Mák Bence[1]

A kibertérben elkövetett bűncselekmények különösen a társadalmi megítélés tükrében

I. Hipotézis

Az elmúlt kevesebb mint száz évben a technológia hatalmas fejlődésen ment keresztül, ennek a folyamatnak szerves része az infokommunikációs eszközök robbanásszerű fejlődése és széles körben való elterjedése a világon. Rövid időn belül jelentek meg olyan szolgáltatások és eszközök, amelyek nélkül életünket ma már el sem tudnánk képzelni. A telefonok, televíziók, okos készülékek, bankkártyák, internetes- és egyéb platformok mind a múlt, mind a jelen, és kifejezetten a jövő társadalmának oszlopait jelentik, nem túlzás azt állítani, hogy ezek nélkül az általunk ismert társadalmi berendezkedés nem létezne. Ezen eszközöknek és technológiáknak a polgári és ipari felhasználása, valamint elterjedése és mindenki számára elérhetővé válása a gazdaság, a politika és a közélet motorját képezi, továbbá jelentős kényelmi funkciókat biztosít
használóik számára. Ezeknek a hatalmas előnyöknek ugyanakkor nagy ára van. Mint mindennek, ennek a fellendülésnek is meg van a maga árnyoldala. A tudomány fejlődésével szükségszerűen együtt jár a bűnelkövetés megváltozása is. Az új technológiák további lehetőségeket biztosítanak a bűnelkövetők számára, hogy cselekményeiket eddig nem ismert módokon hajtsák végre. Erre a jognak természetesen reagálnia kell, ami legalább olyan komplex probléma, mint maga a teljes társadalmi-gazdasági folyamat, és még a mai napig is megoldásra váró kihívást jelent mind hazai, mind nemzetközi szinten.
A technológia fejlődésével ugyanakkor az ember nem mindig képes lépést tartani, vagy csak sokkal lassabban tudja azt követni, és nem feltétlenül érti meg azt, ami körülveszi őt. Projektemben ezen tételmondat alapján kérdőív segítségével felmérést készítettem és azt vizsgáltam, hogy a társadalom hogyan reagál és miként vélekedik az új technológiákkal összefüggő bűnelkövetéssel kapcsolatban. Feltételezésem szerint a társadalom nem tudja megfelelően kezelni az infokommunikációs eszközökkel vagy azok felhasználásával
megvalósított bűncselekményeket, ugyanis azokat vagy nem tartja jelentősnek, vagy fel sem ismeri őket, adott esetben nem tudja, hogy azokra hogyan is reagáljon. Véleményem szerint a társadalom számára mára egyre fontosabb az online tér tudatos használata és tájékozottabb a leselkedő veszélyekkel kapcsolatban. Ezen állításokat a beérkezett válaszok elemzésével igyekszem verifikálni vagy cáfolni.
Dolgozatomban először az ún. „*kibertérben*” elkövetett bűncselekmények problémáiról és jellegéről, valamint a bűncselekményi körről értekezek, majd ezt követően térek át a felmérés eredményeinek vizsgálatára és a konklúziók levonására.

II. A kiberbűncselekmények elméleti alapjai

II.1. Technológiai fejlődés kontra büntetőjog

Elsősorban az informatikatudomány, eszközeink és számunkra elérhető platformok rohamos fejlődése nagy kihívást jelent a jog számára. A nagy intenzitású növekedés, a
technológia térhódítása rengeteg olyan kérdést vet fel, amire nehezen lehet válaszokat adni, így egyre nagyobb a teljes jogrendszer és kiemelten a büntetőjog igénye a dinamikus reakciókra,

[1] Joghallgató, SZTE Állam- és Jogtudományi Kar.

ugyanis a preventív szabályozás a tudományterületek vonatkozásában elképzelhetetlen, mivel gátat szabna a potenciális fejlődésnek.[2] Ugyanakkor a reaktív szabályozással az egyes államok és a nemzetközi szervezetek is küszködnek egyrészről az idő folyása, másrészről a divergáló álláspontok miatt, így ebben a környezetben kell a jogalkotónak helyes döntéseket hoznia. Jól megfigyelhető, hogy a fejlődéssel együtt jár a bűnelkövetés változása és annak fejlődése is. Az infokommunikációs rendszerek, számítógépek és különösen az internet megjelenésével szinte egyidejűleg teljesen új bűncselekmények jelentek meg, melyek kriminalizálása egy hosszas folyamatot vett igénybe és vesz igénybe a mai napig is, ugyanis ez a probléma szinte végeláthatatlan. A folyamatos fejlődés újabb cselekményeket hív életre, valamint lehetővé teszi, hogy a „hagyományos" bűncselekmények egyre nagyobb köre valósuljon meg számítógépes rendszerek felhasználásával[3]. A kodifikáció fő problémája a megfelelő reakció megtalálásán túl az, hogy a büntetőjogi tényállások megszaporodásának, legtöbb esetben azok duplikálásának elejét vegye, és emellett ne devalvája a büntetőjog ultima ratio jellegét, ami napjaink jogalkotására egyébként is jellemző.[2] A tényállások helyes megalkotásánál továbbá figyelembe kell azt is venni, hogy teljesen új, eddig nem létező bűncselekmények mellett új elkövetési módok és „helyek" is megjelentek. A szabályozás teljes hiánya vagy a nem megfelelően megalkotott törvényi tényállások mellett a dogmatika kiforratlansága is jelentős erőként hat közre a jogalkotási és eljárási hibák fennállásában.[4]
Az internet határtalanságával együtt jár az is, hogy az online elkövetett bűncselekmények sem ismernek határokat. Továbbá a kibertérben elkövetett
bűncselekményeknek megvan az a sajátossága is, hogy azonnali és valós idejű kapcsolatot képesek biztosítani, valamint relatív anonimitást és titkosságot jelentnek, és így megnehezítik azok elkövetésének felderíthetőségét különböző védő mechanizmusok által. Továbbá szükséges megjegyezni, hogy ehhez hozzátartozik az is, hogy magas látencia jellemzi ezeket a bűncselekményeket, mivel a sértettek többnyire azokat nem észlelik[5]. Az ilyen módon kiterjedt nemzetközi, határokon átívelő bűnözés jelentős problémákat szül a gyakorlatban. A megfelelő nemzetközi jogsegélyek, kommunikáció és kooperáció hiánya mellett a már létező eljárások hibái, és a nemzeti jogrendszerek eltérései, különösen a joghatósági kérdések is gátat szabnak a hatékony bűnüldözésnek.[6] A 2001-ben született Budapesti Egyezmény elindult a kívánatos úton, de sajnos ezt a mai napig nem sikerült meghaladni. Az Egyezmény többek között rendelkezik a joghatósági kérdésekről, a nemzetközi bűnsegélyről és kapcsolattartásról, ugyanakkor ez nem realizálódik megfelelően. Az Egyezmény hiányosságai több mint kettő
évtized elteltével egyre nőttek, ugyanis az eltelt időben olyan fejlődések következtek be, amikre nem lehet megfelelően alkalmazni a rendelkezéseket. Ilyen például a felhőalapú szolgáltatás, mivel a felhőben tárolt adatok és információk meg nem határozott helyen „vannak", az Egyezmény pedig csak a meghatározott helyen fellelhető készülékekről és adathordozókról rendelkezik. Ehhez kapcsolódóan fontos annak az átértékelése is, hogy mit és hogyan vesz

---

[2] MEZEI KITTI: *A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre*. Állam- és Jogtudomány LXI. évfolyam 4. szám 2020, 65 -81 p.

[2] VARGA ÁRPÁD: A*z informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogrendszerben*. In Medias Res, 2019/1, 145-167. p.

[3] NAGY ZOLTÁN ANDRÁS: *A joghatóság problémája a kiberbűncselekmények nyomozásában*. In: Karsai Krisztina et al.: Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Forum Acta Juridica et Politica. Szeged, Tomus LXXXI. (2018), 755-767. p.

[4] BRENNER, SUSAN W.: *Cybercrie Investigation and Prosecution: The Role of Penal and Procedural Law*. Murdoch University Electronic Journal of Law, vol. 8 no. 2. 2001

[5] MEZEI, 2020

[6] NAGY, 2018

figyelembe a bíróság bizonyítékként, mit is tekintünk bizonyítéknak. Az ősi fogalom szerint a bizonyíték egy ontológiai létező, fizikailag létezik és a hatóság előtt van, ami azt észleli, melynek lényege, hogy megérintheti. Ettől eltérően a számítógépeken, hálózatokon vagy egyéb platformokon, eszközökön tárolt adatok, amelyek adott esetben bizonyítékként szolgálhatnak, mellőzik ezt a „fizikai létező" jelleget.[7]

II.2. A kiberbűnözés definiálása

Az infokommunikációs eszközök és rendszerek felhasználásával elkövetett bűncselekmények rendszere a közvélekedéssel szemben korántsem olyan határozott, mint ahogy azt elképzeljük. Éppen ellenkezőleg, nem adható rájuk olyan egzakt definíció, mint az ún. hagyományos bűncselekmények esetében. Az egyes jogellenes cselekményeken túl az egész ún. kiberbűnözést is egy meghatározatlansági buborék veszi körül[8]. *Susan W. Brenner* 2001-es írásában a dogmatika hiányát fő problémaforrásként jelenítette meg, ez a mai napig nem változott sokat, ugyanis a tudomány nem fogadott el egy olyan álláspontot sem, amely paradigmává válhatott volna a jogirodalomban.
A kiberbűnözés és a kiberbűncselekmények definiálhatatlanságából következik az, hogy ezen cselekményeket csak körülhatárolni és csoportosítani lehet, amivel kapcsolatban szintén probléma merül fel, ugyanis a bűncselekmények köre egyre tágabb és az folyamatos változást mutat, így nincs minden téren tartható meghatározás. [9]
A kiberbűncselekmények meghatározása esetén a kiindulópontot a bűncselekmény jellege jelenti. Ez alapján elkülöníthetünk tisztán informatikai rendszerek felhasználásával vagy azok útján elkövetett bűncselekményeket (cyber-dependent crime), illetve ezen eszközök által elősegítve elkövetett „hagyományos" bűncselekményeket (cyber-enabled crime), melyeket nevezhetünk informatika által elősegített bűncselekményeknek. A két kategória elhatárolásának fő ismérve az infokommunikációs eszközök vagy rendszerek felhasználásának módja és annak szerepe az elkövetés során. Míg a tisztán informatikai bűncselekmények esetében (mint például jogosulatlan belépés, továbbiakban: *hacking*) az infokommunikációs rendszerek teszik lehetővé ezen cselekmények megvalósulását, addig az informatika által elősegített bűncselekmények (mint például az online csalás) esetében ezek a rendszerek könnyítő szerepet játszanak az elkövetésben, azok az elkövetés eszközét vagy módját jelentik[10].
A két fő csoport mellett több álláspont alakult ki a további meghatározások tekintetében. A második felfogás az egyes cselekményeket a fő jellemzőik alapján különíti el, így három kategóriát alkot. Ennek a nézetnek az elemei a számítógépes rendszerek integritását sértő bűncselekmények, melyek nagyjából megegyeznek a tisztán informatikai bűncselekmények körével, de nem teljes az átfedés azzal. A második csoportot a számítógépes rendszerek segítségével elkövetett cselekmények jelentik, míg az osztályozás harmadik eleme a tartalom alapján alakítható ki. E két utóbbi kategória a *cyber-enabled crime* körébe tartozó cselekményeket fedi le, de azokat tartalmuk alapján mégis megkülönbözteti.[11]
Az utolsó módszer az elkövetési magatartás szerinti klasszifikációt helyezi előtérbe, így négy csoportot alakítva ki. Elkövetési magatartás szerint a cselekmények lehetnek engedély nélküli

[7] NAGY, 2018
[8] MEZEI, 2020
[9] VARGA, 2019 – MEZEI, 2020
[10] MEZEI, 2020
[11] VARGA, 2019

behatolással, csalási vagy lopási cselekménnyel, pornográfiával és szeméremsértéssel, illetve ún. „*kibererőszakkal*” elkövetettek.[12]
Álláspontom szerint a infokommunikációs eszközök útján vagy azok felhasználásával megvalósított bűncselekmények azon csoportosítása tartható, amely a „hagyományos”, illetőleg „új” bűncselekményeket választja el. Meglátásom szerint az informatika által elősegített bűncselekmények kategóriájának további, elkövetési magatartás és tartalom szerinti bontása szükségtelen, míg tisztán elkövetési magatartás alapján történő osztályozás nem képes az összes bűncselekményt lefedni a jogellenes cselekmények folyamatosan bővülő köre miatt, ugyanis sok cselekmény nem a felsorolt magatartások valamelyikével valósul meg, elég csak a terheléses (*DoS, DDoS*) támadásokra gondolni. Véleményem szerint az alapvető elkülönítésen túl esetlegesen a jogtárgyak szerinti klasszifikáció elképzelhető.
A kiberbűnözés tehát egy gyűjtő kategóriát alkot, amely úgy foglalható össze mint az infokommunikációs eszközök útján megvalósult bűncselekmények nagy halmaza, amely a számítógépeket az algoritmusokon keresztül az emberekkel összekötő virtuális térben, azaz a kibertérben valósul meg. [13] Így azt mondhatjuk, hogy kiberbűncselekmény mindaz, ami a kibertérben valósul meg.

II.3. A kiberbűncselekmények jelentősége

A kiberbűncselekmények komplex jogi tárggyal rendelkező bűncselekmények, amelyek elsősorban a vagyoni viszonyokat, valamint vagyoni és személyiségi jogokat támadják. Így nem meglepő, hogy a zsarolóvírusok, kártékony szoftverek (*malware*), adathalász e-mailek, túlterheléses támadások (*DoS, DDoS*), valamint a jogosulatlan belépéssel azonosított *hacking*cselekmények jelennek meg a legnagyobb számban.
Ezek mellett új kihívásokat jelentenek a pilóta nélküli robotrepülők, a mesterséges intelligencia térhódítása, valamint az online feketepiac (*darknet* fórumok).[14]
Az ilyen formában előforduló cselekmények kiemelt súlyát jelzik az olyan mérések és tanulmányok, amelyek a bűncselekményekkel okozott károkat veszik számba. A *McAfee* 2017es jelentése szerint a kiberbűnözés a harmadik legnagyobb kárt okozó bűncselekményi kör, amely éves szinten mintegy 600 milliárd dollár kárt okoz világszerte.[15] Ezzel szemben friss mérések azt mutatják, hogy a károk összege nem évente, hanem havi szinten éri el az 500 milliárd dollár körüli értéket.[16]

II. Az empirikus információgyűjtés eredményei

Nem reprezentatív kutatásomban több jelentős kérdésre kerestem a választ, amelyek többnyire a hagyományos és a kiberbűncselekmények különbözőségeivel és megítélésével kapcsolatosak voltak.

---

[12] VARGA, 2019

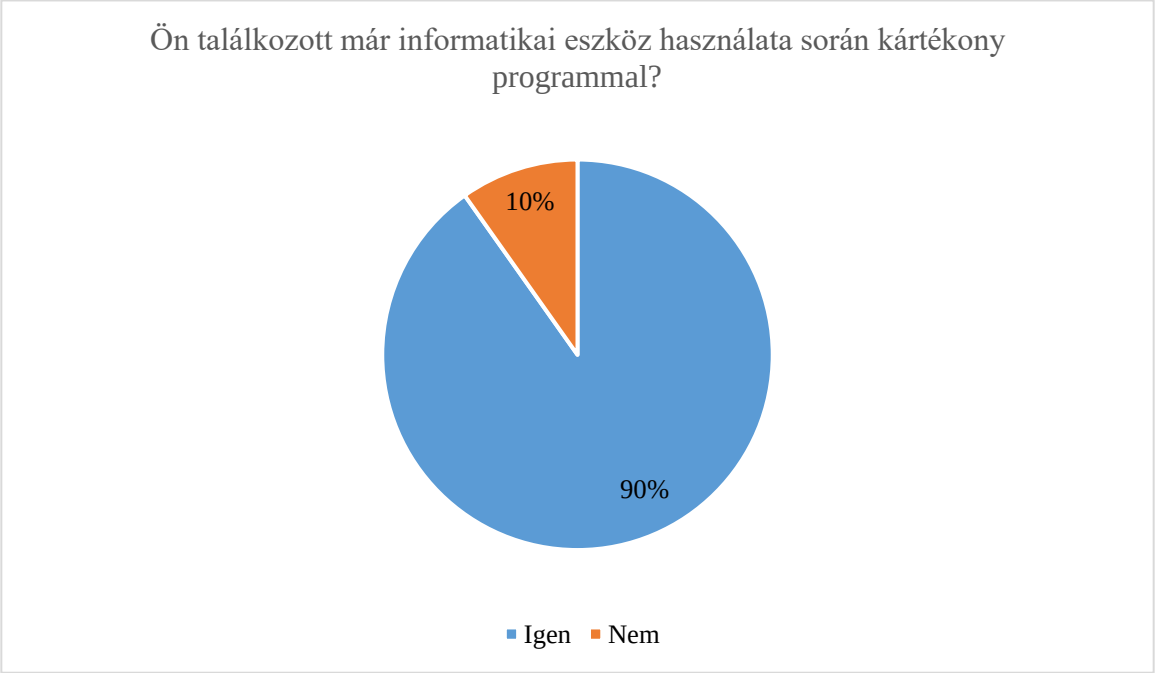
[13] MEZEI, 2020

[14] GÁL ANDOR – SZOMORA ZSOLT: *A drónnal történő megfigyelés kriminalizálása mint a büntetőjogi magánszféravédelem kiterjesztése.* In: Homoki-Nagy Mária et al.: Ünnepi kötet Dr. Szabó Imre egyetemi tanár 70. születésnapjára. Forum Acta Juridica et Politica, Szeged, Tomus XI. (2021), 101-108. p.

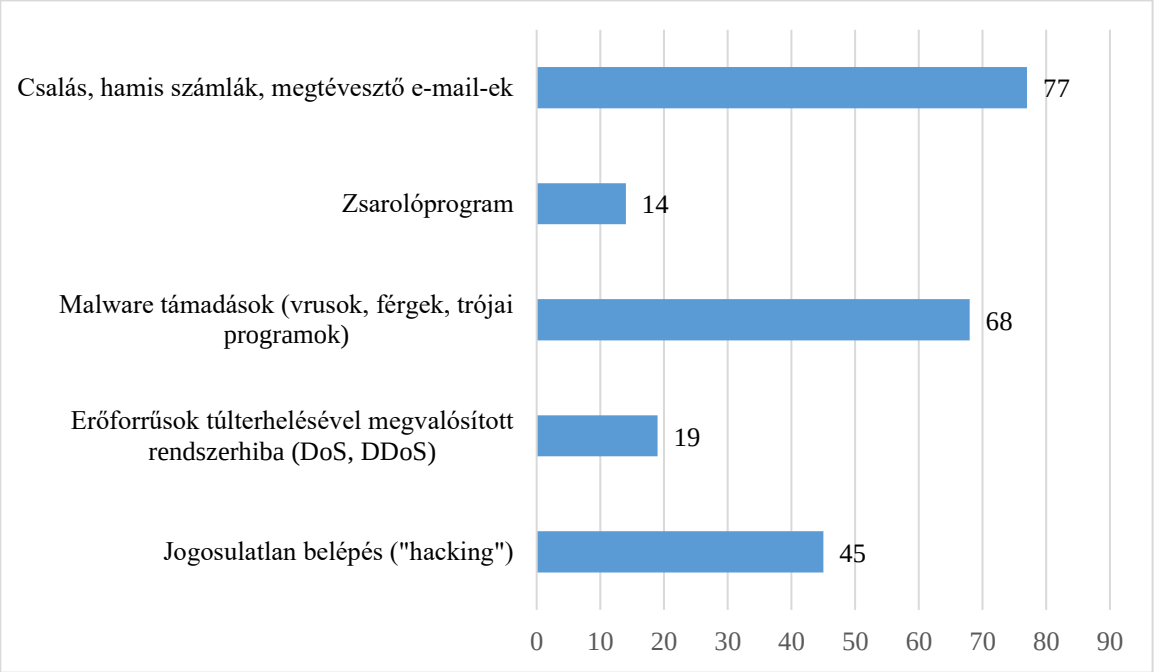
[15] McAfee: The Economic Impact of Cybercrime – No Slowing Down report, 2017

[16] MORGAN, STEVE: *McAfee Vastly Underestimates The Cost of Cybercrime*. Cybercrime Magazine, cybersecurityventures.com, 2020.12.09.

Mindenek előtt fontos kiemelni, hogy a válaszadó több, mint 62%-a 14 és 35 év közötti, így érdekes szempont a korosztályok közötti eltérések megfigyelése is.
Az első kettő kérdésre, mely a mai magyar bűnelkövetés nagyságáról, illetőleg ennek kibertérben elkövetett arányáról szól, jelentős mértékben eltérő válaszok érkeztek. A megkérdezettek 46%-a úgy gondolja, hogy a bűnelkövetések száma nem túl magas, de nem is alacsony, míg további 42% ennél magasabbnak, majdnem 10% pedig kiemelkedően magasnak véli a hazai bűnelkövetést. A válaszadók 61%-a szerint ezeknek a bűncselekményeknek csak csekély része valósul meg infokommunikációs rendszerek felhasználásával, míg a további 39% úgy véli, hogy a bűncselekmények kiemelkedő része ilyen technológiák felhasználásával kerül elkövetésre. Ezzel kapcsolatban kiemelendő, hogy a 35 év feletti korosztály nagyobbnak tartja a teljes bűnelkövetést, mint a fiatalabbak, míg a kibertérben való elkövetés esetében a fiatalok körében jóval nagyobb szórás volt megfigyelhető, az egészen alacsonytól a legmagasabb értékig adtak válaszokat. A 35 év feletti korosztály ebben az esetben is inkább a középközépmagas kategóriát jelölte meg.
Nem ennyire jelentős, de említésre méltó a bűncselekmények elítélésének kérdése, melyről elmondható, hogy a 25-35 év közötti korosztály ítéli el legjobban a bűnelkövetést az eredmények alapján, míg az ennél fiatalabbak között szintén nagy szórás figyelhető meg, a legmagasabb értéken kívül minden más lehetőségre érkezett válasz, de a legjellemzőbb a középérték megjelölése volt. Ezzel összefüggésben állt a következő kérdés, melynek lényege az volt, hogy a kitöltők minden bűncselekményt azonosan elítélnek-e. A válaszok itt túl nagy meglepetést nem hoztak, ugyanis mindössze 19% adott a kérdésre igen választ, ami még így is magasabb, mint az általam előrevetített.
A legjelentősebb kérdés a látenciával volt kapcsolatos. A válaszadók 13%-a úgy véli, a kiberbűncselekményeknek minimális része jut a hatóságok tudomására, míg 38% szerint ezeknek töredéke (az ötös skálán szereplő kettes érték), 39% szerint pedig ennél kicsivel több a felderített bűncselekmények száma, de így sem kimagasló. Az ötös skálán mindössze 9% vélte úgy, hogy a felderítettség mértéke a négyes-ötös csoportba tartozik.
A további kérdések sem jelentettek nagy meglepetést, ugyanis a kitöltők több mint 90%-a találkozott már valamely jogellenes magatartással a kibertérben, ahogy azt válaszok alapján elkészült diagramm is mutatja

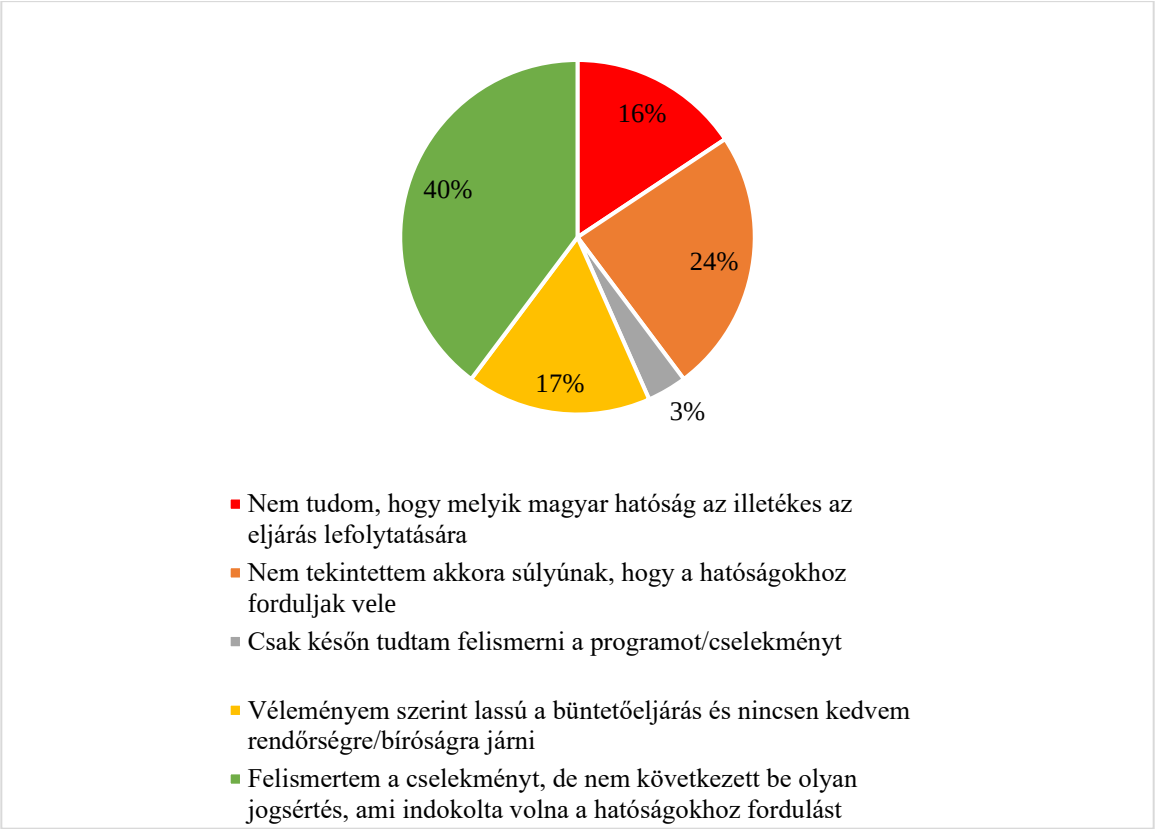


Ezen jogellenes cselekmények közül a legtöbb az internetes csalás és megtévesztés, ezzel a válaszadók mintegy 75,5%-a találkozott. A második legnagyobb számban előforduló bűncselekmény a *malware* támadások, amelyekkel 66% találkozott már.



A kitöltők 87%-ának bevallása szerint időben tudta ezeket a cselekményeket észlelni. Többségük nem hiteles források alapján, míg kisebb részük (30% sem) védelmi szoftverek segítségével ismerte fel ezeket a magatartásokat, a legkevesebben hivatalos tájékoztatók alapján értesültek róluk.

További fontos kérdés volt, hogy a kitöltő jelentette-e hatóságoknak ezeket az eseteket. A válaszadók mintegy 92%-a nem jelezte senkinek a jogellenes cselekményeket. Ennél is érdekesebb, hogy a kitöltők miért nem jelezték ezeket a hatóságok felé. A válaszadók mintegy 16%-a nem tudja, hogy melyik hatóság az illetékes Magyarországon. Több mint 24% azon az álláspontón van, hogy általánosságban nem akkora súlyúak ezek a cselekmények, hogy megérje őket jelenteni, míg további 40% tisztában van azzal, hogy jogsérelmet szenvedett, de ezzel nem foglalkozik, vagy nem sérült olyan vagyoni joga, amiért cselekedne. 17% pedig a büntetőeljárás lassúságát emelte ki, mint olyan tényezőt, ami meggátolta őt abban, hogy a hatóságokat megkeresse.



A kitöltők 84%-a szerint a társadalomnak nagyon fontos az online tudatosság, de ezzel szemben saját bevallásuk szerint nem használják tudatosan az internetet és eszközeiket, mindössze 23% adott olyan választ, hogy teljesen körültekintően és tudatosan jár el minden esetben.
Fontos megemlíteni, hogy a megkérdezettek 93%-a nem hallott hazai vagy nemzetközi kiberbiztonságot és tudatosságot elősegítő vagy azokat támogató kampányokról, programokról, amelyekkel egyébként az Európai Unió is rendelkezik. Ennél is érdekesebb, hogy ezeket a tudatosságnövelő lehetőségeket mindössze 39% venné igénybe.
További fontos megfigyelés volt, hogy a kitöltők 44%-a szerint magas, míg további 39%-a szerint kiemelten magas kockázatot jelentenek a kibertérben elkövetett bűncselekmények. A válaszadók 49,5%-a szerint súlyosabban, 50,5%-a szerint kevésbé súlyosak, mint a „hagyományos” bűncselekmények.

Következtetések

Amint igyekeztem is rámutatni, a kibertérben elkövetett bűncselekmények fogalmi és dogmatikai problémákkal is küszködnek az ennél jelentősebb eljárási és joghatósági problémák mellett. Ennek az állapotnak egy egységesen elfogadott új paradigma vethetne véget, de ennek kidolgozása még a jövő zenéje. A sikeres kibervédelemhez az állami és nemzetközi szerepvállalás mellett jelentős feladata van az egyénnek is, hogy mennyiben használja tudatosan a platformokat és eszközöket, valamint nagy felelőssége van a siker érdekében a magánszektornak is, amely a további fejlesztésekkel, stratégiákkal és a tagállami hatóságokkal való együttműködésekkel segíthetik elő a bűnüldözést.
A hipotézisben felvetett azon állításomat, miszerint a társadalom kevéssé reagál az ilyen jellegű bűncselekményekre, igazolni látszanak az eredmények, ugyanis a válaszadók jelentős része nem jelezte a jogsérelmet a hatóságnak, többnyire azért, mert nem tartotta jelentősnek azt, vagy nem tudta, hogy hogyan reagáljon. Ezzel összefüggésben kiemelném amit a kutatás is igazolt, hogy a társadalom számára fontos a tudatosság, de ennek ellenére a válaszok alapján nem

használják az online teret tudatosan, valamint a plusz információk iránti igény is elég csekély. Az is jól megfigyelhető, hogy a társadalom helyesen fel tudja mérni ezeknek a cselekmények a súlyát és a bennük rejlő veszélyt, valamint a válaszadók majdnem fele veszélyesebbnek tartja a kibertérben elkövetett cselekményeket. A válaszok egy biztatók, ugyanis jól kiszűrhetők belőlük, hogy a társadalom egyre komolyabban reagál a kiberbűnözésre, de még koránt sem éri el azt az ingerküszöböt, mint a „hagyományos" bűnözés.

Felhasznált források

- AMBRUS István: *A mesterséges intelligencia és a büntetőjog.* Állam- és Jogtudomány LXI. évfolyam 4. szám 2020, 4-23 p.
- BRENNER, SUSAN W.: *Cybercrie Investigation and Prosecution: The Role of Penal and Procedural Law*. Murdoch University Electronic Journal of Law, vol. 8 no. 2. 2001 http://classic.austlii.edu.au/au/journals/MurdochUeJlLaw/2001/8.html - letöltés ideje: 2023.11.25.
- GÁL ANDOR – SZOMORA ZSOLT: *A drónnal történő megfigyelés kriminalizálása mint a büntetőjogi magánszféravédelem kiterjesztése.* In: Homoki-Nagy Mária et al.: Ünnepi kötet Dr. Szabó Imre egyetemi tanár 70. születésnapjára. Forum Acta Juridica et Politica, Szeged, Tomus XI. (2021), 101-108. p.
- MEZEI KITTI: *A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre.* Állam- és Jogtudomány LXI. évfolyam 4. szám 2020, 65 -81 p.
- MORGAN, STEVE: *McAfee Vastly Underestimates The Cost of Cybercrime*. Cybercrime Magazine, cybersecurityventures.com, 2020.12.09. o https://cybersecurityventures.com/mcafee-vastly-underestimates-the-costofcybercrime/ - letöltés ideje: 2023.11.22.
- NAGY Zoltán András: *A joghatóság problémája a kiberbűncselekmények nyomozásában*. In: Karsai Krisztinam et al.: Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Forum Acta Juridica et Politica. Szeged, Tomus LXXXI. (2018), 755-767. p.
- VARGA ÁRPÁD: *Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogrendszerben*. In Medias Res, 2019/1, 145-167. p.
- McAfee: The Economic Impact of Cybercrime – No Slowing Down report, 2017 https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/eseconomicimpact-cybercrime.pdf - letöltés ideje: 2023.11.23.