

AMBRUS ISTVÁN: DIGITALIZÁCIÓ ÉS BÜNTETŐJOG
(BUDAPEST: WOLTERS KLUWER 2021) 328.

<https://doi.org/10.51783/ajt.2022.1.07>

Ambrus István *Digitalizáció és büntetőjog* című, a Wolters Kluwer gondozásában megjelent monográfiája nemcsak egy kötet a sok közül, hanem fontos mérföldkő a tudományos munkásságában, ugyanis ez a munka az ELTE Állam- és Jogtudományi Karán benyújtott és 2021-ben megvédett habilitációs érkezése is. Ezenkívül egy hároméves OTKA poszt-doktori kutatás eredményeit foglalja össze.

A könyvet örömmel vettem a kezembe, mert a szerző olyan témát dolgoz fel, ami a saját szakmai érdeklődésemhez és kutatási területemhez is közel áll, jómagam is a modern technológiák jogi kihívásait kutatom. A recenzió megírásakor nem a teljesség igényével érintem a könyv valamennyi részét, hanem azokat a témaköröket és újításokat emelem ki, amelyek véleményem szerint a kötet legérdekesebb részét képezik.

Az Ambrus által választott téma időszerűsége elvitathatatlan, hiszen a digitalizáció folyamatos kihívások elé állítja a jogrendszert, ezért szükség van az olyan művekre, amelyek a változó technológiai fejlődés következtében a joganyagokat monitorozzák, valamint az egyes jogágak fogalmainak újragondolására ösztönözzenek. Monográfiájában arra vállalkozott, hogy ehhez panorámaszerű áttekintést nyújtson a digitalizáció és a büntetőjog kapcsolatára tekintettel. A büntetőkódexünk egyes részeinek elemzésén és nemzetközi kitekintésen keresztül olyan új tárgyköröket is érint,

amelyek nemcsak a jogtudomány, hanem a közbeszéd számára is érdekesek lehetnek. A monográfia négy fő fejezetre és két exkurzusra tagolható, valamint azt a büntetőjogi felosztást követi, hogy külön vizsgálja az általános részi, valamint a különös részi kérdéseket. Az általános részi témakörök között új bűncselekménytani (bűncselekmény fogalmának újragondolása, előkészületi magatartások és az alkalmatlan kísérlet a digitalizáció tükrében, kvázi nyitott törvényi állás tana) és büntetéstani kérdésekkel (automatizált büntetés kiszabás, elektronikus adat végleges hozzáférhetlenné tétele) találkozhatunk. E fejezetben figyelemreméltó az elkövetési tárgy új tudományos fogalmának kialakítása. Ambrus nézete szerint az elkövetési tárgy új fogalma a törvényi tényállásban meghatározott személy, dolog vagy más speciális tárgy, akire vagy amelyre az elkövetési magatartás hatása irányul. Az elkövetési tárgy definíciójába a „vagy más speciális tárgy” kitételt is beépíteni, mert a Btk. rendszerében léteznek olyan élettelen – tehát személynek természetesen nem tekinthető – tárgyak, amelyek elkülönült legáldefiníciójuk miatt nem vonhatóak a dolog fogalma alá sem. (36–37. o.) Például az információs rendszer vagy adat megsértése deliktum esetén a számítógépes adat, míg a személyes adattal visszaélés elkövetésekor a bűncselekmény elkövetési tárgya maga a személyes adat, míg az adat által azonosított vagy azonosítható természete-

tes személy a bűncselekmény sértettjének tekinthető. Például ezzel ellentétes álláspontot képvisel a szakirodalomban Szomora Zsolt, aki szerint a személyes adat eszmei jellegére tekintettel elkövetési tárgynak nem tekinthető.¹

A büntetőjog különös részét jelentősen érinti is a digitalizáció, ezért Ambrus számos bűncselekményt mutat be, művében azonban nem vállalkozik ennek a teljes körű feldolgozására. A dogmatikai csoportosítást a fontosabb tényállások körül járása követi a releváns nemzetközi és európai uniós jogszabályokat áttekintve.

A szerző tágabb kategóriát felölelő, a „digitális bűncselekmények” elnevezést választotta. Ezt a választást azzal indokolja, hogy például olyan XXI. századi közlekedési eszközöket (elektromos roller), valamint bármilyen hálózathoz való csatlakozás nélkül is rendeltetésszerűen használható digitális eszközöket is érint, amelyekre figyelemmel még mindig némileg szűkítő jellegű, így a digitális bűncselekmény kitéltelt tekinti leginkább pontosnak. Ambrussal egyetértve ebben a körben olyan mérvű dogmatikai feszességet nem várhatunk el, mint amilyen a büntető anyagi jog korábbi jogintézményeire alapvetően jellemző. Utal arra is, hogy szóhasználat és a csoportosítás tekintetében a vonatkozó szakirodalom sem egységes, így olvashatunk – egyebek mellett – például kiber-, internetes, számítógépes, informatikai bűncselekményekről is.² (82. o.) Jómagam

a nemzetközi szakirodalomban uralkodó kiberbűnözés kifejezést használok írásaimban, azonban ezekben az online térhez köthető különböző visszaélésekre fókuszálok, így helyénvalónak tartom Ambrus által választott digitális bűncselekmény tágabb kategóriájának alkalmazását az általa felvázolt offline esetekre és eszközökre tekintettel.

A digitális bűncselekmény kategóriáját további két típusra bontja: szoros értelmű vagy tágabb értelmű digitális bűncselekményre. A szoros értelmű digitális bűncselekményt kizárólag a virtuális térben vagy elektronikus formában, illetve eszmeileg létező tárgyak és eszközök kapcsán lehet elkövetni, enélkül megvalósulása fogalmilag sem merülhet fel (például az információs rendszer vagy adat megsértése). A szűkebb értelemben vett digitális bűncselekmények jellemzően a különböző kibertámadásokhoz köthetők (például hackertámadás, számítógépes vírusok stb.), erre példaként szolgálnak a hazai büntetőjogi szabályozásban az információs rendszer elleni bűncselekmények, amelyekkel a szerző maga is részletesen foglalkozik.

A tágabb értelmű digitális deliktum ugyanakkor valójában „offline” is elkövethető (de nem feltétlenül „hagyományos”) bűncselekményeket foglalhat magában, amelyeket könnyebben,

From Cyberspace (Santa Barbara: Praeger, Santa Barbara 2010) 39–47.; Yvonne JEWKES – Majid YAR (szerk.): *Handbook of Internet Crime* (London: Willan Publishing 2010) <https://doi.org/10.4324/9781843929338>; Susan W. BRENNER: „Is there such a thing as »virtual crime«?” *California Criminal Law Review* 2001/1.; NAGY Zoltán András: *Bűncselekmények számítógépes környezetben* (Budapest: Ad Librum 2009); SZABÓ Imre: „Informatikai bűncselekmények” in DÓSA Imre (szerk.): *Az informatikai jog nagy kézikönyve* (Budapest: Complex 2008) 547.

¹ SZOMORA Zsolt: „Btk. XXI. fejezet – Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények” in KARSAI Krisztina (szerk.): *Kommentár a Büntető törvénykönyvhöz* (Budapest: Complex Kiadó 2013) 459.

² Lásd Peter GRABOSKY: *Cybercrime* (London: Oxford University Press 2016) 8–9.; Susan W. BRENNER: *Cybercrime – Criminal Threats*

gyorsabban és nagyobb volumenben valósítanak meg az online térben (például zaklatás, pénzmosás stb.). (82. o.) A nemzetközi szakirodalomban hasonló felosztást találhatunk a szoros vagy tágabb értelemben vett kiberbűnözés kapcsán is.³

A már említett információs rendszer elleni bűncselekmények keretében olyan aktuális kérdéseket érint, mint például az etikus hacking. Helyesen állapítja meg, hogy az etikus hackelés kizárólag azokra az esetekre korlátozódik, amikor a hacker erre kifejezetten speciális vagy általános felhatalmazást kap. Ezért azok a személyek, akik csak saját elhatározásukból, jogosultság hiányában keresnek programhibákat vagy biztonsági rééseket, nem tekinthetők etikus hackernek, hanem csak azok, akik rendelkeznek jogosultsággal valamilyen formában (például az információs rendszer tulajdonosa kifejezetten megbízza őket a rendszer tesztelésével és támadásával). Ennek szemléltetésére a szerző a közelmúltból vett hazai példákat is felsorakoztat (lásd a Magyar Telekom rendszerének meghackelése és az ötven forintért vásárolt BKK-bérlet). (84–84. o.)

Ambrus szerint az említett esetekben a tényállásszerűség szintjén biztosan megvalósul a Btk. 423. §-a szerinti információs rendszer vagy adat megsértése bűncselekmény valamely alakzata az etikus hacker tevékenysége révén. A bíróság azonban értékeli a cselekmény konkrét társadalomra veszélyességét, és a bizonyítékok alapján kialakult meggyőződése szerint megállapíthatja

a társadalomra veszélyesség hiányát, s így felmentheti az illetőt. Azonban az e tevékenység mögött húzódó szándékot is mindig figyelembe kell venni.

Ezt a problémakört közelebbről megvizsgálva, amennyiben az információs rendszerben feltárt biztonsági rést a hacker diszkréten bejelenti a cégnek, akkor az alapvetően etikus hozzáállásnak tekinthető. Azonban ha a nagy nyilvánosság előtt tárja fel a biztonsági rést, akkor ez a részéről nehezen tekinthető etikusnak, különösen azért, mert ezzel felhívja figyelmet a rendszerben található hibára, *de facto* arra, hogy mások is használják ki a rendszer sebezhetőségét. Újszerű megközelítésnek tekinthető e körben, hogy Ambrus véleménye szerint a bíróság a vizsgálat tárgyává teheti például azt is, hogy a hacker eljárása tekinthető-e a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény 1. § (3) bekezdése alapján közérdekű bejelentésnek vagy sem. Ha a joggyakorlat közérdekű bejelentésként és ezáltal jogelleneséget kizáró oknak (Btk. 24. §) ismerné el az ilyen jelzést, úgy a cselekmény, társadalomra veszélyesség hiányában, nem valósítana meg bűncselekményt. (84. o.)

Ambrus továbbá foglalkozik a készpénz-helyettesítő fizetési eszközzel kapcsolatos bűncselekményekkel is, és olyan érdekes kérdést is érint mint a kriptovaluták büntetőjogi megítélése. Helytállóan állapítja meg, hogy miután a kriptovaluta csak a virtuális térben létezik, anyagi jogi értelemben dolognak semmiképpen nem tekinthető, így lopás stb. elkövetési tárgya nem lehet. Kiegészíteném ezt azzal, hogy kivéve, ha a kriptovalutát hardveres pénztárcán, azaz offline tárolják, és azt lopják el. Ezenkívül a hatályos szabályozás értelmében a kriptovaluták

³ Jonathan CLOUGH: *Principles of cybercrime* (Cambridge: Cambridge University Press 2015) 10–11., <https://doi.org/10.1017/cbo9781139540803.002>; GRABOSKY (2. lj.) 8–9.

a készpénz-helyettesítő fizetési eszköz fogalma alá sem sorolhatók, és elsősorban az információs rendszer elleni bűncselekmények valósíthatók meg a virtuális fizetőeszközök kapcsán. (94–96. o.)

Ambrus részletesen vizsgálta még az adattal kapcsolatos bűncselekmények körében az offline és online is elkövethető tiltott adatszerzést, valamint a személyes adattal visszaélést. Külön foglalkozik a tiltott adatszerzés 2021. január 1. napjától hatályos Btk. 422/A. §-ába beiktatott új „drón-tényállásával”. A jogalkotó szerint, ha a drón jogellenes használatához további magatartások is kapcsolódnak (például felvétel készítése, a felvétel nyilvánosságra hozatala), akkor ez már olyan fokú jogsérelmet jelent, amellyel szemben szükséges a szigorúbb állami fellépés lehetőségének megteremtése, ezért indokolttá vált a szabálysértési és a büntetőjogi rendelkezések módosítása. A recens szakirodalomban Csák Zsolt állást foglalt korábban a drónokkal összefüggésben, hogy lényegében valamennyi jogsértésre rendelkezésre álltak már alkalmazható tényállások (az új tényállás megalkotása előtt is). A különböző optikai, elektronikai eszközökkel, kamerával, fényképezőgéppel vagy egyéb lehallgató eszközökkel felszerelt repülő drón is alkalmas lehet például a tiltott adatszerzés megvalósítására.⁴ A miniszteri indokolás ugyanakkor azzal magyarázza az új szabályozás létét, hogy ezáltal ne csak a titokban történő megfigyelés legyen büntetendő – amely továbbra is a Btk. 422. §-a kere-

tei között büntetendő –, hanem a nyílt (tehát az érintett személy által észlelhető módon történő) elkövetés is. Ambrus azonban kritikaként fogalmazza meg az új szabályozással szemben, hogy ez könnyedén a szimbolikus büntetőjognak eklatáns példájává válhat. Véleménye szerint a szubszidiaritási záradék („ha más bűncselekmény nem valósul meg”) alkalmazása nem tekinthető szerencsésnek a tényállásban, mert ellentmondást jelent, ha egy bűncselekmény egy nála elvileg enyhébb büntetéssel fenyegetett másik tényállással szemben is háttérbe léphet. Javasolja, hogy e klauzula teljes elhagyását, esetleg a „ha súlyosabb bűncselekmény nem valósul meg” fordulatra való lecserélését, hogy az új tényállásnak valóban legyen a gyakorlatban betöltött szerepe. (98–100. o.)

Ambrus ezt követően külön fejezetben elemzi a tágabb értelmű deliktumok körét, ennek keretében azonban a teljesség igénye nélkül az alábbi bűncselekményeket vizsgálta: a gyermekpornográfiát, a zaklatást, a vagyon elleni bűncselekményeket a kiskereskedelemben, a pénzmosást, illetve a közzététellel megvalósuló bűncselekményeket.

Először a gyermekpornográfia szabályozásával foglalkozik, különös tekintettel az új hazai tényállásra és külföldi jogi megoldásokra e téren. E körben azt a vitatott témát emelném ki, ami a saját készítésű, 18. életévet be nem töltött személyekről készült pornográf anyagok büntetőjogi értékelésére vonatkozó rész.⁵ Például a gyermekpornográfia büntető-

⁴ Csák Zsolt: „A drónok kapcsán felmerülő egyes büntető és eljárási jogi kérdések” in MEZEI Kitti (szerk.): *A bűnügyt tudományok és az informatika* (Budapest–Pécs: MTA Társadalomtudományi Kutatóközpont – PTE ÁJK 2019) 26–45.

⁵ Lásd A. ATABEKOVA – V. FILIPPOV: „Legislative Response to Use of Minors’ Self-generated Sexual Content for their ICT-facilitated Sexual Coercion” *European Research Studies Journal* 2018/4. 763–772., <https://doi.org/10.35308/ersj/1244>.

jogi tényállása kapcsán felmerült Gyurkó Szilvia által javaslatként, hogy dekriminalizálni kellene, ha például két 17 éves személy egymásnak pornográf felvételt küld saját magáról.⁶ Azonban az ilyen irányú törekvés főszabály szerint európai uniós kötelezettségbe ütközne, mivel a 2011/92/EU irányelv nem tesz különbséget az elkövetők életkora körében. Ambrus a dekriminalizáció kapcsán felhívja a figyelmet arra, hogy a megoldás a bíróságok által az ún. teleologikus (cél szerinti avagy jogtárgyharmonikus) értelmezés alkalmazása. „Eszert, ha a jogalkotó célja nem lehetett a konkrét ügy kriminalizálása (mint például a valódi konszenzuson alapuló, kölcsönös képküldés a fiatalok által), akkor a bíróság jogosult a Btk. 4. § (2) bekezdése alapján – társadalomra veszélyesség (azaz jogtárgysérelem) hiányában – felmentő ítéletet hozni (sőt, a büntetőeljárást ugyanezen a jogcímen akár az ügyészség is megszüntetheti, vádemelés nélkül).” (105–106. o.) A 2021-es új, hazai szabályozás például privilegizált – ugyanakkor a korábbi szabályozásnál nem enyhébb büntetési tételekkel fenyegetett – esetet határoz meg, ha a pornográf felvételen szereplő személy 14–18 éves. Ez alapján tehát megállapítható, hogy a jogalkotó nem értett egyet e körben a dekriminalizációra tett javaslatokkal. Az ilyen felvételeknek a digitalizáció által lehetővé tett, gyors és határokat nem ismerő, szinte korlátlan terjesztési lehetőségei nagyban megnövelték e cselekmények társadalomra veszélyességét,

ezért a gyermekpornográfiát érintő hazai módosítások a szigorítás irányába mozdultak el, például a bűncselekmény büntetési tételei jelentősen megnöttek.

Mint számos bűncselekmény, így a zaklatás is könnyedén elkövethető az új online platformok segítségével, már nemcsak kéretlen SMS, hanem akár gyalázkodó, fenyegető hangvételű Viber- vagy Messenger-üzenetekkel, hívásokkal zavarhatják mások mindennapjait, a *cyberbullying* jelensége egyre gyakoribb. Külön alfejezetben ezért a zaklatás dogmatikai elemzéséről és a vonatkozó joggyakorlattal kapcsolatos kritikai észrevételekről olvashatunk részletekbe menően.

Ezt követően Ambrus a modernizáció egyes lehetséges hatásait tekinti át a köznap értelemben vett kiskereskedelembe megvalósuló kriminális cselekmények minősítésére. Például olyan érdekes kérdéseket érintve, hogy a vonalkód átragasztása vagy hamis mérés esetén lopást vagy csalást kell-e megállapítani, valamint elemzi a Covid-19-világjárvány időszakában megnőtt kiskereskedelmi visszaélések új típusát, az információs rendszer felhasználásával elkövetett csalást is. A vírus elleni védekezés következtében előnyben részesítették a különböző érintésmentes, valamint online fizetési megoldásokat, amelyek egyúttal szélesebb körben teszik lehetővé az ezekkel kapcsolatos csalásokat is.

A következő részben pedig a megújult, 2021. január 1. napjától hatályos pénzmosás tényállásának értékeléséről olvashatunk. Az új szabályozást érintő számottevő változásokra fókuszál a részben. Ezek közül párat kiemelnek, például a pénzmosás valamennyi szándékos esetkór kapcsán alapesetként minő-

⁶ URFI Péter: „Ha a pedofilok „nyilvántartása” a csodafegyver, akkor miért nem vetették be eddig?” *444.hu*, 2020. augusztus 1., <https://444.hu/tdr/2020/08/01/ha-a-pedofilok-nyilvانتartasa-a-csodafegyver-akkor-miert-nem-vetettek-be-eddig>.

sül, ha legfeljebb ötvenmillió forint értékű vagyona követik el. További változás, hogy az ügyvéd nem a minősített, hanem az alapesetért vonható felelősségre. Ezenkívül a törvényhozó megalakította a pénzmosás szabálysértési alakzatát is, ha a pénzmosást legfeljebb ötvenezer forint értékre követik el [Btk. 462. § (2) bekezdés g) pont]. Az „elkövetésben való megállapodás” helyett már az egyéb előkészületi magatartásokra is kiterjeszti a büntetendőséget, amely valamennyi alapesetre nézve megvalósulhat. Számottevő változásként értékelendő, hogy a pénzmosás elkövetési tárgya a „dolog” helyett a „vagyon” lett. A miniszteri indokolás szerint a korábbi szabályozás alapján a dolog fogalmi keretei az elmúlt időszakban megjelent új típusú vagyoni formákra – például a fizetésre használt elektronikus adat különféle formáira – tekintettel szűkössé váltak. Ambrus is felhívta erre a figyelmet, hogy dolognak nem tekinthetők a virtuális fizetőeszközök, ezért annak ellenére, hogy természetüknél fogva (decentralizáltság és pszeudoanonimitás) alkalmasak a pénzmosásra, nem képezheték eddig a hazai szabályozás szerint, annak elkövetési tárgyát. Ennek feloldása érdekében vált szükségessé olyan rugalmas szabályozás kialakítása, amely egyaránt alkalmas az új típusú vagyonelemek kezelésére a pénzmosás tényállásának körében. A pénzmosás elkövetési tárgyának vagyona való módosítása, az európai uniós elvárásoknak megfelelően, kellően rugalmas feltételeket biztosít az új típusú vagyonelemek által megvalósuló bűnözés elleni küzdelemhez. További jelentős újdonságnak számít, hogy az orgazdaság tényállása eltűnt a tételes jogból, és a jogalkotó a pénzmosásba építette be. Ambrus hangsúlyoz-

za, hogy a bünygyi statisztikában ezézt várhatóán nőni fog a pénzmosási esetek száma, hiszen az eddig az orgazdaság körébe sorolt cselekmények is automatikusan a pénzmosás adatait gyarapítják majd.

Végül a különös részi tényállások elemzését a közzététellel megvalósuló bűncselekményekkel zárja. E deliktumokra vonatkozó büntetőjogi rendelkezések nem korlátozódnak bizonyos médiatípusokra vagy offline cselekményekre, ezézt az online közzétételre (például közösségimédia-platfomokra) is kiterjednek. A nagy nyilvánosság előtti elkövetés a 459. § (1) bekezdésének 22. pontjában írt módozatok (elektronikus hírközlő hálózaton való közzététel) útján is megvalósulhat, mint például a gyűlöltre uszítás tartalmat hordozó digitálisan rögzített képi anyag (videoklip) feltöltésével az internet valamely megosztó portáljára. A hazai szabályozásra tekintettel azt a személyt lehet büntetőjogilag felelősségre vonni, aki a bűncselekményt [például a rágalalmazást (Btk. 226. §), a közösség elleni uszítást (Btk. 332. §)] megvalósító megjegyzést szándékosan közzéteszi a közösségi média oldalon. A rágalalmazás megvalósulhat más becsület csorbítására alkalmas közlésének a közösségi oldalon való megosztásával (híresztelésével) is. A joggyakorlatban fellelhető példát is említ, mely eset során a YouTube videómegosztóra feltöltött, becsület csorbítására alkalmas videófelvétel kapcsán a rágalalmazás kapcsán a bűnöség megállapítására került sor (Kúria Bfv.1315/2017/6.). (160–161. o.)

Az elkövetők már kihasználják a modern technológiák nyújtotta lehetőségeket, ezézt Ambrus külön fejezetben, *A digitalizáció új kihívásai* címmel tárgyalja a mesterséges intelligencia és

ezzel szoros összefüggésben az önvezető és egyéb új közlekedési eszközök (segway, e-roller) kurrens büntetőjogi kérdéseit. Utóbbiak esetében szükségesnek tartja a jogszabály-módosítást, amely lehetővé teszi ezeknek a tipikus új eszközöknek a *sui generis* járműkategória formájában történő szabályozását. Felhívja a figyelmet arra a jogbiztonsági problémára, hogy a jelenlegi közlekedési jogi szabályozás keretei között, elsősorban városi közlekedési eszközök kapcsán akár olyan értelmezésnek is helye lehet, amely szerint azok még járműnek sem tekinthetők, így használóik a gyalogosokkal esnek egy elbírálás alá. Más értelmezés szerint az ilyen eszközök lényegében ugyanakkor automatikusan segédmotoros kerékpárnak minősíthetők, ezért e téren a jogszabály-módosítást sürgeti. (220. o.)

A mesterséges intelligencia kapcsán a büntetőjogi felelősség alanyával kapcsolatos elképzelések (arra a kérdésre keresve a választ, hogy kit vagy mit tekinthetünk a bűncselekmény tettesének) után bemutatja a releváns bűncselekmény- és szankciótani, valamint különös részi problémákat, illetve olyan deliktumokat sorakoztat fel, amelyeknél a mesterséges intelligencia mint elkövetési tárgy jelenhet meg. Példaként említhető az az eset, amikor az elkövető akár egy autonóm járművet is meghackelhet, és az elkövetés eszközeként használhatja, például a kibertámadás során arra programozza be, hogy a sértettet megölje, mindezt úgy, hogy nagy sebességgel fálnak vezet a járművet. Ezenkívül más közlekedési bűncselekményt is ugyanúgy elkövethetnek. Ambrus az önvezető járművek kapcsán is körbejárja azt a kérdést, hogy büntetőjogilag ki vonható felelősségre (a vezető, az üzembentartó

vagy esetleg a gyártó), illetve a jelenlegi szabályozás mennyiben alkalmazható (a különböző automatizáltsági fokozatokat figyelembe véve) ezekben az esetekben. Érdekességként kiegészítve ezt a részt, Franciaország lett az első olyan európai ország, amely a francia kormány által 2021. július 1-jén közzétett rendeletével a közúti és közlekedési szabályokat úgy alakította át, hogy lehetővé tegye a teljesen autonóm járművek közlekedését a közutakon. A rendelet módosítja a közúti szabályokat, hogy engedélyezze az autonóm járművek tesztelését a francia közutakon. A rendelet különböző újításokat vezet be a francia közlekedési jogszabályokban, például a büntetőjogi felelősség korszerűsített rendszerét. Az új szabályozás lehetővé teszi, hogy a járművezető mentesüljön a felelősség alól, amint az automatizált vezetési rendszer a használati feltételeinek megfelelően működik. A rendelet egy másik újonnan meghatározott jellemzője a járművezető és az automatizált vezetési rendszer közötti interakció feltételei, valamint a vészhelyzeti manőverek, amelyeket a rendszernek automatikusan végre kell hajtania. A rendelet által bevezetett további változás a járművezetőtől elvárt figyelem szintjének meghatározása a vezetési környezetére, amikor az automatizált vezetési rendszer aktiválására sor kerül.⁷

Az egyes új technológiákat követően az angolszász szakirodalomban jobban ismert, új típusú szexuális visszaélésekről olvashatunk: a „bosszúpornó”

⁷ „France takes lead on allowing automated driving on public roads” *Connected Automated Driving Europe* 2021. július 5., <https://www.connectedautomateddriving.eu/blog/france-takes-lead-on-allowing-automated-driving-on-public-roads/>.

(*revenge porn*), valamint a „szoknya alá fényképezés” (*upskirting*) és a *cyberflashing* jelenségeiről. Ambrus a kompromittáló tartalmakkal való visszaélés-ként a bosszúpornó esetét említi, amely általában féltékenységből, a párkapcsolat megszakítása miatti bosszúból, a volt partner által a sértettől készült pornográf felvételek nyilvánosságra hozatalát jelenti. Az ilyen kép vagy videó készülhet csak magáról a (tipikusan meztelen) sértettől, az elkövető és a sértett közös szexuális cselekményéről, illetve az is elképzelhető, hogy nem valódi, hanem manipulált felvételtől van szó, amikor tehát a bosszúpornográfia a *deepfake*-kel kombinálva jelenik meg. Az *upskirting*-ről tipikusan a női sértettek kapcsán beszélhetünk, és az ágyékukról engedély nélküli kép- vagy videófelvétel készítését jelenti. A *cyberflashing* pedig jellem-

zően a kéréstlen, szexuális tartalmú (nemi szervről készült) képes üzeneteket jelentik. (221–229. o.)

Végül a kötet két olyan a digitalizáció által kevésbé érintett témával zárul, exkurzus keretében, amelyeknek aktualitása azonban vitathatatlan: ez pedig a Covid-19 járvány és az állatkínzás büntetőjogi kérdésköre.

A könyvet elolvastva úgy gondolom, hogy a digitalizáció és büntetőjog kapcsolatát érintő kérdésekről átfogó képet kap az olvasó. Mindezek alapján ajánlom e kötetet mindazon elméleti és gyakorlati szakemberek figyelmébe, akik bővíteni kívánják ismereteiket e téren. Emellett mind a jogalkalmazóknak, mind pedig a joghallgatóknak hasznos tudásanyagként fog szolgálni a munkájuk és kutatásuk során.

*Mezei Kitti**

* PhD, tudományos munkatárs, TK JTI, 1097 Budapest, Tóth Kálmán u. 4.; egyetemi adjunktus; BME GTK, 1117 Budapest, Magyar tudósok körútja 2. E-mail: mezei.kitti@tk.hu.

A recenzió 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.