RECENZIÓ

MISKOLCZI BARNA – SZATHMÁRY ZOLTÁN: BÜNTETŐJOGI KÉRDÉSEK AZ INFORMÁCIÓK KORÁBAN (BUDAPEST: HVG-ORAC 2018) 222.

https://doi.org/10.51783/ajt.2022.3.05

A 20. század derekán indult, majd a 21. században egyre látványosabban gyorsuló digitális fejlődés számos olyan eszköz, technológia és innováció elterjedését is lehetővé tette a mindennapokban, amire a közelmúltig szinte még gondolni sem lehetett. Így akár egy-két évtizeddel ezelőtt is nehezen lett volna elképzelhető, hogy az okostelefonok formájában egy komplett számítógép elfér majd a zsebünkben; hogy nyomtatott térkép helyett, GPS segítségével, a világ bármely ismeretlen táján nagy biztonsággal eligazodhatunk; félig-meddig önvezető járművekkel közlekedhetünk, avagy hogy algoritmusok ezrei fogják befolyásolni gondolkodásunkat. E folyamatot pedig legújabban jelentős mértékben katalizálta a 2020-ban indult és végpontjára sajnos még 2022-ben sem biztosan eljutott Covid–19-világjárvány.

A modern digitális eszközök természetesen új perspektívát jelentenek a bűnügyi tudományok számára is. Ami az empirikus területeket illeti, kriminológiai megközelítésben e technológiáknak jelentős kriminogén hatás is tulajdonítható, hiszen egyrészt számos, egyébként klasszikusnak mondható bűncselekmény (például csalás, zsarolás, az újabbak közül zaklatás, gyermekpornográfia, pénzmosás stb.) elkövetése mára lényegében áttevődött a kibertérbe, azaz a személyes érintkezést igénylő kivitelezés helyett sokkal inkább új eszközök felhasználásával, online valósítják meg azokat. Másrészt nem csekély számban jelentek meg olyan, nóvumnak tekinthető, a társadalomra ugyanakkor egyértelműen veszélyes cselekmények, amelyeket digitális eszközök hiányában egyáltalán nem lehetne elkövetni. Ilyen deliktum mindenekelőtt az információs rendszer vagy adat megsértése, az információs rendszer felhasználásával elkövetett csalás avagy – de lege ferenda – az új típusú szexuális bűncselekmények (így a a *revenge porn*, az *upskirting* vagy a *cyberflashing*).

A digitális technológiák a kriminalisztika/bűnüldözés területén is új fejezetet nyitottak, hiszen olyan bűncselekmények feltárását is lehetővé tehetik, amelyek korábban lényegében bizonyíthatatlanok voltak. Ilyen eszköz lehet például a pénzmosás-gyanús tranzakciókat monitorozó Big Data adatelemzés, a bűnelkövetők külső jegyein és a róluk rendelkezésre álló bűnügyi nyilvántartáson alapuló profilalkotás stb.

A tapasztalati bűnügyi tudományok mellett pedig természetesen a normatív területeket sem hagyják érintetlenül napjaink technikai innovációi. Így a büntető anyagi jogban olyan, alapvető fontosságú és lényegében száznegyven éve változatlan alapokon nyugvó tudományos definíciókat vált szükségessé újragondol-

ni, mint a bűncselekmény, a veszély, a büntethetőségi akadályok, a stádiumok, illetve az elkövetők kategóriái. A büntetőeljárási jog pedig az új típusú bizonyítási eszközök mikénti felhasználásának dilemmája mellett olyan alapelvek relativizálódásával szembesült – például a távmeghallgatások általánossá válása miatt – mint a közvetlenség elve.

Az utóbbi néhány év hazai büntetőjogi szakirodalma igen fogékony volt a digitalizáció által generált elméleti és gyakorlati kérdésekre, és nem elképzelhetetlen, hogy az ilyen irányú kutatások valódi expanziója még csak a közeljövőben fog megindulni. Az „első fecske"[1] – ami a kapcsolódó kérdések monografikus igényű feldolgozását illeti – Miskolczi Barna és Szathmáry Zoltán *Büntetőjogi kérdések az információk korában – Mesterséges intelligencia, Big Data, profilozás* című kötete volt, amely 2018-ban jelent meg a HVG-Orac Kiadó gondozásában. A legfőbb ügyészségi ügyészként dolgozó szerzők nemcsak jelentős joggyakorlati tapasztalattal rendelkeznek, hanem az utóbbi évtizedben, a tágabb értelemben vett büntetőjog újrakodifikálása során is úttörő szerepet játszottak, így a legújabb digitális technológiákkal kapcsolatos elképzeléseik különösen izgalmasak lehetnek az elméleti és a gyakorlatban dolgozó jogászok számára.

A kötet tartalomjegyzékét átlapozva megállapítható, hogy a szerzők, noha a digitalizáció büntetőjogi vonatkozásainak több lényeges kérdéskörét említik, művük elkészítésekor teljességre nem törekedtek. Így például nem került sor valamennyi, új típusú technológiai eszközöket igénylő bűncselekmény bemutatására. Az ugyanakkor megállapítható, hogy amely részterületekre hangsúlyt fektettek, azokat igen mélyreható, a dogmatikai finomhangolásokat is elvégző formában mutatták be.

A szerzőpáros művét öt fő részre osztotta. Az első a „Technológia és társadalom" címet viseli, amelynek keretében meghatározták azokat a fogalmakat és kijelölték azokat a kereteket, amelyek a munka további részeinek irányát megszabják. Rövid történeti áttekintést követően utalnak arra a három fő területre – a gazdasági, a köz-, illetve a magánszférára – amelyeket a technológiai fejlődés befolyásolhat, minden esetben kitérve azon kérdésekre, amelyek büntetőjogi értelemben jelentősek lehetnek (17–36. o.).

A második rész a kötet központi témakörét, a mesterséges intelligencia jogi megítélésének problémáit mutatja be. A vonatkozó szakirodalmi és európai uniós állásfoglalások tükrében a szerzők a mesterséges intelligencia definiálási lehetőségeit járják körbe, amelyben kapcsán azon, negatív megközelítésű álláspontra helyezkednek, amely szerint mindaddig, amíg a mesterséges intelligenciának nem adható meg a pontos, materiális fogalma, addig lényegében meg kell elégendnünk a normatív meghatározással, nevezetesen: mesterséges intelligencia az, amelyet a törvény ekként ismer el. Megítélésem szerint a kötet legizgalmasabb fejtegetéseit jelenítik meg a mesterséges intelligenciához kapcsolódó ontológiai, büntetőjog-dogmatikai és szankciótani kérdések, amely körben a szerzők egy ún. „tovább-redukált" cselekmény-fogalom

[1] Később lásd Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban* (Budapest: L'Harmattan – TK JTI 2020); Ambrus István: *Digitalizáció és büntetőjog* (Budapest: Wolters Kluwer 2021).

kidolgozására tesznek javaslatot annak érdekében, hogy a mesterséges intelligencia által generált károkozás is cselekménynek legyen tekinthető a büntetőjogban. Ugyancsak képviselhető álláspontra helyezkednek a szerzők akkor, amikor a mesterséges intelligencia szankcionálását a jogi személyekkel szembeni büntetőjogi intézkedésekkel analóg módon javasolják lehetővé tenni (39–104. o.).

A rövidebb, a kibertér büntetőjogi kérdéseit bemutató harmadik rész egy alapvetően eljárásjogi problémára, az elkövetés helyének meghatározásán keresztül az illetékesség megállapíthatóságára fókuszál, megállapítva, 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 (107–121. o.).

A negyedik rész olyan büntető anyagi jogi problémákat tárgyal, mint a büntetőjogi felelősségre vonás fontosabb akadályai (jogos védelem, végszükség, a jogszabály engedélye), illetve itt térnek ki a szerzők az ún. „*hacking back*" – mint sajátos, kibertérben megvalósuló eltárító magatartás – problémájára is. A szerzőpáros e helyütt foglalkozik a személyes adattal visszaélés bűncselekményéhez rendelten a profilozás és a *deep fake* technológia mikénti megítélésével. Ugyancsak érdekes kérdések merülnek fel az elektronikus pénz és az ún. kriptovaluták kapcsán. E rész végén olvasható rövid elemzés a *cyberbullying*-ról (internetes zaklatás), amely témakör, kiemelt jelentősége okán, talán hosszabb terjedelmű bemutatást is megérdemelt volna (125–165. o.).

Az utolsó, ötödik rész az új technológiák által generált eljárásjogi problémákat tekinti át, kihívások és lehetőségek felvetése formájában. Előbbi körbe a titkosítás, a hatósági hacking, illetve a joghatósági problémák detekálása tartozik. Utóbbi pedig az automatizált adatelemzésben, illetve a mesterséges intelligenciában rejlő potenciálnak a büntetőeljárás gördülékenyebb és hatékonyabb lefolytatásának szolgálatába állítási lehetőségeit vizsgálja (175–203. o.). A kötet rövid, a kutatás eredményeit informatív formában összefoglaló zárszóval zárul.

E rövid áttekintést követően kiemelek néhány olyan, a szerzőpáros által felvetett problémakört, amelyeket magam továbbgondolásra érdemesnek vagy adott esetben vitathatónak tartok, annak reményében, hogy e diskurzus ugyancsak közelebb hozhat minket az új technológiák által kiváltott, nemritkán gyökeresen új típusú büntetőjogi problémák minél helyesebb megoldásához.

A szerzők a mesterséges intelligencia működésével összefüggésben felmerülő büntetőjogi felelősség kapcsán – Gabriel Hallavy nyomán – három modellt különböztetnek meg (58–61. o.), nevezetesen:

– a közvetett tettességen alapuló modellt (*Perpetration-via-Another Liability Model*),

– egy gondossági kötelezettség megszegésén alapuló felelősségi rendszert (*Natural-Probable-Consequence Liability Model*), végül

– a mesterséges intelligencia közvetlen felelősségre vonhatóságára építő rendszert (*Direct Liability Model*).

Az angolszász szakirodalomra történő kitekintést – nem elszakadva a kontinentális büntetőjogi berendezkedés hagyományaitól – magam is helyesnek tartom. Megjegyzem ugyanakkor, hogy a sorrendiséget helyesebb lenne a mes-

terséges intelligencia közvetlen felelősségének problémájával kezdeni, és innen haladni az egyre mögöttesebb felelősségi formák irányába. Emellett érdemes kiemelni azt is, hogy a legújabb jogirodalomban az említett három mellett egy további, negyedik modellel is találkozhatunk: az elöljárói jellegű büntetőjogi felelősséggel *(Command Responsibility)*.[2] Az e kategóriára történő utalás annál is inkább indokolt, mivel a magyar büntetőjog jelenleg is ismer olyan sajátos, mögöttes felelősségi formát, amely esetében a katonai elöljáró, noha tényállásszerű magatartást önmaga egyáltalán nem fejt ki, tettesként – sőt adott esetben, a közvetlenül cselekvő katona jogi tévedésének hiányában nem csupán közvetett tettesként, hanem általános (önálló) tettesként! – tartozik büntetőjogi felelősséggel.[3]

Figyelemre méltó – bár a legalitás kereteit talán feszegető – az a már kiemelt szerzői álláspont, amely szerint a büntetőjogi felelősséget egy ún. „továbbredukált" cselekményfogalomra lehetne a mesterséges intelligencia esetében építeni, amely nem vagy csak potenciális formában követelne meg emberi magatartást, valamint az akaratlagosság feltételét mint az emberi szubjektumot jellemző kritériumot is kiiktatná, így a cselekményt kizárólag hatóképes magatartásként írná körül. A tényállásszerűség síkján megfogalmazott javaslat szerint pedig abból ki kellene rekeszteni az „emberi tényezőt, amelyet gondolatban, feltételesen az autonóm döntéshozó rendszerrel helyettesítünk" (78. o.). Vitatható ugyanakkor az a megállapítás, amely szerint a mesterséges intelligencia vonatkozásában csak a bűnösségre való képesség kizárt, a cselekmény tényállásszerűsége nem (79. o.). A tényállásszerűség alanyi oldala ugyanis – amely központi elemként magában foglalja a szándékosság/gondatlanság kettősét – maga is szubjektív elemekkel átszőtt kategória, így legfeljebb ettől való megfosztása esetén lehetne a mesterséges intelligencia „cselekménye" kapcsán annak tényállásszerűségéről szólni. Azt a szerzői megállapítást ugyanakkor osztom, amely szerint a mesterséges intelligencia „autonóm döntésével kapcsolatos büntetőjogi felelősségi rendszert a jogi személy büntetőjogi felelősségének analógiájára lehet kialakítani" (88–89. o.). Mindez legfeljebb azzal pontosítható, hogy nem a jogi személy – és jelen esetben nem is a mesterséges intelligencia – büntetőjogi felelősségéről, hanem valójában a felelősség fikciójáról, illetve annak folyományaként a büntetőjogi intézkedések alkalmazhatóságáról lehet beszélni.

Sok vitára okot adó probémát jelent a hagyományos büntethetőségi akadályok alkalmazhatósága a mesterséges intelligencia használata kapcsán. A jogos védelem körében a szerzőpáros annak a véleményének ad hangot, hogy „a támadó fellépés állattól, vagy beszámítási képességgel nem rendelkező személytől is jöhet" (126. o.). Ez a megfogalmazás még annak tükrében is félreérthető, hogy a következő mondat alapján mindezt vélhetően úgy értették, hogy az állat támadása csak akkor alapozhat meg jogos védelmi helyzetet, ha az eszközként szerepelt az ember kezében (mert pl. ráuszította a sértettre). Szükséges ezért külön

[2] Thomas C. King et al.: „Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" *Science and Engineering Ethics* 2019/1. 109–101., *https://doi.org/10.1007/s11948-018-00081-0*.

[3] Lásd a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 130. § (2) bekezdését.

kiemelni, hogy ilyen eszközkénti felhasználás hiányában az állati támadás – *de lege lata*, jogtalanság hiányában – jogos védelmi helyzetet nem hozhat létre.[4]

Némi hiányérzetet kelthet a büntethetőségi akadályok körében, hogy a szerzőpáros lényegében kizárólag a jogellenességet kizáró okok kérdéseivel foglalkozik. A bűnösséget kizáró okokról (és a másodlagos akadályokról) ugyanakkor nem szólnak, jóllehet például a tévedés témaköre kapcsán számos problémát generálhat majd a mesterséges intelligencia, mint például abban az esetben, ha az önvezető jármű hibás számítására alapított döntése okán bekövetkezett baleset kapcsán, e jogcímre alapítottan kéri a felmentését a közlekedési bűncselekmény miatt folyamatban lévő ügy terheltje.[5]

Utolsó kiemelt kérdéskörként a kriptovalutákra utalva egyetértek a szerzőkkel abban, hogy „[a] kriptovaluták jelenleg egyetlen ismert polgári jog skatulyába sem illeszthetők be maradéktalanul, tulajdonképpen csak azt tudjuk megmondani, hogy minek nem minősülnek" (157. o.). Jóllehet ezen virtuális fizetőeszközök valóban nem tekinthetők *de lege lata* sem dolognak, sem pénznek, sem készpénz-helyettesítő fizetési eszköznek, arra mégis érdemes felhívni a figyelmet, hogy bizonyos bűncselekmények kapcsán a károkozás szempontjából – értékük alapján – tekintetbe jöhetnek. Így egy 2021-ben történt hazai esetben az elkövető néhány óra alatt a saját tárcájában lévő kriptovaluta mennyiséget képes volt korlátozás nélkül megtöbbszöröznie. Ilyen módon az eredetileg rendelkezésére álló százezer kriptovaluta tokenből rövid időn belül mintegy 80 millió tokent hozott létre, amelyeket ezt követően elkezdett valódi pénzre váltani egy külföldi kriptovaluta tőzsdén.[6] Ugyancsak sor került már legújabban kriptovaluta-hamisításra is: csalásként minősült az a 2022-es eset, ahol az elkövető harmincmillió forintért cserébe digitális tárcájából látszólag átutalta a sértettnek a megállapodásban szereplő kriptovalutát. A sértett csak utólag észlelte, hogy a digitális tárcájában megjelent elektronikus fizetőeszköz valójában értéktelen, bár annak szimbóluma a megtévesztésig megegyezett egy ismert kriptovalutáéval.[7] Ezzel együtt is egyet kell érteni azon állásponttal, amely a kriptovaluták mielőbbi *sui generis* szabályozását sürgeti.

Miskolczi Barna és Szathmáry Zoltán a büntetőjognak az információk korában végbemenő változásairól szóló köte-

[4] Noha valóban megfontolásra érdemes Tokaji Géza azon álláspontja, amely szerint a megtámadotti jogokat csorbítja, ha egy állat támadásával szemben kevésbé lehet védekezni, mint az emberivel. Vö. Tokaji Géza: *A bűncselekménytan alapjai a magyar büntetőjogban* (Budapest: KJK 1984) 252. Más kérdés, hogy miután az ilyen esetben felmerülő állatkínzás bűncselekménye (Btk. 244. §) csak az állat indokolatlan bántalmazása esetén tényállásszerű, a támadó állattal szemben kifejtett védekezés, indokoltsága okán, nem meríti ki a tényállást, így a jogellenességet itt már nem szükséges vizsgálni.

[5] Vö. Clint W. Westbrook: „The Google Made Me Do It: The Complexity of Criminal Liability in The Age of Autonomous Vehicles" *Michigan State Law Review* 2017/1. 97–147.

[6] Lásd: *https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/80-millio-token-csalas-rendorkezen-a-27-eves-ferfi.*

[7] Kolontár Krisztián: Már a kriptovalutát is hamisítják, 30 milliót húztak le egy fővárosi vállalkozótól, *24.hu,* 2022. április 29., *https://24.hu/belfold/2022/04/29/mar-a-kriptovalutat-is-hamisitjak-30-milliot-huztak-le-egy-vallalkozotol.*

tét 2018-ban publikálta. Jelen recenzió lezárására 2022 tavaszán került sor. Ha egy ennyire új innováció jogi kérdéseiről állást foglaló kötet csaknem fél évtized alatt sem vált elavulttá, akkor megítélésem szerint már elmondható, hogy időtállónak tekinthető. Ha pedig a technológia további fejlődése a jövőben zárójelbe is tenné a műben szereplő egyes gondolatokat, akkor is megállapítható, hogy a Miskolczi–Szathmáry szerzőpáros kötete a későbbiekben is a 21. századi digitalizációval összefüggő büntetőjogi gondolkodás egyik alapmunkája lesz.

Ambrus István[*]

[*] PhD, dr. habil., tudományos munkatárs, TK JTI, 1097 Budapest, Tóth Kálmán utca 4.; tanszékvezető egyetemi docens, ELTE ÁJK, 1053 Budapest, Egyetem tér 1–3. E-mail: *ambrus.istvan@tk.hu*. A tanulmány a 138965. számú NKFIH pályázat és a Mesterséges Intelligencia Nemzeti Laboratórium keretében készült, az Innovációs és Technológiai Minisztérium, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatásával.