutatott annak alapvető jelentőségére, hogy az online platformokon megfelelő intézkedésekkel kell gátat vetni az ilyen tartalmak gyors terjedésének.

Erre reagálva egyes tagállamok és harmadik országok állam- és kormányfői Juncker elnökkel és online platformokkal együtt 2019. május 15-én támogatták az internetes terrorista és erőszakos szélsőséges tartalmak felszámolására irányuló közös lépéseket meghatározó „**Christchurchi cselekvési felhívást**”[4]. A G7-ek[5] és a G20-ak[6] további kötelezettségvállalásokat tettek e tekintetben.

A Bizottság már foglalkozott az online terrorista tartalmak jelentette egyértelmű és fennálló veszély elhárításával azon **jogalkotási javaslat** révén, amelyet Juncker elnök az Unió helyzetét értékelő 2018. évi beszédében jelentett be. E javaslat egyértelmű és harmonizált jogi keretet határoz meg abból a célból, hogy megakadályozzák a tárhelyszolgáltatásoknak az online terrorista tartalom terjesztésére való felhasználását[7]. Az előterjesztett intézkedések kötelezővé tennék az online platformok számára, hogy a terrorista tartalmat egy órán belül eltávolítsák azt követően, hogy bármely tagállam illetékes hatóságától erre vonatkozó eltávolítási végzést kapnak. Emellett abban az esetben, ha egy platformot terrorista tartalom terjesztésére használnak fel, a platformnak kötelező lenne proaktív intézkedéseket tennie az érintett tartalom kiszűrése és újbóli felbukkanásának megakadályozása érdekében, egyértelmű szabályokat és biztosítékokat alkalmazva. A tagállami hatóságoknak a javaslat értelmében külön bűnüldözési kapacitásokat kellene biztosítaniuk e célra, a terrorista tartalom hatékony kiszűrését és az eltávolítási végzések kiadását lehetővé tevő erőforrásokkal együtt.

---

[3] Lásd a tizennyolcadik eredményjelentést a hatékony és valódi biztonsági unió megvalósításáról (COM(2019) 145 final, 2019. március 20.).

[4] https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. A vezetőket és az online platformokat Emmanuel Macron francia elnök és Jacinda Ardern új-zélandi miniszterelnök hívta meg Párizsba, hogy 2019. május 15-én elindítsák ezt a kezdeményezést.

[5] https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

[6] A G20-csoport 2019. június 28–29-i találkozóján a vezetők ismét megerősítették azon elkötelezettségüket, hogy fellépnek annak érdekében, hogy megvédjék az embereket az internet lehetőségeit kihasználó terrorizmust ösztönző terrorista és erőszakos szélsőségességgel szemben (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

[7] COM(2018) 640 final (2018. szeptember 12.).

Ez gyors és hatékony uniós szintű rendszer kialakítását teszi majd lehetővé, és erőteljes biztosítékokat vezet be, többek között hatékony panasztételi mechanizmusokat és a bírósági jogorvoslat lehetőségét. A javasolt intézkedések hozzájárulnak a digitális egységes piac zavartalan működésének garantálásához, miközben fokozzák a biztonságot és javítják a bizalmat az interneten, valamint megerősítik a véleménynyilvánítás és a tájékozódás szabadságának biztosítékait.

A Tanácsban a bel- és igazságügyi miniszterek 2018 decemberében általános megközelítést fogadtak el a javaslatra vonatkozóan. Az Európai Parlament első olvasatban 2019 áprilisában fogadta el álláspontját. **A Bizottság felkéri mindkét társjogalkotót, hogy mielőbb kezdjék meg az intézményközi tárgyalásokat az online terrorista tartalom eltávolítására vonatkozó kiemelt kezdeményezésről** annak érdekében, hogy gyorsan megállapodjanak egy világos szabályokról és biztosítékokról rendelkező uniós szabályozási keretről.

Ezzel párhuzamosan a Bizottság tovább folytatja az együttműködést az online platformokkal az **uniós internetfórum** [8]keretében. Amint ezt Juncker elnök a „Christchurchi cselekvési felhívásról" szóló, 2019. május 15-i párizsi megbeszélésen bejelentette, a Bizottság az Europollal együttműködésben megkezdte egy **uniós válsághelyzeti protokoll** kidolgozását, amely lehetővé tenné, hogy a kormányok és az online platformok gyorsan és összehangoltan reagáljanak az online terrorista tartalom terjesztésére, például közvetlenül egy terrorista merénylet után. Ez a munka a „Christchurchi cselekvési felhívás" végrehajtására irányuló nemzetközi erőfeszítések részét képezi. A tagállamokkal és az ágazattal folytatott további megbeszélések és egy 2019 szeptemberére tervezett, vészhelyzetet szimuláló gyakorlat mellett a Bizottság az uniós válságprotokoll jóváhagyása céljából 2019. október 7-én az uniós internetfórum keretében miniszteri értekezletet hív össze.

A Bizottság emellett továbbra is **támogatja a tagállamokat és a helyi szereplőket** Európa-szerte **a radikalizálódás megelőzése és leküzdése** érdekében gyakorlati szinten, a helyi közösségekben végzett munkájukban. Ehhez olyan hosszú távú, fenntartható erőfeszítésekre van szükség, amelyekben az összes érintett helyi, nemzeti és uniós szintű szereplő részt vesz. A **radikalizálódás megelőzését és leküzdését célzó uniós tevékenységek irányítóbizottsága** 2018 augusztusában jött létre azzal a céllal, hogy tanácsot nyújtson a Bizottságnak arról, hogyan erősíthető meg a területre vonatkozó uniós szakpolitikai válasz. Az irányítóbizottság 2019. június 17-én tartotta második ülését, hogy feltárja, milyen további fellépésekre van lehetőség olyan kiemelt területeken, mint a börtönökben zajló radikalizálódás és a szélsőséges ideológiák visszaszorítása. Mivel gyakran a gyakorlati és helyi szakemberek vannak a legjobb helyzetben ahhoz, hogy észleljék a radikalizálódás első figyelmeztető jeleit és meghatározzák, hogyan lehet fellépni ezekkel szemben, az EU által finanszírozott**uniós radikalizálódástudatossági hálózat**[9] továbbra is támogatja e szakembereket, kapcsolatot hozva létre mintegy 5000 civil társadalmi szereplő, iskolában vagy rendőrségnél dolgozó személy, valamint nemzeti koordinátor és politikai döntéshozó között.

A gyakorlati szakemberek által az utóbbi időszakban a hálózat keretében folytatott együttműködés a szélsőjobboldali szélsőségesség kihívásainak alaposabb megértését eredményezte. Az uniós radikalizálódástudatossági hálózat idén tájékoztatókat ad ki, hogy segítséget nyújtson a szakpolitikai döntéshozóknak és a gyakorlati szakembereknek a szélsőjobboldali és az iszlamista szélsőségesség

---

[8] A 2015-ben indított **uniós internetfórum** keretében az uniós tagállamok belügyminiszterei, az internetes ágazat és más érdekelt felek önkéntes partnerségben együttműködnek annak érdekében, hogy fellépjenek az internet terrorista csoportok általi visszaélésszerű felhasználásával szemben és a polgárok védelme érdekében.

[9] A Bizottság 2011-ben hozta létre az **uniós radikalizálódástudatossági hálózatot** abból a célból, hogy összefogja a gyakorlati és helyi szakembereket. 2015-ben a Bizottság megerősítette a hálózatot az uniós radikalizálódástudatossági hálózat kiválósági központjának létrehozásával, hogy az célzottabb iránymutatást, támogatást és tanácsadási szolgáltatást dolgozzon ki a tagállami érdekelt felek számára, és fejlessze a különböző szereplők szakértelmét és készségeit. Az uniós radikalizálódástudatossági hálózat tevékenységeiről bővebb tájékoztatás itt található: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

főbb formáinak és megnyilvánulásainak – fő narratívák, nyelv, formák jelképek, tipológiák és stratégiák – azonosításához. Végül pedig a Bizottság olyan radikalizálódás elleni kezdeményezéseket is támogat, amelyeket a **városok** vezetnek, tekintettel arra, hogy a helyi szereplők és városok élen járnak a radikalizálódás megelőzésében és az ellene folytatott küzdelemben. A 2019. február 26-án „Uniós városok a radikalizálódás ellen” címmel Brüsszelben tartott konferenciát követően 2019. július 8-án ült össze először egy olyan kísérleti csoport, amelyben 20 város képviselői vettek részt Strasbourg polgármesterének meghívására azzal a céllal, hogy megerősítsék e területen a bevált gyakorlatok cseréjét és a városok erőfeszítéseit.

Ezzel párhuzamosan folytatódik az a munka, melynek célja támogatni a partnerországokat az esetlegesen terrorizmushoz vezető radikalizálódás megakadályozásában, többek között a börtönökben is.

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

- kezdjék el a tárgyalásokat az **online terrorista tartalom** terjesztésének megakadályozására irányuló jogalkotási javaslatról, hogy gyorsan megállapodjanak egy világos szabályokról és biztosítékokról rendelkező uniós szabályozási keretről.

2. A kiberbiztonság megerősítése

A kiberbiztonság továbbra is a legfontosabb biztonsági kihívások közé tartozik. Az EU jelentős eredményeket[10] ért el a rendszerekre és adatokra irányuló „klasszikus” kiberfenyegetésekkel szembeni fellépés terén az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, 2017. szeptemberi közös közleményben[11] meghatározott intézkedések végrehajtásával. Ezek közé tartozik az uniós kiberbiztonsági jogszabály[12], amely állandó megbízatás formájában megerősíti az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) szerepét, és létrehozza a kiberbiztonsági tanúsítás uniós keretét. A Bizottság ágazatspecifikus követelményekkel is foglalkozott, például az energiaágazatban érvényesítendő kiberbiztonságról szóló, 2019. április 3-án elfogadott ajánlásában[13]. Mindazonáltal a rosszindulatú szereplők különféle célokra és áldozatokra irányuló tevékenységének további fokozódása miatt a kiberbűnözés elleni küzdelem és a kiberbiztonság fokozása továbbra is az uniós fellépés egyik prioritása.

Az Európai Parlamentnek és a Tanácsnak meg kell még állapodnia **az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontra és a nemzeti koordinációs központok hálózatára vonatkozó kiemelt bizottsági kezdeményezésről**[14]. A javaslat célja a kiberbiztonsági technológiai és ipari kapacitások támogatása és az uniós kiberbiztonsági iparág versenyképességének fokozása. 2019 márciusában mindkét társjogalkotó elfogadta tárgyalási megbízatását. Mivel az előző parlamenti ciklus vége előtt nem volt lehetséges lezárni az intézményközi tárgyalásokat, az Európai Parlament első olvasatban hivatalosan elfogadta álláspontját. Eközben a Tanácsban folynak az egyeztetések a tagállamok között, amelyek során különös figyelmet kap a Kiberbiztonsági

[10] További információkat nyújt erről a „Hogyan fokozható az Európai Unió kiberbiztonsága? – Ellenálló képesség, elrettentés, védelem” című tájékoztató: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final (2017. szeptember 13.).

[12] Az uniós kiberbiztonsági jogszabály (a 2019. április 17-i (EU) 2019/881 rendelet) első alkalommal vezet be az egész EU-ra kiterjedő szabályokat a termékek, folyamatok és szolgáltatások kiberbiztonsági tanúsítására vonatkozóan. A kiberbiztonsági jogszabály emellett állandó megbízatás formájában megújítja az Európai Uniós Kiberbiztonsági Ügynökség megbízatását, valamint több erőforrást biztosít az ügynökség számára céljai megvalósításához. A pályázati felhívásról részletesebb információk itt találhatók: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final (2019. április 3.) és SWD(2019) 1240 final (2019. április 3.).

[14] COM(2018) 630 final (2018. szeptember 12.).

Kompetenciaközpont és Hálózat létrehozásáról szóló rendeletjavaslat, valamint az Európai horizont és a Digitális Európa program közötti kapcsolat. **A Bizottság felkéri mindkét társjogalkotót, hogy a kiberbiztonság megerősítése érdekében ismét kezdjék meg és zárják le mielőbb az intézményközi tárgyalásokat e kiemelt javaslatról.**

Eközben a Bizottság továbbra is **támogatja a kutatást és innovációt** a kiberbiztonság terén: a jelenlegi többéves pénzügyi keretben 135 millió EUR-t tesz elérhetővé olyan területekre irányuló projektekre, mint a kritikus infrastruktúrák kiberbiztonsága, az intelligens biztonság és adatvédelem, valamint a kifejezetten a polgárok, valamint a kis- és középvállalkozások számára fejlesztett eszközök[15]. 2019 júliusában a Bizottság az Európai Hálózatfinanszírozási Eszköz program keretében új pályázati felhívást tett közzé, amely 10 millió EUR összegű uniós finanszírozást tesz elérhetővé a hálózati és információs rendszerek biztonságáról szóló irányelvben (a kiberbiztonsági irányelvben)[16] meghatározott kulcsfontosságú szereplők, így a számítógép-biztonsági eseményekre reagáló csoportok, az alapvető szolgáltatásokat nyújtó szereplők (pl. bankok, kórházak, közműszolgáltatók, vasutak, légitársaságok, DNS-szolgáltatók) és a különböző hatóságok számára. Most először az európai kiberbiztonsági tanúsítási hatóságok is pályázhatnak erre a programra annak érdekében, hogy végre tudják hajtani az uniós kiberbiztonsági jogszabályt.

A Tanács 2019 május 17-én **szankciórendszert** fogadott el, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést képeznek az EU és annak tagállamai számára. Az új szankciórendszer részét képezi **az EU kiberdiplomáciai eszköztárának**[17], amely keretet biztosít a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedésekhez[18], lehetővé téve, hogy az EU a közös kül- és biztonságpolitikára vonatkozó intézkedések teljes körét felhasználja a rossz szándékú kibertevékenységek megakadályozására és elhárítására.

Az EU a rendszerekre és adatokra irányuló kiberfenyegetések mellett a **hibrid fenyegetésekkel**[19] kapcsolatos összetett és sokrétű kihívásokkal szemben is fellép. Az Európai Tanács 2019. június 21-i következtetéseiben[20] kiemelte, hogy *„az EU-nak biztosítania kell, hogy a hibrid fenyegetésekre és a kiberfenyegetésekre koordinált választ adjon, és meg kell erősítenie a releváns nemzetközi szereplőkkel való együttműködését”.* A Bizottság örömmel fogadja, hogy a hibrid fenyegetésekkel szembeni fellépést a Tanács finn elnöksége is prioritásként határozza meg, valamint azt, hogy a bel- és igazságügyi miniszterek 2019. július 18–19-i nem hivatalos ülésén forgatókönyv-alapú szakpolitikai megbeszélést folytattak a hibrid fenyegetésekről. Az uniós védelempolitikai igazgatók 2019. július 7–8-án, az uniós politikai igazgatók pedig 2019. július 9–10-én hasonló forgatókönyv-alapú megbeszélést tartottak a hibrid fenyegetésekről, és e megbeszélések eredményeiről beszámolnak majd a külügy- és védelmi minisztereknek egy 2019. augusztus 29–30-án megrendezésre kerülő közös informális megbeszélésen.

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 (EU) 2016/1148 irányelv (2016. július 6.).

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf

18 E tevékenységek magukban foglalják a kibertámadásokat és a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is, amelyek például információs rendszerekhez való hozzáféréssel vagy digitális infrastruktúra – például 5G hálózatok – felhasználásával történő adatkifürkészéssel járnak.

19 Lásd a hibrid fenyegetésekkel szembeni fellépésre vonatkozó 2016. évi közös keret, valamint a reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítéséről szóló 2018-as közös közlemény végrehajtásáról szóló jelentést (SWD(2019) 200 final, 2019. május 28.). Lásd továbbá a kettős felhasználású termékek kivitelére, transzferjére, tranzitjára, az azokkal végzett brókertevékenységre és az azokkal kapcsolatos műszaki támogatásra vonatkozó uniós ellenőrzési rendszer kialakításáról szóló rendeletre (átdolgozás) irányuló 2016. szeptemberi jogalkotási javaslatot (COM (2016) 616 final, 2016. szeptember 28.).

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

A kiberbiztonság növelése érdekében a Bizottság a következőkre 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**.

3. A bűnüldöző hatóságok elektronikus bizonyítékokhoz való hozzáférésének javítása

Az EU további intézkedéseket tett annak érdekében, hogy megfossza a terroristákat és a bűnözőket a tevékenységüket szolgáló eszközöktől, megnehezítve számukra a robbanóanyag-prekurzorokhoz való hozzáférést[21], tevékenységeik finanszírozását[22], valamint az észrevétlen mozgást[23].

A bűnüldöző hatóságok **elektronikus bizonyítékokhoz való hozzáférésének** javítására irányuló 2018. áprilisi bizottsági javaslatokról folyó tárgyalásokat mielőbb le kell zárni – jelenleg a nyomozások több mint fele esetében határon átnyúló megkeresést indítanak az elektronikus bizonyítékokhoz való hozzáférés érdekében[24]. A Tanács elfogadta tárgyalási álláspontját a bűnügyi nyomozások során felhasznált elektronikus bizonyítékok határon átnyúló hozzáférésének javításáról szóló rendeletre[25], valamint a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról szóló irányelvre[26] irányuló javaslatokról. Mivel a határokon átnyúló bűncselekményekre – például a terrorizmusra vagy a számítástechnikai bűnözésre – irányuló nyomozás és bűnvádi eljárás során rendkívül fontos az elektronikus bizonyítékokhoz való hatékony hozzáférés, a Bizottság sürgeti, hogy az Európai Parlament tegyen előrelépést e javaslat tekintetében annak érdekében, hogy a társjogalkotók együttműködésével mielőbb el lehessen fogadni azt.

A Bizottság ezzel párhuzamosan az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményének második kiegészítő jegyzőkönyvéről zajló tárgyalások, valamint az Egyesült Államokkal folytatott tárgyalások keretében azon dolgozik, hogy javítsa és garantálja **az elektronikus bizonyítékok nemzetközi cseréjére** vonatkozó szükséges biztosítékokat, összhangban a Tanácstól a Bel- és Igazságügyi Tanács 2019. június 6–7-i ülésén kapott tárgyalási megbízatásokkal[27]. A Bizottság 2019. július 9–11-én részt vett az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményének második kiegészítő jegyzőkönyvéről zajló tárgyalások legutóbbi fordulóján. A Bizottság és az Egyesült Államok jelenleg technikai szintű előkészületeket tesznek az EU és az Egyesült Államok között az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésről kialakítandó megállapodásra irányuló tárgyalások hivatalos elindítására.

---

21 (EU) 2019/1148 rendelet (2019. június 20.) a robbanóanyag-prekurzorok forgalmazásáról és felhasználásáról.

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

23 (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.

24 A nyomozások mintegy 85 %-ában elektronikus bizonyítékokra van szükség, és e nyomozások kétharmada esetében más joghatóság területén letelepedett online szolgáltatóktól kell bizonyítékot bekérni. Lásd a jogalkotási javaslatot kísérő hatásvizsgálatot (SWD(2018) 118 final (2018. április 17.)).

25 COM(2018) 225 final (2018. április 17.). A Tanács a Bel- és Igazságügyi Tanács 2018. december 7-i ülésén elfogadta a javasolt rendeletre vonatkozó tárgyalási megbízatását.

26 COM(2018) 226 final (2018. április 17.). A Tanács a Bel- és Igazságügyi Tanács 2019. március 8-i ülésén elfogadta a javasolt irányelvre vonatkozó tárgyalási álláspontját.

27 https://www.consilium.europa.eu/hu/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

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

- fogadja el az **elektronikus bizonyítékokkal** kapcsolatos jogalkotási javaslatokra vonatkozó tárgyalási megbízatását annak érdekében, hogy haladéktalanul megkezdje a háromoldalú egyeztetéseket a Tanáccsal. *(Az együttes nyilatkozatban meghatározott prioritás)*

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

Nem sokkal azután, hogy elfogadásra kerültek **az információs rendszerek interoperabilitására**[28] vonatkozó szabályok, amelyek megszüntetik az információs hézagokat és a fehér foltokat azáltal, hogy elősegítik a többszörös személyazonosságok felderítését és a személyazonossággal való visszaélés elleni küzdelmet, a Bizottság több kezdeményezést indított annak érdekében, hogy támogassa a tagállamokat a végrehajtási folyamatban, többek között szükség esetén finanszírozással, valamint a szakismeretek és a bevált gyakorlatok cseréjét elősegítő műhelytalálkozók révén. Kiemelten fontos az uniós ügynökségekkel, valamennyi tagállammal és a schengeni társult országokkal való szoros együttműködés ahhoz, hogy 2020-ig megvalósuljon a biztonsági, határigazgatási és migrációkezelési uniós információs rendszerek közötti teljes körű interoperabilitás elérésének ambiciózus célkitűzése.

E cél eléréséhez az is szükséges, hogy gyors ütemben és teljes körűen végrehajtsák azokat a nemrég elfogadott jogszabályokat, amelyek új információs rendszerek – az uniós határregisztrációs rendszer[29] és az Európai Utasinformációs és Engedélyezési Rendszer[30] – kialakítására, valamint a Schengeni Információs Rendszer megerősítésére[31] és az Európai Bűnügyi Nyilvántartási Információs Rendszer harmadik országbeli állampolgárokra való kiterjesztésére[32] irányulnak. A határigazgatás és a migrációkezelés területén használt információs rendszerek szilárdabbá és intelligensebbé tételére irányuló új szerkezet csak akkor fog a gyakorlatban is érzékelhető eredményt hozni, ha annak minden elemét az elfogadott ütemtervnek megfelelően teljes körűen végrehajtják uniós szinten és minden egyes tagállamban.

Emellett a társjogalkotóknak is további lépéseket kell tenniük, hogy lezárják a biztonság, a határigazgatás és a migrációkezelés területén használt információs rendszerek szilárdabbá és intelligensebbé tételére irányuló munkát.
Az **Európai Utasinformációs és Engedélyezési Rendszer** technikai megvalósításának részeként a Bizottság 2019. január 7-én két javaslatot terjesztett elő, amelyek meghatározzák a vonatkozó rendeletnek[33] a rendszer teljes körű kialakításához szükséges technikai módosításait. A Bizottság felkéri a társjogalkotókat, hogy gyorsítsák fel az említett technikai jellegű módosításokkal kapcsolatos munkájukat annak érdekében, hogy mihamarabb megállapodást érjenek el, lehetővé téve ezáltal az Európai Utasinformációs és Engedélyezési Rendszer gyors és időben történő megvalósítását, és azt, hogy a rendszer 2021 elejére működőképessé váljon.

A Bizottság 2018 májusában javaslatot terjesztett el **a meglévő Vízuminformációs Rendszer megerősítésére**[34], előírva a vízumkérelmezők alaposabb háttérellenőrzését, valamint a biztonsági információs hézagoknak a tagállamok közötti jobb információcsere révén történő megszüntetését. A Tanács 2018. december 19-én elfogadta tárgyalási megbízatását, az Európai Parlament pedig 2019. március 13-án megszavazta a javaslatról szóló jelentését, lezárva ezzel annak első olvasatát. A

28 (EU) 2019/817 rendelet (2019. május 20.) és (EU) 2019/818 rendelet (2019. május 20.).
29 (EU) 2017/2226 rendelet (2017. november 30.).
30 (EU) 2018/1240 rendelet (2018. szeptember 12.) és (EU) 2018/1241 rendelet (2018. szeptember 12.).
31 (EU) 2018/1860 rendelet (2018. november 28.), (EU) 2018/1861 rendelet (2018. november 28.), (EU) 2018/1862 rendelet (2018. november 28.).
32 (EU) 2019/816 rendelet (2017. április 17.).
33 COM(2019) 3 final és COM(2019) 4 final (2019. január 7.).
34 COM(2018) 302 final (2018. május 16.).

Bizottság szorgalmazza, hogy az induló új európai parlamenti ciklusban gyorsan kezdjék meg a társjogalkotók közötti tárgyalásokat.

A Bizottság 2016 májusában javaslatot tett az **Eurodac**[35] hatályának oly módon történő kibővítésére, hogy az ne csak a menedékkérők azonosítására, hanem a jogellenesen tartózkodó harmadik országbeli állampolgárok és az EU területére szabálytalanul belépő személyek azonosítására is kiterjedjen. Az Európai Tanács 2018. decemberi következtetéseivel[36] és az európai migrációs stratégia végrehajtására vonatkozó eredményjelentésről szóló, 2019. március 6-i bizottsági közleménnyel[37] összhangban, a Bizottság felkéri a társjogalkotókat, hogy fogadják el a javaslatot. E jogalkotási javaslat elfogadása szükséges ahhoz, hogy az Eurodac az interoperábilis uniós információs rendszerek jövőbeni szerkezetének részévé váljon, ezáltal integrálva a jogellenesen tartózkodó harmadik országbeli állampolgárokra és az EU területére szabálytalanul belépő személyekre vonatkozó, alapvető fontosságú adatokat.

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

- fogadják el az **Eurodacról** szóló jogalkotási javaslatot *(az együttes nyilatkozatban meghatározott prioritás)*;
- gyorsítsák fel a munkát annak érdekében, hogy mielőbb megállapodásra jussanak **az Európai Utasinformációs és Engedélyezési Rendszer** létrehozásához szükséges, javasolt technikai módosításokról.

III. A DIGITÁLIS INFRASTRUKTÚRÁK BIZTONSÁGÁNAK JAVÍTÁSA

Digitális infrastruktúráink ellenálló képessége alapvető fontosságú a kormányok, vállalkozások, a személyes adataink védelme és a demokratikus intézményeink működése szempontjából. Az elkövetkező években alkalmazásra kerülő **ötödik generációs (5G) hálózatok** fogják képezni társadalmaink és gazdaságaink alapvető digitális struktúráit a jövőben, hiszen több milliárd felhasználót, tárgyat és rendszert kötnek majd össze többek között olyan létfontosságú ágazatokban, mint az energetika, a közlekedés, a banki szolgáltatások és az egészségügy, valamint ezek a hálózatok fogják biztosítani a kapcsolatot a bizalmas információkkal dolgozó és a biztonsági rendszereket támogató ipari ellenőrzési rendszerek esetében is.

Mivel az 5G-nek köszönhető várható bevételek összege 2025-re a becslések szerint eléri a 225 milliárd EUR-t, nyilvánvaló, hogy az 5G technológia kulcsfontosságú szerepet tölt be Európa globális versenyképessége szempontjából, és **az 5G hálózatok biztonsága alapvetően fontos az Unió stratégiai autonómiájának biztosításához**. A magas szintű kiberbiztonság garantálásához nemzeti és uniós szinten is összehangolt intézkedéseket kell tenni, mivel ha a tagállamok valamelyikében sebezhető pontjai vannak az 5G hálózatoknak, az az Unió egészére nézve következményekkel jár.

Miután az állam-, illetve kormányfők az Európai Tanács 2019. márciusi ülésén támogatásuknak adtak hangot[38], a Bizottság 2019. március 26-án előterjesztette **az 5G hálózatok kiberbiztonságáról szóló ajánlást**[39], amelyben intézkedéseket javasolt az 5G hálózatokat érintő kiberbiztonsági kockázatok felmérésére, valamint a megelőző intézkedések hatékonyságának növelésére. Az ajánlások összehangolt uniós kockázatértékelési és kockázatkezelési intézkedésekre, az együttműködés és információcsere hatékony keretére, valamint a kritikus kommunikációs infrastruktúrát lefedő közös uniós helyzetismeretre épülnek.

35 COM(2016) 272 final (2016. május 4.).
36 https://www.consilium.europa.eu/hu/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final (2019. március 6.).
38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/hu/pdf
39 C(2019) 2335 final (2019. március 26.).

Az ajánlásban kezdeményezett eljárás **első szakaszaként** 2019. július 15-ig minden tagállam elvégezte **nemzeti kockázatértékelését**, és ezek eredményét benyújtotta a Bizottságnak és az Európai Uniós Kiberbiztonsági Ügynökségnek, illetve jelezte, hogy hamarosan benyújtja ezeket. A nemzeti kockázatértékelések elkészítése során meghatározott iránymutatásokat és az eredményekről való beszámoló közös sablonját követték, amelyet a tagállamok és a Bizottság azért fogadtak el, hogy elősegítsék az egységességet és megkönnyítsék a nemzeti eredményekről uniós szinten folytatott információcserét. Az összes tagállam által vizsgált paraméterek magukban foglalták a következőket:

- az 5G hálózatokat érintő fő fenyegetések és a fenyegetést jelentő szereplők;
- az 5G hálózati alkatrészek és funkciók, illetve az egyéb eszközök érzékenységének mértéke; valamint
- különböző típusú sebezhetőségek, ideértve a műszaki jellegű és egyéb típusú – például az 5G ellátási láncából eredő – sebezhetőségeket.

A nemzeti kockázatértékelések elkészítésében számos tagállami felelős szereplő, többek között – a tagállami felelősségi köröktől függően – a kiberbiztonsági és távközlési hatóságok, valamint a biztonsági és hírszerző szolgálatok képviselői is részt vettek, ami az említett szervezetek közötti együttműködést és koordinációt is javította. Az 5G kiépítésének nemzeti ütemterveivel párhuzamosan és azokat figyelembe véve több tagállam már tett lépéseket az e területen alkalmazandó biztonsági követelmények megerősítése érdekében, számos további tagállam pedig jelezte, hogy a közeljövőben új intézkedéseket szándékozik mérlegelni.

A nemzeti kockázatértékelés eredményei alapján a tagállamok kiberbiztonság hatóságai a hálózati és információs rendszerekkel foglalkozó együttműködési csoport[40] keretében 2019. október 1-jéig elkészíti **az uniós szintű kockázatok közös áttekintését** – ez fogja képezni az ajánlásban kezdeményezett eljárás második szakaszát. Erre alapozva a harmadik szakaszban az együttműködési csoport a feltárt kockázatok kezelése érdekében 2019. december 31-ig kidolgoz egy **közös uniós kockázatcsökkentő intézkedéscsomagot**. A Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség továbbra is támogatni fogja az ajánlás végrehajtását.

A hálózati és információs rendszerekkel foglalkozó együttműködési csoportban folyó munkát számos egyéb fórum támogatja. Az Európai Elektronikus Hírközlési Szabályozók Testülete felmérést készít az összes olyan meglévő biztonsági intézkedésről, amelynek az 5G szempontjából jelentősége lehet. Az Európai Uniós Kiberbiztonsági Ügynökségen belül új, külön e célból létrehozott szakértői csoport kezdett dolgozni az 5G hálózatok fenyegetettségi helyzetének felülvizsgálatán. Emellett a kiberbiztonsági jogszabály 2019. június 27-i hatálybalépése nyomán a Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség meg fogja tenni az ahhoz szükséges lépéseket, hogy létrejöjjön egy, az EU egészére kiterjedő tanúsítási keretrendszer. A tagállamok 2019 júniusában a szabványügyi bizottságon belül is megbeszélést tartottak a kiberbiztonságról és a szabványosításról, reagálva az ajánlásra, amely szorgalmazta a kiberbiztonság területére vonatkozó szabványosítás – és ezen belül többek között az 5G hálózatok – előtt álló jövőbeli kihívások és a megfelelő uniós szintű szakpolitikai kezdeményezések lehetőségeinek feltárását.

Végül pedig az 5G hálózatok biztonsága stratégiai jelentőséggel is bír az Unió számára. A stratégiai ágazatokba irányuló külföldi beruházások, a kritikus eszközök, technológiák és infrastruktúra

[40] A hálózati információk biztonságával foglalkozó együttműködési csoport a hálózati és információs rendszerek biztonságáról szóló, 2016. július 6-i (EU) 2016/1148 irányelv alapján jött létre. Az ajánlás rendelkezéseinek megfelelően a hálózati információk biztonságával foglalkozó együttműködési csoporton belül több tagállam vezetésével kialakítottak egy külön munkafolyamatot. A csoport már három alkalommal – 2019 áprilisában, májusában, illetve júliusában – ülésezett azzal a céllal, hogy megosszák a nemzeti megközelítésekkel kapcsolatos információkat, valamint megvitassák, hogy milyen módon segíthetik az uniós szintű összehangolt kockázatértékelés elkészítését.

felvásárlása az EU-ban, valamint a kritikus berendezések beszállítása is kockázatot jelenthetnek az EU biztonságára.

2019. április 10-én hatályba lépett **a közvetlen külföldi tőkebefektetések átvilágításáról szóló új uniós keret**[41]. Az elkövetkező 18 hónapban a Bizottság és a tagállamok megteszik a szükséges lépéseket annak érdekében, hogy az EU 2020. október 11-jétől teljes mértékben alkalmazni tudja a tőkebefektetések átvilágításáról szóló rendeletet.

IV. A PÉNZMOSÁS ELLENI KÜZDELEM

Ha a bűnelkövetők és a terroristák akár órákon belül képesek pénzt átutalni a különböző bankszámlákra, könnyebben tudják előkészíteni terrorcselekményeiket vagy tisztára mosni a bűncselekményből származó jövedelmet a tagállami határoktól függetlenül. E kihívás kezelésére az Unió a Pénzügyi Akció Munkacsoport által elfogadott nemzetközi standardokkal összhangban kialakította **a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem szilárd szabályozási keretét**.

Tekintettel arra, hogy lépést kell tartani az alakuló trendekkel, a technológiai fejlődéssel, valamint a bűnözők alkalmazkodóképes találékonyságával, amellyel kihasználják a rendszer bármiféle hiányosságait vagy hézagjait, a Bizottság 2019. július 24-én **négy jelentést magában foglaló csomagot** fogadott el, amelyek elemzik a pénzmosással kapcsolatos jelenlegi kockázatokat és sebezhető pontokat, valamint értékelik, hogy a vonatkozó uniós szabályozási keretet hogyan alkalmazzák jelenleg a magán- és az állami szektor érintett szereplői[42].

E csomag magában foglalja az EU-n belüli **nemzeti központi bankszámla-nyilvántartások és adat-visszanyerési rendszerek esetleges összekapcsolásának értékelését** is. E nemzeti központi rendszerek lehetővé teszik bármely olyan természetes vagy jogi személy azonosítását, aki fizetési számlával, bankszámlával vagy széffel rendelkezik vagy ilyenek felett ellenőrzést gyakorol – ezek az információk gyakran döntő jelentőségűek az illetékes hatóságok számára a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem során. Az ötödik pénzmosási irányelv[43] rendelkezései szerint a tagállamoknak ki kell alakítaniuk ilyen nemzeti központi rendszereket, és biztosítaniuk kell az ilyen rendszerekhez való közvetlen hozzáférést nemzeti pénzügyi információs egységeik számára. A pénzügyi információknak a súlyos bűncselekményekkel szembeni fellépés céljából történő felhasználásának megkönnyítése érdekében nemrég elfogadott szabályok[44] közvetlen hozzáférést biztosítanak a kijelölt bűnüldöző hatóságok és vagyon-visszaszerzési hivatalok számára a bankszámlákra vonatkozó adott nemzeti központi nyilvántartásokhoz. Erre alapozva és a pénzmosási irányelv rendelkezéseinek megfelelően a jelentés értékeli azokat a különböző, már működő vagy fejlesztés alatt álló uniós szintű informatikai megoldásokat, amelyek modellként szolgálhatnak a

[41] (EU) 2019/452 rendelet (2019. március 19.) az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról. Az új keret olyan együttműködési mechanizmust hoz létre, amelynek keretében a tagállamok és a Bizottság információkat cserélhetnek, illetve aggályokat vethetnek fel az egyes befektetésekkel kapcsolatban. Emellett lehetővé teszi a Bizottság számára, hogy véleményt fogalmazzon meg, ha egy befektetés egynél több tagállam biztonságát vagy közrendjét fenyegeti, vagy ha a befektetés hátrányosan érinthet valamely, az Unió egészének érdekét szolgáló projektet vagy programot. A befektetés kezeléséről a végső döntést az a tagállam hozza meg, ahol a befektetés végbemegy.

[42] A belső piacot érintő és a határokon átnyúló tevékenységekhez kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázatok értékeléséről szóló jelentés (COM (2019) 370 final, 2019. július 24.), a nemzeti központi automatizált mechanizmusok (központi nyilvántartások és a központi elektronikus adat-visszanyerési rendszerek) összekapcsolásáról szóló jelentés ((COM(2019) 372 final, 2019. július 24.), az uniós hitelintézeteket érintő közelmúltbeli állítólagos pénzmosási ügyek értékeléséről szóló jelentés ((COM(2019) 373 final, 2019. július 24.), és a pénzügyi információs egységek közötti együttműködés keretének értékeléséről szóló jelentés (COM(2019) 371 final, 2019. július 24.).

[43] (EU) 2015/849 irányelv (2015. május 20.).

[44] (EU) 2019/1153 irányelv (2019. június 20.).

nemzeti központi rendszerek lehetséges összekapcsolásához. Mivel a központi mechanizmusok jövőbeli uniós szintű összekapcsolása felgyorsítaná a pénzügyi információkhoz való hozzáférést és megkönnyítené az illetékes hatóságok határokon átnyúló együttműködését, a Bizottság további konzultációkat kíván folytatni az érintett érdekelt felekkel, kormányokkal, valamint a pénzügyi információs egységekkel, a bűnüldöző hatóságokkal és a vagyon-visszaszerzési hivatalokkal, mint a lehetséges összekapcsolási rendszer potenciális végfelhasználóival.

A pénzügyi információs egység munkájára vonatkozó bizottsági elemző munka részeként **a pénzügyi információs egységek közötti együttműködés** értékeléséről készült jelentés egyaránt vizsgálja az Unión belüli és a harmadik országokkal folytatott együttműködést[45]. A jelentés azonosít bizonyos hiányosságokat, amelyek valószínűsíthetően mindaddig fenn fognak állni, amíg a pénzmosás és a terrorizmusfinanszírozás elleni küzdelemre vonatkozó uniós jogi keret nem határozza meg egyértelműbben a pénzügyi információs egységek feladatait és határokon átnyúló együttműködési kötelezettségeit. Az értékelés arra is rámutat, hogy erőteljesebb mechanizmusra van szükség a határokon átnyúló együttműködés és elemzés összehangolásához és támogatásához.

A pénzmosással és a terrorizmusfinanszírozással szembeni fellépésre irányuló eddigi erőfeszítéseken túlmenően, és egyúttal az Európai Parlament felkérésére[46] is reagálva a Bizottság folytatja a terrorizmusfinanszírozás Unión belüli felderítésére irányuló esetleges további intézkedések szükségességének, technikai megvalósíthatóságának és arányosságának vizsgálatát.[47]

V. A BIZTONSÁGGAL KAPCSOLATOS TOVÁBBI KIEMELT KEZDEMÉNYEZÉSEK VÉGREHAJTÁSA

1. A biztonsági unió jogalkotási intézkedéseinek végrehajtása

A biztonsági unió keretében végrehajtandó intézkedésekről való megállapodás nem jelenti az eljárás végét – az ezektől várható előnyök csak akkor valósulnak meg maradéktalanul, ha ezt követően biztosítjuk a rendelkezések gyors és teljes körű tagállami végrehajtását. A Bizottság ezért tevékenyen támogatja a tagállamokat, többek között finanszírozás és a bevált módszerek cseréjének elősegítése révén.
A Bizottság ugyanakkor készen áll arra, hogy szükség esetén teljes mértékben éljen a Szerződések által az uniós jog érvényesítéséhez ráruházott hatáskörökkel, ideértve megfelelő esetekben a kötelezettségszegési eljárást is.

Az **uniós utas-nyilvántartási adatállományról szóló irányelv**[48] végrehajtásának határideje 2018. május 25-én lejárt. Eddig 25 tagállam jelentette be a Bizottságnak, hogy ezt teljes körűen átültette[49]. A teljes körű átültetés két tagállamban még mindig nem valósult meg, a 2018. július 19-én indított kötelezettségszegési eljárások ellenére sem[50]. 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.

---

45 Ezt az értékelést az ötödik pénzmosási irányelv (a 2018. május 20-i (EU) 2018/843 irányelv) 65. cikkének (2) bekezdése írja elő.

46 Az Európai Parlament terrorizmussal foglalkozó különbizottsága 2018 decemberében elfogadott zárójelentésében sürgette a terrorizmus finanszírozásának felderítésére szolgáló európai uniós rendszer létrehozását, amely a terrorizmussal összefüggésbe hozható személyeknek az egységes eurófizetési térségen belüli tranzakcióira és azok finanszírozására irányul.

47 Lásd a tizennyolcadik eredményjelentést a hatékony és valódi biztonsági unió megvalósításáról (COM(2019) 145 final, 2019. március 20.).

48 (EU) 2016/681 irányelv (2016. április 27.).

49 A teljes körű átültetés bejelentésére vonatkozó hivatkozások a tagállamok a tagállamok bejelentéseit veszik figyelembe, és nem érintik a bizottsági szolgálatok által végzett átültetési ellenőrzést.

50 Szlovénia részleges átültetésről tett bejelentést. Spanyolország nem tett bejelentést átültetésről (2019. július 24-i helyzet).

A terrorizmus elleni küzdelemről szóló irányelv[51] átültetésének határideje 2018. szeptember 8-án járt le. Eddig 22 tagállam jelentette be a Bizottságnak, hogy ezt teljes körűen átültette. Három tagállam még mindig nem küldött értesítést az irányelvet hiánytalanul átültető nemzeti jogszabály elfogadásáról, a 2018. november 22-én indított kötelezettségszegési eljárások ellenére sem[52].

A fegyverek megszerzésének és tartásának ellenőrzéséről szóló irányelv átültetésének határideje[53] 2018. szeptember 14-én járt le. Eddig 8 tagállam jelentette be a Bizottságnak, hogy ezt teljes körűen átültette. 20 tagállam még mindig nem küldött értesítést az irányelvet hiánytalanul átültető nemzeti jogszabály elfogadásáról, a 2018. november 22-én indított kötelezettségszegési eljárások ellenére sem[54].

A bűnüldözésben érvényesítendő adatvédelemről szóló irányelvnek[55] a nemzeti jogba való átültetése tekintetében az átültetés határideje 2018. május 6-án járt le. Eddig 20 tagállam jelentette be a Bizottságnak, hogy ezt teljes körűen átültette[56]. 7 tagállam még mindig nem küldött értesítést az irányelvet hiánytalanul átültető nemzeti jogszabály elfogadásáról, annak ellenére, hogy a Bizottság 2018. július 19-én kötelezettségszegési eljárásokat indított[57].

A tagállamoknak 2018. május 9-ig kellett átültetniük nemzeti jogukba a **hálózati és információs rendszerek biztonságáról szóló irányelvet**[58]. Eddig 26 tagállam jelentette be a Bizottságnak, hogy ezt teljes körűen átültette, 2 tagállam pedig az irányelv részleges átültetéséről tett bejelentést[59]. Emellett a tagállamoknak az irányelv értelmében 2018. november 9-ig kellett azonosítaniuk az alapvető szolgáltatásokat nyújtó szereplőket. 2019. május 9-re a Bizottságnak be kellett volna nyújtania egy jelentést az Európai Parlamentnek és a Tanácsnak annak értékeléséről, hogy a tagállamok területén azonosított alapvető szolgáltatásokat nyújtó szereplők azonosítása során alkalmazott megközelítés mennyire volt következetes. Ám mivel eddig az időpontig számos tagállam még nem nyújtott be hiánytalan tájékoztatást az azonosítási eljárásról, a Bizottságnak el kellett halasztania e jelentés elkészítését.

A Bizottság értékeli a **negyedik pénzmosási irányelv**[60] átültetését, miközben azt is ellenőrzi, hogy a tagállamok végrehajtják-e a szabályokat. A Bizottság 24 tagállam ellen kötelezettségszegési eljárást indított, mivel úgy értékelte, hogy a tagállamoktól érkezett bejelentések nem jelentik az irányelv teljes átültetését[61].

---

51 (EU) 2017/541 irányelv (2017. március 15.).

52 Lengyelország részleges átültetéséről tett bejelentést. Görögország és Luxemburg nem tett bejelentést az átültetésről (2019. július 24-i helyzet).

53 (EU) 2017/853 irányelv (2017. május 17.).

54 Belgium, Csehország, Észtország, Litvánia, Lengyelország, Portugália, Svédország és az Egyesült Királyság részleges átültetésről tett bejelentést. Németország, Írország, Görögország, Spanyolország, Ciprus, Luxemburg, Magyarország, Hollandia, Románia, Szlovénia, Szlovákia és Finnország nem tett bejelentést átültetésről (2019. július 24-i helyzet).

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

56 20 tagállam befejezte az átültetést (2019. július 24-i helyzet).

57 Lettország, Portugália, Szlovénia és Finnország részleges átültetésről tett bejelentést. Görögország és Spanyolország nem tett bejelentést átültetésről. Bár Németország teljes átültetésről tett bejelentést, a Bizottság úgy ítéli meg, hogy ez az átültetés nem teljes körű (2019. július 24-i helyzet).

58 (EU) 2016/1148 irányelv (2016. április 27.).

59 Belgium és Magyarország részlegesen átültette az irányelvet (2019. július 24-i helyzet).

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

61 Belgium, Bulgária, Csehország, Dánia, Németország, Észtország, Írország, Spanyolország, Franciaország, Olaszország, Ciprus, Lettország, Litvánia, Magyarország, Hollandia, Ausztria, Lengyelország, Portugália, Románia, Szlovénia, Szlovákia, Finnország, Svédország és az Egyesült Királyság (2019. július 24-i helyzet).

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** esetében 1 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 1 tagállamnak pedig még teljes körűvé kell tennie az átültetésről szóló bejelentést[62];
- a **terrorizmus elleni küzdelemről szóló irányelv** tekintetében 2 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 1 tagállamnak pedig teljes körűvé kell tennie az átültetésről szóló bejelentést[63];
- a **fegyverek megszerzésének és tartásának ellenőrzéséről szóló irányelv** tekintetében 12 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 8 tagállamnak pedig teljes körűvé kell tennie az átültetésről szóló bejelentést[64];
- a **bűnüldözésben érvényesítendő adatvédelemről szóló irányelv** tekintetében 2 tagállamnak kell még bejelentenie a nemzeti jogba való átültetést, 5 tagállamnak pedig teljes körűvé kell tennie az átültetésről szóló bejelentést[65];
- a **hálózati és információs rendszerek biztonságáról szóló irányelv** tekintetében 2 tagállamnak kell még teljes körűvé tennie az átültetésről szóló bejelentést[66]; valamint
- a **negyedik pénzmosási irányelv** tekintetében 24 tagállamnak kell még teljes körűvé tennie az átültetésről szóló bejelentést[67].

2. A dezinformáció elleni küzdelem és a választások egyéb kiberalkalmas fenyegetésekkel szembeni védelme

A demokratikus eljárásoknak és intézményeknek a dezinformációval és más kapcsolódó beavatkozásokkal szembeni védelme világszerte jelentős társadalmi kihívást jelent. E célból az EU **szilárd keretet alakított ki a dezinformációval szembeni összehangolt fellépéshez**, amely teljes mértékben tiszteletben tartja az európai értékeket és az alapvető jogokat[68]. Amint azt a dezinformációval szembeni cselekvési terv végrehajtásáról szóló, 2019. június 14-i közös közlemény[69] kifejti, a számos egymást kiegészítő területen végzett munka hozzájárult a dezinformáció játékterének leszűkítéséhez és az európai parlamenti választások integritásának megőrzéséhez.

Az Európai Tanács 2019. június 21-i következtetéseiben[70] üdvözölte, hogy a Bizottság részletes értékelést kíván végezni **a dezinformáció visszaszorítását célzó gyakorlati kódex**[71] keretében az

62 Szlovénia részleges átültetésről tett bejelentést. Spanyolország nem tett bejelentést átültetésről (2019. július 24-i helyzet).

63 Lengyelország részleges átültetésről tett bejelentést. Görögország és Luxemburg nem tett bejelentést az átültetésről (2019. július 24-i helyzet).

64 Belgium, Csehország, Észtország, Litvánia, Lengyelország, Portugália, Svédország és az Egyesült Királyság részleges átültetésről tett bejelentést. Németország, Írország, Görögország, Spanyolország, Ciprus, Luxemburg, Magyarország, Hollandia, Románia, Szlovénia, Szlovákia és Finnország nem tett bejelentést átültetésről (2019. július 24-i helyzet).

65 Lettország, Portugália, Szlovénia és Finnország részleges átültetésről tett bejelentést. Görögország és Spanyolország nem tett bejelentést átültetésről. Bár Németország teljes átültetésről tett bejelentést, a Bizottság úgy ítéli meg, hogy ez az átültetés nem teljes körű (2019. július 24-i helyzet).

66 Belgium és Magyarország részlegesen átültette az irányelvet (2019. július 24-i helyzet).

67 Belgium, Bulgária, Csehország, Dánia, Németország, Észtország, Írország, Spanyolország, Franciaország, Olaszország, Ciprus, Lettország, Litvánia, Magyarország, Hollandia, Ausztria, Lengyelország, Portugália, Románia, Szlovénia, Szlovákia, Finnország, Svédország és az Egyesült Királyság (2019. július 24-i helyzet).

68 Lásd: Cselekvési terv a félretájékoztatással szemben (JOIN(2018) 36 final, 2018. december 5.).

69 JOIN(2019) 12 final (2019. június 14.).

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf. Az Európai Tanács felhívása a Tanács román elnöksége, valamint a Bizottság és a külügyi és biztonságpolitikai főképviselője által a dezinformációval és a szabad és tisztességes európai választások biztosításával kapcsolatos

online platformok és más aláíró felek által vállalt kötelezettségek végrehajtásáról, továbbá felkérte a Bizottságot és az Unió külügyi és biztonságpolitikai főképviselőjét, hogy gondoskodjanak a folyamatos értékelésről és reagálásról azzal összefüggésben, hogy *„a mesterséges intelligencia és az adatgyűjtési technikák fejlődése miatt változó jellegűek a fenyegetések és növekszik a kockázata a rossz szándékú beavatkozásoknak és az online manipulációnak”*.

A Bizottság és a főképviselő az Európai Tanács következtetéseinek megfelelően folytatja majd az érintett területre irányuló munkáját. 2019 márciusában a Bizottság és a főképviselő az uniós intézmények és tagállamok között létrehozott egy **riasztási rendszert**, hogy könnyebbé váljon a dezinformációs kampányokra vonatkozó ismeretek megosztása és a reagálás összehangolása. Az európai parlamenti választásokat követően a tagállamok kapcsolattartó pontjainak első találkozójára 2019. június 3–4-én került sor Tallinban. A riasztási rendszer további erősítése érdekében a főképviselő és a Bizottság a tagállamokkal szoros együttműködésben 2019 őszén felül fogja vizsgálni a riasztási rendszer működését. Emellett a dezinformációs kampányok elemzését és nyilvánosság elé tárását szolgáló közös módszertan kidolgozására is sor kerül, valamint erőteljesebb partnerségeket alakítunk ki a nemzetközi partnerekkel, így a G7-ekkel és a NATO-val.

Folytatódik a munka az **európai választási együttműködési hálózat**[72] keretében is: az első megbeszélésre 2019. június 7-én került sor az európai parlamenti választások eredményének számbavétele céljából. Ezek az eszmecserék, valamint az érintett nemzeti hatóságoktól, politikai pártoktól és online platformoktól kapott további információk beépülnek majd az európai parlamenti választásokról szóló, 2019 októberében elfogadandó átfogó bizottsági jelentésbe. A tagállamok a hálózatot az európai parlamenti választásokon kívül egyéb választások vonatkozásában is igénybe vették, ami azt jelzi, hogy a hálózat szélesebb körben is hasznos eszköznek bizonyul az EU-n belüli demokrácia integritásának megőrzésére.

A Bizottság emellett továbbra is nyomon követi és előmozdítja a platformok által **a dezinformáció visszaszorítását célzó gyakorlati kódex** keretében vállalt kötelezettségek végrehajtását. A Google, a Twitter és a Facebook által a gyakorlati kódex értelmében benyújtott jelentések azt mutatják, hogy az európai parlamenti választásokra felkészülve valamennyi platform intézkedett annak érdekében, hogy címkézze és a keresőfunkcióval működő, hirdetéseket tartalmazó könyvtárakban nyilvánosan elérhetővé tegye a politikai hirdetéseket. Mindazonáltal az Audiovizuális Médiaszolgáltatásokat Szabályozó Hatóságok Európai Csoportjának megállapításai szerint még van mit javítani[73]. Mindenekelőtt továbbra sem érhetőek el az átfogó ellenőrzéshez szükséges részletes

---

tanulságokra vonatkozóan nyújtott tájékoztatáson, többek között a dezinformációval szembeni cselekvési terv végrehajtásáról szóló közös közleményen alapul.

71 A dezinformáció elleni küzdelem önszabályozási normáit meghatározó gyakorlati kódexet 2018 októberében írták alá olyan online platformok, mint a Facebook, a Google, a Twitter és a Mozilla, valamint a hirdetők és a reklámipar képviselői. A kódex a 2018. áprilisi bizottsági közleményben (COM/2018/236 final, 2018. április 26.) kitűzött célok megvalósítására irányul, és ennek érdekében széles körű kötelezettségvállalásokat határoz meg, amelyek kiterjednek többek közt a politikai hirdetések átláthatóságára, a hamis felhasználói fiókok törlésére és a dezinformáció terjesztői bevételeinek megvonására.

72 Az európai választási együttműködési hálózatban a választási kérdésekben illetékes hatóságokat és a választási környezetet érintő online tevékenységekkel kapcsolatos szabályok nyomon követéséért és érvényesítéséért felelős hatóságokat tömörítő nemzeti választási együttműködési hálózatok kapcsolattartó pontjai vesznek részt. Az európai választási együttműködési hálózat arra szolgál, hogy a fenyegetésekkel kapcsolatos figyelmeztetéseket bocsássanak ki, kicseréljék a nemzeti hálózatok között a bevált módszereket, megvitassák az azonosított kihívásokra vonatkozó közös megoldásokat, valamint ösztönözzék a közös projekteket és gyakorlatokat a nemzeti hálózatok körében.

73 Az Audiovizuális Médiaszolgáltatásokat Szabályozó Hatóságok Európai Csoportja összefogja az audiovizuális szolgáltatások területén működő nemzeti szabályozó hatóságok vezetőit, illetve magas szintű képviselőit, hogy tanácsadást nyújtsanak a Bizottság számára az audiovizuális médiaszolgáltatásokról szóló uniós irányelv (a 2010. március 10-i 2010/13/EU irányelv) végrehajtása terén. A csoport legutóbbi, 2019. június 20-21-i pozsonyi ülésén bemutatta a dezinformációval kapcsolatban végzett eddigi munka

nyers adatok. Végezetül a platformoknak biztosítaniuk kell a kutatóközösség számára az adatokhoz való érdemi hozzáférést, összhangban a személyes adatok védelmére vonatkozó szabályokkal. Ez év második felében a Bizottság átfogó értékelést végez a gyakorlati kódex keretében tett összes kötelezettségvállalásra kiterjedően arról, hogy az első 12 hónap során hogyan valósították meg ezeket. Az értékelés alapján a Bizottság a dezinformációra való hosszú távú uniós reagálás javítása érdekében további, adott esetben szabályozási jellegű intézkedéseket mérlegelhet.

3. Felkészültség és védelem

A hatékony és valódi biztonsági unió megteremtésére irányuló munka egyik fontos eleme a biztonsági fenyegetésekkel szembeni védelem és ellenálló képesség megerősítése. Ez magában foglalja azt, hogy a Bizottság támogatást nyújt a tagállamoknak és azok helyi önkormányzatainak a **nyilvános terek védelmének**[74] megszilárdításához, valamint támogatja a tagállamokat a **vegyi, biológiai, radiológiai és nukleáris biztonsági kockázatokkal** szembeni felkészültség fokozásában[75], többek között a területre irányuló két cselekvési terv végrehajtása révén, valamint annak elemzésével, hogy ezzel kapcsolatban milyen reagálási képességek kifejlesztésére van szükség a rescEU keretében[76]. A jelentkező vegyi fenyegetéseket illetően[77] a Bizottság a tagállamokkal együttműködve és a nemzetközi partnerekkel konzultálva kidolgozta azon vegyi anyagok jegyzékét, amelyek esetében leginkább fennáll a terrorizmus céljából történő visszaélések veszélye. Az uniós jegyzék alapján folytatódik az érintett vegyi anyagok elérhetőségének korlátozására irányuló munka, valamint a gyártókkal a felderítési képességek javítása tekintetében folytatott együttműködés.

A pilóta nélküli légi járművekkel kapcsolatos technológiák a műveletek széles körét teszik lehetővé. A katonai, polgári kereskedelmi és szabadidős célokra használt pilóta nélküli légijármű-rendszerek piacának az elmúlt években bekövetkezett gyors bővüléséből adódóan a **drónok** új lehetőséget kínálnak, de egyúttal egyre fokozódó biztonsági fenyegetést is jelentenek a kritikus infrastruktúra (többek között a légi közlekedés), a nyilvános terek és események, az érzékeny helyszínek és az egyének vonatkozásában. Voltak már olyan esetek Európában, amikor drónokat használtak fel a légi közlekedés és a bűnüldözési műveletek megzavarására, a kritikus infrastruktúra megfigyelésére, valamint arra, hogy csempészárukat juttassanak el börtönökbe vagy a határ másik oldalára.

A Bizottság támogatja a tagállamokat abban, hogy fellépjenek azon fokozódó fenyegetéssel szemben, amelyet a drónok jelentenek a polgárokra és a kritikus jelentőségű társadalmi funkciókra nézve, anélkül, hogy figyelmen kívül hagynánk a drónok hasznos célokra (pl. katasztrófakezelési műveletek

---

eredményeit, a 2019. évi európai parlamenti választásokra, valamint a politikai és témafókuszú hirdetés ehhez kapcsolódó területeire összpontosítva.

74 Lásd a hatékony és valódi biztonsági unió megvalósításáról szóló tizennyolcadik eredményjelentésben (COM(2019) 145 final, 2019. március 20.) a következő részt: „A nyilvános terek biztonságának megerősítésére szolgáló bevált gyakorlatok a hatóságok és a magánszereplők számára”. Ez a nyilvános terek védelmének javítására szolgáló 2017. októberi cselekvési tervre (COM(2017) 612 final, 2017. október 18.) épül. 2019. június 5-én sor került a nyilvános terek védelmével foglalkozó uniós fórum Üzemeltetői Fórumának harmadik ülésére. A találkozón az uniós tagállamok képviselői és a nyilvános tereket üzemeltető magánszereplők vettek részt. Ez utóbbiakat 14 európai szövetség képviselte, amelyek a következő területeket fedik le: vendéglátóipar, élő előadások, zene és szórakoztatóipar, vidámparkok és látványosságok, légi közlekedés, vasúti közlekedés, bevásárlóközpontok, távközlés, személy- és vagyonvédelmi magánszolgáltatások, valamint a biztonsági berendezések gyártói.

75 Ez mindenekelőtt a vegyi, biológiai, radiológiai és nukleáris biztonsági kockázatokkal szembeni felkészültség fokozásáról szóló, 2017. októberi cselekvési terv végrehajtása révén valósul meg (COM(2017) 610 final, 2017. október 18.).

76 Lásd a 2019. március 13-i (EU) 2019/420 határozat által módosított, az uniós polgári védelmi mechanizmusról szóló, 2013. december 17-i 1313/2013/EU határozat 12. cikkének (2) bekezdését.

77 Lásd továbbá a hatékony és valódi biztonsági unió megvalósításáról szóló tizenötödik eredményjelentésben (COM(2018) 470 final, 2018. június.13.) a vegyi fenyegetések elleni megerősített fellépés céljából meghatározott intézkedéseket.

során) való felhasználásának lehetőségeit. A Bizottság nemrég **a drónokkal végzett műveletek biztonságára vonatkozó közös uniós szabályokat**[78] fogadott el, hogy csökkentse a drónok rossz szándékú felhasználásának kockázatát. A rendelkezések többek között előírják az üzemben tartók nyilvántartásba vételét, valamint lehetővé teszik a távoli azonosítást. A Bizottság azzal is támogatja a tagállamokat, hogy nyomon követi a drónok jelentette fenyegetés alakulásának tendenciáit, releváns kutatási projekteket és kapacitásépítési intézkedéseket finanszíroz, valamint elősegíti a tagállamok és más érdekelt felek közötti tapasztalatcserét. E támogatás fokozása érdekében a Bizottság 2019. október 17-én magas szintű nemzetközi konferenciát szervez a drónok jelentette fenyegetés elleni fellépésről.

Tekintettel arra, hogy széleskörűen át kell tekinteni **a kritikus infrastruktúrák védelmére vonatkozó uniós szakpolitikát**[79], a Bizottság 2019. július 23-án előterjesztette a kritikus infrastruktúrák védelméről szóló uniós irányelv[80] értékelését. Ez az irányelv biztosítja az európai kritikus infrastruktúrák azonosítására és kijelölésére, valamint védelmük javítása szükségességének értékelésére vonatkozó jogi keretet. Az értékelés megállapította, hogy az irányelv hatálybalépése óta az európai kritikus infrastruktúrák működésének körülményei jelentősen megváltoztak, az irányelv által különösen érintett ágazatokra – például az energiaágazatra – vonatkozó jogalkotási fejleményekből[81] adódóan is, és a helyzet változása miatt az irányelv rendelkezései csak részben relevánsak. Ugyanakkor a tagállamok továbbra is támogatják, hogy legyen egy olyan uniós szakpolitika a kritikus infrastruktúrák védelmére vonatkozóan, amely tiszteletben tartja a szubszidiaritást és hozzáadott értéket nyújt.

4. Külső dimenzió

Tekintettel arra, hogy az Unió előtt álló biztonsági fenyegetések többsége határokon átnyúló és globális jellegű, az Unión kívüli nemzetközi szervezetekkel és partnerországokkal való együttműködés szerves részét képezi a hatékony és valódi biztonsági unió megteremtésére irányuló munkának.

A többoldalú együttműködés előnyeinek kiaknázása ezen erőfeszítés alapvető eleme, és magában foglalja az EU és az ENSZ közötti együttműködést, amint ezt megerősítette **a terrorizmus elleni küzdelemmel kapcsolatos ENSZ–EU keretmegállapodás** 2019. április 24-i New York-i aláírása is, amelyre a második alkalommal megrendezett ENSZ–EU magas szintű politikai párbeszéd keretében került sor[82]. A keretmegállapodás ösztönzi a terrorizmus elleni küzdelmet, valamint az afrikai, közel-keleti és ázsiai erőszakos szélsőségesség megelőzését és leküzdését segítő kapacitásépítést. Emellett meghatározza az ENSZ és az EU közötti együttműködés területeit és a 2020-ig érvényes prioritásokat.

A **Nyugat-Balkánnal folytatott biztonsági együttműködés** kiemelt regionális prioritás, és ennek keretében számos, a 2018. évi nyugat-balkáni stratégiában meghatározott, biztonsággal kapcsolatos kiemelt intézkedést hajtanak végre[83]. Ezért a Bizottság 2019. április 4-én megrendezte a Nyugat-Balkánnal foglalkozó ügynökségközi munkacsoport első ülését, ahol a hét uniós ügynökség képviselői megosztották tapasztalataikat és továbbfejlesztették a régióbeli partnerekkel való operatív

---

78 A Bizottság (EU) 2019/947 végrehajtási rendelete (2019. május 24.) a pilóta nélküli légi járművekkel végzett műveletekre vonatkozó szabályokról és eljárásokról (HL L 152., 2019.6.11.).

79 Az EU biztonságpolitikájának 2017-es átfogó értékelése (SWD(2017) 278 final, 2017. július 26.) rámutatott arra, hogy el kell végezni a kritikus infrastruktúrák védelmére vonatkozó uniós szakpolitikák széles körű áttekintését.

80 Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelv célja a kritikus infrastruktúrák védelmének javítása az Európai Unióban.

81 Különösen a földgázellátás biztonságának megőrzését szolgáló intézkedésekről szóló, 2017. október 25-i (EU) 2017/1938 rendelet, valamint a villamosenergia-ágazati kockázatokra való felkészülésről szóló, 2019. június 5-i (EU) 2019/941 rendelet.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final, (2018. február 6.).

együttműködést, többek között a szervezett bűnözés, a terrorizmus, a lőfegyverek, a kábítószerek, a migránscsempészés és az emberkereskedelem elleni küzdelem terén. Mind a hat nyugat-balkáni ország esetében felmérést indítottunk a hibrid kockázatokról. A régióval folytatott együttműködés további kézzelfogható példája az Európai Határ- és Partvédelmi Ügynökség tekintetében az EU és Albánia között létrejött, jogállásról szóló megállapodás, amely 2019. május 1-jén hatályba lépett, majd nem sokkal ezután az Európai Határ- és Partvédelmi Ügynökség csapatokat telepített a Görögországgal közös határra. Most először írtak alá ilyen megállapodást harmadik országgal, és első ízben került sor arra, hogy harmadik országba telepítsenek csapatokat. Hamarosan hasonló megállapodásokat kell kötni a régió más országaival is.

Emellett 2019 júliusában Europol összekötő tisztviselőt küldtek ki Albániába azért, hogy az albán hatóságok további segítséget kapjanak a szervezett bűnözés megelőzésére és az ellene való küzdelemre irányuló erőfeszítéseikhez. A tűzfegyverek kereskedelme elleni küzdelem fokozása érdekében a Bizottság 2019. június 27-én előterjesztette az EU és Délkelet-Európa közötti **tűzfegyver-kereskedelem elleni** 2015–2019-es cselekvési terv felülvizsgálatát[84]. Az értékelés rámutat az együttműködés hozzáadott értékére, de kiemeli, hogy további erőfeszítésekre van még szükség, például a tűzfegyverekkel foglalkozó hatékony nemzeti koordinációs központok felállítása vagy a tűzfegyverek lefoglalására vonatkozó információk és jelentések gyűjtésének harmonizálása révén.

Az EU ugyanilyen kiemelt feladatként kezeli a biztonság területére irányuló, **közel-keleti és észak-afrikai országokkal való együttműködés** fejlesztését. Az EU biztonsági párbeszédet kezdeményezett Tunéziával és Algériával. Az EU és Tunézia június 12-én Tuniszban tartotta a biztonságról és a terrorizmus elleni küzdelemről szóló 3. párbeszédet, míg az EU és Algéria között 2018. november 12-én, Algírban került sor a biztonságról és a terrorizmus elleni küzdelemről szóló 2. párbeszédre. Amióta az EU és Marokkó nemrég a Társulási Tanács június 27-én tartott ülésén elismerte, hogy a közös kihívások kezelése érdekében fontos elmélyíteni a biztonsági együttműködést, tárgyalások folynak arról, hogy strukturált biztonsági párbeszéd induljon Marokkóval. Ezzel párhuzamosan folyamatban vannak a megbeszélések az Egyiptommal folytatandó strukturált biztonsági párbeszéd kialakításáról, amelyet az EU és Egyiptom vezető tisztviselőinek július 10-én, Kairóban tartott legutóbbi ülésén is megerősítettek.

A Tanácstól kapott megbízatás alapján a Bizottság informális megbeszéléseket kezdett a legtöbb **közel-keleti és észak-afrikai** országgal annak érdekében, hogy hivatalos tárgyalásokat kezdjenek a személyes adatoknak a Bűnüldözési Együttműködés Európai Uniós Ügynöksége (**Europol**), valamint az illetékes **közel-keleti és észak-afrikai** hatóságok között a súlyos bűncselekmények és a terrorizmus elleni küzdelem céljából történő cseréjéről szóló nemzetközi megállapodásról. Ezzel összefüggésben a Bizottság támogatja olyan munkamegállapodások megkötését is, amelyek közvetlenül az Europol, valamint a **közel-keleti és észak-afrikai** országok partnerhatóságai között jönnének létre, hogy hivatalos keretet biztosítsanak a rendszeres, stratégiai szintű együttműködéshez.

Az EU és az **Egyesült Államok** szoros és stratégiai partnerek a közös fenyegetések kezelésében és a biztonság fokozásában. Az EU és az Egyesült Államok a 2017. június 19-i bel- és igazságügyi miniszteri találkozón megerősítette, hogy a terrorizmus elleni küzdelem a legfontosabb prioritásaik közé tartozik. Ami az utas-nyilvántartási adatállományról szóló EU–USA megállapodást[85] illeti, mindkét fél ismételten hangsúlyozta a megállapodás fontosságát, és vállalta, hogy 2019 szeptemberében a megállapodás rendelkezéseivel összhangban megkezdi a megállapodás végrehajtásának közös értékelését. Mindkét fél elkötelezte magát amellett, hogy fokozzák a terrorizmus elleni küzdelem terén tett közös erőfeszítéseiket, többek között oly módon, hogy kiterjesztik a harci zónákban gyűjtött, a nyomozások és a büntetőeljárások során használandó információk megosztását.

---

84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_hu.pdf

85 HL L 215., 2012.8.11., 5. o.

Ennek az együttműködésének a megerősítésére 2019. július 10-én Brüsszelben a Bizottság – a terrorizmus elleni küzdelem uniós koordinátorával együtt – magas szintű műhelytalálkozót szervezett a hadszíntéri információkról. Ezen a tagállami védelmi, belügyi és igazságügyi minisztériumok, az Egyesült Államok, az Europol és az Eurojust vezető tisztviselői, valamint a nemzetközi szervezetek képviselői gyűltek össze, hogy eszmecserét folytassanak a hadszíntéri információk felhasználásáról, továbbá megvitassák azokat az eljárási, jogi és operatív kihívásokat, amelyekkel jelenleg szembesülnek a terroristák azonosítása és bíróság elé való állítása terén. Az EU és az Egyesült Államok emellett 2019. május 14–15-én Brüsszelben párbeszédet folytatott a vegyi, biológiai, radiológiai és nukleáris kapacitásépítésről, hogy összehangolják a tömegpusztító fegyverek jelentette veszélyek csökkentésére és a vegyi, biológiai, radiológiai és nukleáris biztonság globális szintű megerősítésére irányuló erőfeszítéseket.

Az **EU és az Egyesült Államok között a terrorizmus finanszírozásának felderítését célzó programról létrejött megállapodás**[86] 2010 óta van hatályban, és e megállapodás szabályozza a terroristák és hálózataik azonosítását, felderítését és üldözését célzó adatátadást és -feldolgozást. A megállapodás tartalmaz az uniós polgárok adatainak biztonságát garantáló biztosítékokat, valamint előírja „a biztosítékok, ellenőrzések és kölcsönösségi rendelkezések rendszeres felülvizsgálatát”. A Bizottság a 2019. július 22-i rendszeres értékelő jelentésben[87] kiemelte, hogy a Bizottság meggyőződött a megállapodás, illetve annak biztosítékai és kontrolljai megfelelő végrehajtásáról. A Bizottság üdvözli az amerikai hatóságok részéről tanúsított átláthatóságot az információmegosztás terén, ami jól illusztrálja, hogy a terrorizmus finanszírozásának felderítését célzó program a terrorizmus elleni küzdelemre irányuló nemzetközi erőfeszítések értékes eszközének számít. A megállapodás keretében nyújtott információk elősegítették az Unió területén elkövetett terrortámadásokra – így például a 2017-es stockholmi, barcelonai és turkui merényletekre – vonatkozó nyomozásokat. A tagállamok és az Europol fokozták a mechanizmus alkalmazását, és a terrorizmus finanszírozásának felderítését célzó programon keresztül kapott adatok az előző jelentéstételi időszakhoz képest hétszeres mennyiségű nyomozást segítő bizonyítékot eredményeztek. A megállapodás következő közös felülvizsgálata 2021-ben esedékes.

Ami az **utas-nyilvántartási adatállománynak a terrorizmus és a súlyos bűncselekmények elleni küzdelem céljából történő cseréjére** vonatkozó nemzetközi együttműködést illeti, a 2019. július 17–18-án Montrealban tartott 17. EU–Kanada csúcstalálkozón az EU és Kanada üdvözölte, hogy lezárták az utas-nyilvántartási adatállományról szóló új megállapodásra irányuló tárgyalásokat. Amellett, hogy Kanada jelezte a jogi felülvizsgálat szükségességét, a felek kötelezettséget vállaltak – az említett felülvizsgálat függvényében – arra, hogy mielőbb véglegesítik a megállapodást, elismerve, hogy az fontos szerepet játszik a biztonság fokozásában, miközben biztosítja a magánélet és a személyes adatok védelmét. Az utas-nyilvántartási adatállományról az EU és Ausztrália között már létrejött megállapodás[88] vonatkozásában 2019 augusztusában uniós csoport látogat Canberrába e megállapodás közös felülvizsgálatával és közös értékelésével összefüggésben.

A Bizottság továbbá jelenleg dolgozza ki a Tanácson belül a tagállamokkal együtt az uniós álláspontot a **Nemzetközi Polgári Repülési Szervezet (ICAO)** Közgyűlésének 2019. szeptember 24. és október 4. között tartandó 40. ülésszakára vonatkozóan. A Közgyűlés politikai irányvonalakat határoz meg és utasításokat ad a Nemzetközi Polgári Repülési Szervezet Tanácsa számára a Nemzetközi Polgári Repülési Szervezetnek az utas-nyilvántartási adatállomány feldolgozására vonatkozó előírásaira irányuló technikai munka tekintetében. A Tanács jóváhagyta azt a Bizottság által elkészített tájékoztató dokumentumot, amely felvázolja az uniós álláspontot arról, hogy milyen alapelvekre kellene épülnie az utas-nyilvántartási adatállományra vonatkozó esetleges jövőbeli globális előírásoknak. A tájékoztató dokumentumot a testület elé terjesztik a nem uniós tagállamok közé tartozó tagokra való tekintettel.

[86] HL L 195., 2010.7.27., 5. o.
[87] COM(2019) 342 final (2019. július 22.).
[88] HL L 186., 2012.7.14., 4. o.

VI. KÖVETKEZTETÉS

Az Európai Parlament, a Tanács, a tagállamok és a Bizottság közötti szoros együttműködésnek köszönhetően az EU az elmúlt években jelentős előrelépést tett a hatékony és valódi biztonsági unió megteremtésére irányuló közös erőfeszítések terén, és számos kiemelt jogalkotási kezdeményezésről állapodott meg. A tagállamok a Bizottság támogatásával számos nem jogalkotási operatív intézkedést is végrehajtanak, hogy fokozzák valamennyi polgár biztonságát. Van azonban még néhány olyan függőben levő kiemelt kezdeményezés a biztonsági unióra vonatkozóan, amelyek esetében a társjogalkotók további lépései szükségesek, hogy kezelhetők legyenek a közvetlen fenyegetések. A Bizottság felkéri az Európai Parlamentet és a Tanácsot, hogy tegyék meg a szükséges lépéseket annak érdekében, hogy mielőbb megállapodjanak azokról a jogalkotási javaslatokról, amelyek a terrorista propaganda és az online radikalizálódás elleni küzdelemre, a kiberbiztonság fokozására, az elektronikus bizonyítékokhoz való hozzáférés elősegítésére, valamint a biztonság, a határigazgatás és a migrációkezelés területén használt információs rendszerek szilárdabbá és intelligensebbé tételét célzó munka lezárására irányulnak.

A Bizottság felkéri a tagállamokat, hogy mielőbb és teljes körűen hajtsák végre a biztonsági unió területén elfogadott valamennyi jogszabályt, hogy maradéktalanul megvalósuljanak a várt előnyök. A Bizottság arra is felkéri a tagállamokat, hogy folytassák és fokozzák azokat az elengedhetetlen erőfeszítéseket, amelyek a digitális infrastruktúrák biztonságának fokozására, a dezinformációval és más kiberalkalmas fenyegetésekkel szembeni fellépésre, a felkészültség és a védelem megerősítésére, valamint az Unión kívüli partnerekkel a közös fenyegetésekkel szembeni fellépés érdekében folytatott együttműködés megszilárdítására irányuló gyakorlati intézkedésekhez szükségesek. A felsorolt intézkedések együttesen valamennyi polgár biztonságát javítják.