

Suller Zénó<sup>1</sup>

# Trendi terrorizmus: terroristamarketing, toborzás és megfélemlítés a közösségi médiában

## Veszélyek és az európai megoldások

*Trendy Terrorism: Terrorist Marketing, Recruitment and Intimidation on Social Media*

*Threats and the European Solutions*

A digitális fejlődés és a globalizáció a nemzetközi terrorizmus területén is érezteti hatását. Az új kihívások abból fakadnak, hogy a terrorista szervek is élnek a közösségi média és az internet által nyújtott lehetőségekkel. Ennek köszönhetően a globális toborzás, illetve a megfélemlítés, a dezinformáció soha nem látott hatékonysági fokot ért el. A tanulmány az online terrorista tartalmak konkrét megjelenési formáit, az általuk kiváltott hatást mutatja be. A növekvő nemzetbiztonsági kockázatot a nemzeti jogrendszerek és az európai közösség is felismerte. Bemutatom, hogy milyen nemzetállami büntetőjogi szabályozási megoldások tudják lefedni az online terrorista tartalmakba foglalt fenyegetéseket. Emellett a legfrissebb európai uniós rendeleti szabályozást is ismertetjük, amely az ilyen tartalmak eltávolításának biztosít közösségi normát, ezáltal csökkentve az eltérő nemzetállami szabályozásokban rejlő kollektív biztonsági kockázatot.

**Kulcsszavak:** nemzetközi terrorizmus, online terrorista tartalmak, közösségi média, online terroristatoborzás

*The digital development and globalisation inevitably influence international terrorism. The new challenges are deriving from the fact that terrorist groups are actively using the social media sites and the Internet in general. Due to this tendency, global recruitment*

<sup>1</sup> Doktori hallgató, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Doktori Iskola, e-mail: [suller.zeno@gmail.com](mailto:suller.zeno@gmail.com)

*and intimidation have reached a surprising efficacy. This essay presents the actual forms of online terrorist contents, their effects and possible consequences. The national jurisdictions and the European community have both realised the increasing national and collective security risks. Hence, the paper shows the possible national legislative solutions in criminal law. Also, the most recent European regulation on the measures concerning online terrorist contents will be presented in detail.*

**Keywords:** *international terrorism, online terrorist contents, social media, online terrorist recruitment*

## **A tanulmány tárgya, illetve a vizsgált kérdések**

A tanulmány tárgya az online terrorista tartalmak beazonosítása, az általuk generált veszélyek és kockázatok megnevezése, illetve annak a vizsgálata, hogy a jog milyen eszközökkel tud fellépni az ilyen tartalmak terjesztésével szemben. Írásom nem terjed ki a digitális vagy kiberterrorizmus minden aspektusának elemzésére. Elsősorban a terroristatoborzás, a szervezeti kommunikáció, a megfélemlítés, illetve a propaganda terjesztésének elektronikus, interneten alkalmazott módozatait vizsgálja. Ennek megfelelően a kritikus infrastruktúra, illetve elektronikus rendszerek elleni digitális terrorista hackertámadások a kutatás tárgyát és célját meghaladják, különös tekintettel arra, hogy a két módozat, nevezetesen az online terrorista tartalmak közvetítése és a digitális hackertámadások a terrorizmus különböző szakaszait jelenítik meg. Míg az első esetben az elkövetés előkészítése, illetve a már végrehajtott támadás eredményeinek félelemkeltés céljából való terjesztése történik, addig a második esetben magáról a terrorista támadás elkövetéséről van szó. Jelen tanulmány tehát az első mozzanatra, az online terrorista tartalmakra fókuszál, s a következő kérdésekre keresi a választ. Az internet és a közösségi média mely jellemzői tették lehetővé, hogy a terrorista szervezetek kiaknázzák a platformokban rejlő lehetőségeket? Miért járult hozzá az internethasználat a terrorizmus globális jelenséggé válásához? Milyen nemzetállami büntetőjogi szabályozások igyekeznek fellépni az online terrorista tartalmakkal szemben, illetve milyen változást hozhat az Európai Unió online terrorista tartalmak szabályozásáról szóló rendelete? A kutatás legfontosabb kérdése, hogy mindezek alapján, legalábbis az Európai Unió területén, remélhető-e hatékonyabb fellépés az egyik legsúlyosabb nemzetbiztonsági kockázat, a terrorizmus térnyerésével szemben.

Ezek megválaszolásához az alapvető fogalom tisztázása szükséges. Online terrorista tartalom alatt azokat a szöveges, képi, videó- vagy hanganyagokat értem, amelyeket a terrorizmus népszerűsítése, a lakosság megfélemlítése vagy az elkövetés és toborzás megszervezése céljából valamely, a felhasználók számára nyitott internetes kommunikációs, kapcsolattartó vagy közösségi platformon közzétesznek vagy továbbítanak. Ennek megfelelően a közösségi média az online, felhasználók számára nyitott üzenetközvetítő vagy tartalomszolgáltató, kapcsolattartásra szolgáló oldalakat takarja. Ilyen lehet a Facebook, a YouTube, a Twitter, a Snapchat vagy akár a TikTok, de a nyílt blogfelületek is idesorolhatók.

A tanulmány a nemzeti és az európai uniós jogi források felhasználásával és értelmezésével a megismert jelenségeket jogi kontextusba helyezi, arra keresve a választ, hogy ezekkel a jogi eszközökkel remélhető-e hatékony fellépés az online terrorista tartalmakkal szemben.

## A terrorizmus megjelenése a közösségi médiában

A közösségi média esetében nem arról van szó, hogy egy új elkövetési forma jelenik meg, hanem inkább arról, hogy a hagyományos végrehajtási módok előkészületét, megszervezését, a toborzást, a felbujtást és a kiváltott hatást – a félelmet – hatékonyabb és globálisabb szintre tudja emelni. A közösségi média és általánosságban az internet tehát a katalizátora a terrorizmusnak. Kezdetben úgy tűnt, hogy ezek a platformok a szabad internet legszebb vívmányait felvonultató online közösségi terek lesznek, amelyek a hatalmas távolság ellenére biztosítják az egymással való kapcsolattartást, nyitott eszmecserét tesznek lehetővé, segítik a világban való tájékozódást, és erősítik a szolidaritástudatot. Ezzel szemben a közösségi média ma inkább elzár, izolál, a gondolkodást extremizálja. A legtöbb ilyen platform algoritmusokkal fürkészi, hogy hol realizálódik a legtöbb *like* és kattintás, majd egyre szűkítve a tartalmat, pontosan ilyen oldalakat, közösségi csoportokat helyez a felhasználói hírfolyamba. Másrészt a gyors megosztás, letöltési lehetőség okán a terrorista tartalom elérhetősége és megtekintettsége exponenciálisan növekszik. Nem arról van szó, hogy az egyes felületeken közzétett tartalmat ne lehetne elérhetetlenné tenni, hanem arról, hogy amint ezek a tartalmak felkerülnek az internetre, letölthetővé válnak, és számos egyéb platformon oszthatók meg, esetleg más cím, más megjelölés adható nekik, ennek megfelelően valahol, valamilyen formában elérhetőek maradnak.

Ezt használta ki az ISIS<sup>2</sup> is, amely rendkívül aktívan élt a közösségi megosztás lehetőségeivel, amivel el is érte, hogy fiatalok Európában vagy akár a tengerentúl is szimpatizánsokká váljanak, és vagy a lakóhelyük szerinti országban legyenek beszervezhetők terrorista cselekmények előkészítésére és elkövetésére, vagy beálljanak az ISIS közel-keleti hadviselésének harcosai közé.

A közösségi médiában tehát alapvetően két fő veszélyforrás van a terrorizmussal kapcsolatban: a szélsőségek felé terelés és buborékba zárás, illetve a hatékonyabb megfélemlítés és az üzeneteljuttatás globális jelleggel. A két mozzanat közötti különbség az, hogy az előbbi, tehát az elszigetelődés és a szélsőséges gondolkodás megerősítése a terrorizmus verbuválását könnyíti meg, míg a második körülmény, azaz a megfélemlítés terjesztése – például kivégzéseket, merényleteket bemutató videók megosztásával – már a terrorizmus hatását katalizálja.

<sup>2</sup> Iszlám Állam (IS), később Iraki és Szíriai Iszlám Állam (ISIS), szintén használt elnevezéssel Daesh, az ENSZ Biztonsági Tanácsa által is terrorista szervezetnek minősített közel-keleti extrém militarista csoport.

## Az online terrorista tartalmak mint a terrorista propaganda terjesztésének eszközei

Az online terrorista tartalmak leginkább a terrorista propagandával azonosíthatók, hiszen ez magában foglalja a toborzást, az ideológia terjesztését és az eredmények dicsőítését, de az elkövetés szervezését, irányítását is idesorolhatjuk.<sup>3</sup> Az Európai Bizottság szerint:

„A terroristák online propagandája arra törekszik, hogy egyéneket terrorista támadások elkövetésére buzdítsa, többek között azáltal, hogy részletes utasításokat ad nekik arra vonatkozóan, hogyan lehet maximális kárt okozni. Az ilyen atrocitások után általában további propagandát osztanak meg, ezáltal dicsőítve e cselekedeteket, másokat pedig arra ösztönöznek, hogy kövessék a példát.”<sup>4</sup>

Az üzenet formája lehet kép, hanganyag, videó vagy szöveg.<sup>5</sup> A terrorista tartalmak jelentős társadalmi következményeiről a következők mondhatók ki:

„Az online terrorista tartalom jelenléte – bár nem egyedüli tényezőként – bizonyíthatóan elősegíti az egyének radikalizálódását, ami aztán terrorcselekményekhez vezethet, és ezért súlyos negatív következményekkel jár a felhasználók, a polgárok és a társadalom egésze szempontjából, valamint az ilyen tartalomnak tárhelyet biztosító online szolgáltatók számára is, mivel aláássa felhasználóik bizalmát, és károsítja üzleti modelljüket.”<sup>6</sup>

Az Európai Unió területén végrehajtott terrorista akcióknak valóban jelentős keretet adtak az online terrorista tartalmak. A Samuel Paty professzor ellen 2020 októberében Conflans-ban elkövetett támadás megtervezése és kivitelezése is online zajlott, ami hasonló erőszakos cselekményekre ösztönzött Nizzában pár nappal később.<sup>7</sup>

Az Europol statisztikája szerint az internet terroristák általi használata, különösen a közösségi médiáé, jelentősen növekedett az elmúlt években. Különösen a dzsihádisták csoportok értették meg, hogyan működik a közösségi média, és jól szervezett, koncentrált toborzókampányt indítottak és marketingtevékenységet folytattak, hogy népszerűsítsék az erőszakot és a terrorizmust.<sup>8</sup> A radikalizáció az elmúlt évek egyik olyan tendenciája, amely Európában különösen erőteljesen érezteti a hatását. A közelmúlt terrorista elkövetői ugyanis nem bevándorlók, hanem a legtöbb esetben európai polgárok voltak.<sup>9</sup> A radikalizációban nagy szerepet játszottak a közösségi médiában megtekintett tartalmak. Az Europol éves jelentése szerint az ISIS dzsihádisták propagandája különösen jelentős volt 2020-ban, lefedve több

<sup>3</sup> WAHL 2021.

<sup>4</sup> Európai Bizottság COM(2018) 640 final (3.3) bekezdés.

<sup>5</sup> Lásd: [www.consilium.europa.eu/hu/infographics/terrorist-content-online/](http://www.consilium.europa.eu/hu/infographics/terrorist-content-online/)

<sup>6</sup> 2021/784 európai parlamenti és tanácsi (EU) rendelet (2021. április 29.) (5).

<sup>7</sup> European Commission 2021.

<sup>8</sup> Lásd: [www.europol.europa.eu/about-europol/eu-internet-referral-unit-eu-iru](http://www.europol.europa.eu/about-europol/eu-internet-referral-unit-eu-iru)

<sup>9</sup> Lásd: [www.consilium.europa.eu/hu/policies/fight-against-terrorism/preventing-radicalisation/](http://www.consilium.europa.eu/hu/policies/fight-against-terrorism/preventing-radicalisation/)

közösségimédia-felületet is, így számos befogadóhoz tudott eljutni a szélsőséges üzenet.<sup>10</sup> Az internet széles körű térnyerése óta egyre ritkább jelenség, hogy egy terrorista elkövetésnek ne lenne digitális lábnyoma.<sup>11</sup> A helyzetet tovább súlyosbítja, hogy ma már az internet felhasználóinak zöme több közösségimédia-plafortot is használ.<sup>12</sup> A terrorista csoportok szintén számos felületen fejtik ki tevékenységüket, legyen az weboldal, blog, videómegosztó vagy fórum.<sup>13</sup> Az iraki és szíriai dzsihadista militaristák például használták a legnépszerűbb közösségimédia-alkalmazásokat és fájlmeosztó helyeket, így az Ask.fm, a Facebook, az Instagram, a WhatsApp, a Kik, a Tumblr vagy a Twitter a terrorista propaganda terjesztésének eszköze lett.<sup>14</sup> A legnagyobb szolgáltatók egyénileg utólag elítélték ezeket a tartalmakat, sőt egy közös terrorizmusellenes platformot is létrehoztak, hogy hatékonyabban szűrhessek az online produktumokat.<sup>15</sup> A terrorista tartalmak azonban továbbra is jelen vannak a virtuális közösségi térben, különösen azért, mert a valódi intézkedések egyéni szinten történtek. Ez azt eredményezte, hogy a terroristák egyszerűen áttértek egy másik fórumra, ha az egyikben tiltásba ütköztek.<sup>16</sup>

A terrorista csoportok ugyanazért használják az internetet és a közösségi médiát, mint a legtöbb szervezet vagy vállalkozás: a cél, hogy üzenetet juttassanak el, és hogy kiterjesszék a befolyásukat a felhasználókra.<sup>17</sup> A terroristák tulajdonképpen a marketingtechnikát is átvették: propaganda- és marketingeszközökkel trendivé, vonzóvá tették a terrorizmust. Az internet ráadásul jóval előnyösebb, mint bármilyen más médiafelület, legyen az a televízió, a rádió vagy a nyomtatott sajtó, mert a tartalom nem más által, közvetve kerül megfogalmazásra, hanem közvetlenül a terroristák által. Az érdeklődőkkel *direkt* is felvehető a kapcsolat, kialakítható a személyes kommunikáció és meggyőzés.<sup>18</sup>

Az ISIS is ezt a stratégiát vette alapul, s tagjai mintegy *influencerekként*<sup>19</sup> működtek. Az egyik ékes példa erre a véres profizmusra James Foley újságíró rituális lefejezése volt.<sup>20</sup> Számos hagyományos médiaszolgáltató vállalta fel, hogy nem közli a képeket, azonban az ISIS a közösségi médiában még talán több embert is elért, mint ha a képek a hagyományos médiában jelentek volna meg.

A tapasztalat azt mutatja, hogy a terroristamarketing sikeres: a terrorista sejtek olyan társadalmi csoportokat is meg tudnak célozni, amelyeket eddig nem, vagy csak

<sup>10</sup> Europol 2021: 8.

<sup>11</sup> BEHR et al. 2013: 3.

<sup>12</sup> DUGGAN et al. 2015.

<sup>13</sup> CONWAY 2017.

<sup>14</sup> KLAUSEN 2015.

<sup>15</sup> Facebook 2017.

<sup>16</sup> MACDONALD – GIRO CORREIA – WATKIN 2019: 184.

<sup>17</sup> WEIMANN 2004.

<sup>18</sup> ALY et al. 2016: 3.

<sup>19</sup> Magyarul véleményvezérként is fordítható kifejezés. Azokra az online közösségi tereken tartalmat gyártó egyénekre vonatkozik, akik nagy nézettséggel, követőszámmal rendelkeznek, és e nagy eléréssel érdemben befolyásolni is tudják a közönségük gondolkodásmódját.

<sup>20</sup> Lásd többek között BBC: [www.bbc.com/news/world-middle-east-28862268](http://www.bbc.com/news/world-middle-east-28862268); CNN: <https://edition.cnn.com/2014/08/19/world/meast/isis-james-foley/index.html>; ABC News: <https://abcnews.go.com/Blotter/james-foley-video-appears-show-beheading-journalist-missing/story?id=25043593>; Le Monde: [www.lemonde.fr/proche-orient/article/2014/08/20/les-zones-d-ombre-de-l-enlevement-du-journaliste-americain-james-foley\\_4473986\\_3218.html](http://www.lemonde.fr/proche-orient/article/2014/08/20/les-zones-d-ombre-de-l-enlevement-du-journaliste-americain-james-foley_4473986_3218.html)

nagyon korlátozottan. 2014-ben például három fiatal lány hagyta félbe középiskolai tanulmányait Denverben. A tizenéves lányokat Frankfurtban tartóztatták fel, Szíriába tartottak, hogy csatlakozzanak az ISIS erőfeszítéseikhez.<sup>21</sup>

## Az Európai Unió terrorizmusnak leginkább kitett államainak büntetőjogi szabályozása az online terrorista tartalmakkal kapcsolatosan

A terrorizmus globális volta miatt ma már a nemzeti bűnügyi szervek önmagukban nem képesek azt feltartóztatni. Szükséges a nemzetközi kooperáció a nyomozás és akár a bírósági eljárás, büntetés-végrehajtás területén is. Ez különösen igaz Európában, és még inkább az Európai Unióban, ahol a terrorizmus a migráció és a mozgásszabadság következtében gyakran számos államot együttműködésre készítet.<sup>22</sup> Összességében azonban még mindig elmondható, hogy „a terrorizmus elleni küzdelem területén szükséges intézkedések egyes esetekben a tagállamok kizárólagos hatáskörébe tartozó nemzetbiztonság területét érintik”.<sup>23</sup> Vagyis az államok a terrorista cselekményeket továbbra is államellenes bűncselekménynek, tehát nemzetbiztonsági kérdésnek tekintik, amely területen érthető módon kizárólagos szuverenitásukat fenn kívánják tartani.

A terrorista cselekmények elkövetőinek büntetőjogi felelősségre vonása ráadásul minden esetben valamelyik joghatósággal rendelkező állam nemzeti büntető törvénykönyvének tényállása alapján történik. A tanulmány elsősorban az Európai Unióra fókuszál, így a terrorizmusnak leginkább kitett tagállamok megoldásait tekintti át a továbbiakban.

### A német szabályozás

A német büntetőjogi szabályozásban gyakorlatilag nincs önálló *actus reusa* a terrorista akcióknak. Ehelyett a német büntető törvénykönyv a terrorista csoportok alapítását teszi meg bűncselekménynek.<sup>24</sup> Ezalatt olyan csoportokat ért a jogalkotó, amelyeknek a célja erőszakos bűncselekmények elkövetése<sup>25</sup> azzal a sajátos szándékkal, hogy a lakosságot megfélemlítsék, hatóságot, állami szervet erőszak alkalmazásával vagy azzal való fenyegetéssel kényszerítsenek, vagy megdöntsék az állam politikai, alkotmányos, gazdasági vagy társadalmi berendezkedését.<sup>26</sup> Ez a tényállás önmagában nem tűnik alkalmasnak az online terrorista tartalmak üldözéséhez, a törvény bünteti a csoportnak nyújtott támogatást, illetve a toborzást.<sup>27</sup> Ez utóbbi fordulat

<sup>21</sup> BRUMFIELD 2014.

<sup>22</sup> A migráció és a terrorizmus kapcsolatáról Európában lásd ÉBERHARDT 2019.

<sup>23</sup> Konrád Károly megjegyzése a Bel- és Igazságügyi Tanács (BIÜT) 2020. november 13-ai ülésén. Tudósítás: <https://kormany.hu/hirek/video konferencia-a-bel-es-igazsagugyi-tanacs-soros-ulesen>

<sup>24</sup> Deutsch Strafgesetzbuch (StGB), § 129a Bildung terroristischer Vereinigungen.

<sup>25</sup> StGB. § 129a (1) 1., 2.

<sup>26</sup> StGB. § 129a (2).

<sup>27</sup> StGB. § 129a (5).

már lefedhet egyes online terrorista tartalmakat, hiszen az üzenet posztolása, megosztása, illetve a propaganda toborzásra használása tulajdonképpen megféleltethető a normaszövegnek.

## A francia szabályozás

A francia *Code pénal* ettől eltérő megközelítést követ, a németnél jóval részletesebb szabályokat tartalmaz. Abban hasonlít azonban, hogy olyan általános bűncselekményeket<sup>28</sup> helyez a terrorizmus tényállása alá, amelyeknek „célja a közrend súlyos megsértése megfélemlítés vagy terror által”.<sup>29</sup> A tényállás viszont kifejezetten tartalmazza a számítógépes elkövetést is.<sup>30</sup> Itt azonban a III. könyvben rögzített, tulajdon elleni bűncselekményekre utal,<sup>31</sup> amelyeken feltehetőleg nem a szintén itt taglalt lopás,<sup>32</sup> sikkasztás<sup>33</sup> jellegű bűntetteket kell érteni, hanem a digitális terrorizmushoz inkább köthető kényszerítést,<sup>34</sup> zsarolást,<sup>35</sup> csalást, rongálást, károkozást<sup>36</sup> és leginkább az automatizált adatfeldolgozáshoz való jogosulatlan hozzáférést.<sup>37</sup> bűncselekményeket. Ezek a cselekmények kétséggkívül a digitális terrorizmushoz tartoznak, azonban nem az online terrorista tartalmak közé sorolhatók. Az ilyen tevékenységeket itt is inkább a terrorista csoporthoz való tartozás<sup>38</sup> alapján lehet büntetni, azonban ezen a ponton a francia jog megkötőbb, abban ugyanis nem jelenik meg sem a toborzás, sem a támogatás.<sup>39</sup> Ennek ellenére a terrorista tartalmakat ez a tényállás lefedheti, akkor is, ha az elkövető egyedül ül a számítógépe előtt, fórumokon beszélget terrorista témákról, megismerkedik a robbanószerek készítésével, hiszen így már kapcsolatba hozható egy terrorista szervezettel.<sup>40</sup> Tehát megfelelő súlyosság esetén a kommentelés, fórumozás, tartalommegosztás is megalapozhatja a felelősségre vonást. Ettől azonban konkrétan jogalapot ad a francia büntető kódex azon online-tartalom-gyártóknak, akik nemcsak érdeklődésből *bevonódnak* a terrorista közegbe, hanem akik a másik oldalon vannak, másokat aktívan *be is vonnak*. Mint előkészületi cselekmény<sup>41</sup> büntetendő, ha az illető fegyverkészítésre, -használatra képez<sup>42</sup> online, illetve olyan online közösségi vagy más kommunikációs felületet látogat gyakran, amely közvetlenül terrorcselekmények elkövetésére buzdító dokumentumot tartalmaz, vagy

<sup>28</sup> Code Pénal (CP) Edition: 2022-02-17, § 421.-1. 1°

<sup>29</sup> CP § 421.-1. „[...] pour but de troubler gravement l'ordre public par l'intimidation ou la terreur.”

<sup>30</sup> CP § 421.-1. 2°.

<sup>31</sup> CP § 421.-1. 2°. „[...] ainsi que les infractions en matière informatique définis par le livre III du présent code.”

<sup>32</sup> CP § 311.-1. – § 311.-16.

<sup>33</sup> CP § 314.-1. – § 314.-13.

<sup>34</sup> CP § 312.-1. – § 312.-9.

<sup>35</sup> CP § 312.-10. – § 312.-12.

<sup>36</sup> CP § 322.-1. – § 322.-17.

<sup>37</sup> CP § 323.-1. – § 323.-7.

<sup>38</sup> CP § 421.-2.-1.

<sup>39</sup> CP § 421.-2.-1. „Constitue également un acte de terrorisme le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un des actes de terrorisme mentionnés aux articles précédents.”

<sup>40</sup> ALIX 2014.

<sup>41</sup> CP § 421.-2.-6. I.

<sup>42</sup> CP § 421.-2.-6. I. 2° (b).

azokat helyesli.<sup>43</sup> Ez a fordulat pedig már teljesen egyértelműen az online terrorista tartalmak kriminalizálását jelenti.

## A spanyol szabályozás

A spanyol *Código Penal* szintén egészen széleskörűen taglalja a terrorista bűncselekményeket. Itt is beilleszthetők a korábbi logika alapján az online terrorista tartalmak a terrorista szervezet támogatását, szervezését, irányítását kriminalizáló tényállásba,<sup>44</sup> illetve büntethető még az ilyen elkövetés a terrorista szervezetben való aktív részvétel bűncselekmény alatt is.<sup>45</sup> A terrorizmus fogalma itt sem tér el a korábbiaktól, az általános bűncselekményekhez társított speciális cél az, ami itt is megjelenik.<sup>46</sup> Annyi különbséget azért érdemes kiemelni, hogy a spanyol szabályozás nem a megfélemlítés kifejezést használja, hanem a köznyugalom súlyos megzavarása<sup>47</sup> és a lakosságot vagy annak egy részét érintő rémületkeltés<sup>48</sup> – terrorállapot – jelenik meg. A számítógépes, digitális terrorista cselekmények szintén szerepelnek a büntető törvénykönyvben.<sup>49</sup> A *Código Penal* bünteti azon elkövetőket, akik olyan toborzási, indoktrinálási vagy képzési tevékenységet végeznek, amely célja vagy tartalma miatt alkalmas arra, hogy embereket terrorista szervezethez vagy csoporthoz való csatlakozásra buzdítson.<sup>50</sup> Érdekes eleme a szabályozásnak, hogy amennyiben a terrorista szervezet támogatása gondatlanságból történt, az is büntetendő cselekménynek minősül.<sup>51</sup> Így például nem zárható ki az sem, hogy egy online platform üzemeltetője is felelősségre vonható legyen, amennyiben súlyos gondatlanságból eredően nem ellenőrizte és távolította el a terrorista tartalmat az általa kezelt felületről. A spanyol büntetőjog fellép ráadásul azokkal szemben is, akik nyilvánosan dicsőítik a terrorista akciókat vagy azok elkövetőit, illetve becsmérlik azok áldozatait.<sup>52</sup> Az ilyen cselekmények súlyosabban büntetendők, ha a nyilvánosság számára a médiában, az interneten vagy elektronikus hírközlési szolgáltatásokon keresztül hozzáférhető szolgáltatások vagy tartalmak terjesztésével vagy információs technológiák felhasználásával hajtották végre őket.<sup>53</sup> Ez azért is lényeges, mert ez már az olyan online, digitális tartalmakat is terroristának titulálja, amelyek tulajdonképpen még csak a szimpatizálás fázisában vannak, de konkrét elköteleződést nem feltétlenül érez az elkövető. A spanyol szabályozás annyira előremutató, hogy az online terrorista tartalmak eltávolításának már büntető jogszabályba foglalt keretet ad. Kijelenti ugyanis, hogy

<sup>43</sup> CP § 421.-2.-6. 1. 2° (c).

<sup>44</sup> Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CÓP) § 572. (1).

<sup>45</sup> CÓP § 572. (2).

<sup>46</sup> CÓP § 573.

<sup>47</sup> CÓP § 573. (1) 2. a. „Alterar gravemente la paz pública.”

<sup>48</sup> CÓP § 573. (1) 4. a. „Provocar un estado de terror en la población o en una parte de ella.”

<sup>49</sup> CÓP § 573. (1) 5. a.

<sup>50</sup> CÓP § 577. (2).

<sup>51</sup> CÓP § 577. (3).

<sup>52</sup> CÓP § 578. (1).

<sup>53</sup> CÓP § 578. (2).



„ha a bűncselekményt az interneten vagy elektronikus hírközlési szolgáltatásokon keresztül elérhető szolgáltatásokon vagy tartalmakon keresztül követték el, a bíró vagy a bíróság elrendelheti a tiltott tartalom vagy szolgáltatás eltávolítását. Emellett elrendelheti a tárhelyszolgáltatókat a jogellenes tartalom eltávolítására, a keresőmotorokat a rájuk mutató linkek eltávolítására, az elektronikus hírközlési szolgáltatókat pedig a jogellenes tartalomhoz vagy szolgáltatáshoz való hozzáférés megakadályozására”.<sup>54</sup>

Azok cselekménye is büntetendő, akik nyilvánosan olyan üzeneteket vagy jelszavakat terjesztenek, amelyek céljuk vagy tartalmuk alapján alkalmasak arra, hogy másokat terrorista cselekmények elkövetésére buzdítsanak.<sup>55</sup> Elmondható tehát, hogy az online terrorista tartalmak kriminalizálása terén a spanyol *Código Penal* egészen részletes, számos elkövetési formára, illetve a tartalom eltávolítására is kiterő példát ad.

## Az Európai Unió rendeleti jogalkotása az online terrorista tartalmak eltávolításának szabályairól

Az online terrorista tartalmak azonban nincsenek figyelemmel az államok hatáira.<sup>56</sup> Elég arra gondolni, hogy egy megosztott videót, feltöltött posztot másodperceken belül a világon bárhol meg lehet tekinteni. A rendvédelmi, nyomozati szervezetek a feladata a kiberbűnözés felderítése,<sup>57</sup> azonban ez az eltérő nemzeti szabályozások miatt gyakran nehézségekbe ütközik.<sup>58</sup> Ezért is jelent előrelépést, hogy az Európai Unió területén fokozott figyelem és együttműködés irányul a radikalizmus és a terrorizmus visszaszorítására.<sup>59</sup> Evégből az Unió létrehozta a szélsőséges internetes tartalmakkal foglalkozó egységét (EU IRU), amely az Europolon belüli testületként azonosítja az online terrorista tartalmakat, illetve tanácsot ad a tagállamoknak a hasonló kérdésekben.<sup>60</sup> 2015-ben állította fel a radikalizálódással foglalkozó információs hálózatot (RAN)<sup>61</sup> és az Európai Unió Internetfórumát.<sup>62</sup> Mindkét kezdeményezés szakértőket, rendőröket, tudósokat összehozó hálózat, amelynek fő feladata a párbeszéd és a tapasztalatok megosztása. Miután a közelmúltban számos tagállam ellen irányult terrorista támadás, „az EU úgy járul hozzá polgárai védelméhez, hogy

<sup>54</sup> Cóp § 578. (4) „Si los hechos se hubieran cometido a través de servicios o contenidos accesibles a través de internet o de servicios de comunicaciones electrónicas, el juez o tribunal podrá ordenar la retirada de los contenidos o servicios ilícitos. Subsidiariamente, podrá ordenar a los prestadores de servicios de alojamiento que retiren los contenidos ilícitos, a los motores de búsqueda que supriman los enlaces que apunten a ellos y a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos [...]”

<sup>55</sup> Cóp § 579. (1).

<sup>56</sup> LOPEZ–MÁRD–FENNER 2019.

<sup>57</sup> Vö. SIMON 2018.

<sup>58</sup> GYARAKI 2019: 98.

<sup>59</sup> Lásd: [www.consilium.europa.eu/hu/policies/fight-against-terrorism/preventing-radicalisation/](http://www.consilium.europa.eu/hu/policies/fight-against-terrorism/preventing-radicalisation/)

<sup>60</sup> Lásd: [www.europol.europa.eu/about-europol/eu-internet-referral-unit-eu-iru](http://www.europol.europa.eu/about-europol/eu-internet-referral-unit-eu-iru)

<sup>61</sup> Lásd: [https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran\\_hu](https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran_hu)

<sup>62</sup> Lásd: [https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist\\_hu](https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist_hu)

a tagállamok közötti együttműködés és koordináció fő fórumaként működik”.<sup>63</sup> Az online terrorista tartalmak jogi szabályozása két aspektusban merült fel: egyrészt megelőzésük, másrészt eltávolításuk kapcsán.<sup>64</sup>

Az Európai Bizottság 2018-ban tett javaslatot az online terrorista tartalmak megelőzését célzó rendelet megalkotására.<sup>65</sup> A javaslat nívuma, hogy eltért a korábbi, szolgáltatói önszabályozáson alapuló rendszertől, így a keretet kötelezettségi alapokra helyezte, vagyis az érintett tárhelyszolgáltatóknak hatósági tartalomeltávolításra való felszólításnak kell eleget tenniük.<sup>66</sup> Eddig is az internetes platformok felelőssége volt, hogy megvédjék a felhasználókat a terrorista tartalmaktól, azonban az önkéntes intézkedéseik nem bizonyultak elégségesnek.<sup>67</sup>

A rendeleti szabályozás 2021 tavaszán valósulhatott meg, amikor az Európai Parlament és a Tanács elfogadta az online terrorista tartalom terjesztésével szembeni fellépésről szóló határozatát.<sup>68</sup> Érdekes módon a rendeleti szabályozás alapjául az Unió az egységes digitális piac zavartalan működésének biztosítását jelölte meg.<sup>69</sup> Erre feltehetőleg azért volt szükség, mert a terrorizmus szoros kapcsolatban áll a nemzetbiztonság és a közrend fenntartásával, amely viszont az EUSZ alapján át nem ruházott hatáskörként a tagállamok kizárólagos feladata maradt.<sup>70</sup> A belső piac azonban az unió és a tagállamok megosztott hatásköre alá tartozik,<sup>71</sup> így mindkét fél élhet jogalkotással ezen a területen.<sup>72</sup> Az uniós szabályozás szükségét az indokolja, hogy „a digitális egységes piac zökkenőmentes működésének az online terrorista tartalom terjesztésével szembeni fellépés révén történő biztosítását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban terjedelme és hatásai miatt e cél jobban megvalósítható”.<sup>73</sup> Az érvelés szerint az online terrorista tartalmak szabályozása az egységes digitális piachoz kapcsolódik, mivel

„súlyos negatív következményekkel jár [...] az ilyen tartalomnak tárhelyet biztosító online szolgáltatók számára is, mivel alássa felhasználóik bizalmát, és károsítja üzleti modelljüket. Központi szerepükre és az általuk nyújtott szolgáltatásokhoz kapcsolódó technológiai eszközökre és képességekre tekintettel a tárhelyszolgáltatóknak különösen fontos társadalmi felelőssége van a tekintetben, hogy szolgáltatásaikat megvédjék a terroristák általi visszaélésektől, és segítséget nyújtsanak a szolgáltatásaik révén online terjesztett terrorista tartalommal szembeni fellépéshez”.<sup>74</sup>

<sup>63</sup> Lásd: [www.consilium.europa.eu/hu/policies/against-terrorism/](http://www.consilium.europa.eu/hu/policies/against-terrorism/)

<sup>64</sup> Lásd: [https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online\\_hu](https://ec.europa.eu/home-affairs/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_hu)

<sup>65</sup> Európai Bizottság COM(2018) 640 final.

<sup>66</sup> ROBINSON 2018: 239.

<sup>67</sup> KUCZERAWY 2018: 2.

<sup>68</sup> 2021/784 európai parlamenti és tanácsi (EU) rendelet (a továbbiakban: Rendelet).

<sup>69</sup> Rendelet preambuluma (1).

<sup>70</sup> Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (EUSZ), 4. cikk (2).

<sup>71</sup> Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata (EUMSZ), 4. cikk (2) a).

<sup>72</sup> EUMSZ 2. cikk (2).

<sup>73</sup> Rendelet preambuluma (50).

<sup>74</sup> Rendelet preambuluma (5).

Ugyanakkor még a preambulum második pontjában kiemeli a rendelet, hogy az uniós szabályozás mellett elengedhetetlen a tagállami stratégiák kidolgozása is.<sup>75</sup> Összhangban a fentiekkel, lényeges mögöttes alapelvként jelenik meg, hogy a jogi szabályozás mellett a tárhelyszolgáltatók együttműködése és önkéntes intézkedései is fontosak, illetve, hogy az alapjogok tiszteletben tartása elengedhetetlen követelmény.<sup>76</sup>

A rendelet normatív része a tárgyi hatály megjelölésével kezdődik. Olyan tárhelyszolgáltatásokkal való visszaélések tartoznak a rendelet szabályozása alá, amelyeknek a célja terrorista tartalom nyilvános terjesztése.<sup>77</sup> Ilyen tartalomnak minősül az, amely terrorista bűncselekmény elkövetésére bujt fel azok dicsőítésével, annak reális veszélyével, hogy a bűncselekményt akár el is követhetik,<sup>78</sup> illetve amely egy személyt vagy csoportot bűncselekmény elkövetésére<sup>79</sup> vagy terrorista csoport tevékenységében való közreműködésre, részvételre hív fel.<sup>80</sup> Ide tartoznak még azok a tartalmak, amelyek útmutatást vagy képzést adnak robbanóanyagok, fegyverek elkészítésére és alkalmazására,<sup>81</sup> de az is, ha a terrorista cselekmény elkövetésével fenyeget a tartalom készítője.<sup>82</sup> Kiveszi azonban a rendelet ebből a körből a tudományos, oktatási célú, újságírói és művészeti tárgyú tartalmakat, sőt, meglepő módon a politikai viták részét képező vitatható állásfoglalásokat is.<sup>83</sup>

A személyi hatály az unió területén működő tárhelyszolgáltatókra terjed ki, abban az esetben, ha nyilvánosan terjesztenek információt.<sup>84</sup> Behelyettesítve a definíciókat, a tárhelyszolgáltató a távolról, elektronikus úton információs társadalom szolgáltatását<sup>85</sup> nyújtó személy, aki a tartalomszolgáltató (vagyis az információt szolgáltató felhasználó)<sup>86</sup> kérésére a szolgáltatott információt elektronikusan tárolja vagy nyilvánosan terjeszti.<sup>87</sup> A nyilvános terjesztés az információ hozzáférhetővé tétele potenciálisan korlátlan számú személy számára.<sup>88</sup> Ezt egy egyszerű példával megvilágítva egy Facebookon közzétett terrorista uszítást tartalmazó bejegyzés esetén a tárhelyszolgáltató a Facebook, a tartalomszolgáltató a bejegyzést író felhasználó, a nyilvános terjesztés pedig a poszt megosztása, elérhetővé tétele. Összegezve tehát a személyi hatály ebben a példában a tárhelyszolgáltatóra, a Facebookra vonatkozik. Fontos kiemelni azonban, hogy az interperszonális, vagyis nem nyilvános kommunikációra, így az elektronikus levelezésre, privát üzenetekre vagy felhőszolgáltatásokra a rendelet hatálya főszabály szerint nem terjed ki.<sup>89</sup> A tárgyi és a személyi hatály mellett megjegyzendő, hogy a rendeletet csak 2022. június 7. óta

<sup>75</sup> Rendelet preambuluma (2).

<sup>76</sup> Rendelet preambuluma (3), (9), (10).

<sup>77</sup> Rendelet 1. cikk (1).

<sup>78</sup> Rendelet 2. cikk (7) a).

<sup>79</sup> Rendelet 2. cikk (7) b).

<sup>80</sup> Rendelet 2. cikk (7) c).

<sup>81</sup> Rendelet 2. cikk (7) d).

<sup>82</sup> Rendelet 2. cikk (7) e).

<sup>83</sup> Rendelet 1. cikk (3).

<sup>84</sup> Rendelet 1. cikk (2).

<sup>85</sup> 2015/1535 európai parlamenti és tanácsi (EU) irányelv (2015. szeptember 9.) 1. cikk (1) b).

<sup>86</sup> Rendelet 2. cikk (2).

<sup>87</sup> Rendelet 2. cikk (1).

<sup>88</sup> Rendelet 2. cikk (3).

<sup>89</sup> WAHL 2021: 96.

kell alkalmazni.<sup>90</sup> Ez a terrorista tartalmak terjesztésével kapcsolatban alapvetően két fő intézkedést jelöl meg: az egyik az eltávolítási végzés,<sup>91</sup> ami hatósági hatáskör,<sup>92</sup> a másik pedig a konkrét intézkedések,<sup>93</sup> amelyek a tárhelyszolgáltató – szabályozott – önszabályozásához kapcsolhatók.

## ***Az eltávolítási végzések***

Az eltávolítási végzések kibocsátására minden tagállam illetékes hatóságának hatásköre ki kell terjedjen.<sup>94</sup> A végzés kötelezi a tárhelyszolgáltatót, hogy a megjelölt tartalmat eltávolítsa, vagy hozzáférhetetlenné tegye.<sup>95</sup> Formanyomtatványon,<sup>96</sup> elektronikusan<sup>97</sup> kell eljuttatni a kapcsolattartó pontnak, a tárhelyszolgáltatónak pedig mihamarabb, de legfeljebb egy órán belül teljesítenie kell a benne foglaltakat.<sup>98</sup> A végzésben azonosítható módon meg kell jelölni az eltávolítandó tartalmat,<sup>99</sup> és részletes indokolást kell adni arról, hogy miért minősül terrorista tartalomnak.<sup>100</sup> Erre azért is van szükség, mert az unió nagy hangsúlyt fektetett az alapjogvédelemre és a jogállami követelményekre.<sup>101</sup> Ennek megfelelően a tárhely- és a tartalomszolgáltatót is megilleti a panaszjog, vagyis hogy a végzést bírói úton megtámadhassa.<sup>102</sup> Ha azonban a fellebbezésre rendelkezésre álló idő letelt, a végzés jogerőre emelkedik,<sup>103</sup> vagyis onnantól nem megtámadható.

A tagállamok közötti együttműködés jegyében határokon átnyúló eltávolítási végzés is kiadható. Ez alatt azt kell érteni, hogy amennyiben egy nemzeti hatóság terrorista tartalmat észlel, de a tárhelyszolgáltató ezen államban sem székhellyel, sem jogi képvisellel nem rendelkezik, a hatóság mintegy extraterritoriális jelleggel kötelezheti a tartalom eltávolítására. Viszont az extraterritoriális jelleg miatt ezeknél számos eltérés jelenik meg a rendes végzésekhez képest. Az egyik ilyen, hogy a végzést a székhelyállam<sup>104</sup> hatóságának is meg kell küldeni,<sup>105</sup> egy másik pedig az, hogy ugyan a tárhelyszolgáltatónak el kell távolítania a tartalmat, szintén egy órán belül,

<sup>90</sup> Rendelet 24. cikk.

<sup>91</sup> Rendelet 3–4. cikk.

<sup>92</sup> WAHL 2021: 95.

<sup>93</sup> Rendelet 5. cikk.

<sup>94</sup> Az illetékes hatóságok kijelölése a tagállam kötelessége a 12. cikk alapján. A tagállamnak biztosítania kell, hogy a kijelölt hatóság megfelelő hatáskörrel és erőforrásokkal rendelkezzen a feladatok végrehajtására (13. cikk). A 14. cikk alapján pedig lehetővé kell tenniük a tárhelyszolgáltatókkal, a többi hatósággal és az Európával való hatékony együttműködést.

<sup>95</sup> Rendelet 3. cikk (1).

<sup>96</sup> Rendelet 3. cikk (4).

<sup>97</sup> Rendelet 3. cikk (5).

<sup>98</sup> Rendelet 3. cikk (2).

<sup>99</sup> Rendelet 3. cikk (4) b).

<sup>100</sup> Rendelet 3. cikk (4) c).

<sup>101</sup> Vö. Rendelet preambuluma (3), (33).

<sup>102</sup> Rendelet 9. cikk (1), (2).

<sup>103</sup> Rendelet 3. cikk (9).

<sup>104</sup> Ahol a tárhelyszolgáltató székhelye található, ahol jogi képvisellel rendelkezik vagy letelepedett.

<sup>105</sup> Rendelet 4. cikk (1).

de biztosítani kell, hogy a tartalom szükség esetén visszaállítható legyen.<sup>106</sup> Erre azért van szükség, mert a székhelyállam hatósága 72 órán belül saját kezdeményezésére – vagyis diszkrecionális jelleggel – megvizsgálhatja, hogy a végzés súlyosan vagy nyilvánvalóan sérti-e a rendelet vagy az alapjogi charta<sup>107</sup> által garantált alapjogokat.<sup>108</sup> Ilyen felülvizsgálatot kérhet a székhelyállam hatóságától a tárhelyszolgáltató és a tartalomszolgáltató is a végzés kézhezvételétől számított 48 órán belül, amely kérelmet indokolással kell ellátnia.<sup>109</sup> A meghozott végzést a székhelyállam hatósága haladéktalanul közölni köteles az eltávolítási végzést hozó állam hatóságával, a tárhelyszolgáltatóval és a tartalomszolgáltatóval (ez utóbbival csak akkor, ha ő kezdeményezte a felülvizsgálatot).<sup>110</sup> Ha ez jogsértést állapít meg, akkor az eltávolítási végzés hatályát veszti,<sup>111</sup> és a tárhelyszolgáltató köteles visszaállítani a tartalmat.<sup>112</sup>

## Konkrét intézkedések

A terrorista tartalmak elleni fellépés másik pillére a „konkrét intézkedések” elnevezés alatt futó tárhelyszolgáltatói önszabályozást jelenti. Ez ugyan valóban relatív önállóságot és diszkrecionalitást jelent, azonban a keretrendszert a rendelet határozza meg. Konkrét intézkedéseket nem minden tárhelyszolgáltatónak, hanem csak a terrorista tartalomnak kitett szolgáltatóknak kell foganatosítaniuk. Ezt a minőséget az illetékes hatóság határozata mondja ki,<sup>113</sup> amely határozat meghozataláról a tárhelyszolgáltatót értelemszerűen értesíteni köteles.<sup>114</sup> Az ilyen tárhelyszolgáltatóknak tehát olyan rendelkezéseket kell belefoglalniuk a szerződési feltételeikbe, amelyek lehetővé teszik számukra, hogy konkrét intézkedésekkel élve<sup>115</sup> megvédjék szolgáltatásaikat a terroristák nyilvános tartalomterjesztéseivel szemben.<sup>116</sup> „A konkrét intézkedések megválasztásáról a tárhelyszolgáltató dönt. Ezek az intézkedések a következők közül egyre vagy többre terjedhetnek ki.”<sup>117</sup> kapacitásépítés a jogellenes tartalom eltávolítására,<sup>118</sup> felhasználói jelentés vagy megjelölés lehetővé tétele,<sup>119</sup> felhasználói

<sup>106</sup> Rendelet 4. cikk (2).

<sup>107</sup> Lásd *Az Európai Unió Alapjogi Chartája* 2012/C 326/02.

<sup>108</sup> Rendelet 4. cikk (3).

<sup>109</sup> Rendelet 4. cikk (4).

<sup>110</sup> Rendelet 4. cikk (6).

<sup>111</sup> Rendelet 4. cikk (6).

<sup>112</sup> Rendelet 4. cikk (7).

<sup>113</sup> Rendelet 5. cikk (4) a).

<sup>114</sup> Rendelet 5. cikk (4) b).

<sup>115</sup> Rendelet 5. cikk (2).

<sup>116</sup> Rendelet 5. cikk (1).

<sup>117</sup> Rendelet 5. cikk (2).

<sup>118</sup> Rendelet 5. cikk (2) a): „megfelelő technikai és operatív intézkedések vagy kapacitások, így például megfelelő személyzet vagy technikai eszközök a terrorista tartalom azonosítására és haladéktalan eltávolítására vagy hozzáférhetetlenné tételére.”

<sup>119</sup> Rendelet 5. cikk (2) b): „a feltételezett terrorista tartalom tárhelyszolgáltatónak történő jelentésére vagy megjelölésére szolgáló, könnyen hozzáférhető és felhasználóbarát mechanizmusok a felhasználók számára.”

tudatosság fokozása<sup>120</sup> vagy bármilyen egyéb intézkedés.<sup>121</sup> Az eszközök megválasztása tehát opcionális. Konjunktív azonban a garanciális feltételek listája, amelyek a tartalomszűréskor irányadók: hatékonyak,<sup>122</sup> célzottak és arányosak,<sup>123</sup> a felhasználók alapjogait és érdekeit tiszteletben tartónak kell lenniük,<sup>124</sup> továbbá „körültekintően és megkülönböztetéstől mentesen kell őket alkalmazni”.<sup>125</sup> Megjelenik az az elvárás is, hogy amennyiben a filterfunkciót technikai intézkedések biztosítják, úgy ezek felett legyen humán kontroll.<sup>126</sup>

A tárhelyszolgáltatók kötelesek megőrizni a konkrét intézkedésekkel kapcsolatos és az eltávolítási végzés alapján eltávolított tartalmat és kapcsolódó adatot,<sup>127</sup> főszabály szerint hat hónapig.<sup>128</sup> Ennek kettős célja van. Egyrészt egy felülvizsgálati eljárás, panasz esetén,<sup>129</sup> másrészt a „terrorista bűncselekmények megelőzéséhez, felderítéséhez, nyomozásához és a vádeljárás lefolytatásához” szükség lehet az adatokra.<sup>130</sup>

A jogorvoslati lehetőségekről már volt szó az eltávolítási végzésekkel kapcsolatban. A felülvizsgálat másik ágát a panaszkezelési mechanizmusok adják. A különbség a kettő között, hogy a jogorvoslati lehetőség a hatósági eltávolítási végzéssel szemben, míg a panasz a tárhelyszolgáltató konkrét intézkedésével szemben alkalmazható. A tárhelyszolgáltatónak ugyanis biztosítania kell, hogy a tartalomszolgáltató hozzáférhető mechanizmus keretében panaszt nyújthasson be, és kérhesse a tartalom visszaállítását.<sup>131</sup> A panaszt ráadásul haladéktalanul ki is kell vizsgálnia.<sup>132</sup> Ahhoz természetesen, hogy panasszal élhessen a tartalomszolgáltató, az is szükséges, hogy a tartalom eltávolításáról megfelelő tájékoztatást kapjon a tárhelyszolgáltatótól.<sup>133</sup> Ezek a garanciális szabályok a tárhelyszolgáltatók és az illetékes hatóságok átláthatóságának követelményét is jelzik.<sup>134</sup>

Végül szólni érdemes arról, hogy a rendelet a végrehajtás hatékonysága érdekében az államokra hagyja, hogy a szabályainak tárhelyszolgáltató általi megsértése esetén

<sup>120</sup> Rendelet 5. cikk (2) c): „a szolgáltatásaiban a terrorista tartalommal kapcsolatos tudatosság növelését célzó bármely egyéb mechanizmusok, például a felhasználók moderálására szolgáló mechanizmusok.”

<sup>121</sup> Rendelet 5. cikk (2) d): „minden egyéb olyan intézkedés, amelyet a tárhelyszolgáltató megfelelőnek tart a szolgáltatásaiban a terrorista tartalom elérhetőségével szembeni fellépésre.”

<sup>122</sup> Rendelet 5. cikk (3) a): „hatékonyaknak kell lenniük a tekintetben, hogy csökkenteniük kell a tárhelyszolgáltató szolgáltatásai terrorista tartalommal való kitettségének szintjét.”

<sup>123</sup> Rendelet 5. cikk (3) b): „célzottaknak és arányosoknak kell lenniük, figyelembe véve különösen a tárhelyszolgáltató szolgáltatásai terrorista tartalommal való kitettsége szintjének súlyosságát, valamint a tárhelyszolgáltató technikai és operatív képességeit, pénzügyi erejét, a szolgáltatásait igénybe vevő felhasználóinak a számát és az általuk szolgáltatott tartalom mennyiségét.”

<sup>124</sup> Rendelet 5. cikk (3) c): „alkalmazásuk során teljes mértékben figyelembe kell venni a felhasználók jogait és jogos érdekét, különösen a felhasználóknak a véleménynyilvánítás és a tájékozódás szabadságához, a magánélet tiszteletben tartásához és a személyes adatok védelméhez való alapvető jogát.”

<sup>125</sup> Rendelet 5. cikk (3) d).

<sup>126</sup> Rendelet 5. cikk (3).

<sup>127</sup> Rendelet 6. cikk (1).

<sup>128</sup> Rendelet 6. cikk (2).

<sup>129</sup> Rendelet 6. cikk (1). a).

<sup>130</sup> Rendelet 6. cikk (1). b).

<sup>131</sup> Rendelet 10. cikk (1).

<sup>132</sup> Rendelet 10. cikk (2).

<sup>133</sup> Rendelet 11. cikk.

<sup>134</sup> A tárhelyszolgáltatónak ennek megfelelően a szerződési feltételeiben egyértelműen jeleznie kell a tartalomeltávolítás szabályait, illetve éves átláthatósági jelentést kell tennie (7. cikk), míg az illetékes hatóságnak szintén éves átláthatósági jelentésben kell számot adnia a tevékenységéről (8. cikk).

szankciókat határozzanak meg, amelyeknek hatékonyak, arányosnak és visszatartó erejűnek kell lenniük.<sup>135</sup> Tekintettel arra, hogy regionális kihívásról van szó, ahol ténylegesen elkerülhetetlen az államok együttműködése, különösen jelentőségteljes az Európai Unió rendeleti szabályozása. A rendelet alkalmazása még kérdéses, hiszen számos pontja van, amelynek gyakorlatba ültetése nehézkes lehet. Gondot okozhat például az eltávolítási végzések egy órán belüli teljesítése, de kérdéses lehet az is, hogy a hatóságoknak lesz-e elég kapacitásuk arra, hogy egy ilyen masszív adathalmazt hatékonyan ellenőrizzenek, sőt, az észlelt terrorista tartalmak mindegyikénél kitöltésük a formanyomtatványt, amelyben ráadásul alapos indokolást is kell tenniük. Ahhoz, hogy ténylegesen működhessen ilyen volumenben a tartalom-ellenőrzés, mindenképpen szükséges lesz technológiai megoldások, nevezetesen a mesterséges intelligencia és a gépi tanulás technológiájának alkalmazása. Ugyanakkor az így szerzett eredmények ellenőrzése és az eltávolítási végzések kiállítása, különösen az indokolási kötelezettség miatt, így is hatalmas emberi erőforrást igényelhet. Valószínű, hogy az online tartalmakkal szembeni fellépés tényleges gerince a tárhelyszolgáltató önszabályozása és az általa alkalmazott intézkedések maradnak. Ugyanakkor itt sem kerülhető ki ugyanaz a probléma: csak a technológia és az algoritmusok segítségével lehet ekkora adatmennyiséget ténylegesen szűrni, de ebben az esetben is a humán kontroll biztosítása a rendeletből fakadó kötelezettség. Mindenképpen elismerendő azonban a közösségi törekvés, hiszen egy egységesebb fellépésre ad lehetőséget, harmonizációra kényszeríti a tagállamokat, és kooperációra ösztönzi a nemzeti hatóságokat. Arról nem is beszélve, hogy kifejezetten nagy hangsúlyt fektet a garanciák biztosítására, így az alapvető jogok, különösen a szólásszabadság védelmére. A jogállamiság jegyében a transzparencia, a tájékoztatás és a felülvizsgálatra, panaszra való jog mindenképpen üdvözlendő elemei a szabályozásnak. Az, hogy a rendelet valóban teljesíti-e majd az elvárásokat, vagy csupán egy újabb bürokratikus adminisztrációs és formai nyűg lesz mind a hatóságok, mind a tárhelyszolgáltatók számára, az alkalmazás során szerzett tapasztalatok alapján lesz eldönthető.

## Összegzés

A terroristák azokat a jellemzőket használják ki az internet és a közösségi média esetében, amelyek ezeknek a közegeknek a hatalmas újításai és előnyei. Idetartozik az, hogy globálisan és közvetlenül hozzáférhető, a tartalmat leggyakrabban szerkesztői ellenőrzés nélkül, szabadon lehet készíteni és közzétenni. Gyakorlatilag teljes anonimitást biztosítanak, mégis lehetővé teszik a globális hálózat és egy hatékony kommunikációs rendszer kiépítését. Mivel az internet és a közösségi platformok a szabad véleménynyilvánítás és az információ szabad áramlásának támogatására jöttek létre, kezdetben gyakorlatilag nem létezett tartalomszűrés.

Az internethasználat képes volt megteremteni vagy legalábbis lényegesen leegyszerűsíteni a terrorista szervezet egyes sejtjei, illetve a tagok és a frissen toborzott jelöltek közti kapcsolattartást. Ez tette lehetővé, hogy az ISIS európai fiatalokat

<sup>135</sup> Rendelet 18. cikk (1).

toborozzon a közel-keleti harcokhoz vagy akár az európai merényletekhez, illetve az online terrorista tartalmakkal a megfélemlítés sokkal hatékonyabban juthat el a távoli társadalmakba is, adott esetben akár élő közvetítéssel is. Mindkét eredményben hatalmas szerepe volt és van a közösségi médiának. Egyrészt az algoritmikus felhasználói élményt szolgáló, de lényegében izolálást és extremitást kiváltó működési módjuk miatt, másrészt pusztán a nagy és globális felhasználói lefedettség, valamint a kezelés, a tartalomgyártás és -megosztás egyszerűsége miatt is könnyen katalizátora lehetett a terrorizmus globális jelenségé válásának.

Bár az egyes nemzeti büntetőjogi szabályozások eltérő gyakorlatot alkalmazhatnak, az Európai Unió egyértelműen a klasszikus terrorizmus és az online terrorista tartalmak eltérő szabályozása mellett foglalt állást. Következésképpen az online terrorista tartalmak az uniós álláspont szerint inkább megelőzik, illetve követik a terrorista cselekmények tényleges végrehajtását, így külön jogi szabályozást kaptak, méghozzá rendeleti úton. A korábbi, teljesen önszabályozáson alapuló rendszert egy szigorúbb, gyorsabbnak és hatékonyabbnak szánt megoldás váltotta fel, amelynek értelmében a nemzeti hatóságok is kötelesek az online terrorista tartalmakra eltávolítási végzést kiadni. Ugyanakkor a tárhelyszolgáltatók önszabályozása is megmaradt, de sokkal szigorúbb keretek mellett, illetve komolyabb tartalmi és garanciális elvárásokat társítottak a konkrét intézkedésekhez. Lényeges eleme a szabályozásnak, hogy tisztázza a határon átnyúló ügyeket és a hatóságok együttműködését, illetve hogy nagy hangsúlyt fektet az alapjogvédelemre és a jogállamiság garanciáira.

Összességében azonban elmondható, hogy túlságosan nagy előrelépés nem várható az uniós rendelettől. Az bizonyos, hogy a jogi fellépésnek már jóval stabilabb alapja van, illetve hogy a hatóságok bevonása és az önszabályozás szigorítása mindenképp nehezebbé teszi majd a terrorista tartalmak online terjesztését. Ugyanakkor a nemzeti hatóságokra ez akkora terhet rakhat, amelynek kezelésére feltehetően az egyes tagállamoknak nem lesz humán erőforrása és megfelelő technológiai infrastruktúrája sem. Rendkívül szoros az eltávolítás határideje is, amelynek betartása gondot okozhat. Problémás lehet még maga az adathalmaz elképzelhetetlenül nagy volumene. A tárhelyszolgáltató oldaláról kérdéses, hogy tud-e megfelelő mennyiségű képzett munkavállalót alkalmazni a kötelező humán kontroll ellátására, illetve a vélhetően megnövekedő panaszok kezelésére. A jogorvoslatok intézése pedig a hatóság oldaláról is hasonló problémákat vethet fel. Nem valószínű az sem, hogy a rendelet érdemben tudná kezelni azt a problémát, hogy a terrorista tartalmak több platformon is közzétehetőek, s amennyiben törlik azokat, kisebb korrekcióval, más felhasználó által is újra feltölthetők lehetnek. Arról nem is beszélve, hogy nem feltétlen várható el, hogy a nemzeti hatóságok által elkészített lista a terrorista tartalmaknak kitett tárhelyszolgáltatókról valóban maradéktalanul le is fogja fedni az összes potenciálisan érintett platformot. Így az is megeshet, hogy akár új, akár eddig ilyen célra nem használt szolgáltatókra kerülnek át az online terrorista tartalmak.

Mindezek ellenére az uniós erőfeszítés mindenképp értékelendő, és első lépésként megvan az esély arra, hogy érdemben javulhasson, ha nem is nagy mértékben, a terrorista tartalmakkal szembeni fellépés lehetősége. Nem elhanyagolható körülmény az sem, hogy a gyakorlat fényében, esetleg annak részsikerei által támogatva, újabb szabályozási lépések indulnak meg. Kétség sem férhet azonban ahhoz, hogy



önmagában a jogi fellépés nem elegendő, a társadalom nagyobb fokú védelméhez értelemszerűen a szolidaritástudat, a kritikus gondolkodás és az európai értékek tudatosításának erősítésére is szükség van.

## Felhasznált irodalom

- ALIX, Julie (2014): Réprimer la participation au terrorisme. *Revue de science criminelle et de droit pénal comparé*, 4(4), 849–865. Online: <https://doi.org/10.3917/rsc.1404.0849>
- ALY, Ann – MACDONALD, Stuart – JARVIS, Lee – CHEN, Thomas (2016): Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. *Studies in Conflict & Terrorism*, 40(1), 1–9. Online: <https://doi.org/10.1080/1057610X.2016.1157402>
- BEHR, Ines von – REDING, Anais – EDWARDS, Charlie – GRIBBON, Luke (2013): *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Brussels and Cambridge: Rand Europe. Online: <https://doi.org/10.7249/RR453>
- BRUMFIELD, Ben (2014): Officials: 3 Denver girls played hooky from school and tried to join ISIS. *CNN*, 2014. október 22. Online: <http://edition.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/index.html>
- CONWAY, Maura (2017): Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*, 40(1), 77–98. Online: <https://doi.org/10.1080/1057610X.2016.1157408>
- DUGGAN, Maeve – ELLISON, Nicole B. – LAMPE, Cliff – LENHART, Amanda – MADDEN, Mary (2015): *Social Media Update 2014*. Pew Research Centre: Internet Science and Tech Report. 2015. január 9. Online: [www.pewinternet.org/2015/01/09/social-media-update-2014/](http://www.pewinternet.org/2015/01/09/social-media-update-2014/)
- ÉBERHARDT Gábor (2019): Migráció és terrorizmus. *Hadtudományi Szemle*, 12(3), 37–59. Online: <https://doi.org/10.32563/hsz.2019.3.3>
- European Commission (2021): *Terrorist Content Online*. 2021. április. Online: [https://ec.europa.eu/home-affairs/system/files/2021-05/202104\\_terrorist-content-online\\_en.pdf](https://ec.europa.eu/home-affairs/system/files/2021-05/202104_terrorist-content-online_en.pdf)
- Europol (2021): *European Union Terrorism Situation and Trend Report*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2813/677724>
- Facebook (2017): Facebook, Microsoft, Twitter and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism. *Facebook Newsroom*, 2017. június 26. Online: <https://newsroom.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism/>
- GYARAKI Réka (2019): A kiberbűncselekmények megjelenése és helyzete napjainkban. In MEZEI Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest–Pécs: MTA TK Jogtudományi Intézet – Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 83–103.
- KLAUSEN, Jytte (2015): Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1–22, Online: <https://doi.org/10.1080/1057610X.2014.974948>

- Kontrát Károly megjegyzése a Bel- és Igazságügyi Tanács (BIÜT) 2020. november 13-ai ülésén. Online: <https://kormany.hu/hirek/videokonferencia-a-bel-es-igazsagugyi-tanacs-soros-ulesen>
- KUCZERAWY, Aleksandra (2018): *The Proposed Regulation on Preventing the Dissemination of Terrorist Content Online: Safeguards and Risks for Freedom of Expression*. [h. n.]: Center for Democracy and Technology. Online: <https://doi.org/10.2139/ssrn.3296864>
- LOPEZ, Ariana – MÅRD, Sophia – FENNER, Maximilian (2019): Editorial: Summer Issue: Themed Issue on Technology and Law. *Amsterdam Law Forum*, 11(3), 1–2. Online: <https://doi.org/10.37974/ALF.335>
- MACDONALD, Stuart – GIRO CORREIA, Sara – WATKIN, Amy-Louise (2019): Regulating Terrorist Content on Social Media: Automation and the Rule of Law. *International Journal of Law in Context*, 15(2), 183–197. Online: <https://doi.org/10.1017/S1744552319000119>
- ROBINSON, Gavin (2018): The European Commission’s Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online. *Eucrim. The European Criminal Law Associations’ Forum*, (4), 234–240. Online: <https://doi.org/10.30709/eucrim-2018-024>
- SIMON Béla (2018): A rendészeti szervek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle*, 6(1), 36–58.
- WAHL, Thomas (2021): Regulation Addressing the Dissemination of Terrorist Content Passed. *Eucrim. The European Criminal Law Associations’ Forum*, (2), 95–97.
- WEIMANN, Gabriel (2004): *www.terror.net: How Modern Terrorism Uses the Internet*. Special Report 116. Washington, D.C.: United States Institute of Peace.

## Jogi források

- 2015/1535 európai parlamenti és tanácsi (EU) irányelv (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (kodifikált szöveg)
- Az Európai Parlament és a Tanács (EU) 2021/784 rendelete (2021. április 29.) az online terrorista tartalom terjesztésével szembeni fellépésről
- Az Európai Unió Alapjogi Chartája 2012/C 326/02
- Az Európai Unió Működéséről szóló Szerződés egységes szerkezetbe foglalt változata
- Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (2007. december 13.)
- Code Pénal (CP) Edition: 2022-02-17, § 421.-1. 1°
- Deutsch Strafgesetzbuch (StGB), § 129a Bildung terroristischer Vereinigungen
- Európai Bizottság (2018): *Javaslat az Európai Parlament és a Tanács rendelete az online terrorista tartalom terjesztésének megelőzéséről. Az Európai Bizottság hozzájárulása a 2018. szeptember 19–20-i salzburgi vezetői üléshez*. COM(2018) 640 final. Online: [https://eur-lex.europa.eu/resource.html?uri=cellar:d-c0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0013.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d-c0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0013.02/DOC_1&format=PDF)
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CÓP)