Magyar Rendészet 2021/1. 27–39. DOI: 10.32577/mr.2021.1.2

A modern technológia kihívásai az egyetemi oktatásban

NAGY Zoltán András[1]

Napjaink felgyorsult technikai-technológiai fejlődése új kihívásokat jelent a társadalomban. Az egyetemet elhagyó fiataloknak – bármely egyetemen, karon végezzenek is – a napi gazdasági, politikai, technológiai realitásokkal és a jövő ránk váró kihívásaival, az új technológiák lényegével, az erre adott, adható jogi válaszokkal tisztában kell lenniük.
A jelenben szerzett, általunk átadott ismeretekre, saját kutatómunkájának eredményeire, tájékozottságára alapozva tud majdan lépést tartani a jövőbeni kihívásokkal, amivel munkája során szembesülhet. A technikai-technológiai újdonságok pedig a mindennapi rendészeti tevékenységet közvetlenül érintik, akár mint alkalmazott eszközt munkájuk során, vagy a technikai-technológiai megoldásokkal való visszaélés lehetőségét.

Kulcsszavak: *internet, drón, 3D, Internet of Things, virtuális valuták*

Bevezetés

Az egyetemet elhagyó fiataloknak – bármely egyetemen, karon végezzenek is – a napi gazdasági, politikai, technológiai realitásokkal és a jövő ránk váró kihívásaival, az új technológiák lényegével, az erre adott és adható jogi válaszokkal tisztában kell lenniük. A jelenben szerzett, általunk átadott ismeretekre, saját kutatómunkájának eredményeire, tájékozottságára alapozva tud majdan lépést tartani a jövőbeni kihívásokkal, amelyekkel munkája során szembesülhet.

A Nemzeti Közszolgálati Egyetem Rendészettudományi Karának hallgatói jellemzően jogalkalmazók lesznek, sőt vezetőként, parancsnokként fokozott felelősségük kell hogy legyen abban, hogy napjaink kérdéseivel tisztában legyenek és tudásukat, ismereteiket beosztottjaikkal is megosszák. A technikai-technológiai újdonságok pedig a mindennapi rendészeti tevékenységet közvetlenül érintik, úgymint alkalmazott

[1] Dr. habil. Nagy Zoltán András, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék, egyetemi docens.
Zoltán András Nagy PhD, habil., University of Public Service Department of Criminal Investigation Economy Protection and Cybercrime Prevention, Assistant Professor.
E-mail: nagy.zoltan.andras@uni-nke.hu, ORCID: https://orcid.org/0000-0002-6888-9059

eszközt munkájuk során, illetve a technikai-technológiai megoldásokkal való visszaélés lehetőségét.[2]

STEM és SMAC

Nézzük először az oktatási rendszert érintő kihívásokra adott lehetséges válaszokat. Napjaink oktatással foglalkozó szakirodalmában két rövidítés olvasható leggyakrabban:

„STEM" és „SMAC".

A *STEM* kifejezést először 2011-ben használta Judith A. Ramaley biológus, aki az Amerikai Egyesült Államok Természettudományi Intézetének vezetőjeként dolgozott.

A „STEM" a mit oktassunk[3] és a „SMAC" mire készítsük fel a diákokat, hallgatókat. Már előre jelezzük azt, hogy e követelmények az ipar, a kereskedelem, a gazdasági-pénzügyi szféra igényeit tükrözik, ám elemei hasznosíthatók.

A „STEM" a *science, technology, engineering, mathematic* – szavak kezdőbetűje.[4] A STEM-et a tradicionális természettudománytól és a matematikai oktatástól egy vegyes tanulási környezet jellemzi, amely megmutatja a hallgatóknak, hogy ez a tudományos módszer hogyan alkalmazható a mindennapi életben. A STEM-módszer célja, hogy ismereteket és készségeket hozzon a problémák megoldására, megtanítson értelmezni, értékelni információkat, és tudja, hogyan kell az információkat, bizonyítékokat összegyűjteni és értékelni a döntéshozatalhoz. Nézzük, hogy milyen készséget kívánnak – általában – a természettudományok:

- a legfontosabb a problémamegoldó készség,
- a kreativitás,
- a kritikus elemzés képessége,
- a csapatmunka,
- az önálló gondolkodás,
- a kezdeményezőkészség,
- a közlés technikája (magabiztossága),
- a digitális írástudás.

E képességek, készségek kivétel nélkül nélkülözhetetlenek bármely tudományban, a gazdasági szférákban, nem utolsósorban a rendőri munka során.

---

[2] Boda József – Dobák Imre: A nemzetbiztonság technikai kihívásai a 21. században. In Boda József – Dobák Imre (szerk.): *A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században.* Budapest, Nemzeti Közszolgálati Egyetem, 2015. 17–25.; Dornfeld László: A kiberbűnözés elleni küzdelem kihívásai. *Diskurzus,* 5. (2015) ksz. 27–35.
Marc Goodman: *Future Crime.* London, Corgi Books, 2015. 253–424.

[3] David W. White: What is STEM Education and Why is it Important? *Florida Association of Teacher Educators Journal,* 1. (2014), 14. 1–9.

[4] Government of Western Australia, Department of Education: *What is STEM?* é. n.

A kiképzés, majd valamennyi stúdium oktatása során e képességekre fel kell készítenünk hallgatóinkat az adott oktatási tananyaggal adekvátan, hiszen munkájukban e kompetenciák nélkülözhetetlenek. Például a bűnügyi felderítések során az elemzés, a kreativitás (a corpus delictiből felépíteni egy tényállást vagy verziókat felállítani stb.), de a sikeres nyomozás egyik „motorja" lehet az önálló gondolkodás is, a közlés magabiztossága, meggyőző volta a büntetőeljárások résztvevőivel (gyanúsítottal, ügyvédjével vagy az ügyésszel stb.) szemben a sikeres munka betetőzése.

A digitális képességek fontossága, azok eredményes elsajátítása a 21. században már alapvető követelmény.

A technológia folyamatos fejlődése megváltoztatja, sőt kikényszeríti a naprakész tudást, az élethosszig tanulás követelményét.

A „mire készítsük fel a hallgatókat, diákokat" kérdésre a „SMAC" jelenti a választ, amely rövidítése a *Social Media* (közösségi média), *Mobile* (mobileszközök), *Analytics* (elemzés készsége), *Cloud* (felhőszolgáltatás) angol szavaknak.[5]

A rendőrséget mint korábban konzervatív, a változásokat lassan követő szervezetet többek között a technikai-technológiai fejlődés készteti innovációra. A kriminalisztika területén látványos újítások, eszközök váltak a mindennapi munka részévé, a bűnügyi elemzések (profilalkotás, kriminális predikciós előrejelzések, adatbázisok az egyedi bűnelkövetésekről, elkövetési módokról, használt eszközökről, személyekről stb.) segítik a munkánkat, és folyamatosan születnek új módszerek a bűnfelderítésben, bűnmegelőzésben.

A SMAC a rendészettudományban is iránymutató, ha a rendőrség munkáját, e területekről származó tapasztalatait adekvát módon építjük be mindennapi tevékenységünkbe.

A közösségi média *(social media)* megteremtette és még inkább kiszélesíti a kommunikációt a lakosság felé és vice versa:

- az ügyfélkapcsolatok lehetősége bővíthető (lenne); gyülekezések bejelentését, azok ügyintézését, okiratok benyújtását, elintézését, a bűncselekmények feljelentését, egyes eljárási cselekmények lebonyolítását stb. modernizálja és egyben meggyorsíthatja;
- tájékoztatás a rendőri szervek elérhetőségéről, címeiről, telefonszámairól, a panasznapok (ügyfélsegítő) helyéről, idejéről, a nyilvános e-mail-címekről (ezek klaszszikus Open Data);
- a lakosságtól történő segítségkérések fóruma lehet, körözésekről, eltűnt személyekről, dolgokról (ékszerek, műtárgyak, nagy értékű autók stb.) történő információkérés;
- a lakosság tájékoztatására is megnyílt a lehetőség; a bűnfelderítésről, annak eredményességéről, az újonnan megjelent bűncselekményekről, azok elkövetésének módjairól, újfajta csalásokról azok megelőzéséről stb.;

[5] Hafedh Ibrahim Alfouzan: Introduction to SMAC – Social Mobile Analytics and Cloud. *International Journal of Scientific & Engineering Research,* 6. (2015), 9. 128–130.

- ha jól használjuk az internetes közösségi felületeket, eredményesebb toborzómunkát is végezhetünk (napjaink aggasztó létszámproblémáit enyhítendő).

Mindezek a rendőri munka átláthatóságát, a bizalom megtartását erősítik és segíthetik.

A *mobileszközök* (mobiltelefonok, laptopok, tabletek, külső adattárolók stb.) alkalmazása gyorsabbá, könnyebbé teszik mindennapi tevékenységünket, a kommunikációt, gyorsabb, helyhez nem kötött hozzáférést biztosít az információkhoz, növelheti a reakcióképességet, nem mellesleg csökkenti, csökkentheti a papírmunkát. Ugyanakkor a mobileszközök a bűnözés területén is jelen vannak, amelyek bűncselekmények bizonyítékait hordozzák, és ezek speciális ismereteket követelnek, amelyeket meg kell tanulnunk.

Az elemzés *(analytics)* képessége lehetőséget kínál a különféle forrásokból előállított adatok elemzésére, különböző verziók közüli választásra a döntés-előkészítéshez, majd a döntéshez. Az elemzést segítik az adatbázisok, amelyek akár a mobileszközökön, akár az interneten elérhetők.

A felhőszolgáltatás *(cloud service)* megszünteti a földrajzi akadályokat, és segít az információk tárolásában és elérésében, támogatva a közös munkát. Az egyes tagok munkáikat a felhőben tárolhatják, majd később feldolgozhatják, továbbírhatják stb.

Karunkon a „mit oktassunk?" tantárgyi tematikája kötött, jogszabályok által behatárolt.

A STEM és SMAC mint oktatási-kutatási irányok, „jelszavak" természettudományra, gazdasági-üzleti folyamatok hatékonyságára (profitabilitásának növelésére) szabott, ami egyfelől felhívja a figyelmet a technológiai fejlődés figyelemmel kísérésének fontosságára, trendjére – „meghajolva" e tendencia előtt, annak prioritására a társadalmi fejlődésben –, másfelől módszerei, eszközei átültethetők a társadalomtudományokra is, példákat említve az elemző munka, a digitális írástudás, a csapatmunka, kreativitás fontosságára, illetve eszközrendszerére, a mobileszközök, felhőszolgáltatás ismeretére, ezzel kapcsolatos problémákra, a közösségi média lehetőségeire.

A modern technológia által kikényszerített kihívásokkal, egyszersmind a modern technológiákkal meg kell ismertetnünk a hallgatókat és megértetni azt, hogy a technológia fejlődése folyamatos lesz, és újabb és újabb problémát vet fel a jogalkalmazás minden szintjén, így a büntető jogalkalmazásban is.[6]

Fontos leszögezni, hogy nem szükséges és nem is lehet cél az, hogy egyes technikai-technológiai megoldások, eszközök működésének minden apró részletét mérnöki-számítástechnikai alapossággal ismerjük, elegendő megérteni a folyamatot, annak hatását, eredményét, és ha szükséges, a jog górcsövén keresztül nézni, elemezni, minősíteni.

---

[6] Mezei Kitti – Nagy Zoltán: *Az informatikai bűncselekmények.* Egyetemi jegyzet, Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2017. 30–63.; Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában*. Budapest, HVG-ORAC, 2018. 145–165., 166–174.

Nem kell tudni, hogy a hackinget („elektronikus betörést") hogyan és milyen módszerrel követték el, de azt tudni kell, hogy mit jelent egy jogosulatlan belépés a számítástechnikai rendszerbe. Nem kell részletesen ismernünk a 3D-s nyomtatás minden egyes munkafázisát, de azt tudnunk kell, hogy a technológiával a szabadalmi jogok sérülnek vagy azt, hogy fegyver előállítására is alkalmas a technológia.

Illusztrációk a bűnügyi tudományokat érintő kihívásokra

A technológiai fejlődés okán a bűnügyi tudományokat érő új kihívások közül a büntető anyagi jogot és a kriminalisztikát említjük, és ez utóbbi kapcsán a büntető eljárásjog kikerülhetetlen.[7]

A büntető anyagi jogban, a jogsértések, bűncselekmények minősítése az elektronikus adatok ellen végrehajtott támadások okán jelentik a nehézséget. A személyiségi jogot érintő adatok védelmét meg kellett teremteni, ugyanakkor a közérdekű adatok nyilvános elérése szintén kötelezettség. A virtuális térben való elkövetés lényegének megértése sem minden esetben volt egyszerű. A számítógéppel végrehajtott csalás tényállását 1994-ben megalkották, 1996-ban, 1999-ben és 2001-ben módosították. A sok módosítást követően a 2012-es Btk. a 375. §-ban, egy a tradicionális csalástól különböző bűncselekményként szabályozta az „Információs rendszer felhasználásával elkövetett csalás" bűncselekményét. A jogalkotói felismerés sem késhet, követniük kell a napi tendenciákat, hiszen ez visszaveti a jogalkalmazók munkáját.

Jelezzük, hogy a közérdekű üzem és a kritikus infrastruktúra fogalma részben fedi át egymást,[8] így a kritikus infrastruktúra elleni támadás büntetőjogi minősítése – horribilie dictu – akár enyhébb is lehet, mint a közérdekű üzem elleni kibertámadásé (ez minősített esetként szerepel), és e két körön kívül eső szerverek elleni támadásként – alapesetként is – lehetséges az értékelése (például az egészségügy vagy a közigazgatás intézményei). Holott, elvitathatatlan fontosságú a kritikus infrastruktúrák kiemelt jogi, így büntetőjogi védelme.

A kriminalisztikában is új kérdéseket vetett és vet fel az új technológia. Gondoljunk a valós, illetve a virtuális térben megjelenő bűncselekmények nyomozásával kapcsolatos különbségekre.

A valós térben elkövetett bűncselekmények nyomai, bizonyítékai közvetlenül érzékelhetők, láthatók a személyi sérülés nyomai, a megrongált vagyontárgyak, vagy éppen hiányoznak ezek a dolgok, mert ellopták, elrabolták azokat. Azaz, mint a bűncselekmény elkövetési tárgyai, a bűncselekményre utaló bizonyítékok közvetlenül

---

[7] Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémái.* Doktori értekezés, Pécs, 2019.; Parti Katalin – Kiss Tibor: Informatikai bűnözés. In Borbíró Andrea et alii (szerk.): *Kriminológia.* Budapest, Wolters Kluwer, 2019. 491–517.; Simon Béla: *Csúcstechnológiai bűnözés és nyomozása.* Egyetemi jegyzet. Budapest, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2012. 5–210.

[8] Vö. a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) Korm. határozat 3.3. pontját és a Büntető Törvénykönyvéről szóló 2012. évi C. tv. 459. § 21. pontjával.

érzékelhetők. Ezzel szemben az elektronikus adatok csak más technikai eszköz alkalmazása révén tehetők láthatóvá, nyernek értelmet.

Nem kevés problémát okoz az is, hogy a virtuális térben a sértett nem észleli a támadást, ez növeli a látenciát, és késlelteti a nyomozásuk megindulását.

Meg kell értenünk és fel is kell készülnünk arra, hogy a sértett lényegesen kevesebb információt tud nyújtani egy kibertámadásról, mint amikor a valós térben *face to face* találkozott az elkövetővel, a támadás motívumának, célzatának, a szóba jöhető elkövetők és más körülmények feltárása nagyon fontos kiindulási alapja lehet egy sikeres nyomozásnak.

El kell sajátítani azt a képeséget is, hogy a számítástechnikai adatok fellelése (a kutatás), sértetlenségének biztosítása érdekében rögzítésük, a különböző technikai eszközök lefoglalása, továbbá a technikai eszközök kezelése szakmai felkészültséget igényel, amelyet el kell sajátítani az egyetemi vagy más szakmai képzéseken.

Szükséges az informatika közös nyelvének, az angol nyelvnek viszonylag jó szintű ismerete is.

Illusztrációként – természetesen a teljesség igénye nélkül – lássunk néhány új eszközt, új lehetőséget, amelyek jelzik napjainak technikai-technológiai fejlődését.

A 3D nyomtatás

A 3 dimenzióban történő nyomtatás még a harmadik ipari forradalom vívmánya.[9] Ahogy az első ipari forradalomban a gőzgép mobilitásával kiváltották a helyhez kötött vízenergiát, ma a 3D nyomtatás olyan mobil megoldás, amely a termelést, szervizelést akár a megrendelőhöz is viheti. Ezzel az additív (hozzáadott, építkező) technológiával manuálisan létre nem hozható (mert nem lehet kézzel kivágni, reszelni, formázni stb.) eszközöket, tárgyakat, alkatrészeket, ezáltal egy mérnök „álmait", ötleteit lehet megvalósítani, nem kötik meg a fizikai lehetőségek. Az emberi testbe illesztésbeli problémákat áthidaló protéziseket, hihetetlen látványvilágú képző- és iparművészeti alkotásokat tudnak létrehozni. Ma már az 1 milliméteres dísztárgytól[10] a házépítésig alkalmazzák a technológiát.

A *bionyomtatás* olyan távlatokat nyit, amelyek az emberi szervek azonos genetikai állományból történő pótlása a kilökődés kockázatát nagymértékben csökkenti, remélhetőleg ki is zárja. Ez utóbbi még kísérleti stádiumban van. Hazánkban, Pécsett folynak kísérletek lombikban történő sejttenyészet technológiájával.

---

[9] Grad-Gyenge Anikó: A modern technológiák szerzői jogi és iparjogvédelmi kihívásai – különös tekintettel a fájlcserére, a felhő-programozásra és a 3D nyomtatókra. In Tóth András (szerk.): *Technológia jog: Új globális technológiák jogi kihívásai.* Budapest, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, 2016. 98–115.; Klaus Schwab: *The Fourth Industrial Revolution.* Penguin Random House, 2017. 161., 167.
Nagy Zoltán András: A 3D nyomtatás, mint a jogrendszert érintő új kihívás. *Magyar Jog,* 61. (2017), 10. 613–621.; Bibi van den Berg – Simone van der Hof – Eleni Kosta (eds.): *3D Printing, Legal, Philosophical and Economic Dimension.* The Hague, Asser Press – Springer, 2016. 13–16.

[10] Tudománypláza: *Egy milliméter nagyságú Dávid szobor.* 2019.

A 3D nyomtatás kapcsán felmerülő jogi problémák közül kiemeljük, mivel a technológia lehetővé teszi tárgyak reprodukálását is, így bármely szabadalmi, mintaoltalmi, termék know-how, szerzői jogi sérelmének a lehetőségét magában rejti. A költséges befektetés árán létrehozott új találmányok, újítások, alkatrészek is engedélyek nélkül előállíthatók, sorozatgyártásba bevonhatók, majd értékesíthetők. Mivel (a beteg terápiájához szabott vagy ritka) gyógyszerek házilagos előállítása is megoldott, akkor kábítószerek is előállíthatók, bármilyen összetevőkkel és az összetevők módosításával is. Végül, de nem utolsósorban a *legmodernebb fegyverek is előállíthatók titokban, kontrollálhatatlanul*. A bűnözői és terroristacsoportoknak olyan eszközpark kerülhet birtokába, amely a házilagos kivitelezés miatt ellenőrizhetetlen, jól rejthető, titkolható a hatóságok, szakszolgálatok elől. Ennek megakadályozásában komoly szerep hárul a törvényhozásra.

Drónok (quadrocopterek)

Ugyanígy a törvényhozásra vár a jelenleg szabályok, kötöttségek nélkül a fejünk felett röpködő drónok használatának, használóinak megregulázása is.[11]

A drónok alkalmasak a levegőben, távirányítással röpködni. Ezáltal lehetővé válik távoli fényképek, filmek készítése azokról az objektumokról, tevékenységekről, amelyeket magas falak, kerítések vagy más védelmi berendezések óvnak az avatatlan kíváncsiskodók elől.

A drónok alkalmasak egyfelől üzleti titkok (például zárt területen gyártási, logisztikai folyamatokat, gépeket, munkaerőt megfigyelve információkat stb.) kifürkészni, katasztrófaterületeken fényképeket, videófelvételeket készíteni, másfelől felhasználhatók a drónok a rendezvények, ünnepségek, sportesemények megzavarására, terrortámadás végrehajtására (jelezte a 2019. szeptemberi nagy kárt okozó támadás a szaúd-arábiai olajmezők ellen). Nem utolsósorban magánszféránkat is sérthetik a drónok által készített fénykép- vagy videófelvételek (magántitkainkat stb.).

A katonai felhasználású drónok alkalmasak távközlési kapcsolatok kiépítésére, rádiótechnikai átjátszásra, rádióelektronikai zavarásra, továbbá zavarórepülés végrehajtására és kamikázetípusú célra repüléshez.

Az Európai Bizottság 2019. március 12-én az egész Európai Unióra kiterjedő szabályokat fogadott el a drónokra vonatkozó műszaki követelmények meghatározásáról. Az Európai Repülésbiztonsági Ügynökség (EASA) rendeletével összhangban az új szabályok rögzítik a biztonság, a védelem és a magánélet védelmének, valamint a személyes adatok védelmének alapelveit. Célja továbbá a bürokrácia csökkentése és az innováció ösztönzése, hiszen számtalan előnye van a drónok alkalmazásának (biztonsági

[11] Gyaraki Réka: A drónok használatának hazai szabályozása. *Magyar Rendészet,* 16. (2016), 1. 43–54.; Gyaraki Réka – Rottler Violetta: Drónok kora – személy és vagyonbiztonság a XXI. században. In Bányász Péter – Kiss Dávid – Orbók Ákos (szerk.): *A Tudomány kapujában*. Konferenciakötet. Magyar Hadtudományi Társaság, Budapest, 2016. 108.

funkciók ellátására, például rendezvények esetében, katasztrófahelyzetben az elhárításban, ezek rögzítésében, mezőgazdaságban öntözésre, terményfigyelésre, áruszállításra stb.).

A rendelet kiküszöböli azokat a szabályokat is, amelyek elfojthatják a vállalkozást. Az EU-s norma alapján, Magyarországon is hamarosan megjelenik a drónokra vonatkozó törvényi szabályozás, amely remélhetőleg sok kérdést tisztáz. Ugyanakkor a rendészet számára külön kihívás a jogellenesen használt drónok kiiktatásának, a *drónelhárításnak problémája*.

Internet of Things (IoT)

Ma már természetes, ha az emberek az interneten keresztül kommunikálnak, hiszen erre született. Innen már csak egy lépés a hálózatba kapcsolt eszközök kommunikációja is. Az IoT kapcsolatot teremt az intelligens eszközök és a helyi, központi vagy felhőalapú rendszerek között. A vállalatok alkalmazzák az IoT-technológiát a gyártásban, a szállításban és a logisztikában, a közművekben. Így intelligens gyárak, okos olaj- és gázmezők, intelligens hajók, önvezető járművek (IoV), intelligens kórházak stb. működnek napjainkban. A gyárakban a robotizált gyártás során az eszközök kommunikációja megteremthető, ezáltal hatékonyabbá, gördülékenyebbé válhat a termelés, az alkatrészellátástól, a késztermék előállításán át a csomagolásig, a kiszállításig tartó folyamatban felmerülő hiba, elakadás (alkatrészhiány, robotok, eszközök meghibásodása stb.) azonnal észlelhető, korrigálható. A városban parkolók és az autók közötti kommunikáció jelzi, hogy hol, melyik parkolóban van még hely, az lefoglalható előre, a kórházakban a gyógyszerrendelések és -adagolások az IoT segítségével folyamatossá válhatnak. Az IoT-technológia lehetőség a fogyasztók számára a környezetvédelemben, a háztartásban (gáz-, villanyórák és a szolgáltatók között hálózati kapcsolat lehetővé teszi a fogyasztás leolvasását és nekünk már csak fizetni kell, távolról vezérelhetjük a lakás hűtését-fűtését, a sütők beindítását, ahogy közelítünk haza, hűtőgépünk árut rendelhet, ha érzékeli, hogy valamely termék kifogyott, stb.).

Hackingtámadással különösen fenyegetetté válnak az IoT- és az IoV-hálózatok, mivel minden az internethez csatlakoztatott eszközt veszélyeztet egy hackertámadás. Minél több eszköz kapcsolódik a hálózathoz, annál inkább kitett nemcsak az eszköz, hanem az egész hálózat is egy ilyen támadásnak. A hálózatba történő jogosulatlan belépéssel károk idézhetők elő, a termelési-logisztikai folyamatok megbénításától az okos otthonokban a riasztó kikapcsolásán, a tűzesetek előidézésén át az önvezető járművek baleseteinek okozásáig (fékrendszer, sebesség manipulálásával).

A felhőszolgáltatás

A harmadik ipari forradalomhoz köthető az adattárolás és -hozzáférés új módszere. A növekvő adatmennyiség tárolása, gyors elérése, nem utolsósorban a hardver mértének csökkenése, az internet egyre nagyobb elterjedtsége hívta életre azt az ötletet, majd üzletet, amely találkozott a felhasználók igényével is, hogy tudniillik a felhasználók nem saját számítógépeiken tárolják az adataikat, sőt ma már a programjaikat sem, hanem egy úgynevezett felhőszolgáltatónál.

A felhőszolgáltatás *(cloud computing)* napjaink olyan új technikai megoldása, amely tehermentesíti a felhasználót attól, hogy nagy mennyiségű adatot tároljon, illetve különböző programokat telepítsen a számítógépére.

A felhőalapú szolgáltatások népszerűsége, száma növekszik (kereskedelmi szolgáltatások, például Amazon, E-bay). A szerverek személyes adatokat is tárolhatnak (például bankkártyaszámokat, Gmail- és más e-mail-kliens címeket, nagy kártyatársaságok adatait stb.). A felhasználó által előállított információk (szövegek, képek) kerülhetnek ilyen tárhelyekre (például Dropbox, Evernote). E technikai megoldásnak következménye, hogy a bűnözés is átterjed a felhőre. Az Operation High Roller csalás olyan támadás volt, amely egy malware segítségével kiiktatta a PIN-es és chipes azonosításokat.[12]

A felhőszolgáltatás számtalan előnnyel kecsegtet, lehetővé teszi azt, hogy a felhasználók az adataikhoz, programokhoz, feladatok végrehajtása céljából a világ bármely pontjáról hozzáférhetnek. A felhasználó adatai nem vesznek el, nem kell aggódnia, hogy számítógépe, adathordozói tönkremennek, adatait letörli véletlenül, villámcsapás éri az elektromos hálózatot, így a számítógépet is stb. Jogtiszta programok legfrissebb verziói találhatók ott meg, amelyek garantáltan vírusmentesek, a szolgáltatás gyors és biztonságos. A felhasználó több platformot tud egyesíteni munkája végzéséhez (például munkahelyén, utazása során és másutt a saját számítógépén, laptopján, mobiltelefonján keletkező, előállított adatokat együtt tárolja, dolgozik azokkal).

A felhőben tárolt adatokhoz (cikkek, tanulmányok, konferencia-előadások stb.) a felhasználó bármikor és bárhol hozzáférhet, ahol van internetkapcsolat. De a felhők közvetítik azt a kommunikációt is, amelyek emberek és emberek, emberek és gépek, gépek és gépek között zajlanak. Ismerjük meg és használjuk bátran a felhőszolgáltatás lehetőségeit tanulmányaink és munkánk során. Ugyanakkor nyomozás során a felhőszolgáltatók *együttműködési készsége vagy annak hiánya* a rendészet eredményes munkáját nem kis mértékben befolyásolja. Gondoljunk arra, ha a felhőszolgáltató elzárkózik a hatóság által kért információ megadásától.

[12] McAffee: *Operation High Roller Raises Financial Fraud Stakes.* 2012.

Bitcoin és egyéb altcoinok

A virtuális valuták létrejötte összefügg a mindig új megoldás utáni kutatás igényével és a pénzügyi szféra iránti bizalom megrendülésével. A hagyományos bankrendszer gyengeségei, illetve szabályozó szerepe kiiktatásának ötletéből született, a 2008-as gazdasági válságot követően „bocsátották ki" 2009. január 3-án az első virtuális valutát, a Bitcoint, amit Satoshi Nakamoto néven talált ki egy felhasználó.

A cél a készpénz mellőzésével, az elektronikus adatokkal végzett internet banking és más szolgáltatások, vásárlások megkönnyítése, nem utolsósorban elrejtése, kontrollálhatatlanná tétele. Rögtön tegyük hozzá, hogy nem szükséges pénzben gondolkodni, az ugyanígy értékpapír is lehet.

Népszerűségük titka éppen abban rejlik, hogy a nemzeti bankoktól függetlenek, jellemzően decentralizáltak, konverziós költségeik nincsenek, továbbá a digitális valuták hamisíthatatlanok, valódi valutára vagy más virtuális valutára válthatók. A pénzügyi műveletek nyilvánosak, valamennyi a rendszerbe kapcsolódó felhasználó láthatja valamennyi tranzakciót. Emellett a felhasználók anonimok maradhatnak, nincs személyiséglopás. További előnyként említhetjük, hogy a tranzakcióban részt vevő felhasználók egyenrangúak, amely a valós térbeli pénzügyi intézmény és ügyfél kapcsolatban de jure deklarált, ám de facto hagy maga után kívánnivalót, sőt a magyar pénzügyi békéltető intézmény eddigi működése sem nevezhető ügyfélpártinak. A hálózatban tranzakciókat lehet lebonyolítani anélkül, hogy azok bármelyik résztvevőjében – eladóban, vevőben vagy a bankban – meg kellene bízni. A bizalmat a rendszer matematikai alapjai helyettesítik: minden egyes Bitcoin egyedi, tehát nem lehet őket hamisítani. A tranzakció gyorsan végrehajtható, illetve nem visszavonható.

A rendszert használók egy azonosító számsort látnak – ismételjük –, anélkül, hogy a mögöttük álló felhasználó beazonosítható lenne. Ma már a virtuális valuta „pénztárcája" sem szükségszerű, hogy a felhasználó számítógépén, laptopján, mobiltelefonján legyen. A „pénztárca" a „felhőben" tárolható, így semmi nyoma sincs annak, hogy az adott felhasználó rendelkezik-e virtuális valutával, pláne annak, hogy mit ad el, mit vásárol, bűncselekményből származó pénzt tisztára mosott-e, vagy sem, „vásárolt-e" fegyvert, kábítószert, hamis okiratot, vagy sem, adott-e vagy vett-e pornográf, pedofiltartalmakat, bérelt-e „gyilkost", vagy sem, igénybe vett-e botnet hálózatot egy terheléses támadás indításához, stb.

Oktatási modellek

A modern technológiák megjelenése és térhódítása kiélezte a világban eltérő oktatási szisztémák közötti különbséget. Napjainak oktatási modelljei megérnek néhány gondolatot:

A készségalapú oktatás *(Skill Based Education):* különösen a középfokú és az egyetemi képzésben a hallgató készségeinek kibontakoztatása céljával csapatmunkára,

önálló gondolkodásra, független kutatásra, a reális önértékelésre, problémamegoldásra, az idővel való gazdálkodásra, hatékony kommunikációra és kritikus vagy kreatív tevékenységekre történik felkészítés. Széles az oktatási spektrum és modern oktatási eszközök alkalmazása nyújt lehetőséget a készségek kifejlesztésére. Ebben a modellben leginkább a STEM-módszer működik. Ez az oktatási metódus az angolszász országokban és Távol-Keleten elterjedt.

A másik modell, a jellemzően német oktatási modell a duális képzés, amely egy szakmára, szakterületre készít fel, arra koncentrál, jellemzően a gyakorlati képzést helyezi előtérbe. Az elméleti képzést csökkentve a képzés az oktatási intézményben, míg a gyakorlata a kijelölt vagy a választott partnerszervezetnél, üzemnél, gyárnál történik, folytatódik.

Az elméleti képzés kiegészül minden évben egy a szorgalmi időszakot követő szakmai – gyakorlati képzéssel. A magyarországi szakképzés ezt a modellt veszi át (többek között építve az autógyárak munkaerőigényeire), de az egyetemi képzések is jellemzően (szűkebb) szakmai orientációjúak.

A *jogalkalmazói képzésben* – vélhetően – a kettő valamiféle ötvözete lenne kívánatos.

Az elméleti és az adekvát (szakmai) gyakorlati képzéstől nem lehet eltekinteni, (analóg a duális képzéssel, bár nem nevezzük annak), ugyanakkor az önálló gondolkodás, kutatómunka és a problémák kisebb-nagyobb teammunkában való feldolgozása, például egy-egy szemináriumi keretében, egy-egy jogeset, ismeretanyag kis csoportban történő feldolgozásában (akár több kis csoport ugyanazt az esetet, egymással replikázva).

Önálló kutatási feladat megoldása (például szemináriumi jegyet érő önálló kutatómunka, kisebb tanulmány készítése) növelné a hallgatói aktivitást.

Fontos célkitűzés kell hogy legyen a tananyag feldolgozásában a hallgatóknál már kézben levő technikai eszközök, önálló vagy interaktív kommunikációra bevonása a feladatmegoldásba, akár jogeset, szakirodalom keresésére, OSINT-feladatok végrehajtására. A hallgatói aktivitást növelné az is, hogy egy-egy jogeset, -jelenség kapcsán mit jelenítenének meg a hivatalos és web2 (és melyik közösségi média felületén?) nyilvánossága előtt?

Az önálló prezentációkészítés és annak előadása a hallgatótársak előtt szintén a hallgatói aktivitás, egyszersmind a modern eszközök irányába történő orientáció hatékony eszköze lehet.

Az egyetemen kívüli szakmai tevékenység/feladat végrehajtásában együtt tényked es az idősebb vagy a már dolgozó rendőri vagy más szolgálatok állományával alapvető. Fontos és támogatandó törekvés, hogy már a kiképzés során, a feladatok végrehajtásában a hallgatóink együtt mozgása, az együtt tényked esük dominál janak. Mindenki legyen tisztában saját és hallgatótársa feladatával, helyettesítve társát bármikor, bármilyen helyzetben.

Fontos lépés volt az NKE Rendészettudományi Karán a Belügyminisztérium támogatásával a kiber- és informatikai nyomozóképzés megindítása, amelynek fő

célkitűzése nemcsak a hagyományos bűncselekmények számítástechnikai érintettségével összefüggő nyomozásának, hanem a virtuális térben zajló bűncselekmények, sőt a jövő technológiai eszközei fel- és kihasználásával elkövetett bűncselekmények nyomozásának kriminálmetodikai szempontú oktatása is. A szakirányú képzés nappali és levelező munkarendben a 2020/21-es tanévben kezdődött.

Kiemelkedik a Rendészettudományi Karon a Szent György Szakkollégium tevékenysége, ahol konferenciákat, előadásokat szerveznek, kutatómunkát folytatnak, fontos szerepe van az ismeretek terjesztésében, a szakdolgozatokra felkészülés segítésében.

A szakkollégium legutóbbi konferenciája a 2020. november 30-án rendezett „XXI. század kiberbiztonsági kihívásai" címmel zajlott, számtalan hasznosítható előadással, felvetéssel a kiberbűnözés elleni fellépésről, a kiberbiztonság fokozásáról.

Hasznos lehet a valamennyi kar hallgatói számára nyitott választott szemináriumi rendszer teljesebbé tétele egyetemünkön. A karok együttműködésére, együtt ténykedésére kiváló példa a Magyarországon egyedülálló Közös Gyakorlat.

FELHASZNÁLT IRODALOM

Alfouzan, Hafedh Ibrahim: Introduction to SMAC- Social Mobile Analytics and Cloud. *International Journal of Scientific & Engineering Research,* 6. (2015), 9. 128–130. Online: www.ijser.org/researchpaper/Introduction-to-SMAC–Social-Mobile-Analytics-and-Cloud.pdf

Berg, Bibi van den – Simone van der Hof – Eleni Kosta (eds.): *3D Printing, Legal, Philosophical and Economic Dimension.* The Hague, Asser Press – Springer, 2016. Online: https://doi.org/10.1007/978-94-6265-096-1

Boda József – Dobák Imre: A nemzetbiztonság technikai kihívásai a 21. században. In Boda József – Dobák Imre (szerk.): *A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században.* Budapest, Nemzeti Közszolgálati Egyetem, 2015. 17–25.

Dornfeld László: A kiberbűnözés elleni küzdelem kihívásai. *Diskurzus,* 5. (2015), ksz. 27–35.

Goodman, Marc: *Future Crime.* London, Corgi Books, 2015.

Grad-Gyenge Anikó: A modern technológiák szerzői jogi és iparjogvédelmi kihívásai – különös tekintettel a fájlcserére, a felhő-programozásra és a 3D nyomtatókra. In Tóth András (szerk.): *Technológia jog: Új globális technológiák jogi kihívásai.* Budapest, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, 2016. 98–115.

Gyaraki Réka: A drónok használatának hazai szabályozása. *Magyar Rendészet,* 16. (2016), 1. 43–54.

Gyaraki Réka – Rottler Violetta: Drónok kora – személy és vagyonbiztonság a XXI. században. In Bányász Péter – Kiss Dávid – Orbók Ákos (szerk.): *A Tudomány kapujában.* Konferenciakötet. Magyar Hadtudományi Társaság, Budapest, 2016. 108.

Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémái.* Doktori értekezés, Pécs, 2019.

Mezei Kitti – Nagy Zoltán: *Az informatikai bűncselekmények.* Egyetemi jegyzet, Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2017. 30–63.

Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában.* HVG-ORAC, 2018.

Nagy Zoltán András: A 3D nyomtatás, mint a jogrendszert érintő új kihívás. *Magyar Jog,* 61. (2017), 10. 613–621.

Parti Katalin: Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében. *Belügyi Szemle,* 66. (2018), 23–35. Online: https://doi.org/10.38146/BSZ.2018.10.2
Simon Béla: *Csúcstechnológiai bűnözés és nyomozása.* Egyetemi jegyzet. Budapest, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2012.
Simon Béla: A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet,* 17. (2017), 5. 83–104.
Schwab, Klaus: *The Fourth Industrial Revolution.* Penguin Random House, 2017.
White, David W.: What is STEM Education and Why is it Important? *Florida Association of Teacher Educators Journal,* 1. (2014), 14. 1–9. Online: www.researchgate.net/publication/264457053_What_is_STEM_education_and_why_is_it_important

Jogforrások

2012. évi C. törvény a Büntető Törvénykönyvről
2017. évi XC. törvény a büntetőeljárásról

Internetes források

Government of Western Australia, Department of Education: *What is STEM?* é. n. Online: www.education.wa.edu.au/what-is-stem
McAffee: *Operation High Roller Raises Financial Fraud Stakes.* 2012. Online: www.mcafee.com/blogs/other-blogs/mcafee-labs/upping-the-financial-fraud-stakes-with-operation-high-roller/
Tudománypláza: *Egy milliméter nagyságú Dávid szobor.* 2019. Online: https://tudomanyplaza.hu/egy-millimeter-nagysagu-david-szobor/

ABSTRACT

Challenges of Modern Technology in University Education

Zoltán András NAGY

Today's accelerated technical-technological development poses new challenges in society. Graduates need to be aware of the economic – political – technological realities and the challenges ahead. They must be aware of the essence of new technologies and the legal answers that can be given to them. The technological innovations have a direct impact on everyday law enforcement activities, as well as the tools used in their work and the potential for misuse of technical-technological solutions.

Keywords: *Internet, quadrocopter, 3D, Internet of Things, virtual currencies*