DOI: 10.38146/BSZ.2024.1.1

A jogellenes tartalomközléssel megvalósított kiberbűncselekmények elleni fellépés eljárásjogi dilemmái a nemzetközi együttműködésben

Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations

Sorbán Kinga
Dr. PhD, tudományos segédmunkatárs
Nemzeti Közszolgálati Egyetem,
Információs Társadalom Kutatóintézet
kinga.sorban@gmail.com

Absztrakt

Cél: A tanulmány fő célja, hogy átfogó képet adjon a nemzetközi elemet tartalmazó kiberbűncselekmények nyomozásának eljárásjogi dimenzióiról. E körben két nagy területtel, a joghatósággal és a jogsegéllyel összefüggésben emeli ki azokat a nehézségeket, amelyek lassíthatják, sőt szélsőséges esetekben akár el is lehetetleníthetik az eredményes fellépést.
Módszertan: Mivel a tanulmányban főként jogszabályi megoldásokról esik szó, a tanulmány összegyűjti és összehasonlító elemzésnek veti alá azokat a fontosabb EU-s és nemzetközi jogforrásokat, amelyek az országok közötti együttműködést szabályozzák a kiberbűnözés területén.
Megállapítások: Főként a nemzetközi jogsegély területén aktív európai uniós jogalkotás zajlik, ahol egyre inkább előtérbe kerül a közvetlenség elve, azaz az eljáró hatóságoknak az a lehetősége, hogy közvetlenül keressenek meg más tagállamban letelepedett közvetítő szolgáltatókat. Ez egyrészt gyorsíthatja az eljárásokat, másrészt azt a veszélyt rejti magában, hogy a számtalan rendelkezésre álló eszköz átfedésbe kerül egymással, gyengítve a fellépés hatékonyságát.
Érték: Mivel a jogalkotási eljárások egy része még folyamatban van, mindenképpen további kutatást érdemel, hogy a tagállamok hogyan tudják majd alkalmazni az új eszközöket a gyakorlatban.

Kulcsszavak: kiberbűnözés, nemzetközi együttműködés, joghatóság, jogsegély

Abstract

Aim: The main purpose of this study is to provide a comprehensive overview of the procedural dimensions of the investigation of cybercrimes having an international element. In this context, it highlights the difficulties that can slow down and, in extreme cases, even prevent effective enforcement in two major areas: jurisdiction and mutual legal assistance.
Methodology: As the study primarily focuses on legislative approaches, it brings together and comparatively analyses the main EU and international legal sources that regulate cooperation between countries in the field of cybercrime.
Findings: Especially in the area of mutual legal assistance, the European Union is actively legislating, and the principle of indirectness, i.e., the possibility for the competent authorities to directly contact intermediary service providers established in another Member State, is increasingly gaining prominence. On one hand, this can speed up procedures, but on the other hand, it entails the risk that the numerous instruments overlap, weakening the effectiveness of enforcement.
Value: As some of the legislative procedures are still underway, further research is needed to see how Member States will be able to apply the new instruments in practice.

Keywords: cybercrime, international cooperation, jurisdiction, mutual legal assistance

Bevezetés

Az online térben megvalósított bűncselekmények a legritkább esetekben kapcsolódnak csupán egyetlen országhoz. A tartalomközléssel megvalósított bűncselekmények esetében egyáltalán nem elképzelhetetlen, hogy az elkövető és a sértett eltérő országokban tartózkodnak, kiterjedt malware fertőzések esetén pedig kifejezetten ritka, hogy a fertőzés csak egy országban érint információs rendszereket.[1] Napjainkban az internetes jogsértések esetében már bevett gyakorlat olyan országban tárhelyszervert bérelni, ahol alacsony a nyomozó hatóságok kapacitása az eset felderítésére: az ENSZ Kereskedelmi és Fejlesztési Konferenciája 2020-ban hívta fel a figyelmet arra, hogy a fejlődő országok el vannak maradva a kiberbűncselekmények kriminalizálásában és üldözésében (URL1). A kiberbűncselekmények esetén az elkövetésnek szinte bármelyik

1 Napjaink népszerű kártékony szoftverei világszerte képesek fertőzni. A Kaspersky biztonsági cég adatai alapján a WannaCry zsarolóvírus mintegy 230 000 számítógépet fertőzött meg 150 országban.

mozzanatához kapcsolódhat nemzetközi elem, ez pedig a nemzetközi együttműködés fontosságát kiemelt szintre emeli.

Mindezek ellenére a nemzetközi együttműködés mégis számos ponton ütközik nehézségekbe, Mezei Kitti hívja fel a figyelmet arra, hogy az olyan esetek kétharmadában, ahol az elektronikus bizonyíték külföldön található, nem lehet rendesen lefolytatni a büntetőeljárást (Mezei, 2022).

A nemzetközi elemet tartalmazó kiberbűncselekmények nyomozásának két neuralgikus pontja van: az egyik a joghatóság megállapítása, a másik pedig az eljárási cselekmények külföldi lefolytatása, a nemzetközi jogsegély. Tanulmányom ezzel a két témakörrel foglalkozik. Mivel mind a joghatóság, mind a jogsegély kiterjedt nemzetközi szabályrendszerrel rendelkezik, fő célom, hogy áttekintést nyújtsak azokról a jogi eszközökről, amelyek a külföldi elemet tartalmazó eljárásokban rendelkezésre állnak. Különös figyelmet fordítok az elmúlt években az Európai Unió által jogalkotás révén is támogatott extraterritoriális joghatóság kérdésére, amely alapján egy tagállam bűnüldöző hatóságai közvetlenül elvégezhetnek eljárási cselekményeket más tagállamban is. Az EU jogrendszere erre leginkább akkor biztosít lehetőséget, ha internetes közvetítő szolgáltató jelenik meg az eljárásban. Az internetnek ezek a szolgáltatói ugyanis fontos bizonyítékokat tárolhatnak, vagy éppen tudnak intézkedni afelől, hogy a jogsértőnek vélt tartalom az eljárás lefolytatásáig hozzáférhetetlen legyen. A legnépszerűbb szolgáltatók jellemzően nem Magyarországon telepednek le (a Facebookot üzemeltető Meta európai székhelye például Írországban található), ezért hazai eljárásban – érintettségük esetén – a nyomozó hatóságoknak szükségszerűen a nemzetközi együttműködés szabályait kell alkalmazniuk.

A joghatóság a kiberbűncselekmények elleni fellépésben

A joghatóság lényegében az a rendezőelv, amely az államok közötti ügyeloszlást határozza meg, vagyis amely alapján megállapítható, hogy konkrétan mely ország hatóságainak és bíróságainak joga és kötelessége eljárni. Hazai jogunkban a büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) rendelkezései alapvetően a területi elvet tükrözik, amely szerint a magyar állam büntetőhatalma az ország területén elkövetett cselekményekre terjed ki.[2] Ismeri emellett a személyi (más néven állampolgársági) elvet is, amely alapján magyar joghatóság alá tartozik a saját állampolgár által külföldön

2 Btk. 3. § (1) bekezdés a)-b) pont.

elkövetett bűncselekmény is, amennyiben az a magyar jog szerint bűncselekmény.[3] Kiegészítő elvekként tartalmazza a Btk. a védelmi elvet (állam elleni bűncselekmény esetén a cselekmény magyar joghatóság alá tartozik),[4] illetve az univerzális joghatóság elvét (nemzetközi jog által üldözött cselekmény esetén magyar bíróság is eljárhat). Témánk szempontjából fontos további kiegészítő elv az úgynevezett passzív személyi elv is, amely szerint magyar állampolgár sértett ellen, nem magyar állampolgár által külföldön elkövetett cselekményre is a magyar jog alkalmazandó, ha a cselekmény a magyar jog szerint büntetendő.[5] Ezek a joghatósági szabályok klasszikusan a fizikai térben elkövetett cselekményekre szabottak, például, ha a rendőrség talál egy holttestet késsel a mellkasában egyértelmű, vagy legalábbis könnyen megállapítható az elkövetés helye, és feltételezhető, hogy az elkövető is a helyszínen tartózkodott. Az online térben korántsem ilyen egyszerű a helyzet, hiszen a virtuális világban már az elkövetés helyének megállapítása is komoly fejtörést okozhat. Gyűlöletbeszéd esetében például hová tehető az elkövetés helye: a közlő tartózkodási helyére, vagy oda, ahol az érintett személyek lakóhelye van, és az erőszakos cselekmény közvetlen bekövetkezésének veszélye fenyeget? Esetleg abba az országba ahol az a szerver van, ami a közlést tárolja, vagy annak a közösségi média platformnak a székhelye szerinti országba, amely a szervert tulajdonolja?

Nem könnyű kérdések, a magyar törvények rendelkezéseiből pedig nem következik rájuk egyértelmű válasz. A kiberbűncselekményekre speciális jellegüknél fogva több nemzetközi egyezmény, illetve az EU joganyaga is tartalmaz joghatósági szabályokat, az alábbiakban ezeket tekintem át.

Joghatóság a nemzetközi jogban

A 2021-ben húsz éves Számítástechnikai Bűnözésről szóló Egyezmény[6] (továbbiakban: Cybercrime Egyezmény) 22. cikke szól a joghatóságról. A részes országok nemzeti jogához hasonlóan a Cybercrime Egyezmény is a területi elvet tekinti elsődlegesnek, vagyis az állam joghatósága a területén elkövetett bűncselekményekre terjed ki.[7] Másodlagos kapcsolóelvként a személyi elvet[8] alkalmazza a Cybercrime Egyezmény, vagyis ha a területi elv alapján nem sikerül

3 Btk. 3. § (1) bekezdés c) pont.
4 Btk. 3. §.
5 Btk. 3. § (2) bekezdés b) pont.
6 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.
7 22. cikk 1. pont a)-c) pont.
8 22. cikk 1. pont d) pont.

megállapítani, melyik országnak van joghatósága, az elkövető állampolgársága szerinti állam is jogosult eljárni.

A területi elv alkalmazása a gyakorlatban azonban okozhat nehézségeket. A Cybercrime Egyezmény ugyanis az alkalmazása kapcsán már nem látja el támpontokkal a részes országokat. Ahogy korábban a gyűlöletbeszéd kapcsán feltett kérdések illusztrálják, az elkövetés helyének megállapítása az online közegben nem egyszerű feladat. Megnehezíti az elv alkalmazását, ha a cselekmény kapcsán az eljárás lefolytatására szóba jöhető országok eltérően gondolkodnak az elkövetés helyéről, hiszen ez akár pozitív (több ország kíván eljárni), akár negatív (egy ország sem akar eljárni) joghatósági összeütközésben is kicsúcsosodhat. Tóth Dávid és Gáspár Zsolt a területi elv kritikájaként kifejtik (Tóth & Gáspár, 2020), több esetben előfordul, hogy az elkövetés helye (itt: ahonnan az elkövető végrehajtja a cselekményt) szerinti országban nem is indul büntetőeljárás, mivel az adott ország területén nem volt a cselekménynek sértettje. Ráadásul az elkövető VPN használatával könnyen be tudja csapni a helymeghatározó rendszereket, amelyek a használt IP-cím alapján teljesen más országhoz kapcsolhatják az elkövetést, mint ahol az ténylegesen történt.

A kettős inkrimináció elve (dual criminality) szintén akadályát jelentheti a büntetőeljárás lefolytatásának. A kettős inkrimináció elve azt a követelményt jelenti, amely alapján csak akkor kerülhet sor külföldi állampolgár cselekményének szankcionálására, amennyiben a cselekmény az érintett ország és a külföldi állam joga szerint is bűncselekmény (Blaskó & Budaházi, 2019). Ez olyan univerzális jogelv, amely a nemzetközi bűnügyi együttműködés egyik általános feltétele (Kondorosi & Ligeti, 2008), amelyet valamilyen formában a legtöbb ország alkalmaz,[9] így a büntetőeljárásoknál problémát jelenthet, ha az elkövető cselekménye komoly károkat okoz ugyan, de olyan országból követi azokat el, ahol az adott cselekmény nem bűncselekmény.

A kettős inkrimináció elve képezte akadályát a LoveBug elnevezésű malware készítője ellen lefolytatandó büntetőeljárásnak (Rawat, 2021; Brenner, 2006). A kétezres években villámgyorsan terjedt el az internet keresztül egy vírus, ami tömegesen küldött „ILOVEYOU" (szeretlek) tartalmú fertőző emaileket. A vírus hamar leterhelte a teljes internethálózatot, és több nagyvállalat egész céges levéltárhelyét megtöltötte, ezzel nagyjából nyolcmilliárd dollárnyi kárt okozva. A LoveBug kártevő készítőjét hamar sikerült felderíteniük a nyomozó hatóságoknak: egy fülöp-szigeteki egyetemista, állítása szerint véletlenül, eresztette

9 A nemzetközi egyezmények elsősorban a kiadatás, valamint a kölcsönös jogsegély intézményeivel összefüggésben szólnak a kettős inkrimináció elvéről. Az EU 2002/584/JHA kerethatározata az EU tagállamaiban a kiadatás feltételéül szabja a kettős inkriminációt, vagyis azt, hogy a cselekmény mind a kiadatást kérő, mind az azt teljesítő országban bűncselekmény legyen.

szabadjára a vírust a világhálón. Hiába az óriási összegű kár a Fülöp-szigeteknek a kétezres években nem volt olyan törvénye, amely a malware terjesztést büntetni rendelte volna. A helyi ügyészség megvizsgálta annak a lehetőségét, hogy emelhetnek-e vádat készpénz-helyettesítő fizetési eszközzel visszaélés ügyében, ám arra a következtetésre jutottak, hogy annak semmi köze nincs a számítógépes rendszerek akadályozásához. Mivel nem valósult meg a kettős inkrimináció, az elkövető ellen végül nem emeltek vádat, cselekménye büntetlen maradt (URL2).

A sértett állampolgárságára építő passzív személyi elv mint másodlagos kapcsolóelv pedig a sok sértettes, több országot érintő ügyekben okozhat összeütközéseket (például egy olyan kiterjedt malware fertőzés esete, ami több ország számos számítógépét megfertőzte).

A joghatóság nemcsak a bűncselekmény elkövetőjének felelősségre vonása során okozhat problémát, hanem a határozatok végrehajtása során is, amikor egy bűncselekménynek minősülő tartalom egy olyan szolgáltató szerverén található, amely nem az EU-ban található. Ez esetben a tartalom, az elektronikus adat ideiglenes vagy végleges eltávolítására kötelező bírósági vagy más szerv által hozott határozat végrehajtása csakis a szolgáltató jóindulatán múlik.

A Yahoo-ügyben[10] a joghatóság egy bírósági határozat végrehajthatósága kapcsán merült fel. Az ügy fő kérdése az volt, hogy az amerikai bíróságoknak elő kell-e segíteniük azoknak az ítéleteknek a végrehajtását, amelyet az USA-n kívüli bíróságok hoztak az Egyesült Államokban honos cégek külföldi leányvállalatainak ügyében. Franciaországban például tilos az önkényuralmi jelképek használata,[11] így egy francia bíróság jogsértőnek találta a náci ereklyék online aukciókon történő értékesítését. A francia diszkrimináció-ellenes nonprofit szervezet, a La Ligue Contre Le Racisme et l'antisemitisme pert indított az aukciós oldalt üzemeltető Yahoo ellen, amiért az lehetővé teszi, hogy francia felhasználók is lássák az aukciókat, és licitáljanak az ott meghirdetett termékekre. A Yahoo védekezésképpen arra hivatkozott, hogy amerikai vállalatként a francia jog rendelkezései nem vonatkoznak rá, a francia bíróság azonban nem így látta, és ezer frankos pénzbüntetést szabott ki a vállalatra. A francia bíróság azzal érvelt, hogy ha Franciaország a szolgáltatás célországa, akkor eleget kell tenni a francia jog rendelkezéseinek, és a szóban forgó aukciókat el kell távolítani, vagy a francia IP-címmel internetező felhasználók számára elérhetetlenné kell tenni. A francia hatóságok felvették a kapcsolatot az Egyesült Államokkal a bíróság határozatában foglaltak kikényszerítése

10 Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme, 433 F.3d 1199 (9th Cir. 2006).
11 Code Pénal Article R645-1.

végett, amelyre válaszul a Yahoo pert indított. A cég a szólásszabadságot biztosító első alkotmánykiegészítés sérelmére hivatkozva azt állította, hogy a francia bíróság ítéletének végrehajtása az Egyesült Államok területén az amerikai felhasználók szólásszabadságának csorbulásához vezet, mivel az amerikai jog nem tiltja az önkényuralmi rendszerek használatát, így a náci emléktárgyak internetes árusítását sem.

Az 9th Circuit Court fellebbviteli fórumként eljárva végül arra jutott, hogy amerikai bíróságoknak nincs joghatóságuk egy francia szervezet elleni perben döntést hozni, a kérdés érdemi tárgyalásáig tehát el sem jutottak. Az ehhez hasonló joghatósági problémák természetesen azzal a következménnyel járnak, hogy a bírósági határozat külföldön végeredményben kikényszeríthetetlen.

Brenner és Koops szerint a problémát alapvetően nem az okozza, hogy vannak joghatósági viták az országok között, hanem az, hogy nincsenek egységes mechanizmusok, amelyek segítséget nyújtanak annak megállapításához, hogy mely országhoz kötődik a legszorosabban a cselekmény, s így feloldanák a konfliktust (Brenner & Koops, 2004). A Cybercrime Egyezmény mindössze javaslatot tesz arra, hogy az országok a vitás kérdéseket egyeztetés révén oldják fel,[12] azonban ennek elmaradásához nem rendel jogkövetkezményt. Célszerű lehet tehát olyan nemzetközi testület felállításában gondolkodni, amely döntést tud hozni hasonló kérdésekben, vagy legalábbis amelyhez a Cybercrime Egyezmény részes országai útmutatásért fordulhatnak.

Joghatóság az Európai Unióban

Az EU területén ennél összetettebb joghatósági szabályok érvényesülnek, az egyes uniós aktusok ráadásul cselekményenként külön-külön szabályokat állapítanak meg. Az alábbiakban áttekintem az EU informatikai bűncselekményekkel, köztük a hálózatokon keresztül megvalósuló kiberbűncselekményekkel kapcsolatos szabályainak joghatóságra vonatkozó rendelkezéseit.

A tisztán informatikai bűncselekmények (jogosulatlan hozzáférés, beavatkozás a rendszer működésébe és az adattal kapcsolatos visszaélések) esetében a 2013/40/EU irányelv rendezi a joghatósági kérdéseket. Az irányelv 12. cikke értelmében a területi elv és az állampolgársági elv közösen érvényesül, vagyis egy tagállamnak akkor is van joghatósága eljárni, ha a cselekményt részben vagy egészben a területén követték el, és akkor is, ha azt egy állampolgára követte el. Az elkövetés helyét az irányelv igen tágan értelmezi, helyesen, hiszen ezzel elébe megy annak a problémának mely szerint a virtuális térben elkövetett

12 Cybercrime Egyezmény 22. cikk, 5. pont.

cselekmények esetén az elkövetés valójában több helyhez is kapcsolódhat egyszerre. Az irányelv szerint akkor is tagállam területén elkövetettnek minősül a cselekmény, ha az elkövető fizikailag annak területén tartózkodik az elkövetéskor, és akkor is, ha az elkövető ugyan másutt van, de az információs rendszer, amely ellen a cselekményt elkövetik a tagállam területén található. Az elkövetési hely kiterjesztéséből az a probléma fakadhat, hogy egyszerre több tagállam tekinti a cselekményt a saját területén elkövetettnek. Ez tipikusan akkor fordul elő, ha az elkövető és a cselekménnyel érintett információs rendszer különböző tagállamokban vannak, de akkor is lehetséges, ha az elkövető célpontjai nemcsak a saját tartózkodási helye szerinti tagállamban, hanem számos más országban vannak (például egy számítógépes vírus terjesztése esetén). Ezekben az esetekben a tagállamok közötti egyeztetésen múlik, hogy melyikük fogja lefolytatni a büntetőeljárást. Azonban célszerű olyan ország joghatóságában megállapodni, amelyhez az ügy a legszorosabban kapcsolódik.

A 2011/93/EU irányelv a gyermekpornográfiát, valamint a gyermekkel való szexuális tartalmú kapcsolatfelvételt (grooming) rendeli büntetni a tagállamokban. A kriminalizált cselekmények eredményes üldözése érdekében az irányelv a joghatóság megállapításának közös szabályait is rendezi. E cselekmények tekintetében szintén elsődleges a területi és az állampolgársági elvek kombinált alkalmazása. Egy tagállam lefolytathatja az eljárást akkor, ha a cselekményt részben vagy egészben a területén követték el,[13] illetve ha az elkövető az állampolgára.[14] Kiegészítő elvként a tagállamok diszkrecionális jogkörükben dönthetnek úgy, hogy megállapítják joghatóságukat akkor is, ha a fenti feltételek nem teljesülnek. Erre az alábbi esetekben van lehetőség:

- ha a sértett lakóhelye vagy tartózkodási helye az adott tagállam területén található,
- ha a cselekményt olyan jogi személy javára követték el, amely az adott államban telepedett le, valamint
- ha az elkövető szokásos tartózkodási helye a tagállamban van.[15]

Mivel a cselekmény sértettjei kiskorúak, érthető és logikus lépés az állampolgárság szerinti tagállamnak biztosítani az eljárás lehetőségét. Egy idegen nyelven, adott esetben távoli országban zajló eljárás, az idegen és akár többször megismételt eljárási cselekmények (például tanúkihallgatás) többszörös traumatizációt okozhatnak a sértettnek, akinek a legfőbb érdeke, hogy az eljárás

13 2011/93/EU irányelv 17. cikk (1) bekezdés a) pont.
14 2011/93/EU irányelv 17. cikk (1) bekezdés b) pont.
15 2011/93/EU irányelv 17. cikk (2) bekezdés.

a hozzá legközelebbi helyen, megszokott, biztonságos keretek között folyjék. Az irányelv a kettős inkrimináció elvét is lerontja azáltal, hogy úgy rendelkezik, hogy a tagállam joghatósága nincs alárendelve annak a feltételnek, hogy a cselekmény az elkövetés helyén is bűncselekménynek minősüljön.

A 2019/713/EU irányelv szabályozza a készpénz-helyettesítő fizetési eszközök, a materiális és immateriális készpénz-helyettesítő fizetési eszközök csalárd felhasználását, valamint az információs rendszerekkel kapcsolatos csalást. A joghatóságot megállapító rendelkezések nem térnek el az EU egyéb, kiberbűncselekményekkel foglalkozó jogi aktusaiban fellelhető rendelkezésektől, tehát ugyanúgy elsődleges a területi és az állampolgársági elvek alkalmazása.[16]

Nemzetközi jogsegély a kiberbűncselekmények esetén

Ha egy cselekmény külföldi elemet tartalmaz, általában más állam bíróságát vagy hatóságát kell megkeresni a szükséges eljárási cselekmények foganatosítása érdekében, ezt hívjuk jogsegélynek. A nemzetközi jogsegélynek nincsenek egységesen, minden ország vonatkozásában használatos eljárási szabályai, az egyes országokkal való ilyesfajta kapcsolatot, illetve az egyes jogterületekre vonatkozó szabályokat bi- vagy multilaterális egyezmények külön-külön tartalmazzák. Ezek a jogsegélyegyezmények általában nem egy bűncselekménycsoportra fókuszálnak, hanem általánosságban véve a határokon átnyúló nyomozás fontosabb, együttműködést igénylő eljárási elemeire.[17] Ezekben a jogsegélyegyezményekben tehát olyan szabályokat nem találunk, amelyek külön a kiberbűncselekmények sajátosságaira – különösen az online tér bizonyítékainak illékony természetére – figyelemmel szabályoznák a büntetőeljárási cselekményeket. Ezzel együtt az elektronikus kommunikáció elterjedtsége miatt manapság nehezen képzelhető el olyan bűncselekmény, amelynek nem marad valamilyen nyoma a virtuális térben, vagy valamilyen hírközlési szolgáltató rendszerében. A jogsegélyegyezmények bizonyítékok megszerzésére vonatkozó rendelkezései ezért többnyire foglalkoznak valamilyen formában a hírközlési vagy más információs társadalmi szolgáltatóknál tárolt adatok megszerzésével, megőrzésével, illetve eltávolításával.

16 2019/713/EU irányelv 12. cikk (1) bekezdés.

17 Például a 2006. évi XL. törvényt a Magyar Köztársaság Kormánya és az Amerikai Egyesült Államok Kormánya között a kiadatásról és a kölcsönös bűnügyi jogsegélyről szóló, Budapesten, 1994. december 1-jén aláírt szerződések módosításáról szóló szerződések kihirdetéséről.

Jogsegély az Európai Unió tagállamai között

Az EU tagállamai közötti bűnügyi együttműködésre vonatkozó szabályainak az EU tagállamai közötti bűnügyi jogsegélyről szóló egyezmény[18] (a továbbiakban: Jogsegélyegyezmény[19]) ad keretet. Mivel nemzetközi egyezmény és nem klasszikus uniós jogforrás, elfogadásához tagállami ratifikálásra volt szükség (Villányi, 2003). A Jogsegélyegyezmény egyik legjelentősebb eredménye, hogy megteremti annak a lehetőségét, hogy bűnügyi jogsegély esetében a tagállamok igazságügyi hatóságai közvetlenül lépjenek kapcsolatba egymással. Erre korábban az igazságügyi minisztériumok közreműködésével volt lehetőség, ami rendkívüli módon lassította az eljárásokat.

A Jogsegélyegyezménynek nem célja, hogy teljesen, átfogó jelleggel rendezze az EU tagállamai közötti jogsegély szabályait, ezt már az 1. cikk is világosan tükrözi, amely azt rögzíti, hogy a Jogsegélyegyezmény csak egyéb nemzetközi egyezmények szabályait kívánja kiegészíteni, hogy ezáltal hatékonyabbá tegye az együttműködést e területen. A Jogsegélyegyezmény az 1959. április 20-i kölcsönös bűnügyi jogsegélyről szóló egyezmény, annak 1978. március 17-i kiegészítő jegyzőkönyve, valamint az 1985. évi Schengeni Végrehajtási Egyezmény és a Benelux szerződés szabályaihoz fűz kiegészítéseket, szabályait tehát nem önmagukban, hanem a megjelölt további egyezmények szabályaival szerves egységben lehet és kell vizsgálni, és értelmezni. A Jogsegélyegyezmény azt is rögzíti, hogy amennyiben vannak olyan tagállamok közötti egy- vagy többoldalú megállapodások, amelyek kedvezőbbek a Jogsegélyegyezmény szabályainál, akkor ezek rendelkeznek primátussal, így felülírhatják az abban rögzítetteket.

Jogsegély az Európai Unió tagállamai és harmadik országok között

Az EU tagállamai és a harmadik országok közötti jogsegélyre továbbra is a központi hatóságokon (Magyarországon az Igazságügyi Minisztérium) keresztül van lehetőség, ami nemcsak idő, de erőforrásigényes is.

A büntetőeljárás nyomozati szakaszában gyakran merülnek fel a bizonyítással kapcsolatos jogsegély iránti megkeresések. Számítógépes környezetben főként az adat megszerzésére kötelezés, valamint a hozzáférés biztosítása

18 Egyezmény a Tanács által az Európai Unióról szóló szerződés 34. cikkének megfelelően létrehozott, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről.

19 2005. évi CXVI. törvény az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény és az egyezmény 2001. október 16-án kelt kiegészítő jegyzőkönyve kihirdetéséről.

releváns eszközei a távoli helyeken fellelhető bizonyítékok összegyűjtésének. A Cybercrime Egyezmény eljárásjogi rendelkezései körében szól az elektronikus bizonyítékokkal kapcsolatos minimumszabályokról, amelyeket minden részes államnak be kell vezetnie a saját jogrendszerébe. Az Cybercrime Egyezmény alapján a részes államoknak lehetővé kell tenniük a rendszerben tárolt számítástechnikai adatok (ideértve a forgalmi adatokat) gyors megőrzésének elrendelését,[20] valamint a közlésre kötelezést, azaz a területükön tartózkodó személyek kötelezését a rendszerben vagy az adathordozón tárolt adatok átadására, és az információs szolgáltatókat az előfizetőkre vonatkozó és a forgalmi adatok átadására. A Cybercrime Egyezmény kimondottan rendelkezik a kiberbűncselekmények esetében nyújtott jogsegélyről is azzal, hogy a legszélesebb körű együttműködésre buzdítja a részes államokat ezen a területen. A Cybercrime Egyezmény nem kíván a bilaterális jogsegélyegyezmények helyébe lépni, így kimondja, hogy ha két állam között jogsegélyegyezmény van hatályban, akkor elsősorban ennek a szabályait kell alapul venni a kiberbűncselekmények esetében folytatott nyomozás és bizonyítás során. Ha azonban két olyan országról van szó, amelyek részesei a Cybercrime Egyezménynek, ám közöttük nincsen jogsegélymegállapodás, akkor a Cybercrime Egyezmény szabályai kötelezőek rájuk nézve. A részes államok kötelesek kijelölni olyan központi hatóságokat, amelyek feladata az informatikai, köztük a hálózatokon keresztül megvalósított kiberbűncselekményekkel kapcsolatos jogsegélykérelmek intézése, ideértve azok küldését, fogadását és a válaszadást. A Cybercrime Egyezmény jogsegélyről szóló szabályai értelmében jogsegély keretében az alábbi intézkedések megtétele kérhető a részes államoktól:

- tárolt számítástechnikai adat gyors megőrzése,
- megőrzött forgalmi adat gyors átadása,
- tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély,
- forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély,
- tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély.

Arról azonban már nem szólnak a Cybercrime Egyezmény szabályai, hogy milyen forgalmi adatokat és mennyi ideig kell tárolniuk az államoknak, e tekintetben tehát meglehetősen sokféle szabályozási megoldással találkozhatunk, ha olyan országokra tekintünk, amelyek nem tagjai az Európai Uniónak.

A felhőszolgáltatások népszerűsége szintén fejtörést okoz a nyomozó hatóságoknak, hiszen a felhő alapú adattárolás lényege, hogy az adatok akár több országban, több szerveren vannak jelen. Ez történhet akár úgy is, hogy a teljes

20 Cybercrime Egyezmény 16. cikk.

büntetőeljárással érintett adatnak több másolata található több szerveren, vagy úgy is, hogy annak egyes részei szétszórtan találhatóak meg.

Az Egyesült Államokban a United States v. Microsoft Corp. ügyben[21] merült fel a kérdés, hogy egy ország területén letelepedett szolgáltató köteles-e adatszolgáltatást teljesíteni abban az esetben, ha a nyomozó hatóság által kért adatokat más országban tárolja. Az Egyesült Államokban a nyomozó hatóság egy alkalommal egy kábítószer-csempészet ügyében folyó eljárás kapcsán kérte a céget bizonyos adatok átadására. A Microsoft a forgalmi adatokat ugyan átadta, de a tartalmi adatokat (e-mail üzeneteket) nem, arra hivatkozva, hogy azokat írországi adatközpontjában tárolja. Az ügyben másodfokon eljáró 2nd Circuit Court úgy határozott, hogy az ilyen lefoglalást elrendelő határozatok területi hatálya kizárólag az Egyesült Államok területére terjed ki. A Legfelsőbb Bíróság végül megsemmisítette az ítéletet, és új lefoglalási határozat kiadását javasolta a nyomozó hatóságnak, mivel idő közben a kongresszus elfogadott egy felhőszolgáltatásokról szóló törvényt (Clarifying Lawful Overseas Use of Data Act – CLOUD Act), amely az adatok átadását kötelezővé teszi abban az esetben is, ha azokat külföldön tárolják. Érdekessége az ügynek, hogy Írország, ahol a szóban forgó adatokat tárolták amicus curiae-t terjesztett elő, amelyben jelezte, hogy a harmadik országba történő adattovábbítás ellenétben áll az EU általános adatvédelmi rendeletével (GDPR), valamint az ír joggal is, hiszen az adatokat az USA hatóságainak az USA és Írország között fennálló jogsegélyegyezmény szabályai szerint kellett volna kérniük, nem pedig közvetlenül a cégtől (URL3). Az Európai Adatvédelmi Testület egyébként a CLOUD Act szabályait uniós jogba ütközőnek tekinti (URL4), mindezt annak ellenére, hogy az EU, ahogy alább is látni fogjuk, maga is a közvetlenség elvét hangsúlyozza a határokon átnyúló bizonyításban.

Jogsegély helyett extraterritoriális joghatóság: más tagállam joghatósága alatt álló szolgáltatókkal szemben közvetlenül alkalmazandó intézkedések

A kiberbűncselekmények, a bizonyítékok illékonysága és az elkövetők mobilitása miatt bizonyos eljárási cselekmények sürgős elvégzését igénylik. Fő szabály szerint a külföldön lefolytatandó bizonyítási cselekmények és elvégzendő kényszerintézkedések esetében az eljárást a magyar hatóságok megkeresése alapján a külföldi, az érintett személy vagy szerv felett joghatósággal rendelkező

21 United States v. Microsoft Corp., 584 U.S., 138 S. Ct. 1186 (2018).

ország folytatja le. A többlépcsős folyamaton áteső eljárások esetében viszont a gyors fellépés nem biztosítható. Egyre erősebb igény mutatkozik arra, hogy a nyomozást folytató szervek közvetlenül is elvégezhessenek bizonyos eljárási cselekményeket más tagállamban az érintett tagállam hatóságainak bevonása nélkül, pontosabban egyszerű tájékoztatásuk mellett. A végrehajtásban korántsem egyedi az extraterritorialitás, ugyanis lehetőség van a határozatok külföldi végrehajtására az Európai Unió általános hatályú, közvetlenül alkalmazandó kötelező jogi aktusa, törvény, kormányrendelet vagy viszonosság alapján (Boros, 2016). Az igény mára uniós szintű törekvéssé formálódott, amely jelenleg is zajló, aktív jogalkotás révén tesz a tagállamok közötti bizonyítékgyűjtés, a kényszerintézkedések foganatosításának, illetve az egyes intézkedések végrehajtásának egyszerűsítéséért.

Az alábbiakban a Cybercrime Egyezmény jogsegélyre vonatkozó szabályai között is megjelenő három főbb intézkedéscsoportra bontva vizsgálom meg azokat az eseteket, ahol a büntetőeljárás során lehetőség van a közvetlen fellépésre Magyarország határain túl. Elsőként azokat a szabályokat hasonlítom össze, amelyek az adatkérésre irányuló megkeresésekről rendelkeznek. Ezt követően a digitális bizonyítékok megőrzésének eszközeiről lesz szó, végezetül pedig a jogellenes információk eltávolítására, illetve hozzáférhetetlenné tételére irányuló eszközöket tekintem át.

Más tagállamban letelepedett internetes közvetítő szolgáltatók megkeresése információkérés céljából

A büntetőeljárásban az adatkérés célja, hogy a nyomozó hatóság információt szerezzen a gyanúsítottról, lehetséges tanúkról, az elkövetés körülményeiről, illetve hogy bizonyítékot szerezzen. A hazai közvetítő szolgáltatóktól a Be. 261. §-a alapján van lehetőség információt kérni, azzal a megkötéssel, hogy az elektronikus hírközlési szolgáltatónak minősülő közvetítő szolgáltatóktól (például internetszolgáltatók) csak ügyészi engedéllyel kérhető adatszolgáltatás. A magyar Be. szabályait azonban csak a magyar joghatóság alatt álló szolgáltatókra lehet alkalmazni; amennyiben az információ birtokában lévő szolgáltató külföldi illetőségű, maradnak a jogsegély eszközei. Az EU E-evidence rendelettervezete komoly változást fog hozni ezen a területen, bevezetné ugyanis a közlésre kötelező európai határozatok intézményét, amely alapján magyar bíróság, ügyészség, hatóság közvetlenül kötelezhetne adatszolgáltatásra a más tagállamokban letelepedett szolgáltatókat is.

Új és már létező eszköz a szabályozási palettán a digitális szolgáltatásokról szóló rendelet (a továbbiakban: DSA)[22] által bevezetett információszolgáltatási végzés. Nem tipikus büntetőeljárási eszközről van szó, hiszen célja annak megállapítása, hogy a szolgáltató egyes felhasználói megvalósítanak-e jogsértést a szolgáltatáson keresztül. Noha ez lefedi a büntetőjogi jellegű jogsértéseket is, nem korlátozódik azokra. A végzés kibocsátója ennek megfelelően nem szükségszerűen igazságügyi hatóság, a tagállamok akár közigazgatási hatóságra is testálhatják az ilyen végzések kibocsátásának jogát. A szolgáltató kötelessége tájékoztatni a kibocsátó hatóságot a végzés kézhezvételéről, valamint arról, hogy azt végrehajtotta-e,[23] ami azt sugallja, hogy a felhasználóra vonatkozó információ átadása nem kötelező. Ezt az elgondolást ugyanakkor cáfolja a DSA preambulumbekezdése, amely viszont előírja, hogy *„a végzések nem teljesítése esetére a kibocsátó tagállam számára lehetővé kell tenni a nemzeti jogával összhangban lévő végrehajtást”*.[24] Mindenesetre amennyiben büntetőügyben van szükség fontos információra, nem javasolt az információszolgáltatásra vonatkozó végzések alkalmazása. Ugyancsak nyitott kérdés, hogy az így megszerzett információ felhasználható-e bizonyítékként a büntetőeljárásban.

Az európai e-bizonyíték javaslatcsomag részeként bevezetendő a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendelet szintén tartalmazna információszolgáltatásra irányuló eszközt. Ennek kibocsátója a DSA információszolgáltatásra vonatkozó végzésével ellentétben csak büntetőügyben eljáró szerv lehetne, az információ átadása pedig kötelező lenne a megkeresett szolgáltató számára. Parti Katalin tanulmányában rávilágít arra, hogy a közlésre kötelező európai határozatok elfogadásáról szóló uniós jogszabály elfogadása esetén a magyar jogi szabályozás átgondolására is szükség lesz. A jelenlegi szabályozást alapul véve ugyanis előállhat egy olyan helyzet, hogy a rendelet alapján a szolgáltató köteles teljesíteni a külföldi megkeresést, míg a belső jog ezt kifejezetten tiltja számára, például ha minősített adatnak számít a kért információ (Parti, 2018).

22 Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról.
23 DSA 10. cikk (1) bekezdés.
24 DSA (32) preambulumbekezdés.

1. számú táblázat
Az információszolgáltatás eszközei az uniós jogban

	DSA információszolgáltatásra vonatkozó végzés	Közlésre kötelező európai határozat (e-bizonyíték javaslatcsomag)
Kibocsátó	Nemzeti igazságügyi vagy közigazgatási hatóság.	Bíró, bíróság, ügyész, büntetőeljárás során illetékes hatóság.
Kötelezett	Bármely tagállamban letelepedett közvetítő szolgáltató: - egyszerű hozzáférés szolgáltató, - cache, - tárhelyszolgáltató, - online platform, - videómegosztó.	Elektronikus hírközlési szolgáltatók, olyan információs társadalmi szolgáltatók, amelyek esetében az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak (közösségi oldalak, online piacterek és egyéb tárhelyszolgáltatók), internetes domainnév-szolgáltatók és IP-szám szolgáltatók.
Célja	Annak megállapítása, hogy az igénybe vevők megfelelnek-e az uniós vagy a nemzeti jognak.	Bizonyítékok megszerzése, elkövető azonosítása büntetőeljárásban.
Kötőerő	Nem kötelező.	Kötelező.

Forrás: A táblázatot a szerző készítette.

Az információ megőrzésére irányuló eszközök az uniós és a belső jogban

Az adatmegőrzési kötelezettség telepítése a szolgáltatókra – legyen szó akár általános, akár egyedi ügyben történő megőrzési kötelezettségről – az elektronikusan tárolt bizonyítékok integritásának biztosítását és konzerválását szolgálják. A bizonyítás eredményességét veszélyezteti ugyanis, ha az ilyen adatokat eltávolítják, megváltoztatják vagy törlik. Hatályos magyar jogunk a hírközlési szolgáltatás nyújtása során keletkező forgalmi adatok megőrzését rendeli el, más adatfajták esetében pedig biztosítja az egyedi megőrzésre kötelezés lehetőségét. Ezek azonban szintén olyan eszközök, amelyek a magyar joghatóság alatt álló szolgáltatók esetében jöhetnek szóba. Az általános hírközlési adatmegőrzés korábban az EU-ban is ismert volt a Digital Rights v. Seitlinger egyesített ügyekben, azonban az Európai Unió Bírósága úgy ítélte meg, hogy egy ilyen kiterjedt megőrzési kötelezettség oly mértékben korlátozná a polgárok magánélethez való jogát, amely nem áll arányban a legkomolyabb bűnüldözési érdekkel sem, és érvénytelenné nyilvánította az E-hírközlési irányelv vonatkozó részét. Az E-hírközlési kódex újraszabályozása éppen folyamatban van, a hatályos uniós jog azonban nem ír elő általános adatmegőrzési kötelezettséget. A tagállamok nemzeti jogukban természetesen tehetnek ilyet, ez azonban azt eredményezi, hogy nincsenek egységes szabályai annak, hogy az európai szolgáltatók milyen adatokat és mennyi ideig tárolnak, ami adott esetben a nyomozás sikerét veszélyeztetheti.

Egyedi megőrzési kötelezettség egyelőre csak a terrorista tartalmak tekintetében létezik, és kizárólag a tárhelyszolgáltatókat terheli. Nekik a terrorista tartalmakként azonosított információkat nem csak eltávolítaniuk, de megőrizniük is szükséges, hogy később büntetőeljárásban felhasználhatók legyenek.

Hasonló kötelezettséget vezetne be egy új rendelet a gyermekek szexuális bántalmazásának üldözése körében azzal, hogy ebben az esetben a megőrzés nem volna kötelező, csupán önkéntes.

Az e-bizonyíték javaslatcsomag ezen a területen is változást hozna, hiszen bevezetné a megőrzésre kötelező európai határozatokat, amelyek használatával elrendelhető más tagállam szolgáltatója számára az eljárásban releváns információk megőrzése.

2. számú táblázat
Az adatmegőrzés eszközei az uniós jogban

	Megőrzésre kötelező európai határozat (e-bizonyíték javaslatcsomag)	**Információ megőrzése a gyermekek szexuális bántalmazásáról szóló rendelettervezet alapján**	**A tartalom és a kapcsolódó adatok megőrzése a 2021/784 rendelet alapján**
Kibocsátó	Bíró, bíróság, ügyész, büntetőeljárás során illetékes hatóság.	–	–
Kötelezett	Elektronikus hírközlési szolgáltatók, olyan információs társadalmi szolgáltatók, amelyek esetében az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak (közösségi oldalak, online piacterek és egyéb tárhelyszolgáltatók), internetes domainnév-szolgáltatók és IP-szám szolgáltatók.	Tárhelyszolgáltatók és a személyközi hírközlési szolgáltatást nyújtó szolgáltatók.	Tárhelyszolgáltatók.
Célja	Adatok eltávolításának, törlésének vagy megváltoztatásának megakadályozása.	Bizonyítékként releváns adatok megőrzése későbbi közlésre kötelezés céljából.	Az eltávolított vagy hozzáférhetetlenné tett terrorista tartalmak megőrzése későbbi közlésre kötelezés céljából.
Kötőerő	Kötelező.	Önkéntes.	Kötelező.

Forrás: A táblázatot a szerző készítette.

Jogellenes tartalom eltávolítására és hozzáférhetetlenné tételére irányuló intézkedések

Két, a határokon átnyúló büntetőeljárásban jelentős kényszerintézkedésről kell még szót ejteni. A tartalomközléssel elkövetett bűncselekmények esetében azon túl, hogy a hatóságok gondoskodnak a bizonyítékok megőrzéséről, azt is biztosítani kell, hogy az internet többi felhasználója ne férhessen hozzá a jogsértőnek

vélt tartalmakhoz. Ezt az elektronikus adatok eltávolítása, illetve hozzáférhetetlenné tétele útján lehet elérni. A két intézmény közötti különbség, hogy eltávolítás esetén a szóban forgó tartalom lekerül a tárhelyről, hozzáférhetetlenné tétel esetén azonban az elérési hely nem változik, de a felhasználók vagy azok egy csoportja nem látja a problémás tartalmat. Az eltávolítás kötelezettje jellemzően az a tárhelyszolgáltató, amelynek a szerverén a tartalom elhelyezkedik, a hozzáférés megakadályozása ellenben más közvetítő szolgáltató bevonásával is megvalósulhat, hiszen az internetszolgáltatók is tudnak arról gondoskodni, hogy bizonyos domaineket ne érjenek el a felhasználóik. A magyar joghatóság alatti szolgáltatók esetében az elektronikus adat ideiglenes eltávolítása, illetve hozzáférhetetlenné tétele kényszerintézkedések a Be. 335. §-nak megfelelően alkalmazhatók.

A nem Magyarország területén letelepedett szolgáltatókat a jogellenes tartalmak esetében a DSA alapján,[25] a terrorista tartalmak esetében pedig a 2021/784 rendelet alapján lehet eltávolításra kötelezni. A DSA-ban szabályozott határozatok, az információszolgáltatási végzésekhez hasonlóan, szintén nem klasszikusan büntetőjogi jellegű eszközök, hiszen a jogellenes tartalmak bármely típusa esetén, így például fogyasztóvédelmi ügyekben is igénybe vehetők. A DSA preambuluma kimondottan rendelkezik is a határozatok és a büntetőeljárásjogi eszközök viszonyáról, amikor kimondja, hogy a DSA szabályai „nem feltétlenül alkalmazandók", valamint „kiigazíthatók" abban az esetben, ha a büntetőügyekben kibocsátott elektronikus bizonyítékokra vonatkozó közlésre és megőrzésre kötelező európai határozatokról szóló rendelet, konkrét jogellenes tartalmat szabályozó egyéb rendelet, vagy a nemzetközi polgári- és büntetőjog szabályai eltérő feltételeket szabnak.[26] Tipikusan ilyen uniós norma a terrorista tartalmakat szabályozó 2021/784 rendelet, ahol az eltávolítást a tárhelyszolgáltatónak a megkeresés kézhezvételétől számított egy órán belül kötelessége elvégezni, de elfogadása esetén ilyen lesz a gyermekek szexuális bántalmazásáról szóló rendelet is.

25 DSA (34) preambulumbekezdés szerint az érintett nemzeti hatóságok számára lehetővé kell tenni, hogy jogellenesnek tekintett tartalmakkal szembeni végzéseket adjanak ki és azokat a közvetítő szolgáltatókhoz intézzék, ideértve a más tagállamban letelepedett szolgáltatókat is.

26 DSA (34) preambulumbekezdés.

3. számú táblázat
A jogellenes tartalmak eltávolításának eszközei az uniós jogban

	DSA jogellenes tartalom elleni fellépésre vonatkozó határozat	Eltávolítást elrendelő határozat a gyermekek szexuális bántalmazásáról szóló rendelettervezet alapján	Eltávolítási végzések a 2021/784 rendelet alapján
Kibocsátó	Nemzeti igazságügyi vagy közigazgatási hatóság.	A koordináló hatóság felkérése alapján a székhely szerinti tagállam igazságügyi vagy közigazgatási hatósága.	Tagállami illetékes hatóság.
Kötelezett	Bármely tagállamban letelepedett közvetítő szolgáltató: - egyszerű hozzáférés szolgáltató, - cache, - tárhelyszolgáltató, - online platform, - videómegosztó.	Tárhelyszolgáltatók.	Tárhelyszolgáltató.
Célja	Jogellenes tartalmak eltávolítása.	A gyermekek szexuális bántalmazását ábrázoló anyagként azonosított tartalom eltávolítása.	Terrorista tartalmak eltávolítása.
Kötőerő	A szolgáltató tájékoztatja a kibocsátót, hogy végrehajtotta-e a határozatban foglaltakat. Ha nem, akkor nemzeti szinten végrehajtás kezdeményezhető.	Kötelező, 24 órán belül.	Kötelező, az eltávolítási végzés kézhezvételétől számított egy órán belül.

Forrás: A táblázatot a szerző készítette.

4. számú táblázat
A jogellenes tartalmak hozzáférhetetlenné tételének eszközei az uniós jogban

	Hozzáférés letiltása a gyermekek szexuális bántalmazásáról szóló rendelettervezet alapján	Hozzáférhetetlenné tétel a 2021/784 rendelet alapján
Kibocsátó	A koordináló hatóság felkérése alapján a székhely szerinti tagállam igazságügyi vagy közigazgatási hatósága.	Tagállami illetékes hatóság.
Kötelezett	Internet-hozzáférés szolgáltató.	Tárhelyszolgáltató.
Célja	Felhasználók hozzáférésének megakadályozása a gyermekek szexuális bántalmazását ábrázoló ismert anyagokhoz.	Felhasználók hozzáférésének megakadályozása a terrorista tartalmakhoz.
Kötőerő	Kötelező, a kezdő és a záró időpontot a koordináló hatóság jelöli meg.	Kötelező, az eltávolítási végzés kézhezvételétől számított egy órán belül.

Forrás: A táblázatot a szerző készítette.

Konklúzió

A tanulmányban a nemzetközi együttműködés két olyan területét vizsgáltam, ahol a kiberbűncselekmény elleni fellépés nehézségekbe ütközik. A joghatóság mint az országok közötti ügyelosztás rendjét szabályozó keretrendszer a nemzetközi jog főként bilaterális és csekélyebb számú nemzetközi szabálya miatt

klasszikus jogi szabályozás révén kevéssé befolyásolható. Az ügyelosztás alapját képező joghatósági szabályokon túl itt inkább az országok közötti együttműködésé a fő szerep. Az együttműködés ösztönzésére természetesen kidolgozhatók megoldások, fontos lenne például egy olyan testület, amely segíti az országokat akár a pozitív, akár a negatív joghatósági összeütközések feloldásában.

Jóval nagyobb szerep jut a szabályozásnak abban az esetben, amikor határon túl kell valamilyen eljárási cselekményt végezni. Az EU aktívan figyel erre a területre, ezt mi sem mutatja jobban a számos folyamatban lévő, vagy a közelmúltban lezárult jogalkotási eljárás. A bőség azonban ez esetben ténylegesen zavart okozhat, hiszen az egyes bűncselekménytípusokra különös szabályokat tartalmazó uniós normák megnehezíthetik a megfelelő eszköz kiválasztását. A tanulmányban bemutatott eszközök eredményes alkalmazásának egyik kulcspontja az intézményrendszer, a hatáskörtelepítést azonban a bemutatott uniós jogi aktusoknak nem sikerült megnyugtatóan rendezniük. Az uniós szabályok ugyanis – bár tartalmaznak büntetőeljárásban alkalmazható eszközöket – nem kimondottan büntetőjogi jellegűek, és lehetővé teszik a tagállamoknak, hogy közigazgatási hatóságokra is telepítsenek hatásköröket. A szabályozott, illetve szabályozni kívánt határozatokat és végzéseket a tagállamok arra kijelölt szerveinek közvetlenül a szolgáltatókhoz kell eljuttatniuk, ami a jogalkotó elképzelése szerint jelentősen gyorsítja majd a bizonyítékok gyors összegyűjtését. Magyarországon például a 2021/784 rendelet alapján az eltávolítási végzés kibocsátására jogosult szerv az Ekertv. 12/B. §-a[27] alapján a Nemzeti Média- és Hírközlési Hatóság Hivatala. Hasonló szabályozási megoldás várható hazánkban a DSA esetében is, ahol a digitális szolgáltatási koordinátor szerepét az NMHH tölti majd be.

Megfelelő koordináció és kommunikáció híján könnyen előállhat olyan helyzet, hogy ugyanazon jogellenes tartalom vonatkozásában több szerv, többféle intézkedés megtételére felhívó határozatot hoz, ami egyrészt csökkenti az átláthatóságot, másrészt növeli mind a tagállami hatóságok, mind a szolgáltatók munkaterhét. Szoros intézményközi koordinációval azonban ezek a problémák kiküszöbölhetők, erről azonban majd csak a gyakorlati alkalmazás megkezdését követően lehet számot adni.

Felhasznált irodalom

Blaskó B. & Budaházi Á. (2019). *A nemzetközi bűnügyi együttműködés joga.* Dialóg Campus.

Boros A. (2016). *Közérthető közigazgatási hatósági eljárás.* Wolters Kluwer Kft. eBooks. https://doi.org/10.55413/9789632956220

27 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime Law and Social Change, 46*(4-5), 189–206. https://doi.org/10.1007/s10611-007-9063-7

Brenner, S. W. & Koops, B-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law, 4*(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507

Ligeti K. (2008). A nemzetközi bűnügyi együttműködés általános feltételei. In Kondorosi F. & Ligeti K. (Szerk.), *Az európai büntetőjog kézikönyve* (pp. 60–75). Magyar Közlöny Lap- és Könyvkiadó.

Mezei K. (2022). *A kiberbűnözés aktuális kihívásai a büntetőjogban*. L'Harmattan Kiadó, MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet.

Parti K. (2018). Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntető-eljárás során a gyakorlat tükrében. *Belügyi Szemle, 66*(10), 23–35. https://doi.org/10.38146/bsz.2018.10.2

Rawat, M. (2021). Transnational Cybercrime: Issue of Jurisdiction. *International Journal of Law Management & Humanities 4*(2), 253–266. http://doi.one/10.1732/IJLMH.26049

Tóth D. & Gáspár Zs. (2020). Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle, 9*(2), 35–45.

Villányi J. (2003). Az EU kölcsönös bűnügyi jogsegélyéről szóló egyezményhez kapcsolódó jogalkotási feladatok. *Acta Universitatis Szegediensis: Acta Juridica et Politica: Publicationes Doctorandorum Juridicorum III,* 209–259.

A cikkben található online hivatkozások

URL1: *Least developed countries still lag behind in cyberlaw reforms*. https://unctad.org/news/least-developed-countries-still-lag-behind-cyberlaw-reforms

URL2: *Philippine Prosecutors Drop Charges in 'Love Bug' Case, WSJ*. https://www.wsj.com/articles/SB966862157148570125

URL3: *Ireland's Second Circuit Amicus Brief in Support of Microsoft*. https://www.eff.org/document/irelands-second-circuit-amicus-brief-support-microsoft

URL4: *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence.*
https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf

A cikk APA szabály szerinti hivatkozása

Sorbán K. (2024). A jogellenes tartalomközléssel megvalósított kiberbűncselekmények elleni fellépés eljárásjogi dilemmái a nemzetközi együttműködésben. *Belügyi Szemle*, *72*(1), 7–26. https://doi.org/10.38146/BSZ.2024.1.1