DOI: 10.59851/imr.13.1.6 IN MEDIAS RES 2024/1. • 6, 112–137

FÓRUM

A bűncselekmény helyszíne: az internet

Bizonyítási és eljárási nehézségek az interneten elkövetett bűncselekmények kapcsán

BÉKÉS ÁDÁM* – GÉPÉSZ TAMÁS**

A jelen tanulmány célja, hogy a kiberbűnözéshez, különösen az interneten elkövetett bűncselekményekhez kapcsolódó rövid bevezetést, általános kérdésfeltevéseket követően büntetőeljárás-jogi fókusszal mutassa be a jelenlegi magyar szabályozás és jogalkalmazási gyakorlat anomáliáit. A tanulmány törekszik a témáról átfogó és gyakorlatorientált képet adni a kibertérben az interneten elkövetett bűncselekményekhez kapcsolódó esetleges nemzeti nyomozás általános és konkrét problémáinak, nehézségeinek bemutatásával, kitérve a nemzetközi bűnügyi együttműködés kapcsán felmerülő kérdésekre is. A felvázolt problématérkép alapján a gyakorlat számára is hasznosítható következtetésekkel és azok alapján – legalább az általánosság szintjén – jövőbeli megoldási javaslatokkal zárul a tanulmány. A hatékonyabb büntetőjogi fellépés érdekében a klasszikus büntetőjogi gondolkodáshoz és jogalkalmazáshoz képest egyfajta paradigmaváltás iránti igényt fogalmaz meg a digitális térben, különösen az interneten elkövetett bűncselekményekre vonatkozóan.

Kulcsszavak: kiberbűnözés, internet, büntetőeljárás, nemzetközi bűnügyi együttműködés

Place of Commission: The Internet
Evidentiary and Procedural Difficulties of the Crimes Committed on the Internet

The aim of the present study is to present the anomalies of the current Hungarian (criminal) legislation and enforcement practice with a criminal procedural focus, following brief introductory thoughts and general assumptions on cybercrime, especially crimes committed on the Internet. The paper aims to provide a comprehensive and practice-oriented picture of this topic by presenting the general and specific problems and difficulties of a possible national investigation of a cyber-crime committed on or via the

* Egyetemi docens, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar.

** Doktorandusz, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar.

Internet, including issues related to international criminal cooperation. Finally, on the basis of the problem map drawn by the article, the authors seek to draw conclusions that can be used in practice. On the basis of these conclusions, the study aims to formulate – at least at a general level – some proposals for future solutions, and call for a so-called paradigm shift from the classical criminal law approach and legal practice concerning the crimes committed in the digital area, especially on the Internet.

Keywords: cyber-crime, internet, criminal procedure, international criminal cooperation

1. Alapvetés

A tanulmány az ún. kiberbűnözés[1] egyes eljárásjogi és gyakorlati kérdéseit vizsgálja a jelenlegi szabályozás és joggyakorlat tükrében, különös tekintettel az interneten elkövetett bűncselekmények bűnüldözési kihívásaira. Tehát elsősorban az interneten elkövetett bűncselekmények processzuális és gyakorlati kérdéseire kíván nagyobb hangsúlyt fektetni, míg csak érintőlegesen vet fel a büntető anyagi jog körébe tartozó olyan dogmatikai, esetleg kodifikációs kérdéseket, amelyek a jelenleg is folyamatban lévő büntetőeljárásokban is jelentőséggel bírnak.

Mára a számítógépek használata megkerülhetetlenné vált, ahogyan azt is evidenciaként kezelhetjük, hogy az internet-hozzáférés és az ahhoz kapcsolódó, azon alapuló számtalan szolgáltatás használata egyre inkább integrálódik a mindennapjainkba, beleértve ebbe a személyes és a munkakörnyezetünket egyaránt. Jól illusztrálja ezt a tendenciát, hogy a legnagyobb közösségi médiaszolgáltató által a 2023. első negyedévéről közölt statisztika szerint[2] a platform közel hárommilliárd aktív felhasználóval rendelkezett, vagyis a Föld lakosságának mintegy harmada használja a szolgáltatást. Ennél is beszédesebb talán, hogy az Amerikai Egyesült Államok vonatkozásában elérhető adatok szerint egy átlagos felhasználó napi harminchét percet tölt el az alkalmazás használatával,[3] ami ráadásul az elmúlt évekhez képest minimális csökkenést jelez.

Az információs technológiák, a digitalizáció előretörésével kapcsolatban Tóth Mihály mutatott rá:

1 E fogalomnak jelenleg nincs sem tételes jogi, sem a jogtudomány által kidolgozott és egységesen elfogadott definíciója. A legelterjedtebb kriminológiai megközelítés egy dichotóm rendszeren alapul, amely elfogadja, hogy a kiberbűnözés eltér a „hagyományos" bűnelkövetéstől, és az alapján tesz különbséget az egyes cselekmények között, hogy azok szükségszerűen kötődnek-e az informatikai rendszerekhez, hálózatokhoz. Ez alapján *cyber-dependant* és *cyber-enabled* bűncselekményeket különböztethetünk meg a digitális térben. Az előbbi kategóriába azok a cselekmények tartoznak, amelyek tárgya az informatikai rendszer, vagyis a tevékenység közvetlenül a számítógép vagy más informatikai rendszer ellen irányul, míg az utóbbi típus az információs rendszerek és szolgáltatások felhasználásával elkövetett cselekményeket foglalja magába. Lásd például Jonathan Clough: *Principles of Cybercrime.* Cambridge, Cambridge University Press, 2015, https://doi.org/10.1017/CBO9781139540803, 10–11.; Marleen Weulen Kranenbarg: *Cyber-Offenders Versus Traditional Offenders: An Empicial Comparison.* Doktori értekezés, Amsterdam, Vrije Universiteit, 2018, https://bit.ly/4bAEr1a.

2 Meta Reports First Quarter 2023 Results. *Meta,* 2023. április 26., https://bit.ly/3QM4t9N.

3 A legérdekesebb Facebook-statisztikák. *Facebook,* 2023. május 10., https://bit.ly/3QM4HOb.

> tudjuk, hogy minden új, az életünk könnyebbé, tartalmasabbá tételére hivatott technikai vívmány létrehozásával egyidejűleg kitermeli bűnös haszonélvezőit is [így…] fontos kriminogén kérdéseket vet fel pl. az információhoz való szinte korlátlan hozzájutás és az ezzel való visszaélés összefonódása. Az internet, amellett, hogy „áldás", bizony olykor „átok" is.[4]

Ezzel kapcsolatban egy 2001-es brit tanulmány fogalmazza meg az egyik alapvető kérdést: vajon a virtuális kriminalitás esetében „régi borról beszélünk új palackban",[5] vagy ennél összetettebb a kép? Másképpen fogalmazva: „miért kell ahhoz új tényállás, ha a hamis papír helyébe, engedve a korszerűség kínálta lehetőségeknek, hamis vagy hamisított informatikai program lép?"[6]

Mivel a jelen tanulmány elsősorban nem anyagi jogi központú, nem célunk az előző kérdések átfogó elemzése és részletes megválaszolása. Maguk a kérdések ugyanakkor rámutatnak arra, hogy a számítógépes technológiák fejlődése kéz a kézben jár a bűnözői gondolkodásával, ami új és nagy kihívások elé állítja a jogalkotókat és a jogalkalmazókat, miközben számos ponton erodálódni látszanak a büntetőjog eddig egyértelműnek hitt elvei, szabályai.

Pragmatikus és a bűnüldöző hatóságok alkalmazkodási képességét is alátámasztó példával élve: egy „hagyományos" nyomozás keretében aligha lett volna elképzelhető az a hatósági siker, hogy egy kábítószer-kereskedőhöz a World of Warcraft online játékba való bejelentkezései alapján jussanak el.[7] Az pedig végképp elképzelhetetlennek tűnt, hogy a bűnüldöző szervek huzamosabb ideig üzemeltessenek illegális tartalmakat kínáló weboldalt annak érdekében, hogy annak használóit be tudják azonosítani, majd felelősségre vonni, mindezt egy összehangolt nemzetközi, mondhatni globális bűnügyi együttműködés keretében.[8]

2. A nyomozás kérdései, nehézségei, tapasztalatai a jelenlegi szabályozási környezetben

A következőkben azt mutatjuk be, hogy a jelenlegi szabályozási környezetben az interneten elkövetett bűncselekmények hazai nyomozása milyen akadályokba, eljárási és gyakorlati nehézségekbe ütközhet.[9]

---

4 Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In Gál István (szerk.): *Informatika és büntetőjog.* Pécs, PTE ÁJK, 2006, 180., 188.

5 Peter N. Grabosky: Virtual Criminality: Old Wine in New Bottles? 10(2) *Social and Legal Studies* (2001), https://doi.org/10.1177/a017405, 243–249.

6 Tóth i. m. (4. lj.) 182.

7 Drug fugitive caught thanks to Warcraft addiction. *Destructoid,* 2010. január 4., https://bit.ly/4akFOAe.

8 Az Operation Pacifier a Playpen elnevezésű gyermekpornográfiával kereskedő weboldal használóit célozta meg, és az akció világszerte – Kolumbia, Horvátország, Csehország, Franciaország, Írország, Olaszország, Szlovákia, Svájc és az Egyesült Királyság területén történő végrehajtással – 870 személy letartóztatásához vezetett: https://bit.ly/3UFFWEE.

9 Ezzel kapcsolatban Nagy Zoltán András szerint a számítógépeken és a számítástechnikai hálózaton elkövethető bűncselekmények nyomozását több körülmény is befolyásolja. A nyomozók felkészültsége az inkriminált adatok (például tartalomközlések), a hálózati történések – számítástechnikai rendszerbe történő illegális belépés *(hacking),* weboldal felülírása *(defacing),* a számítástechnikai rendszert érő terheléses támadás (botnett-támadás), a felhasználót fenyegető zsarolóvírus (*ransomware* és más rosszindulatú szoftverek, például *malware*-ek stb. – megér-

2.1. A nyomozás alapvető kérdései

Az egyik elsődleges probléma az, hogy az internet az elmúlt évek során megszűnt „jogmentes" területként létezni:[10] egy globális és szinte követhetetlen hálózatot, az afeletti joghatóságot valamennyi nemzet a saját szabályozása szerint legalább részben magának vindikálja – anyagi és eljárásjogi értelemben is –, anélkül, hogy arra egységes, univerzális jogi szabályozás vonatkozna. Még várat magára, hogy „az online térre is afféle *res communis omnium usus*ként tekintsünk, mint mondjuk a világűrre".[11] Ez viszont azt is eredményezi, hogy a jelenlegi szabályozás mellett a legtipikusabbnak tekinthető, országhatárokon átívelő cselekmények szabályozása teljességgel fragmentált, ahogyan a gyakorlat is.

Az interneten történő elkövetés technikai háttere, az új szolgáltatások, lehetőségek miatt a joghatósági és illetékességi kérdésekben a hagyományos territoriális szemlélet nem vagy csak nehézkesen alkalmazható. Adott esetben tehát egy nyomozás már rögtön az eljárás elején megakadhat annak az egykor egyszerűnek tűnő kérdésnek a megválaszolásán, hogy eljárhat-e a nemzeti bűnüldöző hatóság, és ha igen, akkor mire is alapítja saját joghatóságát. Ezenkívül még ha a nemzeti hatóság meg is állapítja a saját joghatóságát, továbbra is kérdés, hogyan és mennyiben képes eljárása során az intézkedéseit érvényre juttatni, kikényszeríteni.

A nyomozó hatóságnak azt is meg kell vizsgálnia, hogy elérhető-e egyáltalán valamilyen bizonyítási eszköz Magyarországon, és ha igen, akkor arról kell döntést hoznia, hogy szükség esetén a rendelkezésre álló kényszerintézkedések közül melyek végrehajtása lehet a legalkalmasabb az adott helyzetben. Ez a döntési helyzet azonban nemcsak jogi, hanem megfelelő és magas szintű technikai ismereteket is feltételez(ne),[12] arról nem is beszélve, hogy a kibertérben elkövetett deliktum felderítése a hagyományos bűncselekményeknél alkalmazott és bevált nyomozási tervektől, stratégiáktól eltérő krimináltaktikát igényelhet.

Ha a területi kérdésre nemleges a válasz, akkor a nemzeti nyomozó hatóság azzal szembesül, hogy a felderítés kizárólag nemzetközi bűnügyi együttműködés keretében lesz kivitelezhető. Ezzel kapcsolatban pedig már utaltunk rá, hogy jelenleg nincs hatályban olyan globális szabályozás, amely biztosíthatná az összes nemzet társhatóságával való zökkenőmentes bűnügyi együttműködést. Bizonyos ügyekben már az eljárás elején egyértelművé válhat, hogy a nyomo-

tése, ismerete. Emellett ha a számítógépek, hálózatok fizikailag elérhetők, és Magyarországon vagy a zászlóelv miatt magyar felségterületen találhatók, akkor a bizonyítékok megszerzésére irányuló és sajátos megoldásokat kívánó kényszerintézkedéseket kell végrehajtani. Ha viszont a számítógépes hálózat vagy annak részét képező számítógép fizikailag nem érhető el, különösen ha nem is lokalizálható a bizonyítékok megszerzésének helye, akkor a nemzetközi büntetőjogi intézmények formalizmusa jelenthet akadályt. Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In Homoki-Nagy Mária et al. (szerk.): *Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára.* Szeged, SZTE ÁJK, 2018, 759.

10 Klein Tamás: Az online diskurzusok egyes szabályozási kérdései. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018, 11–40.

11 Sorbán Kinga: *Az internetes közvetítő szolgáltatók szerepe és felelőssége az informatikai bűncselekmények nyomozásában.* Doktori értekezés, Budapest, ELTE, 2021, 231.

12 Ezzel kapcsolatban Parti Katalin mutatott rá, hogy „az elkövetőknek sokszor jóval elmélyültebb az informatikai tudásuk, mint a nyomozóhatóság tagjainak, de az ügyészeknek és a bíróknak is, így a gyanúsított félrevezető védekezése sokszor nehezítheti az eljárást". Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In Virág György (szerk.): *Kriminológiai Tanulmányok* 44. Budapest, OKRI, 2007, 98.

zás sikere még elvi szinten sem biztosítható, míg más esetekben az eljárás a nemzetközi bűnügyi együttműködés gyakorlati implementációja, annak akadozása, nehézkessége miatt válhat sikertelenné, lényegében formálissá, és az érdemi kilátások nélküli felfüggesztéshez vezethet. A következőkben a fenti problémaköröket vizsgáljuk meg részletesebben.

2.2. Kezdeti nehézségek: a joghatóság, az illetékesség és az elkövetés helyének dilemmái

A Büntető törvénykönyvről szóló 2012. évi C. törvény (Btk.) 3. §-ában foglalt, a területi és a személyi hatály elvét rögzítő rendelkezés alapján egyértelmű, hogy a jelenlegi szabályozás szerint az állam büntetőhatalmi igénye elsődlegesen territoriális alapokon és szemléleten nyugszik. Retorikai kérdésként merül fel, hogy ez mennyiben fenntartható megközelítés az internet, azaz egy olyan globális hálózat vonatkozásában, amelynek üzemeltetői és gyakorta felhasználói sem lokalizálhatók pontosan. A válasz egyértelműen az, hogy „az elkövetés helyének meghatározása a kibertérben (interneten) keresztül történő elkövetés esetén lényegesen nagyobb dilemmát jelenthet a hatóságok számára, mint a szokványos, személyes jellegű bűnelkövetés esetén",[13] mivel a földrajzi alapú joghatósági és illetékességi megközelítés az interneten elkövetett bűncselekményekkel kapcsolatban nagyrészt értelmezhetetlen vagy jelentős nehézségekbe ütközik.

Az esetek döntő többségében ugyanis az internetes bűncselekményeket az internet felhasználásával követik el, vagyis az internet az elkövetés eszközeként funkcionál, és tulajdonképpen nincs érdemi jelentősége annak, hogy az internethálózat egyes elemei konkrétan hol helyezkednek el. A klasszikus joghatósági elvek alapján így nehezen vagy egyáltalán nem állapítható meg, hogy melyik állam rendelkezik joghatósággal, ami pozitív és negatív joghatósági ütközéshez vezethet. Elképzelhető tehát, hogy egy adott cselekmény kapcsán pusztán földrajzi alapon több állam is magának vindikálja az eljárási jogosultságot, de az is, hogy hiába tűnik érintettnek több nemzet ezen az alapon, végül egyikük sem tud (vagy akar) eljárni. Például nemcsak a felderítés, hanem a joghatóság szempontjából is kérdéseket vet fel, hogy melyik állam járhat el, amikor az elkövetők távoli hozzáféréssel veszik át az irányítást egy idegen országban található eszköz felett, ahol az „áldozat" számítógép legtöbbször csak az utolsó szeme egy hosszú láncolatnak, amely különböző informatikai eszközön és akár államokon át húzódik annak érdekében, hogy egy végső információs rendszer ellen intézzen támadást.[14]

Ezt a problémát egy átfogó, univerzálisan alkalmazható, globális szabályozás tudná a leghatékonyabban megoldani, amelynek kimunkálására és elfogadására, különösen egységes alkalmazására valójában csekély esély mutatkozik. Pragmatikusabb megoldás lehet legalább regionális szinten egységes szabályozás kialakítására törekedni (például egy uniós kódex megal-

[13] Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, big data, profilozás.* Budapest, HVG-ORAC, 2018, 107–121.; Ambrus István: Miskolczi Barna – Szathmáry Zoltán: Büntetőjogi kérdések az információk korában (Recenzió). *Állam- és Jogtudomány,* 2022/3., https://doi.org/10.51783/ajt.2022.3.05, 107–135.

[14] Tóth Dávid – Gáspár Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle,* 2020/2., 145.

kotásával), az egyes nemzeti hatóságok közötti együttműködést segítő, koordináló szervezetek fenntartásával (amilyen például az Europol). Mindezek alapján a kibertérben elkövetett cselekményeknél mind az anyagi, mind az eljárási értelemben vett joghatóság értelmezésekor – lehetőség szerint globális, de legalábbis regionális szinten – indokoltnak tűnik egyfajta szemléletváltás, a territoriális alapú joghatóság meghaladása, a fizikális tértől való elválasztása (például egy univerzálisan alkalmazható „digitális tér" tételezésével).

Az interneten elkövetett bűncselekményeket többféleképpen is csoportosíthatjuk; az itt vizsgált kérdéskör szempontjából célszerű aszerint kategorizálni, hogy az interneten elérhetővé vált adat vagy tartalom, az ahhoz való hozzáférés, annak birtoklása (letöltése) és az azzal való további rendelkezés valósít-e meg bűncselekményt, vagy pedig az internet felhasználásával kinyilvánított valamilyen közlés. Az előbbi kategóriára példa a gyermekpornográf felvételek elérhetővé tétele, letöltése és az ilyen adat vagy tartalom bármilyen módon történő kezelése. Ebben az esetben továbbra is a territoriális szemlélet érvényesül, vagyis az lesz meghatározó, hogy hol történik az adattal vagy tartalommal való rendelkezés, például hol tárolják a felvételeket, ami a legtöbb esetben meghatározható. Azonban egyre gyakoribb a felhőszolgáltatások igénybevétele, márpedig a virtuális felhőt üzemeltető infrastruktúra lényegében nem lokalizálható, az ott tárolt adatok, tartalmak helye lényegében meghatározhatatlanná válhat. Ilyenkor a felhőszolgáltatásban elérhetővé tett adattal, tartalommal kapcsolatos további cselekmények adhatnak támpontot a territoriális szemléletű megközelítéshez, de kérdés, hogy sikeres lehet-e a felderítés egy profi elkövető esetében, aki akár több, anonimitást és követhetetlenséget nyújtó szolgáltatást is igénybe vehet.

A másik fajta, közléssel megvalósított deliktumokra példa az internetes csalás,[15] zaklatás, becsületsértés és rágalmazás. A jelenlegi bírói gyakorlat azonban, úgy tűnik, következetlenül ítéli meg e cselekményeknél a megvalósítás helyét és ezzel együtt az illetékesség kérdését. A BH2011. 332. számon közzétett eseti döntés szerint internetes hirdetéssel megvalósított csalásnál az elkövetési magatartás – a megtévesztés – akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot. A döntés indokolása szerint az internetes szolgáltató (mint közvetítő) székhelye, valamint a vádlott lakó- vagy tartózkodási helye és bankszámlájának helye közömbös. Tehát ilyenkor a sértett tartózkodási helye fogja meghatározni az illetékességet. Ezzel szemben a BH2016. 167. számú eseti döntés kimondja, hogy az interneten közléssel megvalósult rágalmazás vagy becsületsértés esetén a bűncselekmény elkövetésének helye – amely egyben az általános illetékességi oknak felel meg – a weboldalt működtető szerver helye, és ha az külföldön van, akkor a bíróság illetékességét a terhelt lakó- vagy tartózkodási helye határozza meg. Jól látható az ellentmondás a két hivatkozott döntés között, amelyet a Kúria az írott sajtóban és a rádióban, televízióban megvalósított tárgyi deliktumok kapcsán kialakult gyakorlatra hivatkozással igyekezett feloldani.

---

15 Ezzel kapcsolatban Nagy Richárd mutatott rá, hogy 2014 körül jelent meg először Magyarországon és azóta folyamatosan, jelentős ütemben emelkedik az ún. BEC/CEO csalások és az azokhoz kapcsolódó pénzmosási bejelentések száma – itt az elkövetők a célpont informatikai rendszerének feltörését követő manipulációval veszik rá a sértettet, hogy látszólag üzleti partnere részére vagy nevében, valójában az elkövetőknek utaljon át pénzt. Nagy Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. *Belügyi Szemle,* 2018/7–8., https://doi.org/10.38146/BSZ.2018.7-8.6, 89.

Az indokolás szerint e bűncselekményeknél a sértett általi tudomásszerzés másodlagos, a büntetőjogi oltalom elsődlegesen az objektív társadalmi megbecsülést védi, így az elkövetés helye nem az, ahol a sértett az adott becsületcsorbító közleményről tudomást szerez, hanem a közzététel helye. Ez pedig a kialakult bírói gyakorlat szerint az adott médium szerkesztőségének a székhelye, és nincs ok ettől eltérni az elektronikus sajtó újabb formái, így az internet esetében sem. Vitatható, hogy ez utóbbi gondolat megállja a helyét a gyakorlatban, különösen akkor, amikor az eseti döntés is rámutatott arra, hogy „számos, a magyar felhasználók által is széles körben látogatott honlap nem hazai szerverről működik, így a jelen ügyben érintett www.facebook.com sem".[16]

A fentiekkel összefüggésben érdemes kitérni arra, hogy a büntetőeljárásról szóló 2017. évi XC. törvény (Be.) 765. § (3) bekezdése ráadásul a magánvádló feljelentése kapcsán kizárja a 21. § (3) bekezdés b) pontjának alkalmazását, vagyis a sértett lakcíme, tényleges tartózkodási helye nem lehet illetékességi ok. A legtöbb esetben az igénybe vett weboldalt működtető szerver helye valóban külföldön található, ami azt eredményezi, hogy a magánvádlónak ismernie kellene nemcsak a terhelt kilétét, hanem a lakóhelyét is. Ezzel szemben internetes rágalmazás vagy becsületsértés esetén a legtöbbször még az elkövető kiléte sem azonosítható pontosan, nemhogy a lakó- vagy tartózkodási helye. Erre a helyzetre próbál megoldást nyújtani a Be. 767. §-a, lehetővé téve magánvádas eljárásnál is, hogy a bíróság – amely feltehetőleg a Be. 21. § (2) bekezdése szerint, mivel az elkövetés helye nem megállapítható, megelőzés alapján jár el – nyomozást rendeljen el a feljelentett kilétének, személyes adatainak, elérhetőségeinek felderítésére. A nyomozás általános határideje ugyanakkor csak két hónap, ami legfeljebb két alkalommal hosszabbítható további két hónappal. Ha a felderítés a maximális hat hónapon belül nem vezet eredményre, akkor a bíróság az eljárást megszünteti.

Ilyenkor tehát a nyomozó hatóságnak legfeljebb hat hónap alatt kellene beszereznie a külföldi szolgáltatótól a közzététellel kapcsolatos adatokat, majd azok alapján azonosítani az elkövetőt. Nem nehéz belátni, hogy a nyomozás eredményessége meglehetősen kétséges, több tényező miatt is. Először is bizonytalan, hogy a külföldi szolgáltatónál rendelkezésre állnak-e a megfelelő információk, és ha igen, akkor hajlandó-e azokat kiadni, ráadásul ilyen relatíve szűk határidőn belül. Másodszor még ha meg is érkeznek a kért információk a megkeresett szolgáltatótól, profibb elkövető esetén azok nem lesznek elégségesek az azonosításhoz, és további megkeresésekre és/vagy jogsegélykérelmekre lesz szükség.

Emellett a Be. 786. § (5) bekezdése szerint magánvádló távollévő terhelttel szemben vagy külföldön tartózkodó terhelt távollétében bírósági eljárást nem indítványozhat, vagyis ha a nyomozás eredményeképpen kiderül, hogy az elkövető külföldön tartózkodik (legalábbis az informatikai adatok alapján úgy tűnik), akkor az eljárás objektív akadályba ütközhet és felelősségre vonás nélkül véget érhet. Mindezek arra is rámutatnak, hogy szükségessé vált a szolgáltatók aktív közreműködése az internetes közlések „kordában tartásához". Az államokon kívül álló szervezetek által kialakított autonóm szabályozásra tehát nemcsak igény mutatkozik, hanem az egyértelműen indokolt is, és a szerepe a jövőben minden bizonnyal még jobban fel fog értékelődni.[17]

16 BH2016. 167. [38].

17 E kérdés vizsgálatára részletesebben a 2.5. alpontban fogunk kitérni.

Mindezek alapján egyetértünk Szathmáry Zoltánnal, aki szerint máig nem sikerült az internet helyét megtalálni az illetékesség és a joghatóság territoriális fogalmi alapokon nyugvó értelmezési közegében. Ezért a magyar jogalkalmazás „nem tudja következetesen rendezni a hagyományos bűncselekmények internettel való kapcsolatát, azt bűncselekményenként eltérően próbálta az elkövetés értelmezésével vagy analógia útján a már kialakult dogmatikai rendszerhez igazítani", aminek az az oka, hogy „a joggyakorlat jelenlegi útkeresése a technikai fejlődésnek egy már meghaladott állapotára próbál reagálni",[18] ami a jövőben minden bizonnyal tarthatatlanná fog válni. Ezt a problémát álláspontunk szerint legjobban egy – legalább az Európai Unió területén – egységes és minimum a joghatóságot rendező nemzetközi szabályozás tudná feloldani,[19] amely tartalmazhatna iránymutatásokat az illetékességi kérdésekkel kapcsolatban is, ezzel elősegítve az egyes nemzetek jogalkalmazásának, így a magyarénak is, a gyakorlatiasabbá és hatékonyabbá válását.

2.3. A nemzeti nyomozás gyakorlati nehézségei

A joghatósági, illetékességi kérdések körbejárását követően tételezzük fel, hogy a magyar nyomozó hatóság egy eset kapcsán megállapítja joghatóságát és érdemben megkezdi a felderítést. A következőkben egy ilyen nyomozás során felmerülő gyakorlati nehézségeket mutatjuk be.

2.3.1. A speciális felderítési igény és az elektronikus bizonyíték

A nyomozó hatóságnak elsősorban azt kell mérlegelnie, amikor egy digitális térben elkövetett bűncselekmény felderítését kezdi meg, hogy mennyiben alkalmazhatók a klasszikus, már bevált krimináltaktikai módszerek – ugyanis ezek döntő többsége a kibertérben értelmezhetetlen és/vagy értelmetlen. Ráadásul a különböző internetes elkövetések differenciált megközelítést igényelnek, mert nem mindegy – a fenti csoportosítások közül párat alapul véve –, hogy közléssel megvalósított vagy tartalom-bűncselekményről van-e szó, továbbá hogy kizárólag a digitális térben létező, újabb típusú kiberbűncselekmény a nyomozás tárgya, vagy régi – ún. *old wine in a new bottle* – típusú bűncselekményt követtek el az internet felhasználásával.[20] Ennek az alapvető kategorizálásnak az elvégzése után kerülhet abba a helyzetbe a nyomozó hatóság, hogy felmérje az adott elkövetés specifikus jellemzőit, és az alapján vizsgálja, mérlegelje, hogy milyen felderítési igények és lehetőségek mutatkoznak, azokhoz milyen eszközök állnak rendelkezésére, milyen intézkedéseket tud belföldön végrehajtani (ha van egyáltalán ilyen).

---

18 Miskolczi–Szathmáry i. m. (13. lj.) 187., 201.

19 Ennek egyfajta előfutáraként értékelhető az Európai Parlament és a Tanács rendelettervezete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról, amire a 3. pontban térünk ki.

20 Egy angol nyomozó, Paul Hunton, már 2009-ben felhívta a figyelmet az osztályozás és annak alapján a speciális felderítési igények, lehetőségek felmérésének szükségességére a nyomozás kezdőlépéseként, egyben a tipizálás módjára és kategóriáira is tett javaslatot. Paul Hunton: The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. 25 *Computer Law & Security Review* (2009), https://doi.org/10.1016/j.clsr.2009.09.005, 528–535.

Ezenfelül a bűnüldöző hatóság azzal is kénytelen szembesülni, hogy a digitális térhez köthető elektronikus bizonyítékok – bár azt a magyar szabályozás tulajdonképpen tárgyi bizonyítási eszköznek tekinteni – a legkevésbé sem kézzelfoghatók, különösen nem az interneten elkövetett bűncselekmények esetében. A technológia fejlődésével ugyanis egyre kevésbé jellemző, hogy az inkriminált adat ténylegesen, fizikai formában is testet ölt, például egy adathordozón, ráadásul itt nem maga az adathordozó (CD, DVD, pendrive stb.) bírna érdemi jelentőséggel, hanem az azon rögzített adat.[21] Az interneten elkövetett cselekmények többsége pedig már lehet tartalombűncselekmény vagy közléssel megvalósított is, a kifejezetten informatikai eszközöket, hálózatokat támadó deliktumok pedig a digitális térre redukáltak.

Ebből következik, hogy e cselekmények döntő többségénél csak elektronikus bizonyítékok fognak rendelkezésre állni. Ez viszont újabb kihívások elé állítja a hatóságokat már a nyomozás kezdetén. Egyfelől az elektronikus bizonyítékok jellemzően könnyen manipulálhatók, elrejthetők vagy megsemmisíthetők, ezért a gyors, hatékony és szakszerű fellépés elengedhetetlen. Másfelől a nyomozásnak azt is garantálnia kell, hogy a beszerzett adat ne sérüljön vagy módosuljon, bizonyítható legyen az eredetivel való egyezése, valamint a későbbi elemzés se változtassa meg azt.[22] E kritériumok magas szintű informatikai ismeretekkel és megfelelő, modern eszközökkel rendelkező nyomozó hatóság meglétét feltételezik, ami jelenleg Magyarországon a folyamatos és kötelező képzések hiányában sem személyi, sem tárgyi oldalról nem tűnik biztosítottnak.

2.3.2. Kutatás, lefoglalás, az elektronikus adat megőrzésére kötelezés

A fenti általános problémafelvetések után most tételezzük fel, hogy a nyomozást egy tartalombűncselekmény, például gyermekpornográf felvétel miatt rendelik el, és a nyomozó hatóságnak sikerül beazonosítania (például IP-cím alapján), hogy hol töltötték le és feltehetőleg hol tárolják azt. A hatóság ezért a Be. 302. §-a alapján kutatást fog foganatosítani az adott helyen, a rendelkezés második fordulata pedig lehetővé teszi, hogy a kutatás az információs rendszer és az adathordozó átvizsgálására is kiterjedjen. Tehát nincs elvi akadálya annak, hogy a nyomozó hatóság kiberbűncselekmények esetében is eredményes kutatást végezzen.

A gyakorlati végrehajtás során azonban több kritikus kérdés is felmerül, még abban a szerencsés helyzetben is, ha sikerül bizonyítási eszközként értékelhető adatot találni. A fentiekben már utaltunk rá, hogy a profi elkövetők gyakran „áldozatszámítógépet" használnak, így megeshet, hogy az elektronikus bizonyíték azon az eszközön található, azonban a tulajdonosának semmi köze nincs a bűncselekményhez, nem is tud a számítógépe jogellenes felhasználásáról. Technikai szempontból ennél egyszerűbb, de mindenképpen lényeges kérdés, hogy a kutatás helyszínen elérhető-e wifihálózat, az védett-e, vagy elképzelhető, hogy valaki más csatlakozott rá, akár észrevétlenül.[23] Mi történik akkor, ha megtalálják a tiltott felvételt nagy valószínűséggel tároló eszközt, de az ahhoz való hozzáférés titkosítva van? A Be. 305. § (4) és (5) bekezdése

[21] Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. *Ügyészek Lapja*, 2010/2., 25–26.

[22] Shiuh-Jeng Wang: Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. 29(2) *Computer Standards & Interfaces* (2007), https://doi.org/10.1016/j.csi.2006.03.008, 216–218.

[23] Vadász Viktor: A számítógép demisztifikálása. *Ügyészek Lapja,* 2010/2., 20.

alapján egyértelmű, hogy a kutatással érintett személyt együttműködési kötelezettség terheli, legalábbis a bizonyítási eszköz átadására, ugyanakkor a terheltet nem, mert az az önvádra kötelezés tilalmába ütközne.[24] Vagyis könnyen elképzelhető, hogy a megtalált bizonyítási eszköz érdemi vizsgálatához először informatikai szakértő segítségére van szükség, ha a titkosítás az adatok sértetlensége mellett egyáltalán megfejthető.

Ezzel eljutottunk az elektronikus bizonyítékok nyomozás során történő begyűjtésének másik problémájához. Ugyanis a Be. 308. § (2) bekezdése szerint lefoglalni csak elektronikus adatot és elektronikus pénzt lehet,[25] amibe a 309. § (3) bekezdése szerint beletartozhat a még nem továbbított, elektronikus hírközlési szolgáltatás során továbbítandó közlés vagy küldemény is (feltehetőleg ez utóbbi kategória az e-mail-üzenetek „piszkozati" formájára vonatkozik). A Be. 315–317. §-a pedig – felismerve az elektronikus adat speciális jellegét – különös szabályokat állapít meg a lefoglalás végrehajtására. Ezek szerint a fokozatosság elve alapján elsősorban másolatot kell készíteni az elektronikus adatokról, ha ez nem lehetséges, akkor áthelyezhetők az adatok akár az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével is, végül maga az adatot tartalmazó információs rendszer vagy adathordozó is lefoglalható.

Ez utóbbi kapcsán azonban azt is figyelembe kell venni, hogy egy teljes rendszer lefoglalása aránytalan károkkal járhat,[26] éppen ezért a Be. 315. § (4)–(6) bekezdése igyekszik biztosítani a fokozatosság és a szükségesség-arányosság elvének érvényesülését. Hogyan tudná megítélni a hatóság egy komplexebb bűncselekménynél, hogy mely adatok, információk lehetnek relevánsak a későbbiekben, valamint fordítva: fel meri-e vállalni a hatóság azt a kockázatot, hogy egy téves felmérés alapján utóbb nélkülözhetetlennek bizonyuló információkat veszít el? A gyakorlatban éppen ezért továbbra is az a jellemző, a hatóságok számára az a biztos megoldás, hogy még ha fizikálisan nem is veszik el az adott informatikai eszközt, de arról teljes és bitpontos másolatot készítenek, nem válogatva az azon fellelhető adatok közül.

Ki kell térni az elektronikus adat megőrzésére kötelezés kényszerintézkedésre is, amely elviekben a hatóságok számára egyszerűbb a lefoglalásnál, és az elszenvedője számára is kényelmesebb, *soft* megoldás lenne. A hatóságnak ilyenkor nem kellene vesződnie az akár nagy mennyiségű adathalmaz szakszerű kinyerésével, míg a kényszerintézkedéssel érintett számára továbbra is elérhető maradna a teljes informatikai rendszer, hiszen az intézkedés csak a megőrzéssel érintett

---

24 Dornfeld László mutat rá, hogy egyes országokban, például Franciaországban, *sui generis* bűncselekményt valósít meg, aki a titkosítás feloldásához szükséges jelszót nem adja meg a nyomozóknak, míg az Egyesült Államokban ezt már az önvádra kötelezés tilalmába ütközőnek találták. Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 2018/2., https://doi.org/10.38146/BSZ.2018.2.8, 120.

25 Több szerző is felhívja a figyelmet, hogy egyes kriptovaluták – így például a bitcoin – sem tekinthetők elektronikus pénznek. Ezt felismerve terjeszti ki a Be. 315. § (2) bekezdése az elektronikus adat fogalmát, egyben a lefoglalás lehetőségét az ún. fizetésre használt elektronikus adatra, amelynek lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét korlátozza. Lásd továbbá Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11., 639–641.; Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. *Belügyi Szemle,* 2017/1., 29.; Dornfeld i. m. (24. lj.) 126.

26 Trócsányi Sára: Első oldal. *Infokommunikáció és Jog,* 2009/3., 65.

elektronikus adat felett függeszti fel a rendelkezés jogát. A nyomozó hatóságok mégis csak nagyon ritkán alkalmazzák ezt a megoldást, részben mert a feltételezhetően az elkövetőhöz kötődő esetekben a hatóságok a teljes lefoglalásra törekszenek, és a bizonyítékok sérthetetlenségének, megváltoztathatatlanságának biztosítása érdekében szükséges a lefoglalás, részben pedig amikor a kényszerintézkedés elszenvedőjének feltehetőleg nincs közvetlen kapcsolata az elkövetővel (például sértett vagy harmadik személy), akkor az érintett szinte mindig együttműködő, ezért szintén végrehajtható a lefoglalás, kimentés,[27] ami biztosabb megoldás, mint a megőrzésre kötelezés.

Azonban mindezen kényszerintézkedések gyakorlati alkalmazhatósága és végrehajthatósága éppen az interneten elkövetett bűncselekményeknél meglehetősen korlátozott, hiszen egyfelől a hatóságok gyors és informatikai szempontból is szakszerű intézkedését, másrészt a nyomozás érdeméhez tartozó elektronikus adatok belföldi meglétét feltételezi. Ez utóbbi tűnik a problémásabbnak, hiszen a magyar büntetőeljárás elakad, ha nincs belföldön elérhető adat, ami megnehezíti a szükséges kényszerintézkedések foganatosítását, a nemzetközi bűnügyi együttműködés nehézkessége pedig jelentős mértékben elhúzza az eljárást. Ez viszont lényegében azzal jár, hogy a kényszerintézkedések elveszítik vagy elveszíthetik funkciójukat, hiszen minél több idő telik el, annál kevésbé biztosítható a releváns elektronikus adatok elérhetősége vagy sértetlensége – márpedig az internet globalizáltsága folytán a legtöbb esetben a nemzetközi kooperáció elkerülhetetlen.

2.3.3. Elektronikus adat ideiglenes hozzáférhetetlenné tétele

A tárgyi kényszerintézkedés lehetősége elsősorban a súlyos tartalom-bűncselekményeknél bír különös jelentőséggel, amit nevezhetünk az állami tartalomszűrés eszközének is.[28] A Be. LIII. fejezetében foglalt szabályozás, az elektronikus adat hozzáférhetetlenné tétele mint gyűjtőfogalom érdemben három intézkedést takar:

– az elektronikus adat ideiglenes eltávolítása;
– az elektronikus adathoz való hozzáférés ideiglenes megakadályozása;
– felhívás az elektronikus adat önkéntes eltávolítására.

A három intézkedési lehetőség alkalmazása egyfajta fokozatosságon alapul, ugyanakkor jelzi az érintett személyi kör iránti bizalmatlanságot, egyben a kényszerintézkedések gyakorlati megvalósítása, végrehajtása terén fennálló bizonytalanságot is.

A skála legalsó fokán helyezkedik el „a hagyományos büntetőeljárási dogmatikától meglehetősen idegen”,[29] önkéntes eltávolításra vonatkozó felhívás, amely a legszélesebb személyi körnek szólhat, mivel a tárhelyszolgáltató és a tárhelyszolgáltatást is végző közvetítő mellett a mé-

---

27 Sorbán i. m. (11. lj.) 219.

28 A kényszerintézkedés alapjait az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedések címet viselő 25. cikke teremtette meg, és az ennek való megfelelés érdekében került implementálásra a Btk. 63. § (1) bekezdés g) pontjába az elektronikus adat végleges hozzáférhetetlenné tétele mint intézkedés, valamint a Be. LIII. fejezetében foglalt ideiglenes hozzáférhetetlenné tétel mint kényszerintézkedés.

29 Sorbán i. m. (11. lj.) 240.

diatartalom-szolgáltató is kaphat ilyen felhívást. Ez tulajdonképpen hatósági figyelmeztetésként értékelhető, amelyben az ügyészség vagy akár a nyomozó hatóság felhívja a figyelmet egy általa jogsértőnek talált tartalomra, ugyanakkor ahhoz hatósági kényszer nem társul, tehát az érintettek szabad belátására és önkéntes teljesítésére bízza a kifogásolt tartalom sorsát. Ez azonban legfeljebb elvi szinten jelent döntési szabadságot az érintettek számára, hiszen a megfelelő intézkedések elmulasztása, ha büntetőeljárásbeli következményekkel nem is jár, de megalapozhatja a kötelezettek egyéb jogági felelősségét.[30]

A következő lépés az ideiglenes eltávolítás, amelynek révén az inkriminált tartalom lényegében elérhetetlenné válik az adott internetes helyen, ezért az eltávolításra kötelezettek köre a tárhelyszolgáltatóra és a tárhelyszolgáltatást is végző közvetítő szolgáltatóra terjed ki.[31] Ezzel szemben a hozzáférés megakadályozásakor az internetszolgáltató a teljes weblapot teszi elérhetetlenné a magyar felhasználók számára, ezért kötelezettje már „csak" az elektronikus hírközlési szolgáltató lehet. Ez az intézkedés sem jelenti azt, hogy maga a tartalom akár csak ideiglenesen lekerülne a világhálóról, pusztán a magyar internetezők a továbbiakban az adott internetes elérhetőségen nem férnek hozzá. Ez drasztikusabb intézkedés, így csak bizonyos, kizárólag közvádra üldözendő bűncselekmények esetében és csak akkor lehet helye, ha az ideiglenes eltávolításra való kötelezés – a kötelezett együttműködésének hiányában, a jogsegély iránti megkeresés elhúzódása vagy más aránytalan nehézség miatt – nem vezetett eredményre. Ez a szabályozási modell azt is jelzi, hogy a jogalkotó nem bízik a jellemzően külföldi tárhelyszolgáltatók együttműködésében, mint ahogy felismerte a jogsegélykérelmek által előidézett nehézkességet is. Ez alapvetően a hatékony bűnüldözésnek kedvező tendencia, amihez a Nemzeti Média- és Hírközlési Hatóság (NMHH) biztosította további hatósági kényszer is társul az intézkedés végrehajtása tekintetében.[32]

---

30 Uo. Ez a saját belátás szerinti „szabad" döntés annyiban valójában korlátozott – ahogyan Sorbán Kinga rámutatott –, hogy az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) a harmadik személy tartalmáért viselt felelősség alóli mentesülés egyik feltételeként azt jelöli meg, hogy a szolgáltatónak ne legyen tudomása a tartalom jogsértő jellegéről, ami ugyanakkor nehezen állna meg a felhívás kézhezvételét követően, de a szolgáltató nem érdekelt abban, hogy a saját felelőssége alóli mentesülését veszélyeztesse az intézkedések elmulasztásával és/vagy jelentős késedelmével.

31 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.) a közvetítő szolgáltatók következő fajtáit határozza meg: egyszerű adatátvitelt és hozzáférést biztosító szolgáltató, gyorsítótároló szolgáltató, tárhelyszolgáltató, keresőszolgáltató, valamint alkalmazásszolgáltató. Ezzel szemben az elektronikus hírközlési szolgáltatók fogalmára nincsen pontos definíció, az Eht. 188. § 16. pont c) alpontja alapján a szolgáltatás fő ismérve, hogy az „teljesen vagy nagyrészt jeleknek elektronikus hírközlési hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll". Ebből következik, hogy az egyszerű adatátvitelt és hozzáférést biztosító közvetítő szolgáltatók, tehát az internetszolgáltatók elektronikus hírközlési szolgáltatónak is minősülnek. A differenciálásnak abból a szempontból is jelentősége van, hogy a Be. szerint a nyomozó hatóság alapvetően szabadon, bármely szervtől, jogi személytől vagy szervezettől kérhet adatszolgáltatást, de elektronikus hírközlési szolgálatótól csak ügyészi engedéllyel [Be. 262. § (1) bekezdés], ugyanakkor az előkészítő eljárás során kizárólag elektronikus hírközlési szolgáltatótól igényelhet [Be. 342. § (3) bekezdés 4. pont].

32 Ezzel kapcsolatban az NMHH külön nyilvántartást is köteles vezetni, a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát, és noha annak adatai nem nyilvánosak, egy cikk szerint az adatbázisban 2016-ban nem szerepelt bejegyzés. Lásd Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. *Jogalappal,* 2017. június 4., https://bit.ly/3wrsuMx.

Ezzel együtt valójában nem jelent igazi megoldást: még a hozzáférés – akár ideiglenes, akár végleges – megakadályozásakor sem tűnik el a jogellenes tartalom az internetről. A kényszerintézkedés vagy akár az anyagi jogi intézkedés is csökkenteni tudja az adott tartalom országon belüli elérhetőségét, de nem szünteti meg a jogsértést, ami a gyakorlatban annyit tesz, hogy külföldről, VPN vagy speciális böngésző használatával ezek a tartalmak változatlanul elérhetők maradnak, és elegendő az inkriminált tartalmat egy másik URL-re mozgatni, hogy újra elérhetővé tegyék.[33]

Összességében e kényszerintézkedések szabályozása és gyakorlata a hatósági bizalmatlanságon és a valószínűsíthető nem teljesítésen, valamint a nemzetközi bűnügyi együttműködés várható elhúzódásán alapul. Ennek megfelelően a Be. tulajdonképpen csak félmegoldásokat tud nyújtani, ami azonban nem feltétlenül róható fel a jogalkotónak, mivel az egyes nemzeti szabályozások olyan helyzetekre keresnek megoldást, amelyek nemzeti szinten alig kezelhetők megfelelően, és csak sokkal szorosabb, rugalmasabb és gyorsabb nemzetközi együttműködéssel lehetne azokat hatékonyan kezelni.

Szót kell ejtenünk arról is, hogy a nyílt internet csak a jéghegy csúcsa: az ún. dark weben található tartalmakkal szemben egyetlen kényszerintézkedés sem vezet(het) eredményre a gyakorlatban. E kényszerintézkedések ugyanis feltételezik legalább az érintett szolgáltató(k) ismeretét, valamint azt, hogy legalább egy szolgáltatóval szemben mutatkozik reális esély a kikényszerítésére. Sokszor viszont a hatóságok előtt még az érintett szolgáltatók létezése sem ismert. Természetesen erre a problémára is létezik (fél)megoldás, amely jellemzően a dark web használatához köthető szolgáltatások teljes blokkolásán és tiltásán alapul, így például a Tor böngésző és a VPN-ek használatának tiltásával. Ez azonban több veszélyt is hordoz magában: egyfelől egyáltalán nem biztos, hogy e szolgáltatások igénybevétele illegális tevékenységhez kapcsolódik, hiszen elképzelhető, hogy az anonimitáshoz és/vagy a titkosításhoz kifejezetten legitim érdek fűződik,[34] vagyis e technológiák általános jellegű korlátozása alapjogot sérthet, másfelől egyes szerzők szerint az – egyébként szükséges és hasznos – technológiai fejlődést is visszavetheti.[35]

2.4. A nemzetközi bűnügyi együttműködés tapasztalatai, tendenciái

A fentiekből láthatjuk, hogy a kiberbűnözés, így különösen az interneten elkövetett bűncselekmények kapcsán – még akár a legegyszerűbbnek tűnő esetekben is – elkerülhetetlenné válik a

33 Sorbán i. m. (11. lj.) 189.; Dornfeld i. m. (24. lj.) 133.; Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. *Magyar Jog,* 2015/2., 106–115.

34 A Tor böngésző például arra is használható, hogy anonim módon olyan felhasználó is elérje a teljes nyílt internetet, akinek a hazája azt korlátozza. Lásd Michael Chertoff: A Public Policy Perspective of the Dark Web. 2 *Journal of Cyber Policy* (2017), https://doi.org/10.1080/23738871.2017.1298643, 28. Ezzel kapcsolatban az Egyesült Nemzetek Szervezete Emberi Jogi Tanácsa szerint az államnak a vélemény- és a közlési szabadság, valamint a magánélethez való jog védelmére vonatkozó kötelezettsége kiterjed a titkosítás lehetőségének biztosítására is. Lásd Encryption and Anonymity Follow-up Report. Research paper 1/2018. United Nations Human Rights Council, https://bit.ly/3WGWkqL.

35 Matthew Robert Shillito: Untangling the "Dark Web": An Emerging Technological Challenge for the Criminal Law. 28(2) *Information & Communications Technology Law* (2019), https://doi.org/10.1080/13600834.2019.1623449, 189.

nemzetközi bűnügyi együttműködés, és egyre nagyobb igény, sőt szükség mutatkozik a különböző nemzeti bűnüldöző hatóságok közötti gyors és zökkenőmentes, ezáltal hatékony kooperációra. Ezzel szemben a jelenlegi gyakorlat a nemzetközi és a magyar jogirodalom szerint is lényegében diszfunkcionális. Ennek egyik oka az, hogy a különböző joghatóságok alatt a kiberbűnözés szabályozása nem rendszerezett vagy egységes szemléletű – elképzelhető, hogy különféle, büntető és egyéb jogági nemzeti jogszabályokban van elrejtve a teljes normarendszer –, ami eljárási aspektusból fragmentált gyakorlathoz vezet. Sőt az anyagi jogi eltérések miatt az is kérdésessé válhat, hogy egy adott cselekmény valamennyi érintett nemzeti szabályozás szerint a büntetőjogi kategóriába tartozik,[36] azonban ehelyütt csak az eljárási nehézségekre kívánunk kitérni.

A zökkenőmentes nemzetközi bűnügyi együttműködés szükségességét a Budapesti Egyezmény megkötésével is elismerték a részes felek.[37] Az egyezmény 25. cikke szerint a jogsegélyek általános elvét kell képeznie, hogy sürgős esetben a felek a formalitások mellőzésével gyors kommunikációs csatornákon előterjeszthessék kérelmeiket és azokra választ is kapjanak. Ennek eredményeképpen jött létre az Európa Tanács által fenntartott COE 24/7 hálózat, amely az európai országok között a leggyakrabban használt ilyen kommunikációs fórum,[38] és jelenleg több mint ötven ország a részese. A nem európai államok jellemzően az Egyesült Államok igazságügyi minisztériuma által fenntartott G7 24/7 hálózatot használják, amelynek 71 ország a tagja, de az Interpol üzemelteti a legkiterjedtebb ilyen rendszert, az I–24/7 elnevezésű globális rendőri kommunikációs csatornát, amelyben több mint 190 állam vesz részt. Ezenfelül az EU tagállamai között a jogsegélykérelmek valóban hatékony végrehajtását több intézmény, így például általánosságban az európai nyomozási határozat és az Europol kiemelkedően sokrétű koordináló tevékenysége is elősegíteni hivatott. Ennek keretében alakult meg egyrészt a kifejezetten a tagállami bűnüldöző szakegységek vezetőit tömörítő európai kiberbűnüldöző akciócsoport (European Cybercrime Task Force), amely elsődlegesen stratégiai kérdésekben lát el tervezési, véleményezési, tanácsadási feladatokat, másrészt a számítástechnikai bűnözés elleni közös akciómunkacsoport (Joint Cybercrime Action Taskforce), amely nemcsak az uniós tagállamok, hanem további együttműködési megállapodást kötő államok tisztjeiből áll, és kifejezetten operatív feladatokat lát el.[39] E nagy, nemzetközi egyezményeken alapuló együttműködési struktúrákon túl továbbra is a két- vagy többoldalú megállapodások biztosíthatják a hatóságok valódi együttműködését. A különböző bűnüldöző hatóságok közötti gyors és hatékony kommunikáció fórumai tehát elviekben biztosítottak.

A magyar nyomozó hatósági gyakorlattal kapcsolatban egy 2018-as tanulmány szerint az állapítható meg, hogy az együttműködés az Egyesült Államok szövetségi rendvédelmi szerveivel, így a szövetségi nyomozóirodával (Federal Bureau of Investigation) és a belbiztonsági nyo-

36 Kirsty Phillips et al.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. 2 *Forensic Sciences* (2022), https://doi.org/10.3390/forensicsci2020028, 379–398.

37 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt, a Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

38 Szongoth Richárd – Vetter Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. *Belügyi Szemle,* 2018/7–8., https://doi.org/10.38146/BSZ.2018.7-8.1, 16.

39 Az Europol kiberbűnözéssel kapcsolatos tevékenységét lásd részletesebben uo., 7–14.

mozó irodával (Homeland Security Investigation), valamint a német szövetségi bűnügyi hivatallal (Bundeskriminalamt) intenzív.[40] Ennek keretében sor került már az első, az Egyesült Államokkal közös nyomozócsoport felállítására, amely a dark neten elérhető, kábítószereket és illegálisan megszerzett személyazonosító adatokat kínáló oldalt kiszolgáló szerverrel, valamint annak adminisztrátorával kapcsolatos adatok begyűjtésére és lefoglalására szerveződött. Azonban a pozitív példák ellenére a mindennapi joggyakorlat azt mutatja, hogy a nemzetközi bűnügyi együttműködés fogaskerekei mégsem forognak olajozottan, ami egyfelől a jogsegélykérelmek sokszor túlságosan lassú, mondhatni késedelmes teljesítésében mutatkozik meg,[41] másfelől a fenti együttműködésekben nem részes, a bi- vagy multilateriális megállapodásokban sem részt vevő államok esetében a jogsegélykérelmek teljesítése, így a felderítéshez szükséges információk beszerzése gyakorlatilag ellehetetlenül.

A fentieken túl a nemzetközi bűnügyi együttműködést nehezíti az is, hogy a hatóságok kénytelenek olyan helyzetekkel szembesülni, amelyek a kooperáció hagyományos elveit kezdik ki. Nagy Zoltán András ezzel kapcsolatban rámutatott, hogy például az egyre gyakoribb, ún. infrastruktúra-felhőszolgáltatások igénybevétele mellett megvalósított tartalom-bűncselekményeknél a következő problémák merülhetnek fel:

– bizonytalanná válhat a kettős inkrimináció feltételének teljesülése;

– nem meghatározható, hogy az inkriminált tartalmat tároló szerverek pontosan mely országokban találhatók;

– ezzel összefüggésben azt sem lehet meghatározni, hogy a jogsértő adat adott pillanatban éppen melyik szerveren, így melyik országban található meg.

A helyzetet tovább nehezítheti, ha profi az elkövető, így különböző anonimitást lehetővé szolgáltatások útján csatlakozik az internethez, és a felhőszolgáltatást is valótlan adatokat megadva veszi igénybe, ezzel biztosítva, hogy a kiléte és a földrajzi helyzete titokban maradjon, „majd feltölt egy tiltott tartalmat, amely valamely ország szerverére kerül, majd kikerül az internetre egy tükrözött weboldalra egy soha el nem érhető karibi ország domainnevén, [ezzel] a klasszikus bűnügyi jogsegély intézményei fiókban maradnak".[42]

2.5. Társszabályozás, avagy út a valódi együttműködés felé: fény az alagút végén?

A fentiekből kitűnik, hogy a jelenlegi büntető anyagi és eljárásjogi szabályozás és az azon alapuló jogalkalmazási gyakorlat nem képes lépést tartani a technológiai fejlődéssel, gyors és hatékony választ adni a felmerülő új helyzetekre. Ennek gyökerei a kizárólagos állami büntetőhatalom elvére és a büntetőjog *ultima ratio* jellegére is visszavezethetők. E két jellemző ugyanis – már

40 Szongoth–Vetter i. m. (38. lj.) 20.

41 Egy folyamatban lévő ügyben – európai nyomozási határozat ellenére – éppen a német hatóságoknak telt több mint fél évébe egy német honosságú gazdasági társaságnál elérhető, az elkövető kilétére utaló adatok továbbítása a magyar nyomozó hatóságnak, ahogyan egy internetes csaláshoz kapcsolódó pénzmosás miatt folyamatban lévő ügyben az angol hatóságnak is hat hónapig tartott annak megerősítése, hogy folyik náluk eljárás a csalási alapcselekmény miatt.

42 Nagy i. m. (9. lj.) 764.

csak a jogbiztonság és a követhetőség, kiszámíthatóság érdekében is – egyfajta merevséget, a szabályozás biztos voltát, változatlanságát és az eljárások formalizmusát követeli meg a büntetőjogtól. Ezek az elvárások azonban megnehezítik, hogy a büntetőjog a hagyományos elvei és eszközei segítségével, az azok által kijelölt gyakorlat mellett adekvát módon tudjon reagálni a folyamatosan és dinamikusan változó kibertérre.

Többek között ez a felismerés is vezetett arra, hogy az állam újraértékelje a digitális térben meglévő büntetőhatalmi monopolhelyzetét, és a büntetőjogi szemlélettől eddig távol álló olyan megoldásokat tegyen lehetővé, mint a társ- vagy az önszabályozás. Az előbbinél a jogalkotó az állami hatalom érvényesítését speciális együttműködés keretében részben átengedi a szabályozott jogalanyok egy kiválasztott csoportjának, vagyis gyakorlatilag feladatmegosztást valósít meg, az utóbbinál pedig még ennél is nagyobb teret kap a nem közhatalmi jogalany, mivel ebben az esetben a szabályozás és annak végrehajtása is tulajdonképpen a szolgáltató kezébe kerül. A kérdés az, hogy az önszabályozás valójában az állami jogalkotó részéről kívánt és elősegítendő, vagy olyan elkerülhetetlen jelenség, amellyel a normatív szabályozásnak meg kell tanulnia együtt élni.

A társszabályozás tehát az állami és az önszabályozási koncepciók között félúton helyezkedik el. Ennek Magyarországon a médiaigazgatás területén létezik egy egyedi formája, amelynek szabályait a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (Mttv.) VI. fejezete tartalmazza. A szabályozás célja az, hogy az NMHH Médiatanácsával kötött együttműködési megállapodás mint közigazgatási szerződés alapján az érintett – vagyis lényegében a szabályozott – jogalanyok az eljáró szakhatósággal éppen a szabályozás hatékony megvalósítása, az önkéntes jogkövetés előmozdítása, a médiaigazgatás közhatalmi jogérvényesítési rendszerének rugalmasabbá tétele érdekében együttműködjenek [190. § (1) bekezdés]. Nyilvánvaló, hogy ez a szemlélet és megközelítés idegen a büntetőjog logikájától, mégis úgy tűnik, hogy a jogalkotó és a bűnüldöző szervek is kénytelenek a digitális térben eltérni az alapvetően a hatósági kikényszeríthetőségen alapuló, jól megszokott megközelítéstől.

Ezen az új úton tett egyik első lépésnek tekinthető a bűnüldöző hatóságok és az elektronikus hírközlési feladatokat ellátó szervezetek közötti együttműködés alapvető kereteit – még jogszabályi szinten, tehát normatív erővel – szabályozó 180/2004. (V. 26.) Korm. rendelet.[43] A rendelet számos kötelezettséget telepít az elektronikus hírközlési szolgáltatókra a hatályos terminológia szerint a titkos információgyűjtés és a leplezett eszközök alkalmazásának elősegítése körében,[44] valamint lehetővé teszi, hogy a felhatalmazott szervezetek a részletszabályok meghatározása érdekében együttműködési megállapodást kezdeményezzenek a szolgáltatókkal.[45] Ez azonban távol áll a magánjogi szerződések részes feleinek[46] mellérendeltségén és a szerződési szabadság elvén alapuló felfogásától, hiszen az egyoldalú hatósági kezdeményezést követő hatvan napon belül a szolgáltató köteles az együttműködési megállapodást megkötni.

43 180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

44 Uo., többek között a 3. §, valamint a költségviselés kapcsán a 7. §.

45 Uo. 17. §.

46 2013. évi V. törvény a Polgári Törvénykönyvről 1.1., 6:58. és 6:59. §.

A rendelet ezt a kiegyenlítetlen helyzetet próbálja feloldani azzal, hogy ha a felek valamilyen kérdésben nem tudnak megállapodni, akkor az NMHH elnökénél kezdeményezhetik a (jelenlegi megnevezése szerint) egyeztetési eljárás lefolytatását. Ezt az egyeztetési eljárást az NMHH elnökének határozata zárja, amelynek nem teljesítését a rendelet ugyanúgy szankcionálja, mint egyébként a rendeletben előírt kötelezettségek megsértését, valamint a titokvédelmi szerződés vagy az együttműködési szerződés határidőn belüli megkötésének elmulasztását. A szabályozás tehát egyfajta többszörös hatósági kényszerrel terhelt lépés a szolgáltatókkal történő együttműködés irányába, és nem hoz létre kölcsönösségen alapuló, kooperatív partneri viszonyt. A valódi értelemben vett társszabályozás kialakítása a magyar büntetőjogban tehát még várat magára – a jövőben a cél a mostaninál lazább együttműködés lehet, amely végső soron biztosítja a hatósági elvárások kikényszeríthetőségét, azonban inkább partnerként tekint a szolgáltatókra, és érdekeltté teszi őket nemcsak az együttműködés létrehozásában, hanem annak fenntartásában, fejlesztésében is.

E lehetséges fejlődési irányba illeszkedik – bár nem a büntetőjog területén – és szolgálhat egyfajta példaként a Szabályozott Tevékenységek Felügyeleti Hatósága által a kiberbiztonság felügyeleti feladata körében ellátott tevékenységei kölcsönös előmozdítása érdekében több piaci szereplő részvételével újonnan megalakított Kiberkoalíció. A hatóság elnöke, Bíró Marcell megfogalmazása szerint

> a mostani összefogás legfőbb célja az, hogy a kiberteret érintő szabályozás ne a technikai fejlődés akadálya legyen, és hogy közösen ismerjük fel azokat a problémákat, amelyek szabályozással oldhatók csak meg. Azt várjuk ettől az együttműködéstől, hogy egy nyílt és élő szakmai fórum jön létre, ahol lehetőség van megvitatni a legfőbb kihívásokat és az azokra adott válaszokat.[47]

A másik irány, az önszabályozás, az államin kívüli, nem normatív jellegű szabályokat jelenti, amelyek büntetőjogi szempontból legalább annyi előnnyel és hatékony megoldással kecsegtetnek, mint amennyi veszéllyel. Tény, hogy az internetes szolgáltatást nyújtók mindegyike megalkotja saját belső normáit, amelyek betartását a saját eszközeivel megköveteli,[48] így erőteljes ráhatással lehetnek az internet, illetve az interneten alapuló szolgáltatások használatára. Ebből a szempontból kényelmes megoldásnak tűnhet a jogalkotó részéről, hogy a felelősséget elsődlegesen a szolgáltatókra telepítse, amelyek többnyire elérhetők, a hatóságok számára is kézzelfoghatók, vagyis szükség esetén biztosított a szankcionálhatóságuk.[49] Ezzel pedig a normatív szabályozás ösztönözni tudja a szolgáltatókat a szigorú követelmények, magatartási kódexek betartására és betartatására, ami az internet „tisztulásával" járhat.

Ez azonban kétélű fegyver, hiszen szolgáltatói szempontból az esetleges felelősségre vonás és következményeinek réme kétirányú cselekvést indukálhat. Az egyik, hogy a szolgáltatók biz-

---

47 Bíró Marcell: *Digitális biztonságunkat erősíti a Kiberkoalíció.* Szabályozott Tevékenységek Felügyeleti Hatósága, 2023. május 31., https://bit.ly/4bAGbHK.

48 Lásd ezzel kapcsolatban Sorbán i. m. (11. lj.) 98.

49 „[S]zemben az ismeretlen, beazonosíthatatlan felhasználókkal a szolgáltató könnyedén azonosítható és eljárás alá vonható." Dornfeld László: A közvetítő szolgáltatók felelőssége az internetes tartalmakért. *Kriminológiai Közlemények* 78. (2018) 114–115.

tosítani kívánják saját esetleges felelősségük elhárítását arra való hivatkozással, hogy miért felelnének a rajtuk kívülálló harmadik személy, a felhasználó által megvalósított magatartásáért.[50] Ezen a lényegében passzív szolgáltatói attitűdön azzal kíván változtatni a szinte globálisan egységes jogalkotói és jogalkalmazási gyakorlat, hogy egyre szigorúbb szolgáltatói felelősségi klauzulákat vezet be, és megállapítja a szolgáltatók – nem büntetőjogi – felelősségét a közvetlenül és elsődlegesen a felhasználók által kifejtett magatartásokért, például az internetes hírportálokon közzétett nyilvánvalóan jogsértő hozzászólások eltávolításának elmulasztása miatt[51] (ugyanakkor ez sem eredményez korlátlan, automatikus felelősséget).[52]

Kérdés, hogy ez a közvetett felelősség megállapíthatóságán – egyes szerzők szerint az ún. kapuőr kötelességeinek elmulasztásán[53] – alapuló tendencia mennyiben helyes, egyáltalán megengedhető-e a büntetőjog területén. A szolgáltatók részéről a közvetlen érintettségük-cselekvőségük hiányára alapított, az esetleges felelősségük távolítását célzó érvelés ugyanis csak nehezen vitatható az individuális büntetőjogi felelősség elvéből kiindulva, hacsak nem mutatható ki a szolgáltató valamelyik alkalmazottja részéről bűnös közreműködés az internet útján elkövetett bűncselekménnyel kapcsolatban. Önmagában azonban egy szolgáltató valamelyik dolgozójának bűnös közreműködése nem lehet elégséges ahhoz, hogy megalapozza maga a szolgáltató mint önálló entitás felelősségét, különösen nem a büntetőjogi intézkedések alkalmazhatóságát.

Friss adatok szerint a Google anyavállalata, az Alphabet – létszámcsökkentést követően – jelenleg több mint 170 ezer alkalmazottat foglalkoztat, így például nem felelne meg a büntetőjog alapelveinek, legalábbis a büntetőjogias felelősség és következményei alkalmazásának, ha egy ilyen óriási cég egyetlen alkalmazottjának bűnös magatartása önmagában megalapozná az egész vállalat felelősségét pusztán arra alapítva, hogy a bűncselekmény elkövetéséhez a társaság által a munkavállója számára biztosított, hozzáférhetővé tett infrastruktúrát használták fel. A természetes személyhez kötött bűnösség és annak legalább részleges transzformálása a valamilyen módon érintett jogi személyre, annak vezetőire jelenleg is kihívás elé állítja a büntetőjogi gondolkodást, amit jól mutat az is, hogy lényegében csak az elmúlt években kezdődött meg a jogi személlyel szemben alkalmazható büntetőjogi intézkedésekről szóló 2001. évi CIV törvény

---

50 Ezzel kapcsolatban Sorbán fogalmazott úgy, hogy „ha a szolgáltató tisztában van a felhasználó által küldött és fogadott adatcsomagok tartalmával, vagy vállalja, hogy a hálózat biztonságosabbá tétele esetében megismeri ezeket, akkor rá is telepíthető felelősség, amelynek a vállalása a szolgáltatók számára nem lenne sem célszerű, sem gazdaságos". Sorbán i. m. (11. lj.) 98.

51 Az Emberi Jogok Európai Bíróságának (EJEB) e körben legjelentősebb, a hivatkozott szemléletet meghonosító döntése: Delfi AS v. Estonia, no. 64569/09, 2015. Lásd Nádori Péter: Úton a tömeges internetes szólás jogi megítélésének új megközelítése felé – a strasbourgi Nagykamara ítélete a Delfi-ügyben. *In Medias Res,* 2019/2., 343–366.

52 A Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt. v. Hungary ügyben (no. 22947/13, 2016. február 2-ai ítélet) például arra az álláspontra helyezkedett az EJEB – nem sokkal a Delfi-ügyben hozott első döntés után –, hogy a tartalomszolgáltató megfelelően járt el, és nem tartozik felelősséggel a sértő hozzászólások közzétételéért, mivel amint tudomást szerzett azok jellegéről, gondoskodott a hozzászólások eltávolításáról.

53 A felelősségátvitel problémájával számos szerző foglalkozik. Például Giancarlo Frosio egyfajta kapuőrszerepet tulajdonít a közvetítő szolgáltatóknak, és az e szerepükhöz társuló kötelezettségeik vétkes megszegése esetén látja megállapíthatónak a felelősségüket. Giancarlo Frosio: Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility. 26(1) *Oxford International Journal of Law and Information Technology* (2018), https://doi.org/10.1093/ijlit/eax021, 1–33.

(Jszbt.) tényleges alkalmazása.[54] E törvény jelenlegi szabályozási koncepciója pedig aligha alkalmazható az internetes szolgáltatókra, mivel az ő érintettségük értelemszerűen teljesen más természetű, mint például egy ún. haszonhúzó gazdasági társaságé az ügyvezetője által elkövetett költségvetési csalás esetén.

A fentieken túl figyelembe kell venni a szolgáltatókra hárított felelősség másik oldalát is, vagyis hogy ha a szolgáltatókra túlzott felelősséget, szabályozási és fellépési kötelezettséget telepítünk, akkor az – szintén az esetleges felelősség elkerülése érdekében – túlszabályozáshoz és túlzott reakciókhoz vezethet. A szolgáltatók ugyanis az általánosan elfogadott, mainstream etikai álláspontnak megfelelően fogják megítélni a jogsértésgyanús eseteket és saját eljárásrendjük szerint fogják alkalmazni a szankciókat is. Emiatt félő, hogy saját eljárásuk során nemcsak az alapvető, a tisztességes eljáráshoz megkövetelt elvek fognak sérülni, hanem az végeredményben a szólás és a véleménynyilvánítás szabadságának indokolatlan korlátozásához is fog vezetni.[55]

Ez a jelenség a jogsértőnek vélt tartalmak esetében gyakorlatilag állami kontroll és jogállami garanciák nélküli – akár mesterséges intelligencia által vezérelt, automatikus – tartalomszűrést eredményezhet. Ezzel kapcsolatban Koltay András is kifejezte aggályait: véleménye szerint ezzel a szolgáltatók olyan „pszeudojogrendszert" hoznak létre, amelyben egyrészt a döntések „semmiféle jogállami garanciát nem hordozó eljárásban születnek", másrészt a platformok szabályozása az állami szabályozáshoz viszonyítva hol szigorúbb, hol megengedőbb lesz, vagyis lényegében kiszámíthatatlan szabályozási környezetet teremt.[56]

A fentebb felvetett kérdés tehát eldőlni látszik: a szabad, a normatív szabályozást és az állami beavatkozást teljes mértékben nélkülöző önszabályozás az állam számára inkább ijesztő, mintsem támogatandó jelenség. A szolgáltatók által az önszabályozás keretében hozott döntések és azok következményei ugyan természetükből adódóan nem képesek „igazi" büntetőítéletként érvényesülni, ugyanakkor büntetőjogias hátránnyal járhatnak. Egy szolgáltató nyilvánvalóan nem tud szabadságvesztést alkalmazni a vétkes felhasználóval szemben, azonban a felhasználó jogosultságát felfüggesztheti vagy megszüntetheti, amivel az adatokhoz való hozzáférését akár véglegesen is ellehetetlenítheti vagy az internetelérését meggátolhatja.

Nem nehéz belátni, hogy ezek az intézkedések súlyos hátránnyal járhatnak az elszenvedőjük számára, alkalmazásukra pedig jogállami garanciákat nélkülöző eljárás keretében, kiszámíthatatlan szabályozás alapján hozott döntés vezet. Ezek alapján úgy tűnik, Pandóra szelencéje

---

54 A jogi személlyel szemben alkalmazható büntetőjogi intézkedések kriminálstatisztikai adatainak elemzése kapcsán egy nemrég publikált tanulmány arra a következtetésre jutott, hogy „ha az indítványozott eljárások tendenciáit nézzük, akkor azt tapasztaljuk, hogy a jogszabály hatálybalépését követő időszakban az ügyész igen ritkán, évente legfeljebb tíz alkalommal indítványozott intézkedést. Ez az alacsony szám némileg emelkedik 2015-től, és 2019-ben, valamint 2020-ban a korábbinak a többszörösére nő, [ezzel együtt árnyalja a képet, hogy] a rendkívül alacsony esetszámhoz képest van csak növekedés, a 2019-es 93, illetve a 2020-as 73 vádiratban kezdeményezett intézkedés továbbra is igen mérsékelt aktivitásnak mondható." Klotz Péter: Hatásos, arányos és visszatartó? Avagy a jogi személlyel szemben alkalmazott büntetőjogi intézkedések Magyarországon. In Koltay András – Gellér Balázs (szerk.): *Jó kormányzás és büntetőjog. Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára.* Budapest, Ludovika, 2022, 359.

55 Frosio i. m. (53. lj.) 3.

56 Koltay András: Az újmédia kapuőreinek hatása a médiaszabályozásra. In Gellén Klára (szerk.): *Jog, innováció, versenyképesség.* Budapest, Wolters Kluwer, 2017, 99–124.

már kinyílt az önszabályozás terén, így a jogalkotás sem tehet mást, mint hogy megpróbálja kontrollálni a szolgáltatók esetleges szereptévesztését, az önszabályozás indokolatlan túlburjánzásait. Ehhez azonban nem feltétlenül szükséges újabb büntetőjogi eszközök bevezetése; a bűnüldöző szervek részéről a leghatékonyabb megoldásnak e területen is a szolgáltatókkal történő valódi együttműködés és kölcsönös párbeszéd kialakítása tűnik. Ennek ellenére megfontolandó lehet a kirívóan felelősségkerülő magatartást mutató szolgáltatók egyfajta szankcionálása a Jszbt.-ben foglalt büntetőjogi intézkedésekhez hasonló eszközökkel, ugyanakkor a felelősség megállapíthatóságára vonatkozóan más kritériumrendszer szerint, azaz a konkrét szolgáltatói szerepek és felelősségi körök felismerésén alapuló disztingvált szabályozás bevezetése mellett. Azonban továbbra is kérdés, hogy ez nem egy újabb lépést jelentene-e a „settenkedő" közigazgatási büntetőjog megerősítése felé.

3. Következtetések és javaslatok a gyakorlat alapján: mi lehet a megoldás?

A fentiek alapján azt a következtetést vonhatjuk le, hogy a jelenlegi büntetőjogi szabályozás és gyakorlat mellett az interneten, a kibertérben elkövetett bűncselekmények nyomozása jellemzően lassú és körülményes, így nem hatékony – éppen a digitális világban, ahol a gyors és eredményes fellépés lenne a legalapvetőbb nyomozási érdek.[57] A nyomozások számára kihívást jelentő több terület azonosítható, ezek közül a három legkritikusabbként a nyomozó hatóságok részben hiányos technológiai felkészültségét, a nemzetközi bűnügyi együttműködés akadozását, valamint a szolgáltatókkal való döcögős kommunikációt, vagyis a hatékony és a jogállami garanciáknak is megfelelő társszabályozási megoldások hiányát emeljük ki.

Az első problémás terület tűnik a legkönnyebben kezelhetőnek. Ez egyfelől magas színvonalú, a kibertér aktuális tendenciára, az új keletű devianciákra és technológiai lehetőségekre is kiterjedő továbbképzések kötelezővé tételével, valamint a megfelelő információtechnológiai eszközpark biztosításával kezelhető lenne. Ezek megvalósítása elsősorban a felhasználható költségvetési források kérdése. Ezenfelül szükséges lenne nemcsak a technológiai háttér biztosítása, hanem egyfajta szemléletváltás elérése is a kibertérben elkövetett bűncselekmények nyomozása terén, amely azon a felismerésen alapul, hogy semmi sem az, illetve nem feltétlenül az, aminek elsőre látszik.

Ezzel kapcsolatban Cameron Brown egy 2015-ben publikált átfogó tanulmányában mutatja be egy kitalált eset, Mary ügye kapcsán, hogy milyen problémákkal, kihívásokkal és kiszámíthatatlan fordulatokkal számolhat egy büntetőeljárás a nyomozástól kezdve egészen az ítélethozatalig. Mary először áldozatnak tűnik, mert több zaklató üzenetet és hívást is kapott, majd kiderül, hogy erotikus tartalmú külföldi honlapokon tették közzé a nevét és elérhetőségeit, sőt róla készült képeket is. Mary kezdetben nem akar feljelentést tenni, majd mivel a helyzet kezd egyre kritikusabbá válni, mégis eljárást kezdeményez, és átadja a nyomozó hatóságnak a telefon-

[57] Nagy Richárd figyelmeztetett arra, hogy „az interneten megjelenő adatok, képek, fájlok stb. a »kézzelfogható« bizonyítékoknál (kinyomtatott papíralapú szöveg, ujjnyom, egyéb biometrikus jelek stb.) sokkal egyszerűbben és gyorsabban változtathatók, átalakíthatók vagy akár hozzáférhetetlenné tehetők, ez pedig csökkenti a bizonyítékok összegyűjtésére nyitva álló időt, így a nyomozások hatékonysága kerülhet veszélybe". Nagy i. m. (15. lj.) 91.

ján, a számítógépén található inkriminált adatokat és kapcsolódó elektronikus levelezést is. A nyomozás során kiderül, hogy Mary nemrég eléggé viharos körülmények között szakított a barátjával, Paullal. Emiatt a gyanú Paulra terelődik, amit ráadásul a begyűjtött informatikai adatok is megerősíteni látszanak, hiszen azok alapján úgy tűnik, hogy Paul telefonját és számítógépét használhatták az elkövetéshez. Paul viszont tagad, és elmondja, hogy Mary segített neki az informatikai eszközei beállításában, ahogy arra is fény derül, hogy ő szakított Maryvel azt követően, hogy felismerte saját homoszexualitását, és éppen Mary volt az, aki ezt nem tudta megfelelően kezelni. Ezt követően a hatóságok kutatást tartanak Marynél az elektronikus bizonyítékok teljes körű begyűjtésére, azonban a kutatás-lefoglalás nem vezet érdemi eredményre, ugyanis Mary addigra már törölte a telefonján és a számítógépén tárolt adatokat. Az ügy tanulsága az, hogy a kibertérben, különösen az interneten elkövetett cselekmények esetében az első pillantásra egyértelműnek tűnő adatok, bizonyítékok is félrevezetők és/vagy valótlanok lehetnek. Ezért a nyomozás eredményessége és hatékonysága az elektronikus bizonyítékok lehető legteljesebb körének lehető leggyorsabb begyűjtése mellett biztosítható azzal, hogy az adatok biztonságát, sérthetetlenségét és megváltoztathatatlanságát is garantálni kell.

Ezzel szorosan összefügg a második és a harmadik felvetésünk is, hiszen a társhatóságokkal és a szolgáltatókkal történő együttműködés fejlesztésével, zökkenőmentessé tételével biztosítható az elektronikus bizonyítékok leghatékonyabb összegyűjtése. A nemzetközi bűnügyi együttműködés kapcsán utaltunk arra, hogy az interneten elkövetett bűncselekmények felderítésének sikerességét az internethez mint globális számítógépes hálózathoz hasonló, szintén globális és univerzálisan alkalmazható szabályozás, lényegében az összes állam részvételével megvalósuló együttműködés segítené elő. Erre azonban a gyakorlatban a nemzetállamok saját érdekei és megfontolásai miatt kevés esély mutatkozik, így az elérhető cél egy legalább regionális szinten egységes, gyors és hatékony együttműködés kialakítása lehet. Ez az EU területén elvileg a már most elérhető jogi eszközökkel is megvalósítható lenne, azonban a gyakorlat mást mutat, és ezt az uniós jogalkotás is felismerte.

A kibertér szülte kihívásokra válaszul az EU bevezetni tervezi a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendeletet. A rendelet célja az, hogy a tagállami bűnüldöző szervek azokat a szolgáltatókat is kötelezni tudják a közlésre és/vagy megőrzésre kötelező határozatuk útján, amelyek a saját területükön kívül tárolják ezeket az adatokat. A tervezet indokolása szerint az EU a tagállamok igazságügyi hatóságai közötti megkeresések gyors kommunikációját szolgáló biztonságos platform létrehozását is tervezi a gyakorlati megvalósítás érdekében. Az uniós jogalkotó eltökéltségét a probléma kezelésére a normatervezet választott formája is jól mutatja, hiszen a rendelet valamennyi tagállamra nézve közvetlenül és kötelezően alkalmazandó lenne. A tervezet tehát regionális szinten biztosítaná az elektronikus bizonyítékok begyűjtésére vonatkozó egységes szabályozást, ami nem csupán a hatóságok, hanem a szolgáltatók számára is segítség lehet a különböző nemzeti szabályok és kétoldalú egyezmények sokasága által fragmentált jelenlegi szabályozáshoz képest.

Ezen a ponton az uniós tagállamok közötti bűnügyi együttműködés kérdése összekapcsolódik az érintett szolgáltatókkal történő kooperációval, egyben a társ- és az önszabályozás lehetőségeivel, a szolgáltatók esetleges felelősségével. Ugyanis a szolgáltatókkal történő hatékony együttműködés hiányában bármennyire gyors is az egyes tagállami hatóságok közötti kommunikáció, a megkeresések tényleges teljesítése, így a nyomozás eredményessége sem biztosítható.

Emiatt valóban érdekeltté és motiválttá kell tenni a szolgáltatókat a büntetőeljárások sikerességének előmozdításában, a hatóságokkal folytatott érdemi – akár kölcsönös – kommunikációban. Ennek az egyik hatékony módja lehet az alapvetően a társszabályozáson alapuló koncepciók kialakítása, valamint a szolgáltatói önszabályozási kísérletek feletti szabályozott (állami) felügyelet bevezetése, megtartása.

Legtöbbször maguk a szolgáltatók is felismerik a belső szabályozás szükségességét, nyilván a saját tudomásuk és az arra alapított közvetett felelősségük alóli mentesülés érdekében. Ennek egyik jó példája a jogellenes online gyűlöletbeszéddel szembeni fellépést szolgáló kódex[58] elfogadása 2016-ban és az ahhoz kapcsolódó bejelentő rendszerek bevezetése, valamint a 2019-es európai parlamenti választások előtt megalkotott félretájékoztatásról szóló gyakorlati kódex,[59] amely a választásokhoz kapcsolódó álhírek és dezinformációk kiszűrését célozta.

A szolgáltatók szűrőszerepére azonban többféleképpen is reagálhat az állam – jelenleg az Amerikai Egyesült Államok és az Egyesült Királyság is inkább ezt támogatja.[60] A kontinentális jogi gondolkodástól, különösen a büntetőjog területétől viszont igazán távol áll az, hogy egy tartalom jogsértő voltát és annak következményeit egy államon kívüli, piaci szereplő a saját – jellemzően nem formalizált – eljárása alapján állapítsa meg, mesterséges intelligencia alkalmazása segítségével, akár emberi beavatkozást-mérlegelést és további jogorvoslati lehetőségeket sem biztosítva. Ebben a helyzetben a jogellenes és normasértő tartalmak elleni fellépés igénye konkurál az alapjogok érvényülésének megfelelő biztosításával.[61]

A fenti dilemma feloldására kínálhat lehetőséget az, ha a közhatalmi szereplő nem közvetlenül, a hagyományos jogi eszközök útján avatkozik be a szolgáltató által egyébként szabályozott kibertérbe, hanem a szolgáltatóval együttműködve határozza meg a szabályozás és a kapcsolódó eljárás alapvető kereteit, segíti annak organikus fejlődését, valamint biztosít egyfajta kontrollt felette. Ezt felismerve a Bizottság 2018 tavaszán ajánlást adott ki az illegális online tartalom hatékony kezelésére irányuló intézkedésekről,[62] és abban úgy foglalt állást, hogy az automatizált döntések esetében megfelelő biztosítékokat kell adni, különösen az emberi felülvizsgálat és a jogorvoslat lehetőségét azért, hogy a (tárhely)szolgáltatók elkerüljék a szándékolatlan és hibás döntéseket.[63]

Tehát a kiberbűnözéssel szembeni fellépés hatékonyságának növelése érdekében a büntetőjogi jogalkalmazás egyik elképzelhető fejlődési iránya az lehet, hogy a hatóságok a szolgáltatókkal szorosabb együttműködést alakítanak ki, és nemcsak a hatósági megkeresések teljesítése köré-

58 The EU Code of conduct on countering illegal hate speech online, https://bit.ly/3ykyN53.

59 Code of practice on disinformation, https://bit.ly/3ysZBQq.

60 Az internetszolgáltatóknak az Egyesült Államokban önszabályozás keretében is lehetőségük van tartalomszűrést és -blokkolást végezni, sőt a törvények támogatják is a szolgáltatói kezdeményezésre történő szűrést. Az Egyesült Királyságban pedig nemcsak megengedett az önszabályozás keretében végzett internetszűrés, hanem az internetszolgáltatók önkéntes alapon, még arra vonatkozó kötelezettség hiányában is végeznek hálózati szintű szűrést. Lásd Sorbán i. m. (11. lj.) 251. A brit médiahatóság, az Ofcom, 2022-es jelentése: https://bit.ly/3UzK6xG.

61 Ezzel kapcsolatban Sorbán állított össze egy illusztrációt, amely jól mutatja a két igény egymásra hatását egy „homokóraszer" megjelenítésben. Sorbán i. m. (11. lj.) 256., 12. ábra.

62 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről.

63 Uo. (27) preambulumbekezdés és 20. pont.

ben, hanem a kooperációt is kölcsönössé teszik, például azzal, hogy a szolgáltatók kötelesek lennének jelenteni a saját szabályzataik alapján kiszűrt, kirívóan jogellenesnek tűnő tartalmakat a bűnüldöző hatóságoknak (az azokhoz tartozó további informatikai adatok átadása/megőrzése mellett). Egy ilyen, kölcsönösségen alapuló együttműködés valószínűleg hatékonyan tudná csökkenteni az interneten elkövetett bűncselekmények látenciáját. A szolgáltatók részéről az ilyen együttműködési kötelezettségek szándékos megszegése vagy elmulasztása esetére pedig megfontolás tárgyát képezheti a Jszbt. rendszeréhez hasonló, „büntetőjogias" következményekkel járó szabályozás bevezetése. Azonban álláspontunk szerint nem feltétlenül ez a helyes megközelítés, hiszen dogmatikai szempontból az individuális büntetőjogi felelősség elvének részleges áttörésével járna, míg a gyakorlatot tekintve félő, hogy a szolgáltatókat a büntetőjogi eszközök, a szankcionálhatóságuk réme inkább elrettentené az együttműködéstől, és további bizalmatlanságot szülne a hatóságokkal szemben, vagyis végeredményben kontraproduktív volna.

Az önszabályozás másik kritikus kérdése a hozott döntések feletti kontroll, felülvizsgálat lehetősége. A megfelelő jogorvoslati lehetőségek és fórumok biztosítása általánosságban még várat magára, de első hírnökének tekinthető a Facebook által felállított Oversight Board (Ellenőrző Bizottság).[64] Ez a közösségimédia-szolgáltató által létrehozott, azonban tőle független szakértői testület,[65] amely a Facebook és az Instagram (összességében a Meta) döntései felett gyakorol felülvizsgálati jogkört, így az adott döntést fenntarthatja vagy megsemmisítheti, a határozatai pedig kötelező erejűek. Emellett a bizottság ajánlásokat fogadhat el a lehető legjobb (ön)szabályozási rendszer kialakítása érdekében, amelyek ugyan nem kötelezik a szolgáltatót, de az vállalta, hogy nyilvánosan reagál azokra.

Az Ellenőrző Bizottság a honlapján eddig harminchat eseti döntést, valamint három, a „szabályokkal kapcsolatos tájékoztatást-véleményt" tett közzé, valamint utal több mint száz már elfogadott állásfoglalásra is. Ez nem tűnik kevésnek, különösen, ha figyelembe vesszük, hogy a szervezet csak 2020-ban kezdte meg működését. Csakhogy mivel a Meta szolgáltatásainak jelenleg közel hárommilliárd felhasználója van, ez elenyészően kis merítést jelent a vélhetően vitás, de a felülvizsgálati eljárásba végül be nem vont döntésekből. Ráadásul a bizottság a honlapon feltüntetett harminchat eseti döntés közül huszonnégy esetben felülbírálta a Meta elsődleges döntését. Ez egyfelől mutathatja, hogy a bizottság valóban a szolgáltatótól függetlenül és hatékonyan végzi a munkáját, ami egyben remekül eladható marketing a felhasználók és az államok felé. Másfelől ha ezt a felülbírálati arányt az összes döntésre nézve reprezentatívnak vesszük, akkor a Meta az esetek kétharmadában először rossz, azaz megalapozatlan döntést hoz és alkalmaz annak alapján következményeket, jellemzően tartalomeltávolítást.

Egyelőre tehát nehéz eldönteni, hogy az Ellenőrző Bizottság valójában érdemi tevékenységet ellátó testület, amely hozzájárulhat a Meta-felhasználók kommunikációjának tisztulásához, így egy kezdetleges, de érdemi lépés a szolgáltatói önszabályozás kapcsán felmerülő kérdések megoldása felé, vagy ténylegesen egy kevés gyakorlati jelentőséggel bíró, „díszként" szolgáló

64 A testület tevékenységéről bővebben lásd ebben a lapszámban Lendvai Gergely tanulmányát *A Facebook Ellenőrző Bizottság működése és bíráskodása a gyűlöletbeszéd kontextusában* címmel (195–221. oldal).

65 Az Ellenőrző Bizottság az eredeti tervek szerint negyvenfős, nemzetközileg elismert emberi jogi aktivistákból, a jog és a média területén dolgozó szakemberekből álló testület lett volna, jelenleg 22 fős a tagsága, köztük egy magyar szakemberrel, Sajó Andrással.

szerv, amely valójában a szolgáltató ügyes PR-fogásának tekinthető. Az első körös döntések megalapozatlanságának aránya – még ha nem tekintjük is reprezentatívnak – rémisztő, és megalapozni látszik a legalábbis részbeni közhatalmi beavatkozás szükségességét az önszabályozás megfelelő kereteinek meghatározása, egy átlátható, a jogállami garanciáknak is megfelelő eljárásrend megteremtése érdekében, beleértve az érdemi jogorvoslat lehetőségét is.

A fentiek alapján látható, hogy az interneten elkövetett bűncselekmények nyomozása kizárólag a hatóságok értő, technológiai szempontból magas színvonalú és szinte azonnali közbelépésével lehet hatékony. Ez viszont az internet globális világában csak a különböző külföldi bűnüldöző szervekkel és a szolgáltatókkal kialakított gyors, zökkenőmentes és kölcsönös információáramlás mellett biztosítható. A tanulmány elején már hivatkoztunk Tóth Mihály professzor úr egyes gondolataira – a tanulmány zárásként is megfontolandónak tartjuk tőle a következőket a kiberbűncselekmények kapcsán: „törekedjünk inkább arra, hogy a visszaélések ellen pontos és világos jogi szabályaink legyenek, gyorsabban és rugalmasabban reagáljunk az új bűnözési formákra egy, a jelenleginél talán átfogóbb, komplexebb büntetőjogi szemlélettel."[66] Ennek az általa is ajánlott, átfogóbb büntetőjogi szemléletnek az alapját annak felismerése képezheti, hogy a digitális és egyre inkább globalizált világunkban a média gyakorlatilag a negyedik hatalmi ággá nőtte ki magát. E hatalmi ág legfontosabb csatornája az internet, ahol az internetes szolgáltatók tulajdonképpen hatalmi aktorokként lépnek fel, ezért a velük való érdemi együttműködés a büntetőeljárások hatékonysága érdekében elkerülhetetlen. Másképpen megfogalmazva: a nemzetközi bűnügyi együttműködésnek most már nem „csupán" a külföldi társhatóságokkal, hanem a jellemzően globális szolgáltató vállalatokkal történő kooperációra is ki kell(ene) terjednie. Egyetértünk azzal, hogy különösen a „közvetítő szolgáltatók szabályozásának túl kellene lépnie a szabályozó állam, szabályozott jogalany felépítésű hierarchikus kapcsolaton, és egy olyan partnerség kialakítására kellene törekedni, ami a fékek és ellensúlyok rendszerét valósítja meg államon kívüli szereplőkkel".[67]

Azonban álláspontunk szerint a büntetőeljárások hatékonyabbá tétele nem járhat az állami büntetőhatalmi monopólium – akár csak részbeni – átengedésével a szolgáltatóknak, vagyis az esetleges büntetőjogi felelősség megítélésére és szankciók kiszabására kizárólag közhatalmi szereplő kaphat felhatalmazást. Ugyanakkor a büntetőeljárás egyes részkérdéseit illetően elképzelhetőnek és üdvözlendőnek tartanánk a társszabályozási koncepció előretörését, különösen az elektronikus bizonyítékok biztosítását, és a hatóságok és a szolgáltatók közötti, kölcsönösségen alapuló – akár regionális vagy globális – jelzőrendszer kialakítását. Az interneten elkövetett bűncselekményekkel szembeni hatékony fellépés másik alappillére lehet a felhasználók tudatosságának növelése, amit a bűnüldöző hatóságok szintén a szolgáltatókkal közösen tudnának a leghatékonyabban megvalósítani, például a fentebb már említett Kiberkoalíció mint egyfajta szakmaközi egyeztető és társadalmi ismeretterjesztő fórum koncepcióját alapul véve.

66 Tóth i. m. (4. lj.) 188.

67 Sorbán i. m. (11. lj.) 275.

Irodalomjegyzék

Ambrus István: Miskolczi Barna – Szathmáry Zoltán: Büntetőjogi kérdések az információk korában (Recenzió). *Állam- és Jogtudomány,* 2022/3., 107–135. https://doi.org/10.51783/ajt.2022.3.05

Biró Marcell: *Digitális biztonságunkat erősíti a Kiberkoalíció.* Szabályozott Tevékenységek Felügyeleti Hatósága, 2023. május 31., https://bit.ly/4bAGbHK.

Chertoff, Michael: A Public Policy Perspective of the Dark Web. 2 *Journal of Cyber Policy* (2017) 26–38. https://doi.org/10.1080/23738871.2017.1298643

Clough, Jonathan: *Principles of Cybercrime.* Cambridge, Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781139540803

Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 2018/2., 115–135. https://doi.org/10.38146/BSZ.2018.2.8

Dornfeld László: A közvetítő szolgáltatók felelőssége az internetes tartalmakért. *Kriminológiai Közlemények* 78. (2018) 101–117.

Frosio, Giancarlo: Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility. 26(1) *Oxford International Journal of Law and Information Technology* (2018) 1–33. https://doi.org/10.1093/ijlit/eax021

Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. *Magyar Jog,* 2015/2., 106–115.

Grabosky, Peter N.: Virtual Criminality: Old Wine in New Bottles? 10(2) *Social and Legal Studies* (2001) 243–249. https://doi.org/10.1177/a017405

Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. *Jogalappal,* 2017. június 4., https://bit.ly/3wrsuMx.

Hunton, Paul: The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. 25 *Computer Law & Security Review* (2009) 528–535. https://doi.org/10.1016/j.clsr.2009.09.005

Klein Tamás: Az online diskurzusok egyes szabályozási kérdései. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018, 11–40.

Klotz Péter: Hatásos, arányos és visszatartó? Avagy a jogi személlyel szemben alkalmazott büntetőjogi intézkedések Magyarországon. In Koltay András – Gellér Balázs (szerk.): *Jó kormányzás és büntetőjog. Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára.* Budapest, Ludovika, 2022, 349–364.

Koltay András: Az újmédia kapuőreinek hatása a médiaszabályozásra. In Gellén Klára (szerk.): *Jog, innováció, versenyképesség.* Budapest, Wolters Kluwer, 2017, 99–124.

Kranenbarg, Marleen Weulen: *Cyber-Offenders Versus Traditional Offenders: An Empicial Comparison.* Doktori értekezés, Amsterdam, Vrije Universiteit, 2018, https://bit.ly/4bAEr1a.

Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. *Belügyi Szemle,* 2017/1., 22–44.

Lendvai Gergely: A Facebook Ellenőrző Bizottság működése és bíráskodása a gyűlöletbeszéd kontextusában. *In Medias Res,* 2024/1., 195–221. https://doi.org/10.59851/imr.13.1.11

Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, big data, profilozás.* Budapest, HVG-ORAC, 2018.

Nádori Péter: Úton a tömeges internetes szólás jogi megítélésének új megközelítése felé – a strasbourgi Nagykamara ítélete a Delfi-ügyben. *In Medias Res,* 2019/2., 343–366.

Nagy Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. *Belügyi Szemle,* 2018/7–8., 83–95. https://doi.org/10.38146/BSZ.2018.7-8.6

Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In Homoki-Nagy Mária et al. (szerk.): *Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára.* Szeged, SZTE ÁJK, 2018, 755–767.

Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In Virág György (szerk.): *Kriminológiai Tanulmányok* 44. Budapest, OKRI, 2007, 89–110.

Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. *Ügyészek Lapja*, 2010/2., 23–31.

Phillips, Kirsty et al.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. 2 *Forensic Sciences* (2022) 379–398. https://doi.org/10.3390/forensicsci2020028

Shillito, Matthew Robert: Untangling the "Dark Web": An Emerging Technological Challenge for the Criminal Law. 28(2) *Information & Communications Technology Law* (2019) 186–207. https://doi.org/10.1080/13600834.2019.1623449

Sorbán Kinga: *Az internetes közvetítő szolgáltatók szerepe és felelőssége az informatikai bűncselekmények nyomozásában.* Doktori értekezés, Budapest, ELTE, 2021.

Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11., 639–647.

Szongoth Richárd – Vetter Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. *Belügyi Szemle,* 2018/7–8., 7–21. https://doi.org/10.38146/BSZ.2018.7-8.1

Tóth Dávid – Gáspár Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle,* 2020/2., 140–150.

Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In Gál István (szerk.): *Informatika és büntetőjog.* Pécs, PTE ÁJK, 2006, 180–188.

Trócsányi Sára: Első oldal. *Infokommunikáció és Jog,* 2009/3., 65.

Vadász Viktor: A számítógép demisztifikálása. *Ügyészek Lapja,* 2010/2., 13–21.

Wang, Shiuh-Jeng: Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. 29(2) *Computer Standards & Interfaces* (2007) 216–223. https://doi.org/10.1016/j.csi.2006.03.008