DOI: 10.36817/km.2022.1.2

# AZ ONLINE TERRORISTA TARTALMAK ELLENI FELLÉPÉST TÁMOGATÓ UNIÓS ÉS MAGYARORSZÁGI INTÉZKEDÉSEK

## EU and Hungarian Measures to Support Action Against Online Terrorist Content

Eck Gábor[1]

**Absztrakt:** Az online térben rejlő lehetőségek megkönnyítik a terroristák kommunikációját, felerősítik a propagandájuk hangját, segítik a szélsőséges gondolataik és terveik mind szélesebb körben való terjedését Az online terrorista tartalmak terjedésének megakadályozása – a véleménynyilvánítás, valamint az információk és eszmék megismerése és közlése szabadságának maradéktalan szem előtt tartásával - korunk egyik legnagyobb biztonsági kihívásának tekinthető. Célom az online terrorista tartalmak fogalmi körül határolása, az azokkal szembeni uniós és hazai intézkedések ismertetése, valamint online terrorizmus ellen fellépő szervezetek ezirányú tevékenységének bemutatása rávilágítva arra, terrorizmus elleni küzdelem komplexitása csak akkor garantálható, ha a digitális térben megjelenő terrorista tartalmak ellen összehangolt és szabályozott fellépések történnek uniós és nemzeti szinteken egyaránt.

**Kulcsszavak:** online terror tartalom, digitális tér, összetett válaszok, biztonsági mechanizmus

**Abstract:** The potential of the online space facilitates the communication of terrorists, amplifies the voice of their propaganda, and helps to spread their extremist thoughts and plans more widely. Preventing the online spread of terrorist content, with full regard for freedom of expression and freedom of

[1] Eck Gábor, Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktoranduszhallgató.
ORCID azonosító: https://orcid.org/0000-0002-4381-2135
A szerző további munkásságát lásd a Magyar Tudományos Művek Tára oldalán:
https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10083198
E-mail cím: eck.gabor@icloud.com

knowledge and communication of information and ideas, can be regarded as one of the most significant security challenges of our time. The paper aims to delimit online terrorist content around the concept, present European Union (EU) and domestic measures against them, and present the activities of organizations fighting online terrorism in this regard. The paper also highlights that the complexity of the fight against terrorism can only be guaranteed if coordinated and regulated actions are taken against terrorist content in the digital space at both EU and national levels.

**Keywords**: online terror content, digital space, copmlex responses, security mechanism

## BEVEZETÉS

A digitalizáció terjedésével és az online térben folytatott tevékenységek szélesedésével, az ott elhelyezett jogellenes tartalmak keletkezésével kapcsolatosan új biztonsági kérdések jelentkeztek. A jogellenes tartalmak érinthetik a személyiségi, a szerzői, a fogyasztóvédelmi jogokat, kiterjedhetnek a terrorizmus online népszerűsítésére, valamint kapcsolatban lehetnek a gyermekek szexuális bántalmazásával, zaklatásával. A fenti érintettségeken túl, az illegális tartalmak megjelenése, kontroll nélkülisége komoly veszélyt és hátrányt jelent a gazdasági folyamatokra, az információk szabad áramlására és az emberi kapcsolatokra. Ezeket a veszélyeket felismerve az Európai Unió intézményei ajánlások, irányelvek és rendeletek alkotásával törekednek gátolni, illetve ezeken keresztül a tagállami fellépést támogatni a veszélyt jelentő tevékenységekkel és magatartásokkal szemben.

A terrorizmushoz köthető személyek, szervezetek is aktívan használják az online világ által kínált alternatívákat, hiszen azok nagy mértékben képesek támogatni kommunikációjukat, segíteni szélsőséges gondolataik és terveik mind szélesebb körben való terjedését. A terrorizmus aktivitása az információs térben elsősorban a kommunikációra, toborzásra és a finanszírozásra terjed ki.[2] Ezek hatékony ellenszerei a terrortartalmú közleményeket érintő tiltás, eltávolítás, illetőleg a gyanús pénz- és eszközmozgások szűrése, figyelése. Az online terroristatartalmak terjedésének megakadályozása talán korunk egyik legnagyobb biztonsági kihívása, azonban az ellenük való fellépés során egy pillanatra sem szabad megfeled-

[2] KOVÁCS, 2006.

keznünk az Európai Unió szabad véleménynyilvánításhoz és információáramláshoz kapcsolódó alapértékeinek megóvásából fakadó felelősségünkről.

A téma kutatása során áttekintettem az Európai Unió területén a közelmúltban bekövetkezett terrortámadások okait és körülményeit taglaló tudományos munkákat, figyelemmel arra, hogy ezek a támadások minden európai ember számára az addig csak a híradásokból ismert, vagy csak szórványosan érzékelhető borzalmakat elérhető közelségbe helyezte. A támadásokkal kapcsolatban rengeteg biztonsági tanulmány készült, ezek feldolgozása során kifejezetten támaszkodtam Anthony H. Cordesman[3] és David C. Rapoport[4] munkáira. A virtuális tér és a terrorizmus összefüggéseinek vizsgálatakor segítségül hívtam Gabriel Weimann munkásságát, aki könyvében rávilágít a terrorizmus és az online világ közötti szoros kapcsolatokra, a jövőbeli kihívásokra és az azokra adható válaszlehetőségekre.[5] Ezeken a gondolatokon tovább haladva elemeztem az Európai Unió szerveinek és szervezeteinek az online térben való terrorista tevékenységek megakadályozását célzó intézkedéseit, valamint az idevonatkozó magyarországi jogszabályi környezethez kapcsolódó rendelkezéseket, amelyek a későbbiek során lesznek részletezve.

A fentebb említett kihívás kezelésében a tanulmány első fejezetében röviden bemutatja azokat a biztonsági helyzetben beáll változásokat, amelyek indukálják az Európai Unió terrorizmus elleni fellépésének kiterjesztését az online térben zajló esemény irányába is, ismertetve az online terrorista tartalom fogalmát. A második fejezet ismerteti az Európai Unió parlamenti, bizottsági és tanácsi irányelveit, rendeleteit és nyilatkozatokait, amelyek lehetővé teszik a terrorista tartalmak online terjedése elleni hatékony fellépést, támogatva és biztosítva a tárhelyszolgáltatók és hatóságok közötti együttműködést. Az ezt követő fejezet a magyarországi helyzetet tekinti át, bemutatva a jogszabályi környezetet és az ahhoz kapcsolódó igazgatási struktúrákat, folyamatokat. A tanulmányt a konklúziók kifejtése zárja.

[3] CORDESMAN, 2017.
[4] RAPOPORT, 2016.
[5] WEIMANN, 2015. 153. o.

## I. ÚJ KIHÍVÁSOK – ÚJ VÁLASZOK

2016-ban 147 terrortámadást hajtottak végre az Európai Unió területén, ugyanez a szám 2015-ben 211, míg 2014-ben 226 volt.[6] 2014-től az uniós állampolgárok egészen másképpen tekintenek a terrorizmusra az őket ért terroristatámadások miatt. 2014. május 24-én Brüsszelben egy fegyveres tüzet nyitott a járókelőkre. Ez az első olyan igazoltan dzsihadista támadás, amelyet egy, az Iszlám Állam nevű terrorszervezetthez csatlakozott és Európába visszatért harcos követett el, megerősítve a figyelmet a Szíriából hazatérő terroristák vonatkozásában fennálló veszélyekre.[7] A Charlie Hebdo szerkesztőségében 2015 januárjában végrehajtott és 12 ember életét követelő támadás, amely rámutatott, hogy az iszlámmal szembeni vélt vagy valós sértéseket is befolyásolhatják a lehetséges kockázatokat.[8] A 2015-ben Franciaországban elkövetett nagy volumenű terrortámadások[9] nemcsak az európai embereknek tették még testközelibbé a terrorfenyegetettséget, hanem rámutatott a közös biztonságpolitika hiányosságaira is.

Mivel a terrorizmus elleni küzdelem elsődleges az Európai Unió számára – bár a biztonsági intézkedések és a bűnüldözésre adandó válaszok tagállami hatáskörbe tartoznak –, a témakörre vonatkozóan több intézkedéssel igyekszik hozzájárulni a biztonság előmozdításához. Ennek érdekében kijelölésre kerültek azon területek, ahol a tevékenységek magasabb szintre emelésével tovább erősíthető az Európai Unió biztonsági helyzete. Ezek alapján az Európai Unióban kiemelt figyelmet kell fordítani az információcsere bővítésére, a külső határok szigorúbb ellenőrzésére, az online radikalizáció megelőzésére, a tűzfegyverek ellenőrzésének fokozására, az igazságügyi együttműködés digitalizálására, a terrorizmushoz kapcsolódó bűncselekmények büntetendővé tételére, a terrorizmus finanszírozásának akadályozására, a légi utas forgalomra vonatkozó adatok felhasználásának harmonizálására, valamint a nem uniós országokkal folytatott együttműködés élénkítésére.[10]

---

[6] CORDESMAN, 2017. 102-103. o.
[7] RAPOPORT, 2016. 27. o.
[8] RAPOPORT, 2016. 28. o.
[9] 2015. november 13-án második generációs francia, illetve belga állampolgárok Párizsban 7 helyszínen, 150 életet követelő összehangolt terrortámadást követettek el.
[10] EURÓPAI BIZOTTSÁG, 2020.

Mindazonáltal a terrorizmusnak is megvannak az online térrel való kapcsolódási pontjai. A terrorizmushoz köthető személyek is igyekeznek a technológiai újdonságok által biztosított lehetőségeket felhasználni a kommunikáció, a kapcsolattartás és információk továbbítása vonatkozásában. Ezen tevékenységük során szinte azonos magatartást tanúsítanak, mint a jogkövető állampolgárok, a megjelenő technikai és technológia újdonságokat használják, folyamatosan új felületeket vonnak be tevékenységük támogatására. Ugyanakkor nem törekednek a platformok által nyújtott védelmi protokollokon felüli biztonsági fokozatok elérésére, megelégszenek a használt felület alap, a szolgáltató által alkalmazott és biztosított beállításokkal. Az adatok védelme érdekében alkalmazott egyéni titkosítási eljárások egyrészt magasabb szervezettséget, másrészt az átlagtól nagyobb informatikai ismereteket igényelnek, ilyen volt például az al-Kaida nevű terrorszervezett által 2007-ben kiadott *Mujahedeen Secrets* elnevezésű nyílt forráskódú titkosító program, amit hosszú időn keresztül használtak a szervezeten belül, e-mailen folytatott kommunikáció védelmére.[11]

## 1.1. Az online terrorista tartalom elemzése

Ahhoz, hogy a kibertérben megjelenő terrorista tartalmak felismerhetők legyenek a fentebb említett jogszerű felhasználással mutatott hasonlóságok ellenére, illetve az Európai Unió alapértékeihez kapcsolódó elvárások értelmezhetőek és maradéktalanul biztosíthatóak legyenek, szükséges az online terrorista tartalomhoz és annak terjesztésével szembeni fellépéshez kapcsolódó fogalmak tisztázása.

Ennek érdekében segítségül kell a hívnunk a 2017/541 Európai Parlamenti és Tanácsi irányelvben meghatározott, a terrorista bűncselekmények, terrorista csoporthoz kapcsolódó bűncselekmények vonatkozásában használt kategóriákat.

Az irányelv gondolatmenetét követve, így online terrorista tartalomnak kell tekintenünk minden olyan tartalmat, ami: a) a lakosság súlyos megfélemlítése; b) egy kormány vagy egy nemzetközi szervezet jogellenes kényszerítése arra, hogy az valamilyen intézkedést megtegyen vagy ne tegyen meg; c) egy ország vagy egy nemzetközi szervezet alapvető politikai, alkotmányos, gazdasági vagy társadalmi struktúráinak súlyos destabilizálása

[11] STORM, 2014. 182–183. o.

vagy lerombolása[12] céljából terrorista bűncselekmény elkövetésére, abban való közreműködésre szólítanak fel, azok elkövetését szorgalmazzák, dicsőítik, illetőleg terrorista csoport tevékenységében való részvételre hívnak fel.[13] Továbbá a fentebb említett cselekmények elkövetésének érdekében segítséget nyújtanak fegyverek, valamint mérgező, veszélyes vagy robbanóanyagok készítéséhez, használatához, illetve egyéb speciális eljárások, eszközök megismeréséhez.[14] Terrorista tartalmúnak kell tekinteni a terrorcselekményekről készített képeket, leírásokat, hang- és videófelvételeket és élő közvetítéseket. Természetesen a tartalmakat kontextusukban kell vizsgálni, fontos tényező a káros következmények prognosztizálása, valamint a tartalom tulajdonosának, terjesztőjének terror relevanciájának vizsgálata. Éppen ebből fakadóan az oktatói, művészeti, kutatói, újságírói, valamint a terrorizmus elleni küzdelem érdekében folytatott ismeretterjesztői tevékenység nem tartozik a terror tartalmú kategóriába. Ugyanígy nem minősülnek terrorista tartalomnak a nyilvános politikai viták során kifejtett radikális vélemények.[15]

Egy másik fontos fogalmi kör az online terrorista tartalmak szempontjából, hogy milyen tartalom tekinthető nyilvánosnak. A tartalom nyilvánosnak tekintendő, ha az ahhoz való hozzáférés nem kíván meg külön csatlakozási vagy regisztrációs folyamatot, illetve, ha ezen folyamatokat emberi beavatkozás nélkül, külön döntés vagy válogatás hiányában hajtják végre. Nyilvánosnak tekintendő a tartalom, amennyiben a tárolt információk a tartalmat szolgáltató kérésére kerülnek megosztásra, így különösen a különböző kép-, hang-, videó, fáljmegosztó és közösségi média felületeken közzétett információk.

Tehát online terrorista tartalomnak kell tekinteni azokat az online térben megjelenő nyilvános tartalmakat, amelyek mondanivalója, tekintet nélkül annak formátumára, terrorista bűncselekményekkel és terrorista csoporthoz kötődő bűncselekményekkel kapcsolatos tevékenységek elkövetésre, közreműködésre hív fel, ezeket támogatja, dicsőíti, vagy elkövetésükhöz szükséges speciális ismereteket biztosít.

[12] 2017/541/EU IRÁNYELV 3.cikk (2)
[13] 2017/541/EU IRÁNYELV 4-5. cikk
[14] 2017/541/EU IRÁNYELV 7. cikk
[15] 2017/541/EU IRÁNYELV (40)

## II. EURÓPAI UNIÓ

Az Európai Tanács tagjai 2015-ben közös nyilatkozatot tettek, amelyben elkötelezték magukat a félelem és a megkülönböztetések nélküli élet mellett.[16] Ezen értékek védelme érdekében szükségesnek ítélték a terroristák utazásának, visszatérésének észlelését, annak megszakítását, az Európai Unió külkapcsolatainak aktivizálását a terror elleni küzdelemben.

A terrorizmus finanszírozás globális felügyeletét ellátó kormányközi szervezet a Pénzügyi Akciócsoport (FATF)[17], valamint az Európai Unió bűnüldöző ügynöksége az Europol[18] jelentései és értékelései alapján kijelenthető, hogy a terrorizmus működése az információs térben elsősorban a kommunikációra, toborzásra és a finanszírozásra terjed ki. A már említett Európai Parlament és a Tanács 2017/541 irányelvében megfogalmazott gondolatok, amelyek nem csak pontosan meghatározzák a terrorista bűncselekmények, terrorista csoporthoz kapcsolódó bűncselekmények körét, de külön figyelmet fordítanak a terrorista tevékenységekhez kapcsolódó uszító jellegű cselekmények interneten történő megvalósulási formáira és azok elleni fellépés lehetőségeire.[19] Az Európai Unió továbbá felhívja a tagállamok figyelmét, hogy a terrorizmus elleni internetes küzdelem során törekedjenek a terror és uszító jellegű online tartalmak elérésének akadályozására. A jogellenes tartalmak eltávolítására, vagy a hozzáférés megszüntetésére vonatkozó eljárásoknak kidolgozásának jogi alapját az Európai Parlament és Tanács 2010/13/EU irányelve[20] biztosítja. A jogszabály tagállami kötelezettségekre fókuszál, az internetszolgáltatók vonatkozásában az önkéntességet és a támogatást helyezi előtérbe.

Mivel a tagállamok és a nagyobb internetszolgálatók önkéntes együttműködési tevékenysége nem váltotta be a hozzáfűzött reményeket, az Európai Unió irányító és annak tevékenységét koordináló szervei továbbra is folyamatosan és kitartóan dolgoznak azon, hogy megakadályozzák a terroristákat abban, hogy az internetet radikalizálódásra, toborzásra és erőszakra való felbujtásra használják, A Bizottság 2018/334 ajánlásában elismeri az elért eredményeket, de tovább sürgeti a gyorsabb és hatékonyabb

16 EURÓPAI TANÁCS, 2015.
17 FINANCIAL ACTION TASK FORCE, 2021.
18 EUROPOL, 2020.
19 2017/541/EU IRÁNYELV (22)
20 2010/13/EU IRÁNYELV

reagálást a megjelenő online terrorista tartalmakkal szemben.[21] Megállapítja azt is, hogy az internetes terrorista tartalom megjelenését követő első órában okozza a legnagyobb károkat.[22] Ezekre való figyelemmel a Bizottság határozott szándéka a tárhelyszolgáltatók, internetszolgáltatók és az illetékes hatóságok közötti együttműködés fokozása az olyan automatikus rendszerek használatára vonatkozóan, melyek alkalmasak a káros tartalmak felderítésére, azonosítására, hozzáférhetetlenné tételére és akár eltávolítására.[23] Az ajánlásból jól érzékelhető, hogy az eddigi gyakorlattal szemben, a jogellenes tartalmak felismerésével, hozzáférhetetlenné tételével és eltávolításával kapcsolatos felelősséget már nem csak hatósági feladatnak definiálja, hanem aktív szereplőként tekint az internetszolgáltatói szektor képviselőire. Az ajánlásban központi elemként határozták meg a radikalizálódásban szerepet játszó tényezők kezelését szolgáló kezdeményezések, a toleranciát, a szolidaritást erősítő kommunikációs stratégiák kidolgozását, a terrorizmust és a szélsőséget népszerűsítő internetes tartalmak észlelését és eltávolítását, valamint a gyanús tartalmak kezelésével kapcsolatos erőforrások kiépítését az Europol vonatkozásában.

Az Europol számos területen és irányban segíti a nemzeti bűnüldöző szervek sikeres tevékenységét, ehhez széleskörű szolgáltatásokat nyújt, illetve erőforrásokat biztosít annak érdekében, hogy támogassa őket a nemzetközi súlyos és szervezett bűnözés, valamint a terrorizmus elleni küzdelemben. A Műveleti Igazgatóság (OD)[24] látja el az Europol alapvető szakmai-műveleti feladatait, ennek sikeres végrehajtása érdekében működteti – négy másik központtal együtt[25] – az Európai Terrorizmusellenes Központot (ECTC)[26], melynek fő feladata a terrorizmus elleni együttműködés és a terrorizmus elleni információcsere elősegítése a terrorizmus elleni hatóságok között. Az online terrortartalmak felismerése és a partnerekkel történő megosztás érdekében az ECTC keretein belül 2015-ben alakult meg az internet monitoring egység (IRU).[27] Az IRU koordinálja és megosztja a terrorista, erőszakos és szélsőséges online tartalmak

[21] 2018/334 EU BIZOTTSÁG AJÁNLÁSA (31)
[22] 2018/334 EU BIZOTTSÁG AJÁNLÁSA (35)
[23] 2018/334 EU BIZOTTSÁG AJÁNLÁSA (37)
[24] Operations Directorate
[25] Operational and Analysis Centre, European Serious and Organised Crime Centre, European Cyber Crime Center, European Financial and Economic Crime Centre
[26] European Counter Terrorism Centere
[27] Internet Referral Unit

azonosítási feladatait az illetékes hatóságokkal, támogatja a tagállamok internetalapú vizsgálatait, valamint szorosan együttműködik az internethez kötődő szolgáltatói iparág képviselőivel. Ezeken túl az IRU az Europol és az uniós tagállamok számára is tudásközpontként működik az e-bizonyítékokhoz való határokon átnyúló hozzáférés területén, tekintettel arra, hogy a tevékenysége során ötvözi az technológiai, az operatív, a nyelvi és a kulturális ismeretekre vonatkozó szakértelmet.[28] Az interneten zajló, terrorizmushoz köthető tevékenységek elleni fellépést hatékonyabbá tevő gondolkodás folytatásaként jelent meg 2021. április 29-én az Európai Parlament és Tanács (EU) 2021/784[29] számú rendelete az online terrorista tartalom terjesztésével szembeni fellépésről, amely célja az online terrorista tartalmak gyors eltávolítása. A rendelet értelmében az Európai Unióban szolgáltatásokat nyújtó tárhelyszolgáltatóknak – függetlenül attól, hogy fő telephelyük a tagállamokban található-e vagy sem –, a hatóságoktól kapott eltávolítási végzés kézhezvételétől számított egy órán belül el kell távolítaniuk a terrorista tartalmakat, vagy le kell tiltaniuk a hozzáférést.

A 2021/784 számú rendelet a 2022-es hatályba lépését követően, további eszközöket biztosít a tagállamok számára a terrorista tartalmak szükség szerinti gyors eltávolításának kikényszerítésére. A tagállamok illetékes hatóságai jogosultak lesznek eltávolítási végzést kiadni a szolgáltatóknak, eltávolítatni a terrorista tartalmat vagy letiltani az azokhoz való hozzáférést minden tagállamban. A tárhelyszolgáltatóknak konkrét intézkedéseket kell hozniuk a szolgáltatásaikkal való visszaélések kezelése és szolgáltatásaikat terrorista tartalom terjesztéséhez felhasználni akaró tevékenységekkel szembeni hatékony fellépés érdekében. A tiltással végrehajtásának technikai kivitelezésének megválasztásával kapcsolatos döntés a tárhelyszolgáltatónál marad. Ugyanakkor a jogszabálynak kimondottan az a célja, hogy az online térben terjedő terror tartalmakkal szembeni erőteljes fellépést biztosítson, a hétköznapi felhasználók, jogi személyek és vállalkozók jogainak tiszteletben tartása mellett, ideértve a szólásszabadságra, a véleménynyilvánításra, a tájékozódás szabadságára vonatkozó, illetve a tömegtájékoztatás szabadságát és sokszínűségét garantáló jogokat is. Ennek a folyamatnak a támogatására az ECTC lehetőséget fog biztosít a tagállamok számára, hogy az Europol által épített

[28] EUROPOL, 2021a.
[29] 2021/784 EU RENDELET

és a IRU kezelésében, működtetésében lévő egységes PERCI[30] elnevezésű az illegális online tartalmak leküzdésére szolgáló platformon keresztül kezdeményezhetik az általuk veszélyesnek ítélt tartalmak eltávolítását a szolgáltatóknál.[31]

## II. MAGYARORSZÁG

Mindezek tükrében fontos áttekinteni a röviden a hazai helyzetet is. A büntető törvénykönyvről szóló 2012. évi C. törvény (Btk.) XXX. fejezetében a terrorcselekmény és az ahhoz kapcsolódó bűncselekmények tényállásaiban megfogalmazott elemek jelölik azokat a magatartási formákat melyekkel szemben a jogalkotó, a terrorizmus leküzdése érdekében, a bűntetőjogi igényt érvényesíteni kívánja.[32] A terrorizmus online terjedésének megakadályozása szempontjából a Btk-ban megjelenő terrorcselekmény elkövetésével kapcsolatos fordulatokra, úgymint 1) az azzal való fenyegetés; 2) az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítása; 3) az elkövetésére történő felhívással, ajánlkozással, vállalkozással összefüggő tevékenységek helyeződik a hangsúly. Természetesen a terrorizmus online megjelenése kapcsán nem hagyhatók figyelmen kívül az terrorista csoportokhoz való csatlakozások céljából történő utazások és az azokhoz társuló internetes tevékenységek sem. Amennyiben az eljáró hatóságok felismerik ezeket az internetes kivetüléseket, a Btk. lehetőséget biztosít az elektronikus hírközlő hálózaton közzétett adatot véglegesen hozzáférhetetlenné tételére, ha annak hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg, vagy bűncselekmény elkövetéséhez eszközül használtak, vagy bűncselekmény elkövetése útján jött létre.[33] A büntetőeljárásról szóló 2017. évi XC. törvény (Be.) rendelkezései szerint[34] az eljáró hatóságnak lehetősége van az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozására és az adathoz való hozzáférés ideiglenes megakadályozására. Erre akkor kerülhet sor, ha az eljárás közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van

[30] Plateforme Européenne de Retraits de Contenus illicites sur Internet (European platform for takedown of illicit content online)
[31] EUROPOL, 2021b.
[32] 2012.ÉVI C. TÖRVÉNY 314-319.§.
[33] 2012. ÉVI C. TÖRVÉNY 77.§.
[34] 2017. ÉVI XC. TÖRVÉNY

helye, és az a bűncselekmény megszakítása érdekében szükséges. Az elektronikus adathoz való hozzáférés megakadályozásának elrendelésére a bíróság, vagy a külön törvényben meghatározott hatóság jogosult.[35]

Ugyanakkor a jogszabály a bűntető eljárás érdekeinek szem előtt tartásával lehetőséget biztosít az eljáró hatóságoknak arra, hogy közvetlenül megkeressék azon szolgáltatókat, melyek képesek megakadályozni az adat hozzáférését. Ezen megkeresések felhívják a szolgáltató figyelmét arra, hogy illegális tevékenység folyik az általa üzemeltetett, felügyelt felületen, lehetőséget biztosítva arra, hogy a szolgáltató saját eljárási rendjeit használva megakadályozza az adott tartalomhoz való hozzáférést. Ez a jogi lehetőség a hozzáférés megakadályozásának gyorsítása érdekében a hatóság és a szolgáltató közötti önkéntes együttműködést célozza, így a szolgáltatók részéről a megkeresésben foglaltak végrehajtása nem kötelező.[36]

A hatóságok által akadályozni kívánt elektronikus adatok kezelése és az azokkal kapcsolatos intézkedések biztosítása érdekében a Nemzeti Média- és Hírközlési Hatóság (NMHH), 2014 óta működteti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát.[37] Ezen a felületen kell elhelyezni az eljáró hatóságok határozatait melyekben a jogellenes tartalmak korlátozásairól döntött. Az adatbázisban elhelyezett információk nem nyilvánosak, azokba csak a bíróság, a külön törvényben meghatározott hatóság, az ügyész, a nyomozó hatóság, az Országgyűlés illetékes bizottságának a tagjai és az NMHH tekinthet be.

Az NMHH szervező, ellenőrző szerepet tölt be, nem dönt internetes tartalmak sorsáról. A szolgáltatóknak a hatóság közlését követően egy munkanap áll rendelkezésére a határozatban foglalt tartalmak blokkolására, elérhetetlenné tételére. Amennyiben a szolgáltató nem tesz eleget a határozatban foglaltaknak, az NMHH nem szankcionálhat, pusztán értesítési kötelezettsége van az adathozzáférést akadályozó határozatot hozó hatóság irányába.

Érdemes megjegyezni, hogy az NMHH egy internet hotline bejelentő felületet működtet, melyen állampolgári jelzéseket vár olyan online tartalmakkal kapcsolatban, melyek terrorcselekmények elkövetésére buzdí-

[35] Speciális esetekben a 1991.évi XXXIV. törvény alapján szerencsejáték-felügyeleti hatóság, valamint az NMHH és a Nemzeti Élelmiszerlánc-biztonsági Hivatal közötti együttműködési megállapodás alapján (NMHH 2021.) is rendelkezik az elektronikus adat ideiglenes hozzáférhetetlenné tételét lehetővé tevő jogosultsággal.

[36] 2017. ÉVI XC. TÖRVÉNY 338. §

[37] 2003. ÉVI C. TÖRVÉNY

tanak, vagy a terrorizmust népszerűsítik, illetve egyéb jogsértő vagy kiskorúak számára káros mondanivalót tartalmaznak. [38] Ez egy további lehetőséget biztosít arra, hogy akár névtelenül is a hatóságok tudomást szerezhessenek olyan nyilvános káros tartalmakról, melyek szűrése, akadályozás, esetleg eltávolítása szükséges.

A bejelentő felületet működtetése természetesen nem egyedülálló elképzelés, 2021. februárjában az Egyesült Királyságban, a Metropolitan Police és a londoni polgármesteri hivatal együttműködésében, az internet felhasználók részére az online térben fellelt, a terrorizmushoz köthető tartalmak hatóságok részére történő eljuttatását biztosító jelzőrendszer alakítottak ki. Az iREPORTit alkalmazás - akár anonim módon - alkalmas arra, hogy használója a lehető leggyorsabban tájékoztathassa a hatóságot az online terrorista tartalmakról, azok feltalálási helyéről.[39]

## KONKLÚZIÓ

Az online térben zajló események igen gyorsan történnek és változnak, ezért elengedhetetlen az, hogy a biztonságot támogató intézkedések is hasonló intenzitásúak legyenek, és a reagálás helyett a megelőzést részesítsék előnybe. Kiemelten fontos, hogy az Európai Unió irányító és koordináló szervei ügymenetük során figyelemmel legyenek a felgyorsult világunkban zajló eseményekre annak érdekében, hogy az Európai Unió az online térben történő eseményekre lendületes és produktív válaszlépéseket tudjon adni.

Megállapítható, hogy az Európai Unió folyamatos és jelentős figyelmet fordít a terrorizmushoz köthető, az online térben zajló illegális tevékenységek felismerése, eltávolítása és terjedésének akadályozása érdekében. Az Európai Unió jogalkotási, irányítási és végrehajtási mechanizmusai törekszenek az online térben történő eseményeket gyorsan és hatékonyan lereagáló intézkedések meghozatalára és végrehajtására. Ezeken keresztül igyekszik a tagállami hatáskörökbe tartozó a biztonsági intézkedések és a bűnüldözésre, így a terrorista tevékenységek online kiterjedéseire, adandó hatékony nemzeti válaszok megadásához elengedhetetlen támogatások biztositására. A terrorista tartalmak eltávolítását célzó jogszabályok fejlődésénél jól megfigyelhető, hogy a jogalkotók

[38] NMHH INTERNET HOTLINE, 2021.
[39] SAY, 2021.

egyre inkább törekednek arra, hogy a szolgáltatói szektor képviselői mindinkább felelősségi szerepkörökkel legyenek felruházva. Nem szabad megfeledkeznünk arról sem, hogy az online terrorista tartalmakkal szemben eredményes küzdelem érdekében nagyon fontos a nemzeti stratégiák kidolgozása, az egyéni tudatosság és kritikai gondolkodás erősítése, valamint a radikalizáció elleni fellépés és annak megelőzése érdekében tett erőfeszítések.

A hazai viszonyok tekintetében megállapítható, hogy a jogszabályi környezett teljes mértékben biztosítja az információáramláshoz és a szabad véleménynyilvánításhoz fűződő jogokat ugyanakkor a hatóságok részére kellő mozgásteret biztosít a gyors és hatékony intézkedések megtételéhez. A magyarországi helyzetet megvizsgálva kijelenthető, hogy a jogszabályi környezetünk, a hatósági szereplők helyzete megfelelő válaszok adására képes az interneten megjelenő terrorista tartalmakkal szemben.

Mind az uniós mind pedig a hazai vonatkozásban rendelkezésre állnak azok a platformok- akár a hatósági, akár az állampolgári szinteken - melyek a terrorista tartalmak eltávolításának hatékony katalizátorai lehetnek. Ugyanakkor kiemelt jelentőséggel bír, hogy az állami és a szolgáltatói területek szereplői felismerjék, hogy a közös, összehangolt fellépés elengedhetetlen és mindent meghatározó alapeleme az online térben terjedő terrorizmussal összefüggésbe hozható tartalmak elleni fellépésnek. Ezt a közös fellépést támogatja az is, hogy az online terrorista tartalmak pontos beazonosítása komoly szintű együtt gondolkodást követel meg mind stratégiai, mind operatív szinteken. Ezt az azonosítást segítve készült a cikk, abban a reményben, hogy az online terror tartalom értelmezéséhez sikerült használhatótámpontot nyújtania.

## FELHASZNÁLT IRODALOM

2003. ÉVI C. TÖRVÉNY AZ ELEKTRONIKUS HÍRKÖZLÉSRŐL 159/B. § (3) bekezdés

2012. ÉVI C. TÖRVÉNY A BÜNTETŐ TÖRVÉNYKÖNYVRŐL 77.§. 314-319.§.

2017. ÉVI XC. TÖRVÉNY A BÜNTETŐELJÁRÁSRÓL 335.§ 338.§

EURÓPAI BIZOTTSÁG (2020). A Bizottság Közleménye a biztonsági unióra vonatkozó uniós stratégiáról. Letöltés helye: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0605&from=EN (Letöltve: 2022. 05. 05.)

EURÓPAI BIZOTTSÁG 2018. MÁRCIUS 01. 2018/334 AJÁNLÁSA AZ ILLEGÁLIS ONLINE TARTALOM HATÉKONY KEZELÉSÉRE IRÁNYULÓ INTÉZKEDÉSEKRŐL (2018). Letöltés helye: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018H0334&from=FR (Letöltve: 2022 05. 27.)

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2010. MÁRCIUS 10-I2010/13 IRÁNYELVE A TAGÁLLAMOK AUDIOVIZUÁLIS MÉDIASZOLGÁLTATÁSOK NYÚJTÁSÁRA VONATKOZÓ EGYES TÖRVÉNYI, RENDELETI VAGY KÖZIGAZGATÁSI RENDELKEZÉSEINEK ÖSSZEHANGOLÁSÁRÓL (2018). letöltés helye: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A32010L0013 (Letöltve: 2022. 05. 27.)

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2017.MÁRCIUS 15-I 2017/541 IRÁNYELVE A TERRORIZMUS ELLENI KÜZDELEMRŐL, A 2002/475/IB TANÁCSI KERETHATÁROZAT FELVÁLTÁSÁRÓL, VALAMINT A 2005/671/IB HATÁROZAT MÓDOSÍTÁSÁRÓL (2017). Letöltés helye: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32017L0541 (Letöltve: 2022. 05. 27.)

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2021. ÁPRILIS 29-I 2021/784 SZÁMÚ RENDELETE AZ ONLINE TERRORISTA TARTALOM TERJESZTÉSÉVEL SZEMBENI FELLÉPÉSRŐL (2021). Letöltés helye: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32021R0784 (Letöltve: 2022. 05. 27.)

EURÓPAI TANÁCS (2015). Az Európai Tanács tagjainak nyilatkozata. Letöltés helye: https://www.consilium.europa.eu/hu/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/ (Letöltve: 2021. 11. 18.)

EUROPOL (2020). Online jihadist propaganda 2020 in review Letöltés helye: https://www.europol.europa.eu/cms/sites/default/files/documents/online_jihadist_propaganda_2020_in_review_0.pdf (Letöltve: 2021. 12. 13.) DOI azonosító: 10.2813/169367

EUROPOL (2021a). EU Internet Referral Unit - EU IRU Monitoring terrorism online Letöltés helye: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru (Letöltve: 2021.november 30.)

EUROPOL (2021b). How Europol keeping online spaces safe? Letöltés helye: https://www.europol.europa.eu/media-press/newsroom/news/how-europol-keeping-online-spaces-safe (Letöltve: 2021. 11. 30.)

CORDESMAN, ANTHONY H. (2017). Terrorism in Europe. Global Trends in Terrorism: 1970-2016, Center for Strategic and International Studies (CSIS), 101–47, Letöltés helye: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170818_european_terrorsim_trends_1970_2016.pdf (Letöltve: 2021. 12. 10.)

FINANCIAL ACTION TASK FORCE (2021). (FATF) Annual Report Letöltés helye: https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf (Letöltve:2021. 11. 30.)

KOVÁCS LÁSZLÓ (2006). Az információs terrorizmus eszköztára. Hadmérnök, Robothadviselés konferencia különszám. Letöltés helye: http://www.hadmernok.hu/kulonszamok/robothadviseles6/tartalom.html (Letöltve: 2022. 03. 27.)

MNHH INTERNET HOTLINE (2022). Letöltés helye: https://nmhh.hu/cikk/190109/Terrorcselekmenyre_felhivo_terrorizmust_nepszerusito_elosegito_tartalom (Letöltve: 2021. 12. 13.)

NMHH (2021). Letöltés helye: https://nmhh.hu/cikk/220053/Akar_egy_evre_lakat_kerulhet_a_problemas_webshopokra_az_NMHH_es_a_Nebih_egyuttmukodesenek_koszonhetoen (Letöltve: 2022. 04. 10.)

RAPOPORT, DAVID C. (2016). Why Has The Islamic State Changed its Strategy and Mounted the Paris-Brussels Attacks? Perspectives on Terrorism, Vol. 10, No. 2, 24-32. Letöltés helye: https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2016/2016-volume-x-issue-2.pdf (Letöltve: 2021. 12. 10.)

SAY, MARC (2021). London mayor launches 'report terrorist content' app. Letöltés helye: https://www.ukauthority.com/articles/london-mayor-launches-report-terrorist-content-app/ (Letöltve: 2021. 12. 13.)

STORM, MORTEN (2014). Agent Storm: My Life Inside al Qaeda and the CIA. New York, Atlantic Monthly Press, 182–183 ISBN 978-0-8021-2314- 5

WEIMANN, GABRIEL (2015). Terrorism in Cyberspace: The Next Generation, Woodrow Wilson Center Press with Columbia University Press, 2015 ISBN 978-0