Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar

A médiamegosztó portálok terrorista tartalmaival szembeni fellépés külföldi és hazai jogi eszköztára

Szerző: Mihály Laura Dominika

Intézmény: Széchenyi István Egyetem, Deák Ferenc Állam- és Jogtudományi Kar, Győr

Szak, évfolyam: Jogász, IV. évfolyam

Konzulens: Dr. Kelemen Roland, egyetemi tanársegéd

Kézirat lezárásának dátuma: 2020. 10. 25.

TARTALOMJEGYZÉK

BEVEZETÉS

A kibertér rendkívül összetett jelenség, mely számos veszélyt rejt magában. Éppen ezért a rendészet, a hadviselés, valamint a nemzetbiztonsági tevékenység szerepe is kiemelendő, mert az interdiszciplináris megközelítés révén lényeges károktól óvhatjuk meg a társadalmat. Látható az is, hogy e veszélyek fokozott kockázata alátámasztja a jogi felelősséget, akár az állami főhatalom tényleges kiterjeszthetőségét is igényelve. Külön szabályozási mechanizmusok kialakítása és működtetése kerül előtérbe, mely átfogó vizsgálatra alapozottan alakítható ki. A kibertérben zajló rohamos fejlődés és folyamatok radikális változást hoznak mind a társadalmi, politikai, mind az egyéni szférában. Nem elhanyagolandó, sőt, külön kiemelendő az egyénre gyakorolt befolyás, hiszen a kibertér képes hatást gyakorolni az éntudatra, a társadalmi hozzáállásra, valamint számos egyéb olyan pszichológiai jelenségre, melyek az egész közösség életét befolyásolják. Különösen fontos a felnövekvő generáció és a fiatalkorúak esetében az ilyen káros hatások mérséklése, hiszen az ő éntudatuk és önképük még kialakulóban van, könnyen befolyásolhatóak a médiamegosztó portálokon fellelhető tartalmak által. Ez az a lehetőség, melyet a terrorszervezetek érzékkel használnak ki saját programjuk terjesztése érdekében, követőik toborzása során.

Ugyanakkor nemcsak a kibertér gyakorol hatást a hagyományos térre, e jelenség fordítottja is megfigyelhető. A hagyományos tér társadalmi feszültségei, technikai nóvumai és innovációi rányomják bélyegüket a kibertérre, mint látható a terrorizmus széles körű elterjedése esetében is.[1] A kibertér nyújtotta lehetőségeket kihasználva, a terrorszervezetek erősítik határokon átívelő jellegüket, újfajta kihívást állítva az államok és a médiamegosztó portálok elé. Ezt mi sem támasztja alá jobban, mint a tény, hogy a NATO 2016-ban a kiberteret is hadszíntérré minősítette.[2]

A technikai fejlődés lehetővé teszi, hogy a kibertér rendszere egyre gyorsabbá és komplexebbé váljon, azonban pont ez a komplexitás teremti meg sebezhetőségét a terrorista tartalmakkal szemben. Mivel a jog egyik lényeges feladata a társadalmi változások lekövetése, így fontos lépést tartani eme szektor rohamos fejlődésével és fokozott figyelmet fordítani azokra a szabályozási lehetőségekre, melyek a terrorizmus elleni fellépést lehetővé teszik.

[1] KELEMEN Roland, NÉMETH Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése, In: Farkas Ádám (szerk.) *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében*, Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, pp. 147-170.
[2] A NATO hivatalosan is hadszíntérré nyilvánítja a kiberteret, Nemzeti InternetFigyelő.

Hogyan lehetséges az, hogy több millió YouTube felhasználó tekintette meg élőben az amerikai újságíró, James Foley lefejezését, mielőtt a megbotránkoztató tartalom eltávolításra került?[3] Hogyan szervezték meg könnyűszerrel a terrorszervezetek a WhatsApp, vagy a Telegram privát üzenetváltási applikációin keresztül a Párizsban elkövetett merényleteiket?[4] Ilyen, és ehhez hasonló kérdésekre keresem a választ dolgozatommal, mely multidiszciplináris (jogtudomány, szociológia, pszichológia) megközelítéssel és nemzetközi kitekintéssel kívánja bemutatni a terrorszervezetek médiamegosztó portálokon való jelenlétét és ennek lehetséges jogi szabályozását, mintául szolgáló szabályokat, megoldásokat keresve.

Elsősorban arra a jelenségre kívánok fókuszálni, mely a terrorista propaganda és félelemkeltés médiamegosztó portálokon történő terjesztését és megosztását jelenti. A kibertér egyik fő funkciója a szereplők közötti kapcsolattartás megteremtése, így lehetővé teszi azt, hogy a terrorista csoportok ezen keresztül jussanak el a számítógépes rendszereket használók széles köréhez, valamint kapcsolatot tartsanak egymással (mint láttuk azt a párizsi merényletek előkészítése kapcsán).

Fokozott kockázati platformnak minősül többek között a Facebook, valamint a YouTube, melyek lehetővé teszik a videók élő közvetítését. Sajnálatos módon, a károsultak jelentős része csak a kár bekövetkezését követően gondol az IT biztonságára. Sokan azonban észre sem veszik azokat a negatív hatásokat és veszélyeket, melyeket a rendszerek magukban rejtenek e jelenséggel kapcsolatban (is). Ez hívja fel a figyelmet a preventív intézkedések fontosságára, melyek lehetővé teszik, hogy eme káros hatások jelentősen mérséklődjenek. Ebben pedig a jogászoknak, mint a társadalom mérnökeinek kiemelt szerepe és felelőssége van. Hangsúlyozom azonban a társadalomtudományok jelentőségét is, mint amilyen a pszichológia, vagy a médiaszociológia, melyek a terrorista propaganda médiamegosztó portálokon történő terjesztése esetén a társadalomra és az egyénre gyakorolt negatív hatásokat veszik górcső alá, esetleges megoldási módokat keresve. Úgy gondolom, dolgozatom témája rendkívül kurrens kérdéseket feszeget, különös tekintettel a terrorizmus megnövekedett szerepére, valamint a kibertérben rejlő veszélyekre.

[3] Profile: James Foley, US journalist beheaded by Islamic State, BBC News.
[4] Paris attack planners used encrypted apps, investigators believe, The Washington Post.

1. A KÖZÖSSÉGI MÉDIA JELENTŐSÉGE

E fejezetben a közösségi médiaportálok egyénre és társadalomra gyakorolt hatásai kerülnek terítékre, majd a terrorszervezetek motivációinak és szélesebb körű céljainak ismertetésén keresztül médiaszociológiai és szociálpszichológia aspektusból szeretnék rávilágítani a technikai fejlődés esetleges negatív következményeire.

1.1. EGYÉNI ÉS TÁRSADALMI HATÁSOK

Az alfejezetben egy korábbi kutatásom eredményeit felhasználva táblázatban foglaltam össze azokat a negatív hatásokat, melyeket a médiamegosztó portálok okozhatnak.[5]

A média társadalomra gyakorolt negatív hatásai	Megjelenési formái
1. Agresszió	*Cyberbullying, erőszakos tartalmak megosztása, gyűlölködő kommentek*
2. Deszenzitizáció	*Elidegenedő társadalomszerkezet kialakulása, segítségnyújtás háttérbe szorulása*
3. Szorongás, mentális zavarok	*Személyiségzavarok kialakulása, szorongásos tünetek felerősödése, egyéb mentális problémák elterjedése*
4. Tömegpszichózis	*Ideológia átvétele, terjesztése, terrorista tartalmak megosztása*
5. Identitástorzulás	*Terrorista személyiségszerkezet kialakulása*
6. Kisebbségi csoportokat érő atrocitások	*Rasszizmus, diszkrimináció, agresszív fellépés online és a való életben*

Forrás: saját szerkesztés

Kiemelendő az identitástorzulás következtében jelentkező „terroristává válás' jelensége, mely elsősorban a fejlődő országok körében figyelhető meg fokozott mértékben. Ezen jelenség alább bővebben kifejtésre kerül, szélesebb körben bemutatva a terrorszervezetek elsődleges céljait és motivációit, melyek elérése érdekében a médiamegosztó portálokat felhasználják.[6] A fiatal,

[5] MIHÁLY Laura Dominika: Jogsértések a médiamegosztó portálokon – médiaszociológiai és szociálpszichológiai kitekintés, In *Diskurzus*, 2019, 9(1), pp. 19-27.
[6] JASPERSEN, J. G., MONTIBELLER, G.: On the learning patterns and adaptive behavior of terrorist organizations, In European Journal of Operational Research, 2020, 282(11), pp. 221-234.

könnyen befolyásolható, formálódó identitású személyek esetében különösen hatásos a propagandavideók megtekintése, valamint a hasonló tartalmaknak való kitettség.[7]

A táblázatban rögzített negatív társadalmi hatások, valamint etikai dilemmák mind a médiamegosztó portálok fokozott szabályozásának szükségességét indukálják. Emellett lényeges leszögezni az interdiszciplináris megközelítés jelentőségét, mely a hatékony jogi szabályozáshoz más tudományterületek szakértőit, eredményeit is felhasználja. Fontos a megfelelő tájékoztatás, valamint az egyének szerepe, ugyanakkor vannak olyan esetek, amikor a felelősség megosztott voltát kell középpontba állítani.

Emellett a szociális és pszichológiai következmények szoros összefüggésbe hozhatóak az alapvető jogok sérelmével, mint amilyen az emberi méltósághoz való jog, az élet és testi épség védelme, valamint az emberek egyenlősége. Ezen alapjogok gyakran a véleménynyilvánítás következtében sérülhetnek, így ezen esetekben elengedhetetlen a szükségességi-arányossági teszt alkalmazása. Ezt a magyar Alkotmánybíróság a 30/1992-es határozatának[8] keretében dolgozta ki, mely értelmében egy alapvető jog korlátozása csak egy másik alapvető jog, vagy alkotmányos érték védelme érdekében, feltétlenül szükséges mértékben és az elérni kívánt céllal arányosan történhet, ugyanakkor lényegi tartalma semmi esetre sem üresíthető ki.

1.2. MÉDIA ÉS TERRORIZMUS, AVAGY A FŐBB CÉLOK, MOTIVÁCIÓK

A fejezet második felében a terrorszervezetek megközelítésére koncentrálva mutatom be röviden azt, hogy melyek azok az elsődleges célok, motivációk, amelyek a videók feltöltőit, megosztóit vezérlik.

E körben lényegesnek tartom a terrorizmus fogalmának ismertetését, mely esetében a jogi fogalommeghatározásra koncentrálok, a hadtudományi, rendészettudományi megközelítés helyett. Kriminológiai értelemben Korinek László definíciója érdemel említést, mely az alábbiak szerint határozza meg a jelenséget: „A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak alkalmazás, vagy ezzel való fenyegetés, melynek célja politikai törekvések elérése azáltal, hogy az áldozatban, a nézőközönségben, az államban, a társadalomban megalkuvó magatartás alakuljon ki. A meghirdetett cél általában politikai, ideológiai, vallási, etnikai tartalmú radikális változás

[7] ERIKSON, E. H.: Identitásválság önéletrajzi vetületben, In: Erikson: *A fiatal Luther és más írások,* Budapest, Gondolat, 1991, pp. 401–436.
[8] 30/1992. (V. 26.) AB hat., ABH 1992, 167, p. 181.

kikényszerítése, a cél elérésére alkalmazott cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[9]

Nemzetközi értelemben vett terrorizmusról akkor beszélhetünk, ha a terrorizmus félelmet, pánikot, riadalmat kelt a nemzetközi közösség egészében, vagy annak egy részében. Nemzetközi politikai bűnténynek tekintendő, ezért, mint bűn, büntetőjogi fellépést kíván, mint politika, politikai választ, s mint nemzetközi jelenség, csak a nemzetközi közösség együttese által oldható meg.[10]

A terrorszervezetek rendkívül változatos eszközökkel dolgoznak, gyakoriak az emberrablások, bombamerényletek, repülőgép-eltérítések, nyilvános kivégzések. E körben van kiemelt jelentősége a kibertérnek és ezen belül a médiamegosztó portáloknak, ahol ezen tartalmakat félelemkeltési, figyelemfelkeltési célokból, valamint annak érdekében mutatják be, hogy a terrorszervezet céljait megismertessék a „nézőközönséggel". Gyakran nem az anyagi haszonszerzés az elsődleges mozgatórugója ezen tevékenységeknek, hanem a politikai törekvések megvalósítása, a legitim, demokratikus államberendezkedés megdöntése, valamint politikai engedmények kikényszerítése.

A terrorista személyiségszerkezet kialakulása szempontjából számos érdekes pszichológiai és szociológiai kutatás született, melyek annak a felderítését tűzték ki célul, hogy vajon mik azok a faktorok, melyek ezen személyiség, illetve „életpálya" kialakulásához vezetnek. A legelfogadottabb nézet szerint a terrorista lelki és társadalmi faktorok együttes hatásaként előálló személyiségszerkezet.[11] A hivatkozott tanulmányban három faktor kerül górcső alá, melyek konjunktív feltételként vezetnek a radikalizálódáshoz: (1) személyes szükséglet, mely a valahova tartozáson, valamint fontosságérzeten alapul, (2) az ideológiai narratíva, mely igazolja a politikai erőszak alkalmazhatóságát, (3) a közösségi média szerepe, ami a személyes döntést befolyásolja, mely végső soron a radikalizálódáshoz vezet.[12]

A terrorszervezetek elsődleges céljai között a már korábban említett félelemkeltés és elrettentés mellett előkelő helyen szerepel - ezzel szoros összefüggésben - a terrorista-propaganda terjesztése, valamint az ideológiai ismertetése, amely toborzási célokat szolgál.

[9] KORINEK László: A terrorizmus, In *Belügyiszemle*, 2015, pp. 17–19.
[10] SCHMID, A.: Terrorism - The Definitional Problem, In *Case Western Reserve Journal of International Law*, 2004, 36(2), 390. p.
[11] WEBBER, D., KRUGLANSKI, A. W.: The social psychological makings of a terrorist, In *Current Opinion in Psychology*, 2018, 19, pp. 131-134.
[12] Uo.

A kapcsolattartás sem elhanyagolható mozgatórugó, hiszen sokszor a közösségi médiaportálok biztosítják azt a terepet a terrorszervezetek számára, melyen keresztül egymással, valamint a követőikkel megoszthatják aktuális merényleteiket, radikális lépéseiket.

Az alfejezetben említett terrorista motivációkat és a szociális médiaplatformoknak ezek érvényesítésében játszott szerepét az alábbi táblázatban foglaltam össze:

Terrorista motiváció	**Szociális médiaplatformok jelentősége**
1.Félelemkeltés, elrettentés	*LIVE kivégzések (YouTube, Facebook), elrettentő képek/videók*
2.Propaganda terjesztése, ideológia ismertetése	*Tájékoztató videók közzététele, lelkesítő beszédek tartása (YouTube, egyéb videómegosztó portálok), szimbólumok/jelképek használata*
3.Toborzás	*Fiatalabb korosztály megcélzása, elsősorban a YouTube, valamint a Twitter felhasználásával*
4.Kapcsolattartás, szervezés, merényletek koordinálása	*WhatsApp, Telegram, Facebook Messenger, valamint egyéb privát üzenetküldésre alkalmas applikációk*
5.Politikai nyomásgyakorlás céljaik elérése érdekében	*Bármelyik fentebb említett oldalon megjelenő fenyegető tartalom*

Forrás: saját szerkesztés

A felsorolás természetesen nem kimerítő, ugyanakkor a lényegi mozgatórugókat foglalja magában, melyek a terrorszervezeteket arra ösztönzik, hogy a médiamegosztó portálokat alkalmazzák céljaik elérése érdekében.

2. KÜLFÖLDI SZABÁLYOZÁS

Dolgozatomban tölcsér-szerkezetben kerül bemutatásra a nemzetközi, majd azt követően a hazai szabályozás, összehasonlító jogi elemzés keretében ismertetve ezek hasonlóságait, esetleges eltéréseit. Elsőként az Amerikai Egyesült Államok megengedőbb, majd az Európai Unió - különös tekintettel a német - szigorúbb jogi szabályozása kerül bemutatásra. Végül - kuriózumként - ismertetem az ausztrál megközelítést is.

2.1. EGYESÜLT ÁLLAMOK

Az Internet megjelenésének hajnalán az alapvető felfogás az volt, hogy a szabályozásnak a lehető legalacsonyabb szinten kell érvényesülnie, mert ez szolgálja leginkább a nyilvánosság érdekeit.[13] Ez a felfogás mára már módosításra szorul, hiszen elsősorban azt kell megvizsgálnunk, hogy a társadalmi problémák indokolják-e a jogi szabályozást.

Amennyiben a terrorista tartalmakkal kapcsolatos konkrét fellépési lehetőségeket vesszük górcső alá, még árnyaltabb képet kapunk a szabályozási lehetőségekről, melyek az Amerikai Egyesült Államokban érvényesülnek.

A legjelentősebb terrorszervezet, mely a szociális média adta lehetőségeket használja fel annak érdekében, hogy követőket toborozzon, félelmet keltsen és a fentebb kifejtett hatásokat elérje, az ISIS. Elsősorban a Facebook, valamint a Twitter azon médiamegosztó platformok, melyek eszközül szolgálnak a terrorszervezet(ek) céljainak eléréséhez, azonban megemlítendő a WhatsApp, vagy a Telegram is, melyek felhasználók közötti képek, videók megosztását teszik lehetővé és pusztán egy regisztrált telefonszám alapján hozzáférhetőek.[14]

Jelentős probléma, hogy maguk a portálok a társadalmi felháborodás ellenére is csupán esetről-esetre reagálnak a felbukkanó terrorista propagandára, mely azonban nem biztosít hatékony és átfogó fellépési lehetőséget. Emögött elsősorban a megengedő szabályozás áll, melynek köszönhetően az állam gyakorlatilag „ráhagyja" a portálokra a szabályozási koncepció megalkotását, kizárólag a nagyon extrém esetekre reagál. A portálok a szólásszabadság és a szabad véleménynyilvánítás mögé bújva hárítják el magukról a felelősséget, hiszen ezen portálok elsődleges célja a profit megszerzése, nem pedig a felhasználók biztonságának a megóvása.

[13] KOLTAY András, POLYÁK Gábor: Az Alkotmánybíróság határozata a médiaszabályozás egyes kérdéseiről, In *Jogesetek Magyarázata,* 2012, 1, p. 20.
[14] ISIS Online: U.S. Rights and Responsibilities, Counter Extremism Project.

A 2015. novemberi párizsi terrortámadást követően (mely során 130-an meghaltak, és közel 350-en megsebesültek) napvilágra került, hogy a terroristák a WhatsApp és a Telegram privát üzenetváltási applikációján keresztül szervezték meg a támadásokat.[15] Ezt követően a WhatsApp a Telegramra kormányzó hivatkozásokat a csevegőalkalmazás felhasználói szerint blokkolni kezdte, az üzenetben elküldött link látható volt ugyan, rákattintani vagy kimásolni azonban nem lehetett. Erre az "intelligens" szűrésre azért volt szükség, mert ezt az alkalmazást – mely szinte lekövethetetlennek bizonyul – az Iszlám Állam használta toborzásra.

A merényleteket követően tüzetesebb vizsgálat alá kerültek a médiamegosztó portálok, az állami kontroll felszólította őket arra, hogy blokkolják az ISIS-felhasználókat, azonban sajnos tiszavirág életűnek mutatkozott a szigorított fellépés, hiszen a terrorszervezetek hamarosan újra felütötték a fejüket a portálokon.

2.1.1. A PORTÁLOK SZABÁLYANYAGA

Az átláthatóság érdekében, tekintsünk át néhány médiamegosztó oldalt, hogy lássuk, miképpen jelenik meg a terrorszervezetekkel kapcsolatos fellépés az irányelvekben, valamint a felhasználási feltételekben.

A legjelentősebb videómegosztó, a YouTube esetében látható, hogy a portál a megjelölési funkciót biztosítja abban az esetben, ha valaki általa nem megfelelőnek minősített tartalommal találkozik. A YouTube munkatársai 24 órában ellenőrzik, hogy a felhasználók által megjelölt tartalmak valóban sértik-e a közösségi irányelveket, ennek fényében döntenek a korhatárossá tételéről, vagy az eltávolításáról. A felsorolt kategóriák közül, melyek a YouTube szellemiségével ellentétesek, a terrorszervezetek által feltöltött videók elsősorban az alábbiakat érintik: káros vagy veszélyes jelenteket bemutató tartalom, gyűlölködő tartalom, erőszakos vagy megbotránkoztató tartalom, fenyegetések, valamint a gyermekek biztonsága. Azonban az alkalmazandó következmények korántsem szigorúak. Az érintett felhasználó e-mailben történő értesítése mellett a tartalom eltávolításra kerül, három irányelvet sértő magatartást követően kerül csak törlésre maga a fiók.[16]

A felhasználási feltételek azokat a részletszabályokat rögzítik, melyek a fiókkal rendelkezőkre, valamint a videók megtekintőire vonatkoznak. Ezek lényegében a felhasználó kizárólagos felelősségét hangsúlyozzák az általa feltöltött tartalomért.[17] Amennyiben valamely

[15] Uo.
[16] Community Guidelines, YouTube.
[17] Terms of Service, YouTube.

megjelölés hatására, vagy magának a YouTube-nak az észrevételére eltávolításra kerül egy videó, a portál értesíti a videó feltöltőit, kivéve az alábbi esetekben: ha jogszabályt sértene, vagy valamely hatóság utasítását, illetve egyéb módon a YouTube vagy Társult vállalkozásainak jogi felelősségre vonásának kockázatát jelentené; ha megakadályozna egy nyomozást, vagy a szolgáltatás integritását vagy működését; vagy amennyiben kárt okozna bármely felhasználónak, egyéb harmadik félnek, a YouTube-nak vagy Társult vállalkozásainknak.

A Facebook tulajdonjogokat gyakorol az Instagram és a WhatsApp felett, így ezek esetében a Facebook szolgáltatási feltételeit veszem elsősorban alapul, azonban megjegyzendő, hogy a WhatsApp külön rögzíti, hogy a kifogásolható médiatartalom esetén nemcsak a tartalom eltávolítása, hanem jogi következményekhez folyamodás is várható a portál részéről.[18] Erről azonban részletesebb felvilágosítást nem ad, így pusztán józan paraszti ésszel feltételezhető a megfelelő hatóságokhoz fordulás, illetve polgári/büntetőeljárás kezdeményezése. A WhatsApp emellett rögzíti, hogy a platform kizárólag jogilag megfelelő, elfogadható célokra használható, ezt követően egy viszonylag kimerítő felsorolás következik arról, hogy mi nem minősül ilyennek. Külön kiemelendő ebben a körben az erőszakos bűncselekmények promotálása, az erőszak hirdetése, valamint az erőszakos viselkedés tanúsítása, illetve az illegális, fenyegető, félelmet keltő tartalom megosztása. Az egyes felhasználókra vonatkozó jogi szabályozás országonként eltérő – ez külön rögzítésre kerül – tehát az adott felhasználó államának jogi rezsime lesz az irányadó az esetleges jogkövetkezmények alkalmazása esetén.

Végül tekintsünk rá a Facebook felhasználási feltételei és irányelveire, hiszen ezen portál is egy kissé más jellegű felületet biztosít, mint a fentebb említett YouTube, valamint WhatsApp, vagy Telegram. Míg a YouTube esetében akár milliós nézettség elérésére is lehetőség van akár perceken belül, a WhatsApp és a Telegram elsősorban a terrorszervezetek tagjai közötti kommunikációs lehetőséget biztosítja, nem tömegekhez juttatja el az információt. Ezek esetében inkább a merényletek megszervezése és lebonyolítása rejt magában veszélyeket, hiszen a portálok bárki által használhatóak, hozzáférhetőek. A Facebook a két lehetőség ötvözetét biztosítja: lehetőség van LIVE videók feltöltésére, képek, videók megosztására, valamint a felhasználók közötti privát kommunikációra.

A Facebook esetében a felhasználási feltételek rögtön az elején leszögezik a káros tartalmakkal, vagy magatartásokkal kapcsolatban, hogy amennyiben ilyenről értesülnek,

[18] WhatsApp Terms of Service.

megteszik a szükséges intézkedéseket – segítséget kínálnak, eltávolítják a tartalmat, letiltanak bizonyos funkciókhoz való hozzáférést, letiltják magát a fiókot, vagy felveszik a kapcsolatot a bűnüldöző szervekkel. Emellett az adatokat megosztják más Facebook-vállalatokkal, amikor valamely termékük használatakor visszaélést vagy káros magatartást tapasztalnak.[19] Mint említettem, az Instagram és a WhatsApp is a Facebook kezében összpontosul, így portálokon átívelő tartalomkorlátozásra is lehetőség van ezáltal.

Amennyiben megállapításra kerül, hogy egy felhasználó nyilvánvalóan, súlyosan vagy ismételten megszegte a feltételeket vagy a médiamegosztó szabályzatát – ideértve különösen a közösségi alapelveket – akkor elsődlegesen felfüggesztik a fiókhoz való hozzáférést, majd letiltják a fiókot. Itt is lehetőség van a káros, vagy károsnak minősített tartalom megjelölésére, ugyanakkor a Facebook automatikusan szűri a felhasználási feltételeket és irányelveket sértő tartalmakat. A probléma azonban az, hogy ez gyakran hosszabb időt vesz igénybe, így fordulhat elő, hogy élőben közvetítésre kerülnek terroristák általi kivégzések, mielőtt több milliós nézettséget követően eltávolításra kerülnek.[20]

Az Irányelvek alatt érdekes ellentmondásra bukkanhatunk: rögzítve van a felhasználók biztonsága és védelme a káros tartalmaktól, ugyanakkor megjelenik a véleménynyilvánítás szabadsága is, melyet több ponton is megerősít a szabályzat. Külön szerepel az erőszakos tartalom és bűncselekmények korlátozása és visszaszorításra, hasonló szabályozási lehetőségekkel operálva, mint a YouTube: fiók felfüggesztése, felhasználó eltávolítása, tartalom törlése, valamint az illetékes hatóságok értesítése.[21] Itt azonban már megjelenik a szűrés: alapos vizsgálatot követően döntik el azt, hogy az adott tartalom valóban fenyegetést jelent-e a közösségre, valamint a társadalomra, csak ezt követően teszi meg a portál a szükséges intézkedéseket.

A terrorszervezetek külön említésre kerülnek azon felhasználók között, akik minden esetben a Facebook általi eltávolításra és jogkövetkezmények kezdeményezésére számíthatnak, függetlenül a portálon kifejtett tevékenységüktől. A médiamegosztó portál egy cikksorozat keretében reagált a terrorizmussal kapcsolatos fellépésre, mely egész érdekes információkat rögzít a terrorszervezetek technikáit illetően. Egyesek, átlagfelhasználók fiókjainak feltörésével próbálkoznak, míg mások újabb profilok létrehozásával igyekeznek elkerülni a detekciót.[22] A

[19] Facebook Felhasználási Feltételek.
[20] Mayhem and murder: 10 most shocking Facebook Live moments ever, ABC News.
[21] Community Standards: Violence and Criminal Behavior, Facebook.
[22] Hard Questions: What Are We Doing to Stay Ahead of Terrorists?, Facebook.

Facebook azonban egyre precízebb mesterséges intelligenciát dolgozott ki annak érdekében, hogy az olyan tartalmak, melyek ISIS, vagy Al-kaida, illetve hasonló terrorszervezetek által kifejtett tevékenységekre utalnak, minél előbb azonosításra kerüljenek. Az MI-rendszer egy pontozási technika segítségével veszélyesség szempontjából minősíti, majd kategóriába sorolja a megosztott tartalmakat, így a Facebook humán csapata a legmagasabb pontszámot elért jelzésekkel tud elsőként foglalkozni. Ha a pontszám elér egy meghatározott mértéket, a tartalom azonnali eltávolításra kerül, azonban olyan lehetőség is van, hogy a Facebook munkatársai előzetesen meghatározott kritériumok mentén megvizsgálják, valóban sérti-e az említett irányelveket, felhasználási feltételeket. A Facebook szóvivői kiemelték, hogy a hatékony mesterséges intelligencia rendszernek köszönhetően a terrorista tartalmak médiamegosztó portálon töltött ideje átlagosan 43 óráról 18 órára csökkent, a felhasználók általi jelentést követően. A szám jelentősen csökkent, ugyanakkor még így is rendkívül aggasztó, hogy vajon hány emberhez juthat el világszerte 18 óra alatt egy esetlegesen feltöltött propagandavideó, vagy egyéb provokatív, vagy erőszakos tartalom.Az alábbi táblázat átfogóan szemlélteti ezen számadatokat:

	Q1 2018	**Q2 2018**	**Q3 2018**
Eltávolított tartalom			
Összes eltávolított tartalom	1,9 millió	9,4 millió	3 millió
Frissen feltöltött tartalmat észlelő eszközök által	1,2 millió	2,2 millió	2,3 millió
Régebbi tartalmat észlelő eszközök által	640.000	7,1 millió	710.000
Felhasználók által megjelölt	10.000	15.000	16.000
Proaktív eltávolítás (%)	99	99	99
Platformon eltöltött idő az eltávolítást megelőzően			
Frissen feltöltött tartalmat észlelő eszközök esetében	Kevesebb, mint 1 perc	14 óra	Kevesebb, mint 2 perc
Régebbi tartalmat észlelő eszközök esetében	970 nap	860 nap	770 nap
Felhasználók általi megjelölés esetén	43 óra	22 óra	18 óra

Forrás: https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/ (saját fordítás)

Visszatérve az erőszakos tartalmakra, melyek a Facebook részéről fellépést vonnak maguk után, a terrorista csoport, valamint fogalom speciális meghatározása is rögzítésre kerül, mely elsősorban az erőszakkal elkövetett megfélemlítő, társadalom nagyobb csoportját érintő magatartásokat sorolja ide, melyeket valamilyen ideológia, vagy felsőbb cél elérése, vagy kifejezésre juttatása érdekében követnek el. A gyűlölet, vagy erőszakszervezet meghatározása szintén szerepel: eszerint a háromnál több főből álló csoport, mely meghatározott szimbólumok használatával, saját ideológiáját promotálva alkalmaz erőszakot társadalmi csoportok ellen nem, faj, bőrszín, szexuális orientáció, vagy egyéb megkülönböztető jegy alapján.[23] A tömeggyilkosság, valamint a tömeggyilkos fogalma is meghatározva van, melybe természetesen a terrorszervezetek tagjai, a merényletek elkövetői egyértelműen besorolhatóak. Kiemelendő, hogy ezen szervezetek szimbólumai, az általuk használt jelképek, a Facebook által rögzített tiltólistán szerepelnek, ezek használata nem engedélyezett, eltávolítást és jogi következményeket vonnak maguk után.

Szintén elítélendő és szankcionálandó a hasonló szervezeteket és tevékenységeket éltető, támogató tartalmak közzététele, megosztása. Ezen nem csak magukat a terrorszervezeteket értik véleményem szerint a Facebook felhasználási feltételei, hanem azon személyeket is, akik pusztán megosztanak egy terrorszervezetet pozitív színben feltüntető információt.

A „Kifogásolható tartalom” alkategória alatt szerepel az erőszakos és grafikus tartalom tilalma, mely különösen olyan képek, videók közzétételét és megosztását tilalmazza, mint a csonkítás, belső szervek nyílt ábrázolása, égő emberi testek bemutatása (ez alól kivételként szerepel, amennyiben oktatási célokat szolgál a tartalom), torok elvágása, valamint a kannibalizmus. A kivégzés élőben történő közvetítése (melyre számos példát láthattunk sajnos a közelmúltban, mielőtt a hasonló videók eltávolításra kerültek volna) szintén külön említést kap azon tartalmak között, melyek következményeket vonnak maguk után.

Az alfejezetben bemutatott szabályozási lehetőségek felvetik a kérdést, hogy vajon mennyiben van lehetősége a konkrét médiamegosztó portáloknak fellépni, vagy az állam részéről szükséges-e a szabályozás szigorítása. A felelősség hárítása az USA-ban erősen jelentkezik, az első alkotmánykiegészítés pedig értékes táptalajul szolgál ahhoz, hogy a portálok a visszásságokat követően a véleménynyilvánítás szabadságával takarózzanak.

[23] Dangerous Individuals and Organizations, Facebook.

2.1.2. JOGI KÖRNYEZET

Az Egyesült Államok jogszabályai kifejezetten tiltják a terrorszervezeteknek történő „tudományos, technikai vagy egyéb speciális ismeretekből származó tanácsadást vagy segítségnyújtást”.[24] Annak érdekében, hogy minél szélesebb körben szorítsák vissza a terrorizmus elterjedését, kiszélesítésre került az „anyagi támogatás” fogalma, hogy bűncselekménnyé nyilvánítsa a terroristáknak nyújtott „szakértői segítséget vagy tanácsot”.[25] Előfordultak olyan jogesetek, melyek során a terrorizmus puszta támogatása is bűncselekménynek lett minősítve. 2010-ben a Legfelsőbb Bíróság a Holder kontra Humanitarian Law Project ügyben kimondta, hogy a beszéd kriminalizálható, ha az „egy külföldi terrorszervezettel összehangoltan, vagy annak irányában végzett tevékenységnek minősül”.[26] Mint azt a precedensjog is mutatja, a terrorszervezetek támogatása akár a Facebookon, vagy Twitteren tett megjegyzéssel is elkövethető, azonban az, hogy mi sorolható be a „szakértői segítség, vagy támogatás kategóriába”, tágan értelmezendő.

A Patriot Act-re történő hivatkozással akár az ilyen tevékenység is büntetőeljárást vonhat maga után, abban az esetben is, ha az egy privát csetablakon keresztül történik a felhasználók között, mint például amilyen a WhatsApp, vagy a Telegram. Ehhez természetesen a médiamegosztó portálok és a hatóságok közötti együttműködésre van szükség, melynek segítségével hatékony fellépés biztosítható a terroristák által elkövetett jogsértésekkel szemben.

Tekintsük át, milyen módon valósul meg ez az együttműködés. 1994 októberében a Kongresszus elfogadta a bűnüldözéshez nyújtott kommunikációs segítségnyújtásról szóló törvényt (továbbiakban: CALEA), hogy egyértelművé tegye a távközlési szolgáltatók együttműködési kötelezettségét a bűnüldözési célú kommunikáció lehallgatásában. A Szövetségi Hírközlési Bizottság szerint, a törvény arra kötelezte a távközlési vállalatokat, hogy módosítsák a berendezéseiket, létesítményeiket és szolgáltatásaikat annak biztosítása érdekében, hogy rendelkezzenek a szükséges felügyeleti képességgel ahhoz, hogy hatékonyan vegyék fel a harcot a terrorizmussal szemben.[27]

A törvény egyebek mellett előírta a vállalatok számára, hogy biztosítsák a kormánynak az erőforrásokat a vezetékes-, valamint az elektronikus hírközlés lehallgatásához, és hozzáférést kapjanak a hívásokat azonosító információkhoz, bírósági végzés, vagy más jogi

[24] Patriot Act of 2001, 805. § (a)(2)(b)
[25] Uo.
[26] Holder v. Humanitarian Law Project, 561 U.S. (2010).
[27] The Communications Assistance for Law Enforcement Act (CALEA) of 1994.

felhatalmazás esetén.[28] Az FCC (Federal Communications Commission) kifejtette, hogy a CALEA arra az aggodalomra ad hatékony választ, hogy a digitális és a vezeték nélküli kommunikáció, mely az interneten keresztül valósul meg, gyakorlatilag lehetetlenné teszi a bűnüldöző szervek számára az engedélyezett felügyelet érvényesítését. A törvény azonban lehetőséget biztosít arra, hogy jogszabályi keretek között érvényesüljön a médiamegosztó portálokon közzétett illegális tartalom állami felügyelete.

Bár a CALEA kifejezetten a telekommunikációs társaságokra vonatkozott, a törvény célja az volt, hogy kezelje azokat a technológiai problémákat, amelyek előreláthatóan az üzenetküldő alkalmazások esetében is felbukkannak. A törvényt később módosították annak biztosítása érdekében, hogy az olyan újabb technológiák, mint az internet-hozzáférés szolgáltatói és a VoIP-szolgáltatók is megfeleljenek a CALEA szabványoknak.

A CALEA által meghatározott kötelezettségek mind a mai napig nem vonatkoznak azonban a magánhálózatokra, a mobiltelefonokra, az e-mailre, a webtárhelyre vagy a domain név alapján működő keresési szolgáltatásokra. Mindazonáltal a törvény - a közbiztonság védelme érdekében - összhangban áll annak szükségességével, hogy a bűnüldöző szervek törvényes felhatalmazással legyenek képesek hozzáférni az új kommunikációs technológiákhoz, például a titkosított alkalmazásokhoz, mint amilyen a WhatsApp, vagy a Telegram. A CALEA eklatáns példaként szolgálhat arra, hogyan teremtsük meg az egyensúlyt a magánélet, valamint az adatok védelme és a terrorizmussal szemben fellépést garantáló állami kontroll között. Egy 2011-es felmérés adatai azt igazolják a banki tranzakciók állami monitorozásával kapcsolatban, hogy a válaszadók 55%-a a biztonság érdekében megengedő álláspontón van ezen tevékenységgel kapcsolatban. Ez a hozzáállás ugyanúgy érvényesülhet a szociális médiaplatformok esetében, így egy hasonló kutatás hozzájárulhat a társadalmi értékítélet megítéléséhez.

A Counter Extremism Project (továbbiakban: CEP) keretében Dr. Hany Farid által kifejlesztett, egyedülálló eGLYPH technológia 2016 júniusa óta üzemel, a szélsőséges képek, videók és hangok felderítésére és eltávolítása céljából, mely követendő sablonként szolgálhat a terrorista tevékenység online kezeléséhez.[29] Az eGLYPH-hez hasonló módon elő lehetne írni, hogy az internetes szolgáltatók és weboldalak objektíven, a nyilvánosság számára átlátható

[28] ISIS Online: U.S. Rights and Responsibilities, Counter Extremism Project.
[29] Hany Farid's eGlyph Can Help Europe Fight Online Extremism, Berkeley.

módon jelentsék terrorista tartalmakat, megakadályozva ezzel a radikalizálódást és a szociális médiaplatformok terrorszervezetek általi felhasználását.[30]

Az USA-ban számos képzést indítottak a médiamegosztó portálok üzemeltetői számára, melyekkel a terrorizmus online terjedésének veszélyére hívják fel a figyelmet. 2018-ban a Belbiztonsági Minisztérium (Department of Homeland Security) otthont adott az erőszakos szélsőségesség elleni küzdelemről szóló tréningnek, mely elsősorban a terrorizmus elleni küzdelem online lehetőségeit boncolgatta.[31] Az ehhez hasonló képzések azóta gombaként szaporodtak el világszerte. Ugyanebben az évben hozták létre a terrorizmus elleni küzdelem globális internetes fórumát (GIFCT).[32]

A próbálkozások ellenére azonban számos olyan esettel találkozhatunk, amikor a hashtagek segítségével több millióan értesülnek és válnak szemtanúivá az élő kivégzések közvetítésének, mint történt ez James Foley, amerikai újságíró 2014-es kivégzése esetén is. A Foley videójához társított #A_Message_To_America és #NewMessageFromISIStoUS hashtagek a SITE Intelligence Group felmérése szerint a videó megjelenésének első három órájában több, mint 2000 tweetet eredményeztek, több millió emberhez eljutva ezáltal. Ugyanez történt Nick Berg, Kenneth Bigley, vagy Daniel Pearl, amerikai újságíró kivégzése esetén is.[33] Látható tehát, hogy a szociális média gyors információáramlásának előnyei mellett jelentős hátrányokat is magában rejt, amelyek az állami beavatkozás fokozott mértékét indukálják. Az USA-ban ugyanis problémaként jelentezik az, hogy egységes jogszabályi keret hiányában a portálok önkényesen, esetről-esetre reagálnak az erőszakos tartalmakra.[34]

2018-ban az Egyesült Királyságban egy olyan eszközt mutattak be, mely az extremista tartalmak felismerésén és blokkolásán keresztül rendkívül hatékonyan ismeri fel a médiamegosztó portálokon fellelhető terrorista propagandát.[35] A javaslat értelmében, egy törvény által tennék kötelezővé a platformok számára a mesterséges intelligencia használatát, mely az eddigi tesztelések eredményei szerint 94%-os hatékonysággal szűri ki a szélsőséges tartalmakat.[36] „Betanítására" több ezer órányi terrorista tartalmat futtattak le. Az Egyesült Királyság kormánya felvette a kapcsolatot az Amerikai Egyesült Államokkal, valamint a

[30] Tech & Terrorism: Tech Companies Fail to Curb Online Abuses, Counter Extremism Project.
[31] DHS Announces the Launch of the "Countering Terrorists Exploitation of Social Media and the Internet" Training, DHS.
[32] Uo.
[33] ICASCON, Zann: Combating Terrorism Online: Possible Actors and Their Roles, Lawfare.
[34] Uo.
[35] UK unveils extremism blocking tool, BBC News.
[36] New technology revealed to help fight terrorist content online, Gov.uk.

nagyobb médiamegosztó platformokkal az együttműködés megteremtése és az egységes fellépés ösztönzése érdekében.[37]

A tény, hogy a terrorista tartalmak hatalmas nézettséggel rendelkeznek, saját (és implicit módon a médiamegosztó portálok) felelősségének fokozott mértékét is kérdésessé teszi. A televíziós műsorok esetében kissé eltérő a helyzet, hiszen itt lehetőség nyílik az epizódok előzetes áttekintésére, a YouTube-hoz hasonló videómegosztók, vagy a WhatsApp és a Telegram mintájára működő csetelési lehetőséget biztosító oldalak esetén azonban csak utólagos felülvizsgálat és moderáció történik. Ugyanakkor azáltal, hogy az oldalak lehetővé teszik ezen felhasználók számára, hogy elérjék a több millió feliratkozót/követőt/nézőt, valamint biztosítják számukra a fizetett hirdetési lehetőségeket, felelősségük megkerülhetetlen. A terrorizmussal szembeni fellépés elengedhetetlen részét képezi az is, hogy ezen területen is fokozott mértékű legyen a videók szűrése, és ne fordulhassanak elő olyan helyzetek, mint pl. az említett kivégzések élő közvetitése a Facebook-on, vagy egy „Hogyan készítsünk bombát?" című videó elterjedése a YouTube-on, vagy más videómegosztó portálon.

A YouTube, a Facebook, vagy a Twitter mind disztribúciós platformok, ez azonban nem jelenti azt, hogy ne tudnánk őket elszámoltatni. Társadalomként dönthetünk úgy, hogy amennyiben a hasonló esetek és azok káros következményei indokolják, a médiamegosztó portálok is olyan feltételeket teljesítsenek, mint a televíziós csatornák. A klasszikus média szabályozásának áttekintése és az online rezsimmel való összevetése egy következő dolgozat alapjául szolgálhat, szintén érdekes kérdéseket felvetve, azonban terjedelmi korlátok miatt ennek áttekintésére nincs lehetőség.

A portálok elsődleges célja, hogy a tartalmat feltöltők szabadon rögzíthessék véleményüket, melyet a szólásszabadság által rögzített elvárás indokol.[38] Ez azonban nem jelenti azt, hogy a platformok ne rendelkeznének felelősséggel a rajtuk megosztott tartalmakért.

[37] Uo.
[38] NUNZIATO, D. C., First Amendment Values for the Internet, In *First Amendment Law Review*, 2014, 13, pp. 282-314.

2. 2. EURÓPAI UNIÓ

Térjünk át az Európai Unió szabályozásának bemutatására, mely egy fokkal szigorúbb és korlátozóbb fellépési lehetőséget garantál, mint az Amerikai Egyesült Államok. Mindenekelőtt fontos leszögezni, hogy a terrorizmus elleni küzdelem elsődleges prioritást jelent az EU és annak tagállamai, valamint nemzetközi partnerei számára, hiszen a legsúlyosabb veszélyt jelentik az Unió alapértékeire,[39] a jogállamiságra, valamint a demokráciára.[40] Az Uniós szabályozás leszögezi, hogy a terrorizmus elleni küzdelem elsődlegesen a tagállamok feladata, mindazonáltal az EU támogatást nyújt abban, hogy hatékonyan tudjanak fellépni e jellemzően országhatárokon átnyúló veszéllyel szemben,[41] melyben szerepet játszik az EUROPOL és az EUROJUST is, melyek elsődleges feladata a nemzetközi együttműködés megteremtése a nemzeteken átívelő bűncselekmények leküzdése érdekében.[42]

Tekintsük át tehát az uniós jogi szabályozást, a terrorizmus kérdéskörére fókuszálva. E szabályozás sajátossága, hogy az elmúlt néhány évben alapvetően háromirányú célkitűzés bontakozott ki. Egyrészt, megfigyelhető a szabályok szigorítása, a terrorizmus új formáinak kiküszöbölése és megakadályozása érdekében. Másodsorban a külső határokon végzett ellenőrzések számának emelése, minőségének javítása is előtérbe került. Ami azonban dolgozatom szempontjából a leglényegesebb, egy kifejezetten az online terrorista propaganda megfékezésével foglalkozó szervezet létrehozása is terítéken szerepel, melynek feladata az interneten keresztül terjesztett terrorista propaganda, valamint a kibertéri támadások elhárítása és megfelelő mederben tartása lenne.

2007 óta Gilles de Kerchove a terrorizmus elleni küzdelem uniós koordinátora, aki az Unió terrorizmus elleni stratégiájának végrehajtását felügyeli, valamint aktív szerepet vállal abban, hogy az EU fokozott szerepet játsszon a terrorizmus elleni hatékony fellépésben.[43]

2015 májusában a Tanács az Európai Parlamenttel közösen irányelvet fogadott el a pénzmosás, valamint a terrorizmus finanszírozásának megakadályozása érdekében, melynek közvetlen indukálói a párizsi terrortámadások voltak. Az Európai Bizottság módosítójavaslatának köszönhetően az Unió fokozott szerepe és felelőssége került előtérbe,

[39] Az Európai Parlament és a Tanács (EU) 2017/541 irányelve a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról (2)
[40] BLUTMAN László: Az Európai Unió joga a gyakorlatban, HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2014, 519 p.
[41] EU 2017/541 irányelve (5)
[42] Az Unió a terrorizmus elleni harcban, Consilium Europa.
[43] A terrorizmus elleni küzdelem koordinátora, Consilium Europa.

több nemzetközi jogi előírást az uniós jogba ültetve, mint például az ENSZ Biztonsági Tanácsának 2178.-ik számú határozatának rendelkezései a külföldi terrorista harcosokról, vagy az Európa Tanács terrorizmus megelőzéséről szóló egyezményének kiegészítő jegyzőkönyve.[44]

Bár az irányelv még egyik tagállamban sem került implementálásra, mégis kijelöli azokat a sarokköveket, melyek az Unió terrorizmussal szembeni hozzáállását képviselik. Az irányelv a tagállamok számára olyan kötelezően elérendő célkitűzést állapít meg, melynek átültetése és konkrét jogszabályi köntösbe burkolása az egyes országok feladata.

Dolgozatom témája szempontjából kiemelt jelentősége van annak, hogy a javaslat megerősítette azon rendelkezéseket is, melyek kriminalizálják a terrorista propaganda terjesztését, beleértve ennek interneten megvalósuló formáit is.[45]

Az Unió irányelve szerint „a terrorista bűncselekmény elkövetésére való nyilvános uszítás bűncselekményének minősül többek között a terrorizmus dicsőítése és igazolása – például a terrorizmus áldozataival kapcsolatos – üzenetek vagy képi felvételek abból a célból online vagy offline módon történő terjesztése, hogy a terroristák ügye támogatást kapjon, vagy hogy a lakosságot súlyosan megfélemlítsék.”[46] A szabályozás azonban leszögezi, hogy az eset konkrét körülményeit mindig figyelembe kell venni, nevezetesen azt, hogy ki az üzenet szerzője és címzettje, valamint, hogy milyen kontextusban került sor a cselekmény elkövetésére.[47] Az egyes nemzeti jogi szabályozás eltérései előtérbe kerülhetnek az adott magatartás értékelése során, mely véleményem szerint tágabb teret biztosít a terrorszervezetek általi visszaéléseknek és nagyobb felelősséget hárít a hazai jogalkotásra.

A 11.-ik szakasz a „terrorista kiképzésben való részvétel” bűncselekményi körét szélesíti ki azzal, ha valaki az interneten keresztül olyan oktatóanyagokat tanulmányoz, melyek később terrorcselekmények, merényletek elkövetését indukálják. Itt többletkritériumok is érvényesülnek, ugyanakkor a médiamegosztó portálok felelőssége is előtérbe kerül. A robbanószerkezet-készítésről szóló információk, videók gyakran ezekről az oldalakról érhetőek el, így a szigorúbb szabályozás, vagy a hatékonyabb terrorista-ellenes szervekkel történő együttműködés a portálok részéről egy lehetséges megoldást kínálna erre a problémára.

[44] EU 2017/541 irányelve
[45] „Az ilyen magatartásoknak akkor is büntetendőnek kell lenniük, ha azokat az interneten követik el, a közösségi médiát is beleértve.” EU 2017/541 irányelve (6)
[46] Uo. (10)
[47] Uo.

Témám szempontjából a leglényegesebb a 22.-ik szakasz, amely a terrorista bűncselekmény elkövetésére való nyilvános uszításnak minősülő online tartalom forrásnál történő eltávolítását tűzi ki célul. Amennyiben e tartalom harmadik ország területéről származó IP címről érkezik, a tagállamok feladatává teszi ezen országok kiemelt szerveivel való hatékony együttműködést. Elsődleges tehát közvetlenül a forrásnál történő eltávolítás, amennyiben ez nem lehetséges, akkor kerül előtérbe a tartalom blokkolása az Unió területén belül.[48] Fontos azonban leszögezni, hogy kivételként jelenik meg a tagállami jogalkotási, nem jogalkotási, valamint igazságügyi fellépésen belül az internetszolgáltatók általi önkéntes fellépés, vagy az ehhez nyújtott támogatás, amely a terrorizmussal összefüggő tartalmak kiszűrésére és megjelölésére vonatkozik. Így tehát megállapítható, hogy az irányelv kizárólag a tagállami feladatokat tűzi ki célul, a portálok felelőssége háttérbe szorul. Korlátként jelenik meg a jogbiztonság és a kiszámíthatóság elvének érvényesülése, a felhasználók jogainak tiszteletben tartása, valamint az Unió Alapjogi Chartájának (továbbiakban: a Charta)[49] való megfelelés.

Emellett az eltávolítás, vagy a tartalomkorlátozás nem érintheti a 2000/31/EK európai parlamenti és tanácsi irányelvben rögzített szabályokat sem. A szolgáltatás nyújtójának a jogellenes tevékenységről való tényleges tudomásszerzést követően haladéktalanul intézkednie kell, a véleménynyilvánítás szabadságának elvét tiszteletben tartva, illetve a nemzeti eljárásoknak megfelelve. Azonban, a hazai jogalkotás speciális körülményeket is megállapíthat, így szélesebb mozgásteret biztosít az Unió.[50]

A szabályozási korlát vonatkozik továbbá arra is, hogy nem írható elő a szolgálatók számára olyan általános kötelezettség, amely a jogellenes tartalmak utáni aktív kutatási tevékenységet, vagy a tárolt, vagy továbbított információ figyelemmel kísérését írná elő.[51] A szolgáltatókat továbbá mindaddig nem lehet felelősségre vonni, amíg ténylegesen tudomást nem szereztek a jogellenes tevékenységről, vagy nem állapították meg, hogy jogellenes tartalomról van szó.

A korábban említett terrorista bűncselekmény elkövetésére való nyilvános uszítás, mint bűncselekmény – amely nemcsak offline, de online formában is elkövethető – a terrorista tevékenységhez kapcsolódó bűncselekmények között jelenik meg.[52] Ezek olyan felbujtás

[48] Uo. (22)
[49] Az Európai Unió Alapjogi Chartája (2016/C 202/02)
[50] Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (46)
[51] EU 2017/541 irányelve (23)
[52] Uo. III. cím, 5. cikk

jellegű magatartások, melyek a merényletek elkövetését indukálják, ilyen lehet például a terrorista cselekmények dicsőítése.

A 6. cikk a terroristák toborzását határozza meg, mint az Unió értékei alapján bűncselekményként értékelt magatartást. Ez, mint láthattuk, a médiamegosztó portálokon közzétett propagandavideók által is megvalósítható, hiszen alkalmas lehet a „felsorolt bűncselekmények egyikének elkövetésére vagy elkövetésében való közreműködésre való felhívásra".[53] A 8. cikkben kifejtett terrorista kiképzésben részesítés már fentebb említésre került, itt tehát elsősorban azokat a felhasználókat büntetik, akik tájékoztató anyagokat töltenek le, vagy vesznek igénybe merényletek elkövetése céljából. Ezen bűncselekményi kör esetében a portálok felelőssége kevéssé érvényesül, ugyanakkor véleményem szerint szerepük nem elhanyagolható. A 14. cikk egyértelművé teszi, hogy a részesi magatartások, tehát a bűnsegély és a felbujtás, valamint az egyes bűncselekmények kísérlete is büntetendő a tagállami jogalkotó által.[54]

A nyilvános uszításnak minősülő online tartalmakkal szembeni intézkedések körében az irányelv az alábbi célkitűzéseket határozza meg a tagállamok számára: elsősorban gondoskodniuk kell a tartalom eltávolításáról, amennyiben azok a területükön üzemeltetett szerveren találhatók. Azonban a területükön kívül üzemeltetett szerverek esetében is meg kell kísérelniük ezen tartalmak minél előbbi eltávolítását.[55]

Mint korábban kifejtésre került, a második lépcső a területükön élő felhasználók esetében a tartalom blokkolása, amely abban az esetben érvényesül, ha az elsődleges intézkedésre nincs lehetőség.[56] Mindkét esetben tájékoztatni kell a felhasználókat az intézkedések okairól, azoknak szükségesnek és arányosnak kell lennie. Foganatosításukra csak átlátható eljárást követően van lehetőség és biztosítani kell a jogorvoslati lehetőséget velük szemben.[57]

Kiemelendő, hogy a Tanács 2015-ben megbízta az Europolt azzal a feladattal, hogy egy külön egységet alkosson az interneten terjesztett terrorista propaganda felszámolása érdekében. E szélsőséges tartalmakkal foglalkozó uniós egység (EU IRU) 2015 júliusában alakult meg. Az EU IRU feladatai közé tartozik, hogy azonosítsa a terrorista célú, valamint az erőszakos, vagy

[53] Uo. III. cím, 6. cikk
[54] Uo. III. cím, 16. cikk
[55] Uo. IV. cím, 21. cikk (1)
[56] Uo. IV. cím, 21. cikk (2)
[57] Uo. IV. cím, 21. cikk (3)

szélsőséges tartalmakat az interneten, és ezekkel kapcsolatban tanácsokkal lássa el a tagállamokat.

Az Unió szempontjából különösen a Jihadista csoportok szerepe említhető, melyek a szociális médiában rejlő lehetőségeket korán felismerték és rendszeresen kiaknázzák.[58] Ennek keretében követőket gyűjtenek, valamint a terrorista értékrend terjesztésén keresztül érvényesítik propagandájukat. Az EU IRU feladata a terrorista tartalmak kiszűrése, majd ezt követően támogatás nyújtása az érintett tagállamok számára, a hatékony fellépés érdekében.[59] Az Unión belüli fokozott együttműködés és adatbázis-összesítés ennek elengedhetetlen eszköze, valamint a tagállamok tájékoztatása a hatékony fellépési lehetőségekről. Gilles de Kerchove kiemelte, hogy különösen fontos, hogy az Unió részéről koordinált fellépés valósuljon meg. Ennek érdekében együttműködési megállapodások születtek több szociális média platformmal, melyek lehetővé fogják tenni a közeljövőben az Unió intézményei részéről történő fokozottabb beavatkozási lehetőséget. Emellett a tagállamok részéről minden év végén statisztikai jelentés készül az adatokról, melyek a terrorizmussal szembeni küzdelemmel kapcsolatban felmerültek az online platformokon.

2.3. NÉMETORSZÁG

A Hálózati Végrehajtási Törvény (továbbiakban NetzDG) 2017. október 1-jén lépett hatályba Németországban. Ezen törvény képezi a médiaszabályozás gerincét. A törvény kettős célkitűzést támaszt. Egyrészt, a jogszerűtlen tartalmakra vonatkozó panaszok kezelését áttekinthető eljárás keretében szabályozza, másrészt a közösségi hálózatokat arra kötelezi, hogy félévente jelentést készítsenek, melynek közzétételére kötelesek.[60] Ez hasonló célt szolgál, mint az EU-s jelentési rendszer. Rögzíti az eltávolított tartalmakat, valamint a panaszok mennyiségéről is tájékoztatással szolgál, tehát a gyakorlatban egyfajta statisztikai adatbázisként funkcionál. A jelentés emellett következtetéseket rögzít az eltávolítások gyakoriságáról, lényegi információkra reflektálva.[61]

A törvény hatálya a közösségi hálózatokra terjed ki, beleértve azokat is, melyeket egyedi kommunikációra (pl. WhatsApp, Telegram), vagy meghatározott tartalom terjesztésére szántak (pl. Facebook, YouTube).[62] A kétmilliónál kevesebb regisztrált felhasználóval rendelkező

[58] Terrorism and social media, Wikipedia.
[59] EU Internet Referral Unit – EU IRU EU, Europol.
[60] RADSCH, Courtney C.: Proposed German legislation threatens broad internet censorship, CPJ.
[61] PATEL, Faiza: EU 'Terrorist Content' Proposal Sets Dire Example for Free Speech Online, JustSecurity.
[62] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) 1. § (1)

közösségi hálózatok szolgáltatója mentesül a jelentéstételi kötelezettség alól.[63] Az illegális tartalom a német büntető törvénykönyv meghatározott törvényi tényállásának megfeleltethető tartalom, mely alább részletesen kifejtésre kerül.[64]

A 2. § a jelentésre vonatkozó lényegi információkat rögzíti. Eszerint a portáloknak saját honlapjukon félévente jelentést kell közzétenniük az eltávolított illegális tartalmakról. E jelentésnek könnyen felismerhetőnek, azonnal hozzáférhetőnek és folyamatosan elérhetőnek kell lennie.[65] Emellett a Szövetségi Közlönyben is meg kell jelennie. Tartalmaznia kell azt a mechanizmust, amely az eltávolításhoz vezetett, a panaszokra vonatkozó információkat, valamint egyéb adatokat.[66]

A 3. § éppen a panaszok bejelentésére alkalmas hatékony módszer kritériumát rögzíti. Fontos, hogy átlátható, hozzáférhető és könnyen kezelhető legyen. A cél a tartalom eltávolítása, második lépésben jelenik meg a tartalom hozzáférhetetlenné tétele Németország területén belül. Ez a kétlépcsős folyamat megfeleltethető az EU irányelvében foglaltaknak. Fontos, hogy a portál eltávolítás esetén a tartalmat bizonyítási célokra rögzíti, és ebből a célból tíz hétig tárolja a 2000/31/EK[67] és a 2010/13/EU[68] irányelveknek megfelelően.[69] Emellett a poráloknak haladéktalanul tájékoztatniuk kell a panaszost és a felhasználót minden döntésükről, indokolási kötelezettség mellett.

A fentebb kifejtett mechanizmusokat közigazgatási hatóság által megbízott szerv ellenőrizheti.[70] A portálok által működtett önszabályozó intézményeknek meghatározott ismérveknek kell eleget tenniük: az ellenőröknek függetlennek és szakértelemmel rendelkezőnek kell lennie, biztosítaniuk kell a megfelelő felszerelést és a tartalom gyors tesztelését, eljárási szabályoknak kell megfelelniük, valamint panaszirodát működtetniük.[71] Ezen intézmény elismeréséről az említett közigazgatási hatóság dönt, amely a jóváhagyást bármikor visszavonhatja, ha az intézmény már nem felel meg a feltételeknek.[72]

[63] NetzDG, 1. § (2)
[64] NetzDG, 1. § (3)
[65] NetzDG, 2. § (1)
[66] NetzDG, 2. § (2)
[67] EU 2000/31/EK irányelve
[68] Az Európai Parlament és a Tanács (EU) 2010/13/EU irányelve a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról
[69] NetzDG, 3. § (2)
[70] NetzDG, 3. § (5)
[71] NetzDG, 3. § (6)
[72] NetzDG, 3. § (7)-(8)

Amennyiben a portál nem tesz eleget az eltávolítási, vagy tartalomblokkolási, illetve jelentéstételi kötelezettségnek, közigazgatási szabálysértést követ el, mely tetemes bírságot vonhat maga után.[73] A 4. § (3) bekezdése értelmében a közigazgatási szabálysértés akkor is elkövethető, ha azt nem Németországban követték el.

A NetzDG előírása szerint a közösségi hálózatok kötelesek a „nyilvánvalóan jogsértő" tartalmak helyi eltávolítására az értesítés beérkezésétől számított 24 órán belül. Ennek feltétele az, hogy valamely felhasználó, vagy megtekintő panasszal jelezze az adott tartalom jogsértő voltát, tehát a platformok felelőssége ebben az esetben is háttérbe szorul. Ugyanakkor elrettentő erőként jelenik meg a médiamegosztó portálok előtt az akár 50 millió eurót is elérő büntetés,[74] amennyiben a megjelölt tartalom nem kerül eltávolításra.[75] Ennek kiszabása az Igazságügyi Minisztérium hatáskörébe tartozik.

Rögzíti továbbá a törvény, hogy amennyiben a jogsértés nem egyértelmű, vagy nyilvánvaló, a platformnak egy hete van a döntés meghozatalára. Bizonyos esetekben a döntés ennél tovább is elhúzódhat, amennyiben szükséges hozzá a tartalmat feltöltő felhasználók véleményének kikérése, vagy a döntés fokozott mérlegelést igényel. Mivel azonban az esetek nagy része a gyakorlatnak megfelelően nem minősül kivételesnek, így a portálok ügyelnek arra, hogy a lehető legrövidebb időn belül intézkedjenek.[76]

A platformoknak emellett együttműködési kötelezettségük van a hatóságokkal. 48 órán belül hatékony tájékoztatást kell adniuk a gyűlölködő tartalmakkal kapcsolatban, ellenkező esetben szintén bírságra számíthatnak.[77]

Tekintsük át, milyen esetekben kell a bepanaszolt tartalmat eltávolítani. A NetzDG értelmében akkor, amennyiben a német büntető törvénykönyvben (StGB) szereplő 21 bűntetőjogi jogszabály egyike vonatkozik rá. Emellett, amennyiben bármely más helyi jogszabály alapján jogsértőnek minősül, helyileg korlátozásra kerül.

A bejelentési felület nehézsége, a jogi szakzsargon nehezen értelmezhető volt a jogi képzettséggel nem rendelkező átlagfelhasználók számára. Ezáltal a német büntető törvénykönyv vonatkozó passzusainak értelmezhetetlensége gátat szabhatott a bejelentés beküldése előtt. Azon eshetőség is előállhatott, hogy az érintett tartalom több bűncselekmény

[73] NetzDG, 4. § (1)
[74] NetzDG, 4. § (2)
[75] Merkelék nem viccelnek: életbe lépett a törvény, amellyel iszonyatosan megbüntethetik a Facebookot, HVG.
[76] Uo.
[77] REINBOLD, Fabian: Behörden nehmen viele soziale Netzwerke ins Visier, Der Spiegel.

törvényi tényállását is kimerítette, éppen ezért az ezek közötti választási lehetőség is nehézséget okozott. Vegyünk egy példát: egy terrorszervezet által közzétett propagandavideó (StGB 129., 129a. §) nagy valószínűséggel jelképeket is tartalmaz, mely az StGB 86., 86a. §-a értelmében büntetendő, ugyanakkor egyéb törvényi tényállást is kimeríthet.[78]

Ennek kiküszöbölése érdekében számos olyan lehetőséget próbáltak biztosítani, amely az átlagfelhasználók számára megkönnyítette a vonatkozó bűncselekmények beazonosítását.

Hét tartalomkategória lett kialakítva ennek biztosítása érdekében, melyek az alábbi osztályokba sorolták a panaszban hivatkozható bűncselekményeket: a „gyűlöletkeltés vagy politikai szélsőségesség" címszó alatt az uszítás és gyűlöletkeltés (StGB 130. §), valamint a vallásgyalázás, illetve vallási vagy ideológiai szervezetek rágalmazása (StGB 166. §) volt kiválasztható. Számunkra relevánsabb a második osztályban szereplő bűncselekmények köre, mely a „terrorista vagy alkotmányellenes tartalom"-ba sorolható bűncselekményi kört ölelte fel. Ide többek között a következő tényállások tartoztak: alkotmányellenes szervezetek propagandaanyagainak terjesztése (StGB 86. §), alkotmányellenes szervezetek jelképeinek használata (StGB 86a. §), az államrendet veszélyeztető, súlyosan erőszakos cselekmény előkészülete (StGB 89a. §), az államrendet veszélyeztető, súlyosan erőszakos cselekményre való felbujtás (StGB 91. §), hazaárulás és nemzetbiztonságot veszélyeztető visszaélés (StGB 100a. §), bűnszervezetek létrehozása (StGB 129. §), terrorszervezet létrehozása (StGB 129a. §).

A következő tartalomkategória szintén gyakori volt a közösségi médiában megjelenő terrorista tartalmak jelentése kapcsán: a büntető törvénykönyv 131.-ik szakasza értelmében büntetendő az erőszak ábrázolása is.[79]

A negyedik osztályban a „káros vagy veszélyes cselekmények" kerültek feltüntetésre. Ide tartoztak a bűncselekményre való nyilvános felbujtás (StGB 111. §), a közrend megzavarása bűncselekménnyel való fenyegetéssel (StGB 126. §), valamint ezzel összefüggésben az utóbbi jogsértések támogatása. Szintén itt szerepelt az erőszakos bűncselekmény elkövetésével való fenyegetés (StGB 241. §) tényállása is.

Az ötödik, hatodik, valamint a hetedik tartalomkategória („rágalmazás vagy becsületsértés", „adatvédelem", illetve „szexuális tartalom") kevésbé hivatkozott a terrorista

[78] NetzDG (2017)
[79] Strafgesetzbuch (1998)

tartalmak jelentése kapcsán, ugyanakkor a szexuális tartalmak szabályozása sok esetben nagyon hasonlóan alakul, mint a propagandavideók jogi kontrollálása.

Ezen szabályozás egy áttekinthető platformot teremtett, könnyen hozzáférhető és egyértelmű lépéseken keresztül lehetővé téve azt, hogy minél könnyebb legyen az átlagfelhasználók számára panaszuk bejelentése. Látható, hogy a német szabályozás sokkal szigorúbb és merevebb, mint az amerikai megközelítés. A tetemes bírság hatékony motiváló erő a portálok számára, hogy intézkedjenek. A Facebook például 7500 fős moderátor-csapatot alkotott ennek hatására.[80]

2.4. AUSZTRÁLIA

Kuriózumként tekintsük át Ausztrália lényegi jogi szabályozását. Az USA-hoz hasonlóan, itt is történtek olyan váratlan terrortámadások (nevezetesen két mecset ellen, Christchurch városában, valamint Új-Zélandon)[81], melyek esetében az internet lehetett a merényletek megszervezésének középpontja.[82]

A terroristák élőben közvetítették a lövöldözéseket a Facebook LIVE funkciója segítségével, amely néhány percen belül hatalmas nézettségre tett szert és rendkívül széles körben megosztásra került. A YouTube, illetve a Facebook nagyon lassan és inaktív módon blokkolta a terrorista csoportok tevékenységét, a videók milliós nézettségre tettek szert, mielőtt eltávolításra kerültek.

Az események hatására központi kormányzati tárgyalásokat tartottak, melynek keretében a legfontosabb internetszolgáltatók, valamint a kormányzati szervek képviselői (különös tekintettel az e-biztonságért felelős biztosra, illetve a Kommunikációs Szövetségre) hatékony tervezetet dolgoztak ki a terrorizmussal szembeni fellépés érdekében. A tervezett intézkedési javaslat, mely irányadó a szociális médiaplatformok esetében, az alábbi kulcselemekre koncentrál:

- **Proaktív technikai beavatkozás:** Ennek keretében a médiamegosztó portáloknak jelentési kötelezettsége van az ausztrál kormány felé, amennyiben terrorista tartalom kerül feltöltésre, valamint együtt kell működniük terroristaellenes szervezetekkel az algoritmusok megerősítése érdekében. Lényeges kitétel az

[80] Merkelék nem viccelnek: életbe lépett a törvény, amellyel iszonyatosan megbüntethetik a Facebookot, HVG.
[81] Terrortámadás Új-Zélandon, negyvenkilencen meghaltak, Index.
[82] Report of the Australian taskforce to combat terrorist and extreme violent material online, PMC.

algoritmusok és az MI-rendszerek folyamatos felülvizsgálata, valamint az átlátható fellépés biztosítása a felhasználók számára, az erőszakos tartalmakkal szemben.

- **Fokozott moderáció:** A portáloknak olyan technikai rendszereket kell kidolgozniuk, amelyek a megjelölt tartalmakat felülvizsgálják, az ausztrál jogszabályokkal összevetve.

- **Élő közvetítés felügyelete:** Ez a hatékony észlelési rendszer kifejlesztését jelenti az élő közvetítések esetében, valamint az új, vagy folyamatosan felhasználási feltételeket sértő felhasználók tevékenységének átmeneti korlátozását (hosszabb várakozási idő beiktatása két videó feltöltése között, nézőszám csökkentése, fióktevékenység monitorozása, stb.). Kiemelt jelentőséggel bír továbbá a megjelenési lehetőségek kiszélesítése is.

- **Együttműködés:** Feladat a médiaszolgáltatók általi támogatás biztosítása a kutatási csoportoknak, melyek a terrorizmussal szembeni online fellépési lehetőségeken dolgoznak. Fontos továbbá olyan kormányzati szervek létrehozása is, melyek a terrorizmussal szemben veszik fel a harcot. Emellett a platformoknak ésszerű időn belül az Ausztrál Szövetségi Rendőrséget (AFP) is tájékoztatniuk kell, amennyiben erőszakos tartalomra bukkannak.[83]

- **Tartalomblokkolás:** Az 1997-es Telekommunikációs Törvényre hivatkozva (581)(2A) blokkolni kell az illegális tartalmakat, melyek terrorista tevékenységre utalnak[84], illetve protokollt kidolgozni egy esetleges online válság esetére (MI-rendszer által működtetve). Ennek keretében a telekommunikációs szolgáltatóknak, mint amilyen a Telstra, az Optus, vagy a Vodafone lehetőségük van a hozzáférés megszakítására, amennyiben online válságesemény történik.[85] Ezt az e-biztonságért felelős biztos irányítja, akinek az utasítása alapján az weboldalak akár 5 napra is hozzáférhetetlenné tehetőek.

- **Vészhelyzeti hálózati reagálás:** Kiemelt jelentőséggel bír a médiamegosztó portálok és a kormányzati szervek együttműködése azonnali reagálást biztosító hatékony fellépés érdekében. Online válsághelyzetről akkor beszélhetünk, ha egy merényletet követően az eseményt bemutató anyagokat rendkívüli gyorsasággal megosztják az interneten.[86]

[83] Stronger action against terror content, Prime Minister of Australia.
[84] Telecommunications Act of 1997.
[85] To prevent a repeat of Christchurch, websites hosting violent videos could be blocked, ABC News.
[86] Uo.

- **Periodikus jelentés:** A médiamegosztó portálok feladataként jelenik meg kijelölt kormányzati szervnek történő jelentés három hónappal a javaslat életbe lépését követően, az intézkedések implementálásáról. Emellett félévente jelentés-közzétételi kötelezettségük is van a detektált terrorista tartalmakról, ezáltal biztosítva az állam számára a fellépési lehetőséget a terrorszervezetekkel szemben.

- **Fiók felülvizsgálat:** Biztosítani kell a médiaplatformok részéről a kétes fiókok felülvizsgálatát, valamint megfelelő jogorvoslati lehetőséget a visszaélések elkerülése érdekében.

- **Kapacitásbővítés:** Működtetni kell egy önálló, független szervezetet (GIFCT), akik teljes munkaidőben a terrorizmus elleni online küzdelmen dolgoznak, emellett olyan kisebb szerveket támogatni, melyek az erőszakos tartalmakkal szemben lépnek fel.

A politikai vezetők éppen ennek hatására súlyos pénzbüntetést (akár a platform éves forgalmának 10%-át), valamint komoly büntetőjogi szankciókat léptettek hatályba az internetes platformok vezetőivel szemben, arra az esetre, amennyiben nem tartják be az intézkedéseket.[87] A javaslatot törvényi köntösbe szeretnék önteni, mely várhatóan a 2015-ös Online Safety Act[88] módosításával, vagy felváltásával lép majd hatályba.[89]

Scott Morrison miniszterelnök hangsúlyozta, hogy központi kérdésként jelenik meg az élő közvetítés, valamint az üzenetek gyors terjedése az internetes fórumokon, médiamegosztó portálokon keresztül.[90]

A Christchurchi merényletet követően az ausztráliai internetszolgáltatók önkényesen közel 40 olyan portált blokkoltak, melyeken az erőszakos tartalom megtalálható volt.[91] A fellépéssel azonban probléma volt, hiszen nem egységes mederben történt, egységes jogszabályi alap hiányában.

Emellett a büntető törvénykönyv az „erőszakos anyagok jogellenes bemutatása” tényállásával bővült, mely a médiamegosztó portálok felelősségre vonásának lehetőségével kecsegtet.[92]

[87] Australia’s plans for internet regulation: aimed at terrorism, but harming human rights, AccessNow.
[88] Online Safety Act (OAS) of 2015.
[89] Australia passes social media law penalising platforms for violent content, The Guardien.
[90] Stronger action against terror content, Prime Minister of Australia.
[91] Australia to block internet domains hosting extremist content during terror attacks, Reuters.
[92] Criminal Code Act of 1995.

A törvényjavaslat[93] értelmében az ausztrál kormánynak (az e-biztonságért felelős biztoson keresztül) felhatalmazása lenne arra, hogy megadályozza a médián keresztül terjedő terrorista tartalmakat, ugyanakkor hatalmas problémát jelentene a polgároknak, ha a médiát jelentős mértékben korlátoznák, ami nem más, mint a demokrácia és a véleményszabadság 21. századi fóruma.

A szabályozás egyik Achilles-sarka éppen a „terrorista tartalom" definíciójának meghatározása. A kormány számításba vette az „erőszakos tartalmak" megnevezést, azonban a homályos, nem egyértelmű fogalmak könnyen az emberi jogok megsértéséhez vezethetnek, így ezzel csínján kell bánni. Az ausztrál kormány szabályozásának gerincét az alábbi mondattal foglalhatjuk össze: "Távolítsd el, vagy jól megbüntetünk!". Így tehát az állam a portálok feladatává teszi azt, hogy detektálják, és minél előbb blokkolják a terrorszervezetek által közzétett tartalmakat, ellenkező esetben az oldalak vezetőit éri büntetőjogi szankció.[94] Ez valamilyen szinten egyfajta nyomást gyakorol a portálok üzemeltetőire, talán gyorsabb fellépésre ösztönözve őket.

Aggasztó azonban, hogy a tartalom megfelelő biztosítékok nélküli eltávolítása megkockáztathatja a döntő bizonyítékok elenyészését és az emberi jogi visszaélések nyomon követésére, és jelentésére irányuló erőfeszítések meghiúsulását.

Ausztrália szabályozási struktúrája rendkívül átlátható és egyszerű. Lényegi koncepciója a problémák online platformokra történő hárítása, valamint a fenyegetéssel történő cselekvésre ösztönzés, amely akár börtönnel is kecsegtet abban az esetben, ha nem tartják be a megfelelő előírásokat a platformok felelősei (tehát nem implementálják a fentebb kifejtett intézkedéseket).[95]

Kérdés, hogy ez a fajta szigorúbb megközelítés vajon mennyiben ösztönzi arra a médiamegosztó portálokat, hogy együttműködjenek a hatóságokkal. Véleményem szerint a szigorúbb állami kézben tartás megfelelő irányvonalat jelöl ki, ugyanakkor kissé kifinomultabb eszközökre lenne szükség ahhoz, hogy ne ellenszenvet, hanem kooperációt érjenek el a disztributív platformok üzemeltetői részéről.

[93] Media Release: New Online Safety Act to keep Australians safe, Paul Fletcher.
[94] Az internetszolgáltatók továbbra is blokkolják az erőszakos grafikai tartalmakat Ausztráliában, ZDNet.
[95] Laws targeting terror videos on Facebook and YouTube 'rushed' and 'knee-jerk', lawyers and tech industry say, ABC News.

3. HAZAI SZABÁLYOZÁS ÁTTEKINTÉSE

Mint ahogy az Uniós irányvonalat bemutató alfejezetben említésre került, a hazai szabályozás erőteljesen támaszkodik az Európai Unió megoldásaira, ugyanakkor az is leszögezendő, hogy az EU az egyes tagállamokra és azok szabályozási megoldásaira bízza a médiamegosztó portálok ellenőrzését és az erőszakos tartalmak felülvizsgálatát. Mivel a részletesen kifejtett irányelv még egyik tagállamban sem került implementálásra, így ezek a technikai megoldások egyelőre csupán elméleti síkon léteznek, iránymutatásként szolgálva a szabályozás fejlesztésére és a későbbi jogi megoldásokra.

Hazánkban az önálló szabályozó szervként működő Nemzeti Média- és Hírközlési Hatóság (továbbiakban: NMHH) az, amely elsődlegesen és szinte kizárólagosan a médiaszabályozással foglalkozik. Vezetője az Alaptörvény felhatalmazása alapján jogszabályt alkothat, a szervezet által kifejtett tevékenységéről évente beszámol az országgyűlésnek.[96] Az NMHH 2014. január elseje óta működteti a „központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát" (továbbiakban: KEHTA), amely meghatározott weboldalak blokkolására vonatkozó határozatok tárolásáért felelős, amennyiben a terrorizmus, a gyermekpornográfia, vagy az állam ellen elkövetett bűncselekmények gyanúja merül fel a közzétett tartalmak tekintetében. A KEHTA elindulása óta ellentétes fogadtatásra tett szert: egyesek hatékony eszközként, mások viszont könnyedén megkerülhető, kijátszható korlátozásként, vagy éppen internetcenzúraként tekintenek a működésére.[97] Az ellentétes fogadtatás ellenére azonban lényegi jelentősége van, hiszen ez az a rendszer, amely a terrorista tartalmak kiszűréséhez és rögzítéséhez segítséget nyújt, így működésének áttekintése elengedhetetlen a szabályozás megértése szempontjából.

Az NMHH az internetszolgáltatókkal együttműködve üzemeltik ezt a rendszert, melyek az adatbázisába bekerülő honlapokat átmeneti jelleggel, vagy végérvényesen elérhetetlenné teszik Magyarországon. A KEHTA, abban az esetben, amennyiben az internetszolgáltatók nem hajlandóak a megjelölt visszás tartalmakat törölni, blokkolni, vagy egyéb módon eltávolítani, akkor a bíróságoknak az adott ügyben hozandó jogerős ítéletének meghozataláig ideiglenesen, - vagy az ítélet függvényében véglegesen – elérhetetlenné teszi az erőszakos tartalmakat.

Létezik azonban számos olyan bűncselekmény, amelyek esetében nem szabad mérlegelési lehetőséget biztosítani az internetszolgáltatóknak, vagy a médiamegosztó

[96] Nemzeti Média- és Hírközlési Hatóság, kormany.hu.
[97] Így működik az állami internetcenzúra Magyarországon, Arsboni.

portáloknak, fokozott társadalomra veszélyességük okán. Ilyen például a már több helyen említett gyermekpornográfia (amely az USA-ban viszonylag hatékonyan működő szabályozási mechanizmussal rendelkezik), vagy a számunkra releváns terrorcselekmények. Az ilyen és ehhez hasonló tartalmak azonnal eltávolítása lényegi kérdés, hiszen képzeljük el azokat a károkat, amelyeket az áldozatok elszenvedhetnek abban az esetben, amennyiben a hatóságok nem reagálnak megfelelő gyorsasággal az elkövetett jogsértésekre.

Adódik a kérdés, hogy vajon mi volt a KEHTA rendszer megalkotásának jogi, valamint politikai célja. A hazai Büntető törvénykönyv (továbbiakban: Btk.) alapján azért volt erre szükség, mert az elektronikus hírközlő hálózat útján is elkövethető számos bűncselekmény, melyekkel szemben a kibertérben is biztosítani kell a védelmi mechanizmust. A hatályos szabályozás tükrében azonban nem volt jogszabályi előírás arra, hogy az ilyen jogellenes tartalmakat az eljáró hatóságok elérhetetlenné tegyék. Ez a joghézag – melyet a technikai fejlődés és a digitalizáció széleskörű elterjedése indukált – teremtette tehát meg a szabályozás szükségességét. A társadalmi fogadtatás sem elhanyagolható, hiszen ez tette indokolttá többek között a bankszektorban érvényesülő fokozottabb átvilágítást és felügyeletet.[98]

Kezdetben, a büntetőeljárásról szóló 1998. évi XIX. törvény alapján (régi Be.) csupán a gyermekpornográfia, az állam elleni bűncselekmények, vagy a terrorcselekmények esetén volt kötelező a tartalom mielőbbi hozzáférhetetlenné tétele hazánkban, más esetekben ez csupán lehetőségként volt feltüntetve.[99] Ezen bűncselekményi kör az elmúlt évek folyamán bővült, azonban ebből is látható a terrorszervezetek által elkövetett jogsértő cselekmények fokozott jelentősége és társadalomra veszélyességének kiemelt szerepe.

A KEHTA-rendszert létrehozó 2003-as törvény indokolása szerint: „a KEHTA adatai nem nyilvánosak, azokba a bíróság által elrendelt ideiglenes vagy végleges hozzáférhetetlenné tétel esetén a bíróság, az ügyész, a nyomozó hatóság és az Országgyűlés illetékes bizottságának a tagjai, a külön törvényben meghatározott hatóság által elrendelt hozzáférhetetlenné tétel esetén a külön törvényben meghatározott hatóság, a bíróság, az ügyész, a nyomozó hatóság és az Országgyűlés illetékes bizottságának a tagjai tekinthetnek be.” [100]

Mi lenne a hatékony megoldás a terrorizmus online terjedésével szemben? Egyre kikristályozódottabban jelenik meg az az álláspont, miszerint a közösségi médiaplatformoknak

[98] A Pénzügyi Szervezetek Állami Felügyelete Felügyeleti Tanácsának 3/2008. (XI.20.) számú ajánlása a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
[99] 1998. évi XIX. törvény a büntetőeljárásról, 158/D. § (1)(b)
[100] Az elektronikus hírközlésről szóló 2003. évi C. törvény, 159/B. § (3)

terrorista tartalmakat felismerő algoritmust kellene működtetniük, mely a szélsőséges anyagokat eltávolítja. Ariel Victoria Liebermann ennek, valamint a büntető igazságszolgáltatás fellépésének és együttműködésének a szerepét hangsúlyozza.[101]

A hazai berendezkedésben a büntető törvénykönyv (továbbiakban: Btk.) az, amely az elektronikus adat hozzáférhetetlenné tételét meghatározza meghatározott kritériumok teljesülése esetén.[102] Ez egy büntetőjogi intézkedésnek minősül, bevezetve az ideiglenes hozzáférhetetlenné tétel intézményét a hatályos büntetőeljárási törvényben (új Be.).[103] A törvény értelmében ez kétféleképpen valósulhat meg: elsődlegesen az elektronikus adat ideiglenes eltávolításával, másodlagosan a hozzáférés ideiglenes megakadályozásával.

Amennyiben ideiglenes eltávolításra kötelezik a szolgáltatót, a határozat közlésétől számított egy munkanapon belül intézkednie kell.[104] A tárhelyszolgáltató fogalmát a 2001. évi CVIII. törvény határozza meg.[105]

A Be. 337. §-a az elektronikus adathoz való hozzáférés ideiglenes megakadályozását tartalmazza. Itt is bírósági határozat szükséges ahhoz, hogy a szolgáltató intézkedésre legyen kötelezve. Első lépcsőben a határozatot közölni kell az NMHH-val is, aki a kényszerintézkedés végrehajtását szervezi és ellenőrzi.[106] Itt jön be a képbe a KEHTA, melynek rendszerébe be kell vezetni az NMHH részéről a tartalmat, valamint közölni a határozatot a szolgáltatóval. A szolgáltatónak ebben az esetben is egy munkanapja van az intézkedés végrehajtására,

---

[101] Dr. Serbakov Márton Tibor: A terroristák internethasználata, Az Új Btk.

[102] 2012. évi C. tv., 77. § (1) Véglegesen hozzáférhetetlenné kell tenni azt az elektronikus hírközlő hálózaton közzétett adatot,
a) amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg,
b) amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy
c) amely bűncselekmény elkövetése útján jött létre.

[103] 2017. évi XC. törvény a büntetőeljárásról (új Be.)
335. § (1) Az elektronikus adat ideiglenes hozzáférhetetlenné tétele az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozása és az adathoz való hozzáférés ideiglenes megakadályozása.
(2) Az elektronikus adat ideiglenes hozzáférhetetlenné tételét akkor lehet elrendelni, ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény megszakítása érdekében szükséges.
(3) Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság rendeli el.
(4) Az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendelhető
a) az elektronikus adat ideiglenes eltávolításával, vagy
b) az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával.
(5) Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról. A tájékoztatás tartalmát külön jogszabály határozza meg.
(6) Az elektronikus adat ideiglenes eltávolítása és az elektronikus adat megőrzésére kötelezés együttesen is elrendelhető.

[104] Be. 336. § (1)

[105] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. Törvény (Ekertv.) 2. § (k)

[106] Be. 337. § (2)-(4)

amennyiben ennek nem tesz eleget, az NMHH haladéktalanul tájékoztatja a bíróságot. Amennyiben az intézkedés elrendelésének indoka megszűnt, az NMHH tájékoztatása alapján a szolgáltató egy munkanapon belül ismét hozzáférhetővé köteles tenni a tartalmat, azt az NMHH törli a KEHTA rendszerből.[107]

A 338. § rögzíti, hogy az ügyészség vagy a nyomozó hatóság akár közvetlenül a médiatartalom-szolgáltatót, illetve a tárhelyszolgáltatót is felhívhatja annak érdekében, hogy önkéntesen távolítsák el az elektronikus adatokat. Ennek azonban a portálok nem kötelesek eleget tenni, semmiféle szankciót nem támaszt a jogalkotó.

Látható tehát, hogy az elektronikus adat eltávolítására a tárhelyszolgáltató a kötelezett, ez az elsődleges megoldás. Amennyiben ez nem történik meg, akkor a hírközlési szolgáltató köteles a hozzáférés megakadályozására, egyfajta szűrés keretében, ez azonban ultima ratio jelleggel érvényesül.[108]

Az NMHH szerepe tehát az alábbiakban merül ki: működteti a KEHTA adatbázist, valamint egyfajta szervező-ellenőrző tevékenységet végez a tartalmak eltávolítása és hozzáférhetetlenné tétele kapcsán.[109] Emellett a legjobb gyakorlatról ajánlásokat adhat ki, illetve segítséget nyújthat a szolgáltatók számára a KEHTA-rendszer kezelésével kapcsolatban. Feladata továbbá a megfelelő technikai környezet kialakítása is.

Mint láthatjuk tehát, a bíróságok az elrendelők, akik határozatot hoznak a tartalom eltávolításáról, vagy hozzáférhetetlenné tételéről.

Az NMHH egyfajta szervező-ellenőrző szerepet tölt be, ellenőrzi, hogy a szolgáltatók végrehajtották-e a határozatot, szükség esetén értesíti a bíróságot ennek elmaradásáról, aki kikényszeríti azt, akár rendbírság kiszabása mellett.

A szolgáltatók pedig végrehajtóként működnek a folyamatban melyhez az NMHH technikai segítséget biztosít.[110] Megjegyzendő, hogy a bírósági határozat végrehajtása továbbra is a szolgálató felelőssége, ugyanakkor díjmentesen segítséget igényelhet az NMHH-tól a tartalom szűréséhez. Ez azonban nem váltja ki a KEHTA-hoz történő csatlakozást.

A hazai szabályozás kapcsán fontos megemlíteni azt a rendszert, amelyen keresztül a felhasználók által bejelenthető a szélsőséges tartalom. Erre az NMHH Hotline keretében

[107] Be. 337. § (8)
[108] Az elektronikus adatoknak a bíróságok által elrendelt hozzáférhetetlenné tételéről, NMHH.
[109] Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.)
[110] Eht. 159/B (8)

működő bejelentő űrlap segítségével van lehetőség, amelynek segítségével a VII. kategória alatti „Terrorcselekményre felhívó, terrorizmust népszerűsítő, elősegítő tartalom" kiválasztható.[111] Ehhez mindössze egy adatvédelmi nyilatkozaton (amelynek kitöltése nem kötelező), valamint a biztonsági ellenőrzésen kell átesni, így rendkívül egyszerű a kezelése.

Az NMHH meghatározza, mit tekint az alábbi kategóriába tartozó tartalomnak.[112] A megsértett jogi normák a Btk. 314-316.-ik szakaszai.

Fontos azonban leszögezni a médiamegosztó portálok felelősségét a hazai gyakorlatnak megfelelően. Amennyiben ugyanis a sértett, vagy a médiafelügyeleti hatóság felszólítására nem távolítják el a sérelmezett tartalmat, azért úgy felelnek, mintha maguk lennének a tartalomszolgáltatók.[113]

Az Európai Parlament által elfogadott tervezet alapján (fentebb kifejtett irányelv) az internetszolgáltatóknak egy órán belül törölniük kell majd a terrorista tartalmakat. Ebbe bármely olyan információ beleértendő, mely terrorcselekményre buzdít, vagy terror jellegű eseményeket támogat, ideértve az olyan videókat is, melyek robbantóanyagok előállítását mutatják be. Kifejtésre került, hogy a kisebb szolgáltatók esetében ezen kötelezettség háttérbe szorul (lsd. EU alfejezete), ugyanakkor a nagyobb médiamegosztó portálok bírságra számíthatnak abban az esetben, ha nem tartják be a határidőt.[114]

Érdekes tény, hogy az elektronikus adatok végleges hozzáférhetetlenné tétele mindössze két esetben történt Magyarországon egészen 2016 közepéig, ráadásul egyik sem a gyermekpornográfia, az állam elleni bűncselekmények, vagy a terrorcselekmények tényállási kategóriái közé tartozott.[115]

---

[111] https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00120/

[112] Ebbe a kategóriába tartozik minden olyan tartalom az interneten, amely terrorcselekmény elkövetésére buzdít, vagy a terrorizmust népszerűsíti. Terrorcselekményre felhívó, terrorizmust népszerűsítő, elősegítő tartalomnak azokat a weboldalakon, csevegőszolgáltatáson vagy e-mailben megjelenő üzeneteket tekintjük, amelyekben vélhetően terrorcselekményre buzdítanak, illetve népszerűsítik vagy elősegítik a terrorizmust.
Terrorcselekményre felhívó, terrorizmust népszerűsítő, elősegítő tartalom, NMHH.

[113] PARTI Katalin: Harc az online illegális tartalom ellen, Okri.

[114] Az internet szolgáltatóknak egy órán belül törölniük kell majd az online terrorista tartalmakat, Nemzeti Kibervédelmi Intézet.

[115] Így működik az állami internetcencúra Magyarországon, Arsboni.

4. DISZKUSSZIÓ

A 20. században jelentkező dinamikus technikai fejlődésének köszönhetően kikerülhetetlen az IT (information technology) szektor előtérbe kerülése, mely nem csupán az egészségre és az elidegenedésre gyakorolt káros hatásainak köszönhetően került napjainkban a diskurzusok középpontjába, hanem a terrorista tartalmak rohamos megjelenésének és terjedésének okán is. E körben kiemelt jelentősége van a jogi szabályozás fontossága mellett más tudományágak megközelítésének is, többek között a társadalomtudományok, vagy a hadtudományok átfogó, interdiszciplináris problémafelvetésének. Dolgozatomban igyekeztem pszichológiai, valamint médiaszociológiai kitekintéssel szemléltetni azokat a jelenségeket, melyek ezen tartalmak következtében jelentkeznek mikro-, valamint makroszinten egyaránt.

Mivel a jog feladata a társadalmi változások lekövetése és az, hogy választ adjon égető társadalmi problémákra, így lényegesnek tartottam ennek a témának a részletesebb bemutatását, különböző tudományterületek és jogi rezsimek összevetésén keresztül.

Az informatikai rendszereknek az egész világon az a feladata, hogy informatikai folyamatokat, emberi beavatkozás nélkül bonyolítsanak le. E rendszerek elszeparált számítógépeken keresztül működnek és végzik el a feladatot, miközben kommunikációt folytatnak más számítógépekkel. Az ilyen folyamatok mögött egy humán ember áll, aki programokkal, utasításokkal irányítja őket.

Fontos azonban, hogy nem csupán a két végpontot (küldőt és címzettet) kell figyelembe venni, hanem azokat az entitásokat is, melyek e két végpont közötti hatékony, és gyors információ-, és adatcserét, kimagasló infrastruktúrát biztosítják. Ezek azok a közvetítő szolgáltatók, akik működtetik az Internet világát. Ők azok, akik hozzáférést biztosítanak a társadalom tagjainak az informatikai vívmányok megismeréséhez és kihasználásához, ugyanakkor negatív velejárója, hogy elősegítik az interneten keresztül elkövetett bűncselekmények rohamos terjedését. Ezek a szolgáltatók vállalták, hogy a társadalom deviáns viselkedésének médiamegosztó portálokon történő terjedését visszaszorítják, felvéve a harcot az olyan égető problémákkal szemben, mint amilyen a terrorizmus elterjedése.[116]

[116] A Facebook blokkolta a terroristaappot, Origo.

Több irányvonal is megszületőben van, ezeket az eltérő állami szabályozásokon keresztül igyekeztem bemutatni, rávilágítva azon lehetséges megoldásokra, melyek a leghatékonyabbnak bizonyulnak a terrorszervezetekkel szembeni harc során.

Dolgozatom végén, ezekről szeretnék egy átfogó következtetést levonni, de lege ferenda javaslat keretében bemutatva, melyik szabályozási módot tartom a leghatékonyabbnak a terrorista csoportokkal szembeni fellépés érdekében.

Az ismertetett külföldi szabályozási módok mindegyike tartalmaz hasznosítható megoldásokat, éppen ezért egy nemzetközi konferencia összehívását tartanám szükségesnek, amely a terrorizmussal szembeni online fellépés lehetőségeire koncentrálna. Az USA-ban hasonló kurzusok és konferenciák működnek, így bár maga a szabályozás túlzottan megengedő, ezt a részét követendő példának tartom a megoldás szempontjából. Erre azért volna szükség, mert igazán egyik állam szabályozási mechanizmus sem tekinthető kielégítőnek, a jogszabályi háttér sok esetben szerteágazó és követhetetlen, ami az egységes fellépést akadályozza.

Természetesen számos kétség merült fel azzal kapcsolatban, hogy egy ilyen szabályozás nem korlátozná-e túlzottan a véleménynyilvánítás szabadságát, vagy az államok önrendelkezését. Véleményem szerint azonban a terrorizmus olyan égető társadalmi probléma, amely a nemzetek feletti összefogást indokolja. Ezt azok a társadalmi és egyéni hatások indokolják, melyeket az első fejezetben részletesen ismertettem.

A konferencia keretében mindenképpen multidiszciplináris megközelítésre van szükség, tehát nem csupán az állami vezetők, vagy az IT-szektor tagjai vennének részt rajta, hanem a szociológia, a hadtudomány, valamint a pszichológia képviselői is, hogy minél átfogóbb képet alakítsanak ki arról a rendszerről, amely a lehető legnagyobb pontossággal szűrné a terrorista tartalmakat. Emellett fontosnak tartom a médiamegosztó portálok üzemeltetőinek a részvételét, hiszen ők azok, akik első kézből találkoznak azokkal a fenyegetésekkel, amelyek portáljaikon megvalósulnak.

Ennek keretében egy olyan mesterséges intelligencia rendszer kidolgozását javasolnám, amely a 8.-ik oldalon szereplő táblázathoz hasonló kritériumok mentén szűrné az erőszakos tartalmakat. Erre mintaként szolgálhat az Egyesült Királyság által készített rendszer, amely 94%-os hatékonysággal detektálja a terrorista tartalmakat.[117] Véleményem szerint azonban a

[117] DHS Announces the Launch of the "Countering Terrorists Exploitation of Social Media and the Internet" Training, DHS.

nemzetközi összefogás segítségével ennél is hatékonyabb szűrőmechanizmust alkothatunk, ha a szociológusok, vagy a pszichológusok tudását is igénybe vesszük.

A hagyományos szabályozási mechanizmusok a technikai fejlődéssel nem tartanak lépést, így ezt a problémát mindenképpen a kibertérben kell megoldani. A bemutatott szabályozásokból érzékelhető, hogy valamennyi kezdetleges szinten van, egyik állam berendezkedése sem jelent maradéktalan megoldást, érezhető a sporadikus jelleg és a jogi megoldások hiányossága.

Az említett MI-rendszer megalkotását követően egy olyan szerv létrehozását indítványoznám, amely kifejezetten a terrorizmussal szembeni online fellépésre koncentrál, vagy egy már létező állami szerv hatásköreit bővíteném ki a hatékony fellépés érdekében.

Hazánk esetében mindenképpen az NMHH hatásköreinek bővítését tartanám szükségesnek, kiszélesíteném a puszta szervező-ellenőrző szerepet, a bíróságokhoz hasonló hatósági határozat meghozatalát tenném számára lehetővé és specifikusan csak az online terrorista tartalmakra fókuszáló egységet hoznék létre, amely a Facebook csapatához hasonlóan teljeskörűen ezzel a problémával foglalkozik.[118] A bírósági határozatok meghozatala, mint láthattuk, hazánkban előfeltétele a tartalom eltávolításának, ez azonban rendkívül időigényes folyamat. Számos példával illusztráltam, hogy ennek köszönhetően akár több millió felhasználóhoz is eljuthat egy-egy videó, vagy egyéb tartalom, mielőtt eltávolításra, vagy korlátozásra kerül.

Mivel az NMHH egy önálló szabályozó szervként funkcionál, így a terrorizmussal szembeni fellépés biztos kezekben lenne, emellett bizonyos fokig tehermentesítené a bíróságokat.

A szűrést tehát a nemzetközi konferencia eredményeképpen kialakított MI-rendszer végezné, amit találóan „Big Eye”-nak neveznék el. Ez egy olyan egységes fellépést garantálna, amely nem engedne teret a portálok sporadikus szűrési mechanizmusának. Ezt a keménykezű fellépést a veszély megnövekedett jellege indokolja, amire ekletáns és elrettentő példaként szolgál a dolgozatban ismertetett számos merénylet, mely rengeteg ember életét követelte.

A szűrés eredményét maga az NMHH vizsgálná, a hatósági határozatot is ezen szerv hozná meg arról, amely a médiamegosztó portálokat a tartalom eltávolítására - amennyiben erre

[118] Merkelék nem viccelnek: életbe lépett a törvény, amellyel iszonyatosan megbüntethetik a Facebookot, HVG.

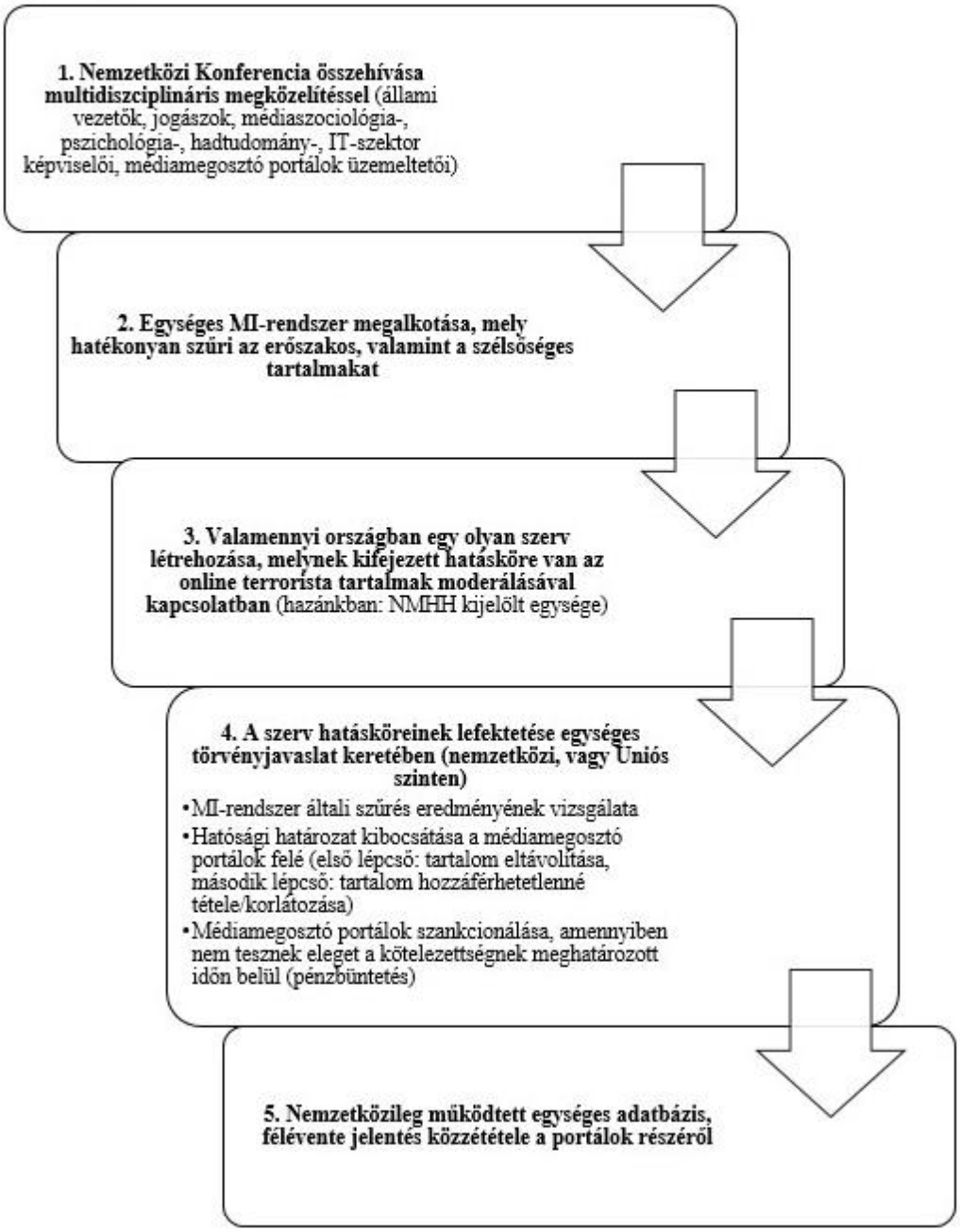
nincs lehetőség - annak hozzáférhetetlenné tételére szorítaná. Az EU által bevezetett kétlépcsős folyamatot tehát követendőnek tartom.[119]

Az NMHH hatáskörét a tekintetben is bővíteném, hogy amennyiben a portálok nem tennének eleget az eltávolítási kötelezettségüknek, szakcionálhatóak lennének az önálló szabályozó szerv által. Ugyanakkor a nagyon szigorú szabályozást, amit Ausztrália vezetett be (börtönbüntetés a portálok üzemeltetői számára, vagy busás pénzbüntetés)[120], finomítanám, mert véleményem szerint ez nem kooperációra ösztönzi a médiamegosztó portálokat, hanem ellenállásra.

Végezetül egy nemzetközileg működtetett, egységes adatbázis üzemeltetését javasolnám, amely a portálok által félévente közzétett jelentéseket tartalmazná és bárki által hozzáférhető lenne. Ez segítené a fellépés koordinálását és átlátását, a hatékonyságnövelést, valamint az igazságszolgáltatás szerveivel való hatékonyabb együttműködést.

Az általam ideálisnak tekintett megoldási javaslatot a következő oldalon látható táblázatban foglaltam össze:

[119] EU 2017/541 irányelve, IV. cím, 21. cikk (2)
[120] Australia passes social media law penalising platforms for violent content, The Guardien.



Forrás: saját szerkesztés

IRODALOMJEGYZÉK

Szakirodalom

1. BARTKÓ Róbert: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései*, Universitas-Győr Nonprofit Kft., Győr, 2011, pp. 18–22.
2. BLUTMAN László: Az Európai Unió joga a gyakorlatban, HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2014, 519 p.
3. DR. SERBAKOV Márton Tibor: A terroristák internethasználata, 2018.12.12., https://ujbtk.hu/dr-serbakov-marton-tibor-a-terroristak-internethasznalata%C2%B9/
4. ERIKSON, E. H.: Identitásválság önéletrajzi vetületben, In: Erikson: A fiatal Luther és más írások, Budapest, Gondolat, 1991, pp. 401–436.
5. ICASCON, Zann: Combating Terrorism Online: Possible Actors and Their Roles, 2018.09.02.), https://www.lawfareblog.com/combating-terrorism-online-possible-actors-and-their-roles
6. JASPERSEN, J. G., MONTIBELLER, G.: On the learning patterns and adaptive behavior of terrorist organizations, In European Journal of Operational Research, 2020, 282(11), pp. 221-234.
7. KELEMEN Roland; NÉMETH Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése, In: Farkas Ádám (szerk.) Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében, Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, pp. 147-170.
8. KOLTAY András, POLYÁK Gábor: Az Alkotmánybíróság határozata a médiaszabályozás egyes kérdéseiről, In *Jogesetek Magyarázata,* 2012, 1, p. 20.
9. KORINEK László: A terrorizmus, In *Belügyiszemle*, 2015, pp. 17–19.
10. MIHÁLY Laura Dominika: Jogsértések a médiamegosztó portálokon – médiaszociológiai és szociálpszichológiai kitekintés, In *Diskurzus,* 2019, 9(1), pp. 19-27.
11. NUNZIATO, D. C., First Amendment Values for the Internet, In *First Amendment Law Review*, 2014, 13, pp. 282-314.
12. PARTI Katalin: Harc az online illegális tartalom ellen, http://www.okri.hu/images/stories/KT/KT_49_2012/004_parti.pdf
13. PATEL, Faiza: EU 'Terrorist Content' Proposal Sets Dire Example for Free Speech Online, 2019.03.05., https://www.justsecurity.org/62857/eu-terrorist-content-proposal-sets-dire-free-speech-online/
14. RADSCH, Courtney C.: Proposed German legislation threatens broad internet censorship, 2017.04.20., https://cpj.org/2017/04/proposed-german-legislation-threatens-broad-intern/
15. REINBOLD, Fabian: Behörden nehmen viele soziale Netzwerke ins Visier, 2017.10.01., https://www.spiegel.de/netzwelt/netzpolitik/facebook-gesetz-behoerden-nehmen-viele-soziale-netzwerke-ins-visier-a-1170820.html
16. SCHMID, A.: Terrorism - The Definitional Problem, In Case Western Reserve Journal of International Law, 2004, 36(2), 390. p.
17. WEBBER, D., KRUGLANSKI, A. W.: The social psychological makings of a terrorist, In Current Opinion in Psychology, 2018, 19, pp. 131-134.

Internetes hivatkozások

1. A Facebook blokkolta a terroristaappot, 2015.12.01., https://www.origo.hu/techbazis/20151201-telegram-facebook-blokkolja-whatsapp-terrorista-alkalmazas-iszlam-allam.html

2. A NATO hivatalosan is hadszíntérré nyilvánítja a kiberteret, 2016.06.22., https://internetfigyelo.wordpress.com/2016/06/22/a-nato-hivatalosan-is-hadszinterre-nyilvanitja-a-kiberteret/
3. A terrorizmus elleni küzdelem koordinátora, https://www.consilium.europa.eu/hu/policies/fight-against-terrorism/counter-terrorism-coordinator/
4. Australia's plans for internet regulation: aimed at terrorism, but harming human rights, 2019.03.26., https://www.accessnow.org/australias-plans-to-regulate-social-media-bound-to-boomerang/
5. Australian taskforce to combat terrorist and extreme violent material online, 2019.06.21., https://www.pmc.gov.au/sites/default/files/publications/combat-terrorism-extreme-violent-material-online.pdf?fbclid=IwAR0NySm6uzPDR36Xid9dR9Q-qJgM-pp1cRuGic859dSWPYtZner0xAsN9MQ
6. Australia passes social media law penalising platforms for violent content, 2019.04.04., https://www.theguardian.com/media/2019/apr/04/australia-passes-social-media-law-penalising-platforms-for-violent-content
7. Australia to block internet domains hosting extremist content during terror attacks, 2019.08.25., https://www.reuters.com/article/us-australia-security-internet-idUSKCN1VF05G
8. Az elektronikus adatoknak a bíróságok által elrendelt hozzáférhetetlenné tételéről, 2013.04.16., https://nmhh.hu/dokumentum/157418/konzultacio_eloadasok_20130416.pdf
9. Az internet szolgáltatóknak egy órán belül törölniük kell majd az online terrorista tartalmakat, https://nki.gov.hu/it-biztonsag/hirek/az-internet-szolgaltatoknak-egy-oran-belul-torolniuk-kell-majd-az-online-terrorista-tartalmakat/
10. Az internetszolgáltatók továbbra is blokkolják az erőszakos grafikai tartalmakat Ausztráliában, 2020.03.24., https://www.zdnet.com/article/isps-to-continue-blocking-graphic-violent-content-in-australia/
11. Az Unió a terrorizmus elleni harcban, 2020.10.20., https://www.consilium.europa.eu/hu/policies/fight-against-terrorism/
12. Community Standards: Violence and Criminal Behavior, https://www.facebook.com/communitystandards/violence_criminal_behavior
13. Dangerous Individuals and Organizations, https://www.facebook.com/communitystandards/dangerous_individuals_organizations/
14. DHS Announces the Launch of the "Countering Terrorists Exploitation of Social Media and the Internet" Training, 2018.07.11., https://www.dhs.gov/blog/2018/06/11/dhs-announces-launch-countering-terrorists-exploitation-social-media-and-internet
15. EU Internet Referral Unit – EU IRU, https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
16. Hany Farid's eGlyph Can Help Europe Fight Online Extremism, 2019.09.18., https://www.ischool.berkeley.edu/news/2019/hany-farids-eglyph-can-help-europe-fight-online-extremism
17. Hard Questions: What Are We Doing to Stay Ahead of Terrorists?, 2018.11.08., https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/
18. Így működik az állami internetcenzúra Magyarországon, 2018.04.09., https://arsboni.hu/igy-mukodik-az-allami-internetcenzura-magyarorszagon/#_ftn7
19. ISIS Online: U.S. Rights and Responsibilities, https://www.counterextremism.com/content/isis-online-us-rights-and-responsibilities

20. Laws targeting terror videos on Facebook and YouTube 'rushed' and 'knee-jerk', lawyers and tech industry say, 2019.04.04, https://www.abc.net.au/news/science/2019-04-04/facebook-youtube-social-media-laws-rushed-and-flawed-critics-say/10965812
21. Mayhem and murder: 10 most shocking Facebook Live moments ever, 2018.04.06., https://abc13.com/10-most-shocking-facebook-live-moments-ever-captured/3302314/
22. Media Release: New Online Safety Act to keep Australians safe, 2019.12.11., https://www.paulfletcher.com.au/media-releases/media-release-new-online-safety-act-to-keep-australians-safe
23. Merkelék nem viccelnek: életbe lépett a törvény, amellyel iszonyatosan megbüntethetik a Facebookot, 2017.10.03., https://hvg.hu/tudomany/20171003_nemetorszag_gyuloletbeszed_buntetese_torveny_birsag_facebook_twitter_youtube_netzwerkdurchsetzungsgesetz_netzdg
24. Nemzeti Média- és Hírközlési Hatóság, https://2010-2014.kormany.hu/hu/mo/az-allam-mukodese-szempontjabol-fontos-intezmenyek/nemzeti-media-es-hirkozlesi-hatosag
25. New technology revealed to help fight terrorist content online, 2018.02.13., https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online
26. Paris attack planners used encrypted apps, investigators believe, 2015.12.17., https://www.washingtonpost.com/world/europe/paris-attack-planners-used-encrypted-apps-investigators-believe/2015/12/17/e798d288-a4de-11e5-8318-bd8caed8c588_story.html
27. Profile: James Foley, US journalist beheaded by Islamic State, 2014.08.20., https://www.bbc.com/news/world-28865508
28. Tech & Terrorism: Tech Companies Fail to Curb Online Abuses, 2019.10.03., https://www.counterextremism.com/press/tech-terrorism-tech-companies-fail-curb-online-abuses
29. Terrorcselekményre felhívó, terrorizmust népszerűsítő, elősegítő tartalmak, https://nmhh.hu/cikk/190109/Terrorcselekmenyre_felhivo_terrorizmust_nepszerusito_elosegito_tartalom
30. Terrorism and social media, https://en.wikipedia.org/wiki/Terrorism_and_social_media
31. Terrortámadás Új-Zélandon, negyvenkilencen meghaltak, 2019.03.15., https://index.hu/kulfold/2019/03/15/uj-zeland-lovoldozes-christchurch-mecset/
32. To prevent a repeat of Christchurch, websites hosting violent videos could be blocked, 2020.03.23., https://www.abc.net.au/news/science/2020-03-24/websites-hosting-terrorist-videos-blocked-by-internet-providers/12082062
33. UK unveils extremism blocking tool, 2018.02.13., https://www.bbc.com/news/technology-43037899

Jogforrások

1. 1998. évi XIX. törvény a büntetőeljárásról (régi Be.)
2. 2012. évi. törvény a Büntető Törvénykönyvről (Btk.)
3. 2017. évi XC. törvény a büntetőeljárásról (új Be.)
4. 30/1992. (V. 26.) AB hat., ABH 1992, 167, p. 181.
5. Az elektronikus hírközlésről szóló 2003. évi C. törvény
6. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.)
7. Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017.03.15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról, HL L 88., 2017.03.31., pp. 6–21.

8. Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000.06.08.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól, HL L 178., 2000.07.17.
9. Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010.03.10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról, HL L 95., 2010.04.15., pp. 1–24.
10. Az Európai Parlament és a Tanács 2012/29/EU irányelve (2012.10.25.) a bűncselekmények áldozatainak jogaira, támogatására és védelmére vonatkozó minimumszabályok megállapításáról és a 2001/220/IB tanácsi kerethatározat felváltásáról, HL L 315/57, 2012.11.14.
11. Az Európai Unió Alapjogi Chartája, HL C 326., 2012.10.26., pp. 391–407.
12. Criminal Code Act of 1995
13. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) (2017)
14. Holder v. Humanitarian Law Project, 561 U.S. (2010)
15. Online Safety Act (OAS) of Australia (2015)
16. Patriot Act of 2001
17. Strafgesetzbuch (1998)
18. Telecommunications Act of 1997
19. The Communications Assistance for Law Enforcement Act (CALEA) of 1994

Egyéb források

1. A Pénzügyi Szervezetek Állami Felügyelete Felügyeleti Tanácsának 3/2008. (XI.20.) számú ajánlása a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
2. Community Guidelines, https://www.youtube.com/intl/hu/about/policies/#community-guidelines
3. Facebook Felhasználási Feltételek, 2019.07.31., https://hu-hu.facebook.com/legal/terms
4. https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00120/
5. Terms of Service, 2019.07.22., https://www.youtube.com/static?template=terms
6. WhatsApp Terms of Service, 2018.04.24., https://www.whatsapp.com/legal/#terms-of-service