Magyar Rendészet 2022/1. 231–234. DOI: 10.32577/mr.2022.1.14

Recenzió Mezei Kitti *A kiberbűnözés aktuális kihívásai a büntetőjogban*[1] című könyvéről

GYARAKI Réka[2]

Úgy érzem, hogy a 21. században kevesebb fontos téma van a rendvédelemben a jogalkalmazók és a jogalkotók számára, mint a kibertérben elkövetett jogellenes cselekmények.

Az elmúlt évek során annyit fejlődött a technológia, hogy az magával hozta az új típusú bűncselekmények megjelenését, és új helyszíneket biztosít az elkövetők számára a kibertérben. Amikor naponta nézem a híreket, mindig szembe találom magam az újabb és újabb típusú kiberbűncselekményekkel és kibertámadásokkal, amelyek minden országban, többek között gazdasági, pénzügyi, nemzetbiztonsági és -védelmi, illetve politikai kockázatokat jelentenek.

Az áldozatok között ugyanúgy megtalálhatók az egyszerű felhasználók, mint éppen a sok millió forintot befektető és megforgató pénzügyi szervezetek, valamint a felhasználók érzékeny adatait kezelő egészségügyi, oktatási intézmények, vagy a közlekedésben részt vevő szervezetek, kormányzati portálok.

Ma már nem elég beszélni róla, nem elég egy-egy kampánnyal felhívni a figyelmet, gyakorlatokkal megelőzni, hogy mind a közszférában, mind az üzleti világban működő szervezetek munkatársai ne essenek egy-egy adathalász levélnek áldozatául, hanem szükséges, hogy a témával kapcsolatos, összefoglaló, szélesebb körű művek szülessenek, amelyek alkalmasak arra, hogy a leendő szakemberek és a téma iránt érdeklődők megismerjék az aktuális trendeket.

Az elmúlt években többnyire kevés, inkább a felsőoktatásban tanuló rendvédelmi szakemberek számára írt tankönyv vagy egyetemi jegyzet született e témakörben, viszont szerencsére egyre több, a rendvédelmen kívüli szakember ír doktori disszertációt a kiberbűnözésről.

A könyv szerzője, Mezei Kitti 2019-ben védte meg doktori értekezését *A kiberbűnözés egyes büntetőjogi szabályozási kérdései* címmel,[3] amely kutatásán alapul

---

[1] Budapest, Társadalomtudományi Kutatóközpont Jogtudományi Intézet – L'Harmattan, 2020.

[2] Rendőr őrnagy, egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék; doktorandusz, Rendészettudományi Doktori Iskola.
Police Major, University of Public Service Faculty of Law Enforcement Department of Criminal Investigation, Economy Protection and Cybercrime Prevention; PhD student Doctoral School of Police Sciences and Law Enforcement, e-mail: Gyaraki.Reka@uni-nke.hu

[3] Mezei Kitti: *A kiberbűnözés egyes büntetőjogi szabályozási kérdései.* Doktori (PhD-) értekezés. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2019.

e monográfiája. A szerző a doktori védése óta is a kiberbűnözés büntetőjogi összefüggéseivel foglalkozik, és számos publikációja jelent meg ebben a témában.

Mezei Kitti e könyvében olyan megközelítésben mutatja be ezt a területet, hogy nem támad hiányérzete az olvasónak, mert a kiberbűnözés kapcsán jól összefoglalja napjaink legnagyobb kihívásait, legyen szó a különböző kibertámadásokról, a kriptovalutákkal vagy bankkártyával kapcsolatos visszaélésekről, vagy akár az online pénzmosásról.

A könyv jól felépített, tiszta nyelvezetű, rengeteg példával és jogesettel, ami miatt a téma iránt érdeklődő teljes, jól összefoglalt művet vesz a kezébe, míg azok, akik saját maguk találkoznak ezekkel a bűncselekményekkel is megértik, hogy mi történik, történt velük, és arra, milyen hazai, illetve nemzetközi jogszabály ad választ.

A kiberbűnözés aktuális kihívásai a büntetőjogban című könyv jól felépített, átlátható műve a szerzőnek, amely hasznos a felsőoktatásban tanuló leendő, vagy már éppen gyakorló rendvédelmi szakembereknek és a jogi egyetemek hallgatóinak is.

A szerző a könyvet alapvetően öt fejezetre osztotta, de összesen három fejezet, amely a könyv érdemi része, és amely megadja a kiberbűncselekmények „zamatát". Ezek közül a fejezetek közül a legalapvetőbb ismereteket, amelyek a kiberbűncselekmények hazai és külföldi szabályozásával foglalkoznak a II. fejezetben találjuk, amely az egyik legterjedelmesebb fejezete a könyvnek, és amelynek témája kifejezetten az úgynevezett *„cyber dependent crimes",* vagyis a szűk értelemben vett kiberbűnözéssel foglalkozik. E fejezet *A kiberbűnözés büntetőjogi szabályozásai* címet viseli. A kiberbűnözés jogi szabályozásának történetével kezdődik, amit olyan jogi szabályozás bemutatása követ, mint a NIS-irányelv[4] és az információs rendszerek elleni támadásokról szóló irányelv. Véleményem szerint, mivel sok szakember a kiberbűnözés és a kibervédelem feladatait és kihívásait külön-külön említi, a laikus sokszor közös szó, a „kiber"-en kívül nem tudja összekapcsolni, így nem érzékeli a kibertámadás és a kiberbűncselemények összefüggéseit. Mezei Kitti ezzel a fejezettel, a leírt uniós és nemzetközi jogi instrumentumok és fogalmak áttekintésével ezeket a sokak számára nehezen követhető összefüggéseket feloldja és érthetővé teszi.

Ez a fejezet olyan további problémákkal foglalkozik, mint például a 2017-es WannaCry zsarolóvírus megjelenése és hatása, valamint a Petya zsarolóvírus, amelyek szinte a kezdetei voltak annak, hogy a felhasználók is elkezdjék megérteni, és komolyan foglalkozzanak egy-egy kibertámadással.

Annak ellenére, hogy a kibertérben elkövetett jogellenes cselekmények és támadások oktatása során kihangsúlyozzuk, hogy a bűncselekmények nemzetközi jellege határokon átnyúlva mindenhol érezhető, jól szemlélteti azt a sokak által hangoztatott problémát, hogy a bűnüldözés egyik nagy kihívása éppen az országok

[4] Az Európai Parlament és a Tanács (EU) 2016/1148. irányelve a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.

között eltérő jogi szabályozás megléte. Nagyon jól érzékelteti a szerző, hogy az Egyesült Államokban mennyire másképp szabályozzák a CFAA-val *(Computer Fraud and Abuse Act)* a számítógépes bűncselekményeket, ahol már 1986-ban rájöttek arra, hogy szükséges az eltérő jogi szabályok megalkotása a megfelelő bűnüldözés kialakítása és a megfelelő büntetés kiszabása miatt.

Ugyanúgy figyelemre méltó annak megemlítése és hangsúlyozása, hogy szintén az Egyesült Államokban a kormányzati információs rendszereket és nemzetbiztonsági adatokat érő támadásokat és rendszerfeltöréseket eltérően szükséges szabályozni a hagyományos információs rendszerek elleni támadásoktól.

A második fejezet olyan további „szürke zónákat" tesz világosabbá, hogy mi és mi a feladata a CSIRT-eknek, valamint milyen támadási formák valósulnak meg a kibertérben, és erre a hazai jogi szabályozás hogyan reagált az 1978. évi IV. büntetőkódextől kezdve. Az egyik, az oktatás során általam is sokat emlegetett jogeset is bemutatja a szerző. Ez az Elender-ügy, amely a magyar kiberbűncselemények történetének egyik példaértékű esete volt, és amelynek az ítélete rámutatott arra, hogy mennyire fontos ennek a bűncselekménynek a jogi szabályozása.

A harmadik fejezet *A technológiai fejlődés hatása az egyes gazdasági bűncselekményekre* címet viseli. Alfejezetei a készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekményekkel, a darknet-fórumok térnyerésével összefüggésben megjelenő szervezett bűnözéssel kapcsolatos bűncselekményekkel, valamint a technológiai fejlődés fényében a pénzmosással foglalkozik.

Nagyon jól összegezi ez a fejezet azokat a kérdéses pontokat, ahol a fenti deliktumok megjelentek, és amivel mind a hazai szervezetek, mind pedig az Europol vagy akár az FBI is foglalkozik, és érnek el egyre többször sikereket a működő bűnözői csoportok felszámolásában, vagy személy(ek) kézre kerítésében.

A fejezet kitér az egyik, egyébként legálisan is használható, blockchain-technológia részletes bemutatására és a kriptovaluták ismertetésére is, amelyet sokszor tévesen, kizárólag a pénzmosással vagy más deliktummal hoznak összefüggésbe. Ugyanakkor az is téves elgondolás, hogy nem jelent kihívást a hatóságoknak.

A negyedik fejezet a *Technológiai kihívások a büntetőeljárásban* elnevezést viseli. A büntetőeljárásról szóló 2017. XC. törvényben jelent meg a digitális bizonyítékok szempontjából kiemelten fontos „elektronikus adat" fogalma, aminek köszönhetően végre tisztázódott az online rendszerben és a számítástechnikai eszközökön tárolt és fellelhető bizonyítékok lefoglalására vonatkozó szabályozás. Olyan fogalmakat használ, amelyeket többek között a rendvédelmi szakembereknek kell ismerni, és amelyek ismerete nélkül sem a felhasználni kívánt bizonyítékokat, sem a szakértő-kirendelés során a kirendelő határozatot és a szakértői vizsgálatot értelmezni nem lehet. Ezeket a fogalmakat, kifejezéseket jól felépítve, érthetően írja le a szerző, meghatározva a jelenlegi jogszabályi hátteret.

Nagy Zoltán András *Bűncselekmények számítógépes környezetben* című, 2009-ben megjelent könyve[5] óta ennyire összefoglalt mű nem született. Elmondható, hogy *A kiberbűnözés aktuális kihívásai a büntetőjogban* című könyv a 2021-es évben a legaktuálisabb és leginkább összefoglaló szakirodalom, amely mind a felsőoktatásban tanulóknak, mind pedig a kibertérrel foglalkozó érdeklődőknek ajánlott.

[5] Nagy Zoltán András: *Bűncselekmények számítógépes környezetben.* Budapest, Ad Librum, 2009.