Magyar Rendészet 2025/2. 195–214.
DOI: 10.32577/MR.2025.2.14

KIBERBIZTONSÁG

Kutatásom naplója, avagy gondolatok és anomáliák az online fizetésekkel kapcsolatos visszaélések köréből

Diary of my Research, or Thoughts and Anomalies about the Scope of Crimes Related to Online Payments

Packosz NIKIFOROSZ[1]

Bevezetés: Az online fizetések megbízhatósága alapvető fontosságú a gazdasági rendszer stabilitása szempontjából, ezért az ezekhez kapcsolódó bűncselekmények kérdésköre napjaink digitális társadalmának egyik kulcsterülete. A cikk az online fizetésekhez kapcsolódó bűncselekmények multidiszciplináris vizsgálatát tűzi ki célul, rámutatva a kriminalisztikai, jogi és szociológiai nézőpontokból eredő kihívásokra.

Célkitűzések: A kutatás célja az online fizetési visszaélésekhez kapcsolódó jelenségek komplex elemzése a jogtudomány, kriminalisztika és szociológia területeinek szintézisével. Kiemelt figyelmet fordít arra, hogyan definiálható a kibertér és a fizikai tér metszéspontjain keresztül a bűnelkövetői tevékenység, valamint milyen eszközökkel és módszerekkel növelhető a bűnüldözés és a bűnmegelőzés hatékonysága.

Módszertan: A kutatás jogdogmatikai elemzésre, statisztikai trendvizsgálatokra és szekunder adatokra alapozva tárja fel a bűncselekmények természetét. A multidiszciplináris megközelítés lehetővé teszi az elméleti alapok és a gyakorlati alkalmazások összekapcsolását, miközben innovatív megoldásokat keres a kriminalisztikai és jogi eszközök fejlesztésére.

Eredmények: A kutatás előzetes eredményei alapján az online fizetési visszaélések mögött meghúzódó legfontosabb tényezők a kibertér anonimitása, a pszichológiai manipulációs technikák elterjedése, valamint a szabályozás hiányosságai. A szervezett bűnözés kibertérbeli formái újradefiniálják

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola, e-mail: pnikko82@gmail.com

a bűnszervezet fogalmát, míg a bűnmegelőzés hatékonyságát jelentős mértékben befolyásolja a szolgáltatók és a hatóságok együttműködése.

Konklúzió: A tanulmány rávilágít arra, hogy az online fizetési visszaélések elleni küzdelemben a proaktív bűnüldözési stratégiák és a magas szintű szolgáltatói együttműködés kulcsszerepet játszhatnak. Az eredmények alapján az elkövetők elleni hatékony fellépés érdekében elengedhetetlen a multidiszciplináris szemlélet, valamint a társadalmi tudatosság „tudatosabb" növelése.

Kulcsszavak: online fizetések, szervezett bűnözés, geográfiai kivetülések, pszichológiai manipuláció, kiberbiztonság

Introduction: The issue of online payments and related crimes is one of the key areas of today's digital society. Their reliability is fundamentally important for the stability of the economic system. The aim of this article is to provide a multidisciplinary analysis of crimes related to online payments, highlighting the challenges that arise from a forensic, legal, and sociological perspective.

Objectives: The research aims to synthesise the fields of jurisprudence, criminalistics, and sociology to perform a complex analysis of the phenomena related to online payment fraud. Particular attention is paid to how criminal activity can be defined through the intersections of cyberspace and physical space and what tools and methods can be used to increase the effectiveness of law enforcement and crime prevention.

Methods: The research reveals the nature of crimes based on legal dogmatic analysis, statistical trend studies, and secondary data. The multidisciplinary approach enables the connection of theoretical foundations and practical applications while seeking innovative solutions for developing forensic and legal tools.

Results: Based on the preliminary research results, the most important factors behind online payment frauds are cyberspace's anonymity, the spread of psychological manipulation techniques, and deficiencies in regulation. Cyberspace forms of organised crime redefine the concept of a criminal organisation, while the effectiveness of crime prevention is significantly influenced by the cooperation of service providers and authorities.

Conclusions: The study highlights that proactive law enforcement strategies and a high level of service provider cooperation can play a key role in the fight against online payment fraud. Based on the results, a multidisciplinary approach and a more "conscious" increase in social awareness are essential to effectively combat perpetrators.

Keywords: online payments, organised crime, geographic projections, psychological manipulation, cybersecurity

Bevezetés

Az államilag, nemzetközileg elismert fizetési formákba, illetve fizetési rendszerekbe vetett bizalom, tehát a lakosság, a kereskedelmi és pénzügyi szektor ez irányú szubjektív biztonságérzetének fenntartása a pénzügyi rendszer működésének fundamentuma. Úgy tűnhet, hogy ez főként a pénzforgalmi szolgáltatók (magán)érdeke. Valójában azonban ez az egyik alappillére a nemzeti és globális gazdasági működésnek, így kompromittálása kulcsfontosságú érdeket sért, amellyel szemben ehhez igazodó súlyú ellenlépésekkel, eszközökkel kell(ene) fellépni. Ezen állításomat támasztja alá a Nilson Report[2] 2025 januári előrejelzése, miszerint a bankkártyával történő visszaélések mindösszesen 404 milliárd dollár kárt okoznak majd a következő tíz évben (Marek 2025).

Jelen írás egy hosszabb kutatómunka első lépéseként az online fizetésekkel kapcsolatos visszaéléseket három nézőpontból vizsgálja. Ezen kereteken belül kíván irányt találni, s talán mutatni a témakör mélyebb megismeréséhez, a rendészeti szempontból releváns kihívások azonosításához és az ezekkel szembeni hatékony fellépéshez. Egy időben nem titkolt cél az is, hogy a témához kapcsoló kutatás részeként felmérje, tesztelje a szakmai közeg reakcióját.

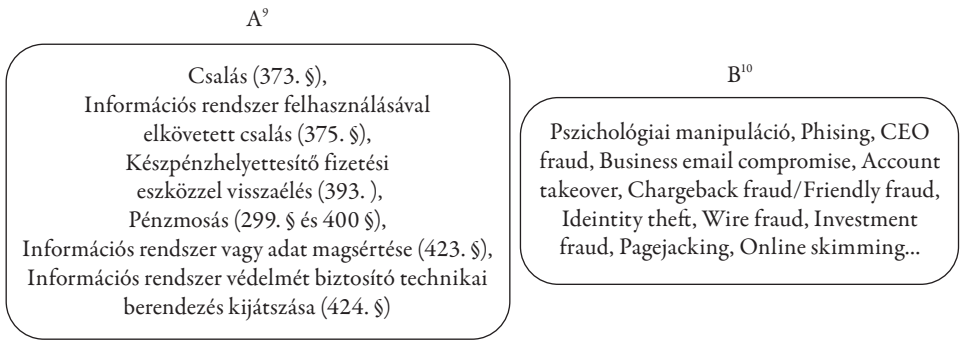
Mielőtt rátérnék a jogi, kriminalisztikai és szociológiai nézőpontú megközelítésekre, szükséges ennek a „trükkös" bűncselekményi körnek a meghatározása. A címben szereplő bűncselekmény-kategória szóösszetételének első alkotóeleme („online fizetés") álláspontom és saját definícióm szerint főként technikai attribútumok alapján a következőképpen írható le tudományos[3] igénnyel. Online fizetésnek tekinthető minden olyan pénzügyi tranzakció, amelyet pénzintézet vagy egyéb, nem készpénzes fizetésre szakosodott pénzforgalmi szolgáltató[4] által biztosított

- eszközzel[5] és/vagy
- platformon[6] vagy számítógépes programon[7] vagy
- egyéb módszerrel vagy eljárással

hajtanak végre, úgy, hogy a pénzmozgással járó művelet feldolgozása/engedélyezése élő internetkapcsolaton alapul.

A szóösszetétel második alkotórésze („kapcsolatos visszaélések") – szemben az első elem jelentős fogalomkör-szűkítő hatásával – szabadságot enged a technológiai fejlődésnek. Ugyanakkor elgondolásom szerint nem a Büntető törvénykönyvben[8] (a továbbiakban: Btk.) rögzített törvényi tényállások, hanem a modus operandi perspektívájába helyezi a szókapcsolatot. Az online fizetéseket és fizetési rendszereket közvetlenül vagy közvetett módon támadó elkövetési módszerek tág értelemben vett főhalmaza nyitott fogalomkör, amelyet alkotóelem szinten kizárólag a Btk. törvényi tényállásainak történő megfeleltetéssel lehet taxatív listába rendezni.

[2] A legelismertebb hír- és adatforrás a bankkártya-, feltöltőkártyás és mobilfizetési iparágakkal kapcsolatban.
[3] Az online fizetés definíciója a pénzügyi szektorban elég változatos, sokszor inkább példálózó jellegű. Ugyanakkor az új technológiákra figyelemmel változó fogalom.
[4] Ideértve a kriptovaluta-kereskedésre szakosodott szolgáltatókat és online fizetési rendszereket, például: PayPal.
[5] Ideértve az eszközhöz kapcsolódó adatokat. Tipikusan készpénz-helyettesítő fizetési eszközök.
[6] Például: weboldal.
[7] Például: mobilapplikáció.
[8] A Büntető Törvénykönyvről szóló 2012. évi C. törvény.



1. ábra: Az online fizetéssel kapcsolatos visszaélések csoportosítása
Forrás: a szerző szerkesztése

Összegezve és leegyszerűsítve az online fizetésekkel kapcsolatos visszaélésekre jelenleg nincs közmegegyezésen vagy jogszabályon alapuló általános definíció. Ez egy általam használt hibrid elnevezés, amelynek életre hívása éppen azért szükséges, mert olyan elkövetéseket foglal magában, amelyek a rendészetet feltehetően átfedésben levő jogi, kriminalisztikai és szociológiai kihívásokkal szembesítik, így azt remélem, újszerű eredményre vezet együttesen vizsgálni őket. Más, de egyáltalán nem elhanyagolható érvem, hogy az FBI IC3[9] 2023-as évre vonatkozóan kiadott internetes bűnözési jelentésében (FBI 2024: 20–21) a sértettek számát alapul véve a top 10 bűncselekményből 5, míg az okozott kár összeget alapul véve a top 10 bűncselekményből 4 sorolható az online fizetésekkel kapcsolatos visszaélések körébe.

Szintén megjegyzendő, hogy az Europol által legújabban használt terminológia szerint külön kategóriának tekintik az online csalásokat *(online fraud schemes)* és a fizetési csalásokat *(payment fraud),* amely utóbbit a kiberbűncselekmények közt jegyzik, és főként a készpénz-helyettesítő fizetési eszközzel visszaéléseket értik alatta. Az online csalások közt találhatjuk a különböző adatszerzéseket *(phising),* befektetlési csalásokat *(investment fraud),* a romantikus csalásokat *(romance fraud)* és a különböző megtévesztő üzleti e-mailes csalásokat *(CEO fraud),* valamint a saját ügyfél megtévesztő magatartásán alapuló csalásokat *(chargeback fraud vagy friendly fraud)* (Europol 2024). Az általam jegyzett fogalomkörbe mindez értelemszerűen beletartozik, amennyiben a bűncselekmény célzataként akár önkéntes, akár csalárd úton megvalósuló online fizetésre kerül sor.

A bevezetést lezárandó a jelen cikk alapját képező kutatás alternatív elméleti keretét tekintve a klasszikus tudományos kutatási módszerek körén kívülről indul el a téma szubjektivizált[10] bemutatásával és feldolgozásával.

[9] Federal Bureau of Investigation – Internet Crime Complaint Center (Szövetségi Nyomozó Iroda – Internetes Bűncselekmények Panaszközpontja).

[10] William Faulkner Nobel-díjas író úttörőként a szépirodalom területén alkalmazta, míg Quentin Tarantino Oscar-díjas rendező a filmművészetben implementálta az események szubjektivizált bemutatását, azaz ugyanazon események különböző, de egymással összefüggő (sőt interakcióban lévő) nézőpontokból történő bemutatását.

Jogi aspektus

Az elején leszögezhetjük, hogy az online fizetésekkel kapcsolatos visszaélések vonatkozásában sosem volt és sosem lesz könnyű helyzetben a jogalkotás és az igazságszolgáltatás sem.[11] A teljesség igénye nélkül számba vett és magyar szempontból kötőerővel rendelkező nemzetközi szabályozás sarokpontjai a Budapest Egyezmény,[12] a PSD1[13] és PSD2,[14] valamint a 2019/713 EU irányelv.[15] Ezek szabályozzák a bűncselekménnyé nyilvánítandó cselekményeket, a nemzetközi bűnügyi együttműködés kereteit, és kötelezettséget rónak a privát/szolgáltatói szektor szereplőire is (kiemelten az ügyfélbiztonság, illetve a szolgáltatás biztonságossága vonatkozásában). A jogalkotói cselekvésből jól kitapintható a felismerés, hogy a szolgáltatói szektor együttműködése (értsd: adatszolgáltatása, bűnmegelőzési és biztonságos szolgáltatásra törekvő tevékenysége) nélkül nem lehet eredményesen fellépni a bűnelkövetőkkel szemben.

A jövőre nézve és a fentiekhez képest – mind a jogalkotói reakcióidő, mind a tényleges szabályozási/szakmai tartalom tekintetében – jelentős fejlődést jelent a PSD2 hatáselemzése alapján bevezetni kívánt pénzforgalmi szolgáltatásokra vonatkozó szabálycsomag (PSD3[16] és PSR[17]). Ezt egészíti ki magyar részről a 2024. évi XVIII. törvény[18] (a továbbiakban: online csalások elleni tv.), amely 2024. augusztus 1-jétől hatályos.

A PSD3 és PSR együttesen nagyobb felhatalmazást ad, illetve szabadságot enged a fizetési szolgáltatóknak. Ezen intézkedések közül kiemelendő, hogy 1) hatálybalépésüket követően a fizetési szolgáltatók megoszthatják egymás közt a csalással kapcsolatos információkat; 2) szigorúbb szabályozást követel meg a fizetési rendszerekhez és számlainformációkhoz való hozzáférés területén; 3) valamint még erősebb ügyfél-hitelesítési előírásokat ír elő.

Ugyanitt kell kiemelni az Európai Parlament és a Tanács 2023/1543 számú rendeletét[19] (a továbbiakban: Elektronikus bizonyíték rendelet), amely a jogi aktus típusára tekintettel Magyarországra nézve közvetlen hatályú (nem szükséges a rendelet

[11] A jogalkotás a szabályozandó terület állandó változása, míg az igazságszolgáltatás a későbbiekben kifejtett felderítési és bizonyítási nehézségek okán.

[12] Az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye, amelyet hazánkban a 2004. évi LXXIX. törvény implementált, hirdetett ki.

[13] Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról. Hatályban volt 2018. január 12-ig.

[14] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról.

[15] Az Európai Parlament és a Tanács 2019/713 (2019. április 17.) irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről.

[16] Az Európai Parlament és a Tanács irányelve a belső piaci pénzforgalmi szolgáltatásokról és elektronikuspénz-szolgáltatásokról, a 98/26/EK irányelv módosításáról, valamint az (EU) 2015/2366 és a 2009/110/EK irányelv hatályon kívül helyezéséről (javaslat, Brüsszel, 2023. június 28.).

[17] Az Európai Parlament és a Tanács rendelete a belső piaci pénzforgalmi szolgáltatásokról és az 1093/2010/EU rendelet módosításáról (javaslat, Brüsszel, 2023. június 28.).

[18] Az online csalások elleni fellépés érdekében szükséges törvények és egyéb büntetőjogi tárgyú törvények módosításáról szóló 2024. évi XVIII. törvény.

[19] Az Európai Parlament és a Tanács 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról.

implementációja a hazai jogba). Ugyan elfogadott és hatályos rendeletről van szó, de a 34. cikk (2) bekezdésére figyelemmel csupán 2026. augusztus 18. napjától alkalmazandó, így ezt is a jövőbe mutató kategóriába sorolhatjuk. Nem túlzás azt állítani, hogy új időszámítás kezdődik jövő év augusztus közepén, mert ez az uniós rendelet két erős fegyvert (ti. a közlésre kötelező európai határozat és megőrzésre kötelező európai határozat; a továbbiakban: KKEH és MKEH) ad a bűnüldözési és igazságszolgáltatási szervek kezébe. A KKEH és az MKEH legfontosabb jellemzője, hogy részletesen szabályozott keretek közt, de immár lehetőség nyílik az Európai Unió tagállamában letelepedett vagy képviselettel rendelkező szolgáltató közvetlen megkeresésére tíznapos általános és nyolcórás soron kívüli válaszadási kötelezettséggel. A kikérhető adatok körét az Elektronikus bizonyíték rendelet a 3. cikk 3. pontban említett szolgáltatásokhoz kapcsolódó adatokban (főként internet- és elektronikus hírközlési szolgáltatási adatok) határozza meg. Emellett az adatokat a személyes szférába történő beavatkozás mértéke alapján rangsorolja, s ehhez igazodóan írja elő a hozzáféréshez szükséges súlyú – például legalább három év szabadságvesztéssel fenyegetett – bűncselekmény gyanúját. Figyelemre méltó, hogy a jogszabály kiemelt bűncselekményként tekint a készpénz-helyettesítő fizetési eszközzel visszaélésre és az információs rendszer felhasználásával elkövetett csalásra.

A nemzeti hatáskörben meghozott és Magyarországon hatályos online csalások elleni tv. két kiemelten fontos intézkedése nem akkora horderejű, mint az előbbi uniós rendelet, mégis egyértelmű jelzés arra nézve, hogy a bűnüldözési kapacitások és képességek támogatásra szorulnak. Az ügyészi jóváhagyást igénylő adatkérések körének leszűkítésével a rendészeti szervek adatkérési ideje is lerövidül, mivel ezen esetekben már nem szükséges a gyakorlatban szükségképpen időveszteséggel járó ügyészi jóváhagyás bevárása. Emellett a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) 9. § (2) bekezdésével együttesen értelmezve az online csalások elleni tv. 35. szakasza „megteremti annak lehetőségét, hogy hatósági szankció kilátásba helyezése nélkül is megkereshetők legyenek különféle szervezetek, az általuk önkéntesen adható adatok megszerzése érdekében. Ebben az esetben az adatszolgáltatás jogalapja nem a hatósági kötelezés, hanem a megkeresett szervekre vonatkozó magánjogi rendelkezések alkalmazása, különösen a megkeresett szerv és a vele szerződött ügyfél közötti megállapodásban foglalt rendelkezések, ideértve a megkeresett szerv általános szerződési feltételeit, üzletszabályát is."[20] Hozzáteszem, hogy álláspontom szerint az adott szolgáltató polgári úton perelhetővé válik, ha az adatszolgáltatás elmaradása és a bűncselekményből eredő kár megtérülése között ok-okozati összefüggés állapítható meg. Ebből a perspektívából nézve mégsem tét (szankció) nélküli a hatósági megkeresés negligálása.

Helyes tehát az irány, az önkéntes alapú adatszolgáltatás azért hangsúlyozottan fontos, mert a szolgáltatói szektornak gyakran nem (csupán) a motiváció, hanem a jogi felhatalmazás hiánya (ti. különféle titoksértésektől vagy személyes adatok megsértésétől való félelem) jelentette az akadályt az egymással vagy a nyomozó hatósággal történő közös fellépésben.

A fentiek tükrében dicséret illeti a jogalkotókat (EU- és nemzeti szinten egyaránt), de hátradőlni sajnos nincs ok, előrelépés szükséges az adatkérések szintjén, méghozzá két

[20] Részlet az online csalások elleni tv. 35. §-hoz fűzött indoklásából.

irányban. Az adatok beszerzésének időtartamát tovább kell csökkenteni, míg a megkereshető szolgáltatók földrajzi lefedettségét növelni kell az EU határain kívülre is.

Hogyan lehet érdekeltté tenni a szolgáltató szektort az önkéntes együttműködésben? Az ügyfélbizalom lehet az egyik kulcs. Meggyőződésem, hogy a pénzügyi ágazat felügyeletét ellátó szerv által nyilvános, megbízható szolgáltatói védjegy hozható létre az online fizetési körben, ami a rendészeti vagy más hatósági szervekkel történő együttműködést deklarálja. Az ügyfél eldöntheti, hogy egy saját vagy más személy sérelmére elkövetett bűncselekmény esetén a biztonságosabb vagy a kevésbé biztonságos szolgáltatót választja (előbbi esetben nagyobb eséllyel térülhet meg a kár[a]). Nyilván, amennyiben nem működik együtt a szolgáltató, az is vonzó lehet bizonyos ügyfélkörnek (leginkább a bűnelkövetői körnek), de így lassan, piaci alapon válhatnak szét a prudens és szürke vagy fekete zónában működő piaci szereplők. Hozzá kell tennem, hogy ez a védjegy típusú megkülönböztetés főként demokratikus keretek között működő országokban lehet vonzó a felhasználók számára.

Szintén a jogi szabályozás területéhez tartoznak a szervezett bűnözéssel, illetve a bűnszervezet kibertérbeli megállapíthatóságával vagy épp meg nem állapíthatóságával összefüggő szempontok. Egytértek Mezei Kittivel abban, hogy „a kiberbűnözői csoportok [...] természetüknél fogva nehezen illeszthetőek be a szervezett bűnözés hierarchikus, homogén struktúrájába" (Mezei 2020: 256). Gyakran ugyanis minden egyéb, a Btk. 459. § (1) bekezdés 1. pontjában meghatározott feltétel teljesülése ellenére sem állapítható meg a bűnszervezetben történő elkövetés (vagy részvétel), mivel a „hierarchikusan szervezettség" mint attribútum hiányzik. Az online térben szerveződött laza együttműködések tehát nem felelnek meg a szervezett bűnözés fogalmának, azonban komoly társadalmi veszélyt jelentenek, és jelentős károkat okoznak (Leukfeldt–Lavorgna–Kleemans 2017).

Amennyiben a jogszabályi definíció csupán egyetlen elemével lenne probléma, akkor a szervezett bűnözés fogalommeghatározásának módosítása, kiegészítése, pontosítása mellett érvelnék. Azonban az online fizetésekkel kapcsolatos visszaélések zászlóshajója, a készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. szerinti információs rendszer felhasználásával elkövetett csalás) alapesete mindössze három évig terjedő szabadságvesztéssel büntetendő. Ráadásul az ilyen típusú bűncselekményt elkövető szervezett csoportok átlagos működési ideje Mátyás Szabolcs 2018-as tanulmánya szerint alig több mint négy hónap (Mátyás 2018: 164). Így tulajdonképpen ezekkel együtt már három szükségképpeni elem megléte is kérdéses a bűnszervezet megállapíthatóságához.

Amennyiben a vizsgált cselekmény nem éri el az ötéves büntetési tételt, és a bűnszervezetben történő elkövetést mint minősítő körülményt sem lehet alkalmazni, továbbá a hároméves büntetési tételt elérő cselekménnyel kapcsolatban pedig egyéb okokból nem állapítható meg az üzletszerű vagy bűnszövetségben történő elkövetés, akkor a bűnelkövetővel (eljárásjogi terminológiával gyanúsítottal) szemben a Be. alapján nem vethetők be a bírói engedéllyel alkalmazható leplezett eszközök. Következésképpen egy társdalom számára veszélyes jelenséggel szembeni arányos rendészeti fellépés lehetősége vész el.

Meg kell jegyezni azt is, hogy az online fizetésekkel kapcsolatos visszaélések nem feltétlen, ám gyakori, mondhatni természetszerű velejárója a pénzmosás, amelynek a Kúria Bvf.I.830/2017 számú határozata szerint térben és időben el kell különülnie az alapbűncselekménytől. Ez esetben viszont a legalább ötévi szabadságvesztéssel büntetni rendelt

pénzmosás kapcsán alkalmazhatóvá válnak az általam hiányolt leplezett eszközök. Persze korántsem bizonyos, és gyanú szintjén sem feltétlenül állapítható meg, hogy az alapbűncselekmény és a pénzmosás elkövetője egy és ugyanazon személy, ellenben ennek az elvi s gyakorlati lehetősége sem kizárt.

Tizenöt-húsz évvel ezelőtt még komoly viták folytak a hazai jogalkalmazásban (a rendőrség-ügyészség-bíróság tengelyben) arról, hogy az akkor még készpénz-helyettesítő fizetési eszközzel visszaélés (ma információs rendszer felhasználásával elkövetett csalás) bűncselekménynek kit tekin(s)tünk sértettjének? Kialakult ugyanis egy olyan gyakorlat, hogy a nyomozó hatóság a bankkártya-kibocsátó pénzintézetet jelölte meg sértettként a gyanúsítások során. Amennyiben több kibocsátó bankot érintett a visszaélés, akkor a rendbeliséget is a kibocsátó bankok száma határozta meg, az azonos bank sérelmére elkövetett cselekmények elkövetési értékei (a minősítés szempontjából és a folytatólagos egységre figyelemmel) pedig összeadódtak. Ezen típusú megközelítés alapja az volt, hogy akkoriban tipikus elkövetési forma volt az úgynevezett skimming,[21] amely során a világ különböző pontjain megszerzett bankkártyaadatokkal egy teljesen másik helyen (országban) éltek vissza. Ilyen esetben egyértelműen a sértetti érdekkörön kívüli okból történt az adatszerzés, azaz maga a sértett semmilyen tőle elvárható módon nem tudta volna azt megakadályozni. A „hiba" tehát a szolgáltatónál történt, az ő biztonsági intézkedését játszotta ki az elkövető, így a keletkezett kárért automatikusan a bankkártya-kibocsátó pénzintézet felelt. Amennyiben nem a kibocsátó bankot tekintik sértettnek, rendkívül nehézkes (jogsegély útján időigényes és nem feltétlenül eredményes) lett volna a sértettek megszólítása (kihallgatása vagy egyéb formailag helyes nyilatkoztatása). Véleményem szerint ebben a formátumban a bűncselekmény tényálláson belüli minősítése arányban állt az elkövetés súlyával (ti. kárértékkel), azaz a károsszeg Btk. által meghatározott sávok szerinti emelkedésével megnőtt a kiszabható szabadságvesztés időtartama.

Ezzel a régi – lássuk be, jogi és logikai bakugráson alapuló – értelmezéssel szakított a jogalkalmazás, és kialakult az az egyöntetű álláspont, hogy a sértett az a természetes vagy nem természetes személy, akinek vagy amelynek a jogát vagy a jogos érdekét a bűncselekmény közvetlenül sértette vagy veszélyeztette. A bankkártyaszerződés ugyanis egy fizetési számlához kapcsolódó kötelem, amely a jogosult fizetési számlájának egyenlege feletti rendelkezési jogosultságot és lehetőséget biztosítja. A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény (a továbbiakban: Pft.) IX. fejezete alapján a pénzforgalmi szolgáltató helytállása nem feltétel nélküli. A kár jogosulatlan fizetési megbízási teljesítésével már bekövetkezik, ehhez képest a kár tényleges viselése időben elkülönülten történik. Az utólagosnak tekinthető kárviselés érvényesülése tartalmilag a számlatulajdonos kárának megtérítésében realizálódik.

Az újabb, jogi szempontból helyes értelmezés azonban nem feltétlenül várt vagy bekalkulált következménnyel járt. Szemléltetésképpen vegyünk két elméleti példát:

[21] A skimming bankkártyaadatok technikai (mágnescsík-leolvasás és PIN-kód kifürkészésére alkalmas mikrokamera) úton történő jogosulatlan megszerzése tipikusan pénzkiadó automatáknál, esetleg POS-termináloknál. Újabb formája az úgynevezett digital skimming, amelyet ugyanezen az alapelven, de nem pénzkiadó automata „kihasználásával", hanem a kibertérben, online szolgáltatók fizetéssel kapcsolatos biztonsági intézkedéseinek kijátszásával hajtanak végre.

Az első esetben az elkövető hat hónapos időtartam alatt 150 darab, különböző személyekhez köthető bankkártya adatainak jogosulatlan felhasználásával követ el visszaéléseket (hajt végre online tranzakciókat), bankkártyánként (mögöttes számlatulajdonosonként) egységesen 400 ezer Ft kárt okozva. A bűncselekmény minősítése ebben az esetben a Btk. 375. § (5) bekezdésébe ütköző és az (1) bekezdés szerint minősülő információs rendszer felhasználásával elkövetett csalás bűntette (alapesete), amely bűncselekmény büntetési tételének felső határa három év szabadságvesztés. Az alapeseti tényállás ugyanis 500 ezer Ft károkozásig nem veszi figyelembe az üzletszerűséget (és a bűnszövetséget sem) mint felminősítő körülményt. Az összesített kártérték 60 millió forint, az elkövetés egyébként megfelelne az üzletszerűség megállapításához, de mindez kizárólag a büntetés kiszabásánál lehet szempont, azaz a büntetés – a Btk. halmazati büntetésre vonatkozó rendelkezéseire figyelemmel – legfeljebb a négy év hat hónapos tételt érheti el.[22]

A második esetben az elkövető egyetlen bankkártya adatainak jogosulatlan felhasználásával követ el egyetlen visszaélést, amivel 5 050 000 Ft kárt okoz[23]. A bűncselekmény minősítése ebben az esetben a Btk. 375. § (5) bekezdésébe ütköző és a (2) bekezdés szerint minősülő információs rendszer felhasználásával elkövetett csalás bűntett, amely bűncselekmény büntetési tételének felső határa öt év szabadságvesztés.

Talán többen egyetértenek velem abban, hogy az első példában leírt cselekménynek nagyobb a társadalomra veszélyessége, és az általános igazságérzet szerint súlyosabb cselekmény, mint a második bűneset. (Költői) kérdés, hogy vajon ez volt-e a jogalkotói szándék?

Kriminalisztikai aspektus

Az online fizetésekkel kapcsolatos visszaélések vonatkozásában felmerül, hogy a hagyományosan alkalmazott rendészeti erők/eszközök/módszerek mi módon adaptálhatók a kibertérre. Mielőtt azonban ezt taglalnánk, álláspontom szerint külön kell választani az ilyen típusú bűncselekmények nyomozásának két fő irányvonalát. Egyrészt a sértettközpontú megközelítésben rendkívül fontos az elkövetési (kár)összeg elkövetőnél történő realizálódásának megakadályozása, vagy a kár megtérülésének biztosítása. Másik (cél) halmazt alkotnak az elkövető azonosítása, felelősségre vonása érdekében végzett nyomozási cselekmények.

A pénzvisszaszerzés sikere – figyelemmel a jogi fejezetben már részben kifejtett hazai és nemzetközi szabályozásra – elsősorban a sértetti bűnfelismerési reakcióidőn, másodsorban a sértetthez tartozó pénzforgalmi szolgáltató cselekvési készségén múlik. Ezt követi csupán a rendészeti közbeavatkozás és a rendészeti csatornákon történő tranzakciófelfüggesztés vagy számlazárolás.

[22] A Btk. 81. § (3) bekezdése alapján bűnhalmazat esetén a büntetési tétel felső határa a legmagasabb büntetési tétel felével emelkedik. Jelen esetben tehát a hároméves tételt lehet a felével emelni.

[23] Figyelembe véve a bankkártya-limitációs és egyéb kártyahasználati szokásokat a példa nem túl életszerű, de nem is zárható ki. De ugyanilyen megítélés alá esik, ha az elkövető belép a sértett online bankolási rendszerébe, és 5 050 000-Ft összeget jogosulatlanul utal át magának, ami reálisabb helyzetnek tekinthető.

Vagyonvisszaszerzési szempontból úttörő intézkedésnek számít, hogy az Európai Unió Tanácsa 2024. május 30-án elfogadta a pénzmosás elleni szabályok új csomagját,[24] amely főként a kriptoágazat szolgáltatóira telepít új kötelezettséget, miután kiterjeszti rájuk a pénzmosás elleni szabályokat. Emellett – egyebek között – szigorúbb ügyfél-átvilágítási követelményeket határoz meg (például a kriptovaluta-átváltókra nézve), szabályozza a tényleges tulajdonlás kérdését, valamint 10 ezer eurós felső határt állapít meg a készpénzfizetésekre (Európai Tanács 2024). Mindez azt is jelenti, hogy több mint 16 évvel a Bitcoin megjelenése után[25] jogszabályi kötelezettség alapján a kriptovaluták nyomonkövethetővé, tulajdonosaik azonosíthatóvá válhatnak.

Az elkövető azonosítása (és földrajzi tartózkodási helyének megállapítása) ennél összetettebb, kreatívabb protokollt igényel. Az anonimitást biztosító lehetőségek tárháza jelentős, Amelyről azóta is érvényes, számomra irányadó összefoglaló tanulmányt olvashatunk az *American Behavioral Scientist* tudományos folyóiratban *Eltérések a kiberbűnözés forgatókönyvétől, avagy az anonimitást biztosító online eszközök nyomában* címmel. A szerzők az elkövetői anonimitást biztosító eszközöket proxyalapú szolgáltatások (virtuális számítógépek, VPN[26]-ek és SOCKS proxyk,[27] TOR böngésző,[28] MAC-cím[29] maszkolók), pénzügyi szolgáltatások (kriptovaluták és valutaváltók) és offline (fedő postai címek; postaládák; postafiókok használata) kategóriákba sorolták. A tanulmány a proxyalapú szolgáltatások lényegi céljaként tudatosítja az elkövetésre használt számítógép IP-cím alapján történő nyomonkövethetőségének és magán a számítógépen hagyott digitális ujjnyomatok számának minimálisra szorítását (Van Hardeveld – Webber – O'Hara 2017). Mindezek azt jelentik, hogy a kibertérben fellelhető nyomok a különböző szolgáltatók által tárolt adatokra szűkülnek, azonban a szolgáltatók együttműködése (adatszolgáltatása) korántsem biztosított még Európán belül sem.

A párhuzamos (virtuális) valóságban az elkövetési mozzanatok, műveletek elkülönülten zajlanak a fizikai tértől. E kettő között (ti. kibertér és fizikai tér) kevés átfedés, szűk átjárás van. A nyomozások nehézsége éppen ebben rejlik, mert a cél, hogy az elkövetőt kiszakítsuk a virtuális térből, és olyan környezetbe (valós térbe) helyezzük, ahol vele szemben eljárást és/vagy intézkedést lehet (le)folytatni. A nyomozó hatóság feladata

[24] Az Európai Parlament és a Tanács (EU) 2023/1113 rendelete (2023. május 31.) a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról.

[25] A Bitcoint 2009. január 3-án „bocsátották ki".

[26] A virtuális magánhálózat (Virtual Private Network) egy biztonságos „alagutat" hoz létre a felhasználó és az internet között, elrejtve a felhasználó személyazonosságát és online tevékenységeit.

[27] Olyan kiszolgáló, amely a SOCKS (Socket Secure) protokollt használja az adatok továbbítására. A SOCKS protokoll egy olyan utasításkészlet, amely megszabja, hogy egy kliens hogyan irányíthatja át a forgalmat egy proxyszerveren, miközben a böngészési adatait titkosan és biztonságban tartja. Ez azt jelenti, hogy az eszköz és a meglátogatni kívánt webhelyek között helyezkedik el, így az internetre irányuló kérések először a SOCKS proxyn keresztül mennek keresztül. A SOCKS proxy továbbítja kéréseit a meglátogatni kívánt erőforrás webszerveréhez, így a fogadó szerver csak a proxyszerver IP-címét látja, nem pedig a kliens valódi IP-címét.

[28] Webböngésző, amely lehetővé teszi a felhasználók számára, hogy olyan hálózathoz férhessenek hozzá, amely anonimizálja a webforgalmat, hogy privát böngészést biztosítson. A gyakran az úgynevezett Dark Web eléréséhez használt Tor böngésző elrejti az IP-címeket és a böngészési tevékenységeket azáltal, hogy a webes forgalmat csomópontoknak nevezett különböző útválasztókon keresztül irányítja át.

[29] A MAC-cím (Media Access Control-cím) egyedi azonosító, amelyet minden hálózati eszköz kap, hogy azonosítható legyen a hálózaton belül.

tehát a kibertér geográfiai kivetüléseinek, azaz a kibertér és a fizikai tér metszéspontjainak azonosítása, amely az elkövető valós földrajzi pozíciójának[30] meghatározásán keresztül elvezethet a személyazonosságának megállapításához (mindez persze fordítva is igaz lehet). Az elkövető és az eljárás valós térbe helyezése elengedhetetlen az elkövető által használt mobil-, számítástechnikai vagy egyéb eszközökhöz történő hozzáférés (forenzikus vizsgálat) és kulcsfontosságú bizonyítékok beszerzése szempontjából. Visszatérve a kibertér geográfiai kivetüléseire, érdemes ezen fogalomkör jelentését tisztázni, kezdve azzal, hogy vonatkozásában kizárólag a rendészetileg releváns információkról beszélünk. Geográfiai kivetülés az az információ, amely az elkövető (aktuális vagy egykori) földrajzi pozíciójára vagy mozgására vagy személyazonosságára utaló elektronikus vagy más formátumú adat, vagy cselekvés, amely a kibertérben keletkezett, történt, vagy a kibertérből származik, és a fizikai térhez (a tér egy meghatározható pontjához vagy a tér leszűkített területéhez) közvetlenül vagy közvetett módon társítható.[31] A geográfiai kivetülés tág értelmezésére ad okot, hogy a nyomozás során – figyelembe véve más rendelkezésre álló információkat és azok összevetését – nem csupán egy adott földrajzi pozíció vagy jól körülhatárolható földrajzi terület lehet releváns. Gondoljunk egy termék online megrendelésénél a kiszállításra, ami szintén egyfajta kivetülése a kibertérben lezajlott cselekvésnek, mégis csupán közvetett módon (ti. a csomagküldő szolgálat cselekvésén keresztül) kapcsolódhat az elkövető földrajzi helyzetéhez.

A nyomozás kibertérben kutakodó fázisában adatkérési, információszerzési céllal szükségképpen bevonják a szolgáltató szektort (e-mail-, mobil-, közösségimédia-, pénzforgalmi szolgáltatók stb.). A rendészeti kapacitások és képességek a kibertérben fokozottan korlátozottak. Ezért ezek növelése, vagyis a (köz)feladat hatékony ellátása érdekében az adatszolgáltatáson túlmenően is bevonhatók lennének a bűnüldözési feladatokba a szolgáltató szektor szakosodott szereplői.[32] Jelenleg a Be. alapján (egyedileg) lehetőség van külső szereplő bevonására szakértő kirendelése útján, ám itt indokolt egy magasabb együttműködési szintben gondolkozni. Létező példaként állhat előttünk a 2002-ben az Egyesült Királyságban létrehozott hibrid finanszírozású[33] rendészeti szerv, a Dedicated Card and Payment Crime Unit (a továbbiakban: DCPCU), amely a pénzügyi ágazat elleni – ezen belül kiemelten fizetésekkel kapcsolatos – visszaélések nyomozásáért felelős. A DCPCU szoros együttműködésben dolgozik a finanszírozó (UK Finance[34]) 300 tagszervezetével, amely gyakorlatilag lefedi valamennyi, az Egyesült Királyság területén elérhető pénzforgalmi szolgáltatót. Emellett szintén szoros, operatív munkakapcsolatban állnak a kulcsfontosságú csalás- és kiberbűnözés elleni küzdelemmel foglalkozó szervezetekkel, a távközlési ipar és a közösségi média vállalataival.

[30] Ez a földrajzi pozíció lehet az elkövetéskori, de akár az elkövetést követő pozíció- vagy mozgásspektrum is, illetve ezek átfedésben.

[31] Tipikusan ilyen információ az eszköz azonosítására alkalmas IP-cím, MAC-azonosító, de ilyen információ lehet például egy csalárd módon rendelt termék kiszállítási címe, vagy akár az elkövető által használt e-mail-címmel megrendelt fizikai térben megvalósult szolgáltatás.

[32] Például a piaci alapon működő, magánkézben lévő kiberbiztonsági laborok.

[33] A DCPCU finanszírozását a City of London Police (London Városi Rendőrség), a Metropolitan Police (Főváros Térségi Rendőrség) és a UK Finance (Pénzügyi Szolgáltatások Együttműködési Központja) együtt biztosítja.

[34] A UK Finance az Egyesült Királyság banki és pénzügyi szolgáltatási szektorának brit kereskedelmi szövetsége, amely 2017. július 1-jén alakult.

Az Európai Unió Elektronikus bizonyíték rendelete fényében már nem tűnik teljesen utópisztikusnak egy olyan – első körben EU-n belüli – szabályozás, amely valamennyi online fizetési szolgáltatást nyújtó entitás részére kötelezővé teszi a rendészeti szervek számára 0–24 órában elérhető és azonnali válaszadásra képes adatszolgáltató részleg működtetését. Ez a mesterséges intelligencia robbanásszerű fejlődése mellet az eddiginél jóval költséghatékonyabb módon valósítható meg. A valós idejű reakciót lehetővé tevő, de nyilvánvalóan rendkívül komplex, részletes szabályozást, valamint számítástechnikai értelemben homogén kiépítésű rendszert igénylő bűnmegelőzési és bűnüldözési infrastruktúra kifejlesztésével jelentősen visszaszorítható lenne az eredményes (kárt okozó) és/vagy kármegtérülés nélküli bűncselekmények száma.

Álláspontom szerint számos, néhol némi „átalakítással" kiválóan működő módszer (a korábbi titkos információgyűjtés fogalomhasználata szerinti erő/eszköz/módszer) áll a nyomozó hatóságok rendelkezésére, de ezek tényleges alkalmazási gyakorlata/gyakorisága elmarad a fenyegetettség magas szintjéhez képest. Ilyen módszer például az informátor, a bizalmi személy vagy a nyomozó hatósággal egyéb módon együttműködő személy (a továbbiakban: együttműködő személyek) alkalmazása. Az együttműködő személyek személyazonossága a büntetőeljárás során alapesetben kizárólag a nyomozó hatóság számára (azon belül is korlátozottan) ismert, és a nyomozó hatóság a szakma szabályainak megfelelően ezen anonimitás megtartására törekszik. A kibertérben működő szervezett bűnözői csoportok felderítése és az ellenük történő fellépés eredményessége érdekében megfontolandónak tartom olyan (kiber-)együttműködő személyek alkalmazását, akikkel mind a kapcsolattartás, mind az esetleges javadalmazás online és anonim formában történik. Személyazonosságuk felfedésére még a nyomozó hatóság számára, illetve semmilyen más formában sem kerülhetne sor. A szokatlannak, idegennek tűnő és bizonyos szempontból kockázatos felvetést a kizárólag kibertérben tevékenykedő bűnözők eltérő profilja (személyisége), valamint az ezen személyek együttműködési hajlandóságának emelkedésével arányosan megnövekvő információszerzési képesség igazol(hat)ja.

A büntetőeljárásról szóló 2017. évi XC. törvényben (a továbbiakban: Be.) jól szabályozott sértetti szerepkör eljátszása és/vagy a csapda rendszeres alkalmazása esetén a social engineering,[35] azaz adathalász jellegű bűncselekmények felderítése lehet eredményesebb. Mi több, ez kellő elrettentő erőt is mutathat az elkövetők vagy potenciális elkövetők felé. A sértetti szerepkör végigjátszásával, vagyis a színlelt tévedésbe eséssel az elkövetőre nézve érzékeny adatokhoz juthat közelebb a nyomozó hatóság. Problémát okozhat azonban, hogy a bűncselekmény elszenvedése során nem feltétlenül biztosítható a bűncselekmény tárgyát képező pénzösszeg megtartása, nyomon követése. Itt jegyezném meg azt is, hogy a fedett nyomozó kibertérbe applikálása számos fizikai térben meglévő problémakörtől mentesen valósulhat meg. Dekonspirálódás esetén kizárólag rendőri mivoltára derül fény, azonban ő maga (a személye) nem lepleződik le és nem „kopik el", szinte azonnal

[35] A social engineering csalás egy tág fogalom, amely azokra a csalásokra utal, amelyekben a bűnözők visszaélnek egy személy bizalmával annak érdekében, hogy közvetlenül pénzhez vagy bizalmas információkhoz jussanak egy későbbi bűncselekmény lehetővé tétele érdekében. A közösségi média a preferált csatorna, de nem szokatlan a telefonos vagy személyes kapcsolatfelvétel sem (Interpol [é. n.]).

bevethető másik feladatra. Sőt párhuzamosan több ügyben is tud online feladatokat (vagy feladatokat online) végrehajtani.

A (nyomravezetői) díj kitűzését a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) 27. § (1) bekezdése a felderítési képességet növelő, a nyomozás eredményességét segítő intézkedésként nevesíti és a 91/A. § (1) bekezdés e) pontjában felsorolt bűncselekmények esetében teszi lehetővé alkalmazását. A felsorolásban megtalálhatók az online fizetésekkel kapcsolatos visszaélések, így véleményem szerint a díjkitűzést a kibertérben oly módon (is) biztosítani kellene, hogy arra bárki anonim módon jelentkezhessen, és akár anonimizált formában (kriptovalutában) manifesztálódjon számára a díj. Ez a kiterjesztő és megengedő adaptáció egyúttal kizárná az Rtv. 27. § (2) bekezdésében előírt kizárási ok ellenőrizhetőségét, így jogszabály-módosítási kötelezettséggel járna. Tekintve, hogy a nyomravezetői díj kifizetése polgári jogi értelemben egyfajta eredménykötelem terméke, nem látom annak veszélyét, hogy dupla haszonszerzés céljából anonim módon maga az elkövető jelentkezne a nyomozó hatóságnál. Ugyanakkor egy ezt kizáró jogszabályi rendelkezés megalkotását sem tartanám feleslegesnek.

Tapasztalatom szerint a tipikusan adatszerző jellegű (és csalárd online fizetési visszaélést elősegítő) bűncselekményekhez használt módszereket a nyomozó hatóság maga nem alkalmazza, vagy szintén nem elég széles körben alkalmazza. Gondolok itt a legegyszerűbb, e-mailen keresztül küldött vírusra vagy más, az elkövetői eszköz anonimitását biztosító intézkedések kijátszására képes vagy távoli rejtett hozzáférést biztosító egyéb számítástechnikai programra. Az elkövetők ugyanis szinte minden általuk kibertérben (fel) használt segítő szolgáltatáshoz (e-pénztárcák, kriptovaluta-váltó és -kereskedő platformok, azonnali üzenetküldő alkalmazások) és a sértettekkel történő csalárd szándékú kapcsolatfelvételhez/kommunikációhoz is tipikusan e-mail-postafiókot használnak. Mindez növeli saját sérülékenységüket, amit a nyomozó hatóságnak a Nemzetbiztonsági Szakszolgálat közreműködésével érdemes lenne rendszerese(bbe)n tesztelni, kihasználni.

A proaktivitásra reflektálva idekívánkozik, hogy az Európai Unió Rendőrségi Hivatala 2017-ben első ízben tartotta meg a Cyber-patrolling Week[36] elnevezésű műveletét, amely az online térben kiemelten veszélyes bűncselekmény-területekre – elsők közt a fizetési visszaélésekre – fókuszált. Azóta állandó kiberjárőrözési tevékenységre szakosodott rendőri erővel rendelkezik az indonéz rendőrség, míg a hongkongi rendőrség különböző egységei a bűnmegelőzés és felderítés érdekében az internet nyilvános felületein folytatnak rendszeres kereséseket bűncselekményekkel (például csalárd banki honlapok, illegális sportfogadási tevékenységek, gyermekpornográfia, kábítószer-kereskedelem) összefüggő adatokra vonatkozóan.

Szociológiai (bűnmegelőzési) aspektus

Számos tanulmány (például Peersman et al. 2024) foglalkozik a kibertérben tevékenykedő bűnelkövetők hátterével, motivációival, illetve az elkövetési hajlamra ható tényezőkkel. Ezek közül kiemelendő az anyagi haszonszerzés, a gazdasági nehézségek (beleértve

[36] Kiberjárőrözési hét.

a munkanélküliséget), az online közösségek támogató szubkultúrája (szélsőségesen az elkövetők dicsőítése), az anonimitás (alacsony mértékű lebukási veszélyérzet) és a fejlett technikai tudású egyének jelenléte.

A tanulmányok hangsúlyozzák, hogy az online fizetésekkel kapcsolatos visszaéléseket nem lehet kizárólag egyéni erkölcsi kudarcoknak tulajdonítani, hanem tágabb társadalmi kontextusban kell értelmezni. Az olyan tényezők, mint a rendszerszintű egyenlőtlenség, az oktatáshoz való hozzáférés hiánya és a vagyon felhalmozását előtérbe helyező társadalmi normák hozzájárulnak a csalárd magatartások igazolásához. Sőt, az online közösségek szerepe az identitásformálásban és az összetartozás-érzés kialakulásában is hangsúlyos. Ezek a virtuális közösségi terek tehát nem csupán technikai támogatást kínálnak, a tagok morálisan legitimizálják egymás cselekedeteit, csökkentve ezzel a bűntudat vagy a megbánás érzését.

A fentieket kiegészítendő a félelem (az elkövető által sugalmazott következménytől), a kapzsiság, a tájékozatlanság és a hiszékenység mind olyan alapvető sértetté válást befolyásoló tényezők, amelyekkel szemben ellenálló képességgel kizárólag a tudatos felhasználók rendelkeznek.

Kapcsolódó problémakörként azonosíthatók a különböző tömeges felhasználói profilok létrehozására (és az ezekkel történő különböző interakciókra) szakosodott és a kibertérben megvalósuló felhasználói interakciókra jelentős hatást gyakorló úgynevezett mobilfarmok. A több (akár ezres nagyságrendű) mobilkészülék egyidejű, valós irányítására alkalmas hálózat megtévesztő célokat szolgál. Ezek közé tartozhat a népszerűség színlelése (nézettség, kedvelések, kommentek generálásával, valamint a követők számának növelésével) és a jogszerű, biztonságos tevékenység/működés illúziójának megteremtése.

Magyarországra fókuszált statisztikák szerint

- 2024 harmadik negyedévében közel 10,3 millió kibocsátott fizetési kártya volt forgalomban (*A fizetési kártyák száma a negyedév végén* 2024);
- az internethasználók aránya 2023 évben (a 16–74 éves népesség százalékában) – az EU átlaggal pontosan megegyezően – 91% volt (KSH 2024);
- 6,2 millióan használnak okostelefont és nagyjából 6 millióan interneteznek mobiltelefon-készüléken a 18–69 éves korosztályban – derült ki az eNET legújabb reprezentatív kutatásából (MTI 2022);
- az internetezők 44%-a online bankolásra (is) használja a világhálót (NMHH 2023).

A fenti számok és azok következetesen emelkedő tendenciája határozza meg a céltábla nagyságát, azaz az elkövetők számára szinte minden második magyar állampolgár célpont lehet valamilyen szempontból. Képletesen szólva nem szükséges tűpontos „lövéseket" leadni, hogy ezen potenciális sértettek elérhetővé váljanak. Az, hogy nagy(obb) számban eredményes a megtévesztés, arányosan következik a nagyobb számú sértetti elérésből és a jelenleg leginkább veszélyt jelentő pszichológiai manipuláción és megtévesztésen alapuló adathalászat kifinomult módszereiből.

A social engineering terjedése mutatja, hogy az online fizetésekkel kapcsolatos bűncselekmények célkeresztjébe ismét az ember(i) (tényező) került. Nem véletlenül. A jogi aspektusban kifejtett nemzetközi és hazai szabályozás a szolgáltatók ügyfél-azonosítási

és tranzakció-jóváhagyási protokolljainak szigorítását eredményezte, ezáltal az elkövetők közkedvelt kifejezéssel élve a leggyengébb láncszem/ellenállás felé terelődtek. Nem szükséges az erős, bonyolult technikai intézkedések kijátszása, ha maga a sértett adja meg az érzékeny adatokat. Az elkövetői kör tehát gyorsan adaptálódik, változtat, és természeténél fogva is rugalmasabb, mint az erre reagáló jogalkotási vagy igazságszolgáltatási gépezet.

Ismét kiemelendő, hogy a felhasználói tudatosság, a potenciális sértettek önvédelmi reflexeinek kialakítása minden eddiginél fontosabb, hangsúlyos szerepet követel. Gondolok itt arra, hogy a megtévesztés eszköztára a deepfake-jelenség[37] és a mesterséges intelligencia párosításával már nem csupán a figyelmetlen, idős vagy tapasztalatlan állampolgárokra jelent különös veszélyt. Ezt támasztja alá az FBI IC3 2023. évre kiadott internetes bűnözési jelentése (FBI 2024: 17), amelyben a bejelentők, azaz a bűncselekmény áldozatául esettek száma alapulvételével képzett statisztika nem mutat szignifikáns eltérést a 20 és 60 év közötti korcsoportokon belül (62 ezer és 88 ezer között mozog a négy korcsoport bejelentési átlaga). Ugyanez a statisztika jelentős negatív irányú kilengést mutat a 20 év alatti korosztálynál (16 ezer bejelentés), míg ellentétes kilengés tapasztalható a 60 évnél idősebb korosztálynál (100 ezer bejelentés).

A felhasználói tudatosság növelése tehát kapacitásmegtakarítást eredményez mind a rendészeti, mind a szolgáltatói szektorban. Láthatunk egy erre az érdekközösségre alapozó kiváló kezdeményezést, amelyet Kiberpajzs[38] néven többek közt a Magyar Nemzeti Bank, a Bankszövetség és az Országos Rendőr-főkapitányság hozott létre. Kérdés, hogy a platform képességei milyen tényleges ügyfélelérési lehetőséget biztosítanak, vajon letörhető-e a pszichológiai manipulációval okozott károsszeg standardnak látszó magas száma?

Az online fizetésekkel kapcsolatos visszaélések további facilitátora az elkövető oldaláról az internetes technológiák proliferációja (köszönhetően a Darkneten elérhető fórumokon szerveződött „szabadegyetemeknek”[39]), míg a sértett szempontjából az, hogy az új technológiák hozzáférhetősége, használata megelőzi, ha tetszik beelőzi az ezen technológiákkal kapcsolatos felhasználói tudatosság kialakulását vagy megszerzését. Hozzáteszem, a mesterséges intelligencia abszolút térnyerése ez esetben nem kizárólag az elkövetések kifinomultságában, hanem a (potenciális) sértetti elérések számában is megmutatkozik.

[37] Deepfake alatt az olyan médiatartalmat értjük, amelyben egy személy vonásait mesterséges intelligencia segítségével úgy módosítják, hogy az valaki másnak tűnjön. A kifejezés a deep learning és a fake kifejezések kombinációja. Az alkotó tehát szándékosan akarja megtéveszteni a befogadót, és ehhez gépi tanulást és mesterséges intelligenciát használ (Magony 2023).

[38] „[A]z MNB mellett a Magyar Bankszövetség (mint a hazai bankok érdekképviseleti szerve), az Országos Rendőrfőkapitányság, a Nemzetbiztonsági Szakszolgálat, a Nemzeti Kibervédelmi Intézet, valamint a Nemzeti Média- és Hírközlési Hatóság 2022 őszén KiberPajzs néven közös kommunikációs és edukációs kampányt indított, amelyhez időközben az Igazságügyi Minisztérium, a Szabályozott Tevékenységek Felügyeleti Hatósága, a Magyar Államkincstár és a Nemzetgazdasági Minisztérium is csatlakozott. A szervezetek az együttműködés során folyamatosan vizsgálják a fogyasztói szokásokat, azok változásait, valamint a pénzügyek, illetve a pénzforgalom lebonyolítása kapcsán megfigyelhető visszaélési mintázatokat és kiberbiztonsági kockázatokat” (forrás: https://kiberpajzs.hu/a-kezdemenyezesrol). Megjegyzés: Azóta további jelentős csatlakozók is voltak, mint például a Nemzeti Védelmi Szolgálat, a Szerencsejáték Zrt. vagy a Mastercard.

[39] A Darknet-fórumokon a felhasználók nem csupán illegális kereskedelemmel (bankkártyaadatok, kábítószer, drogok), de egymás okításával is foglalkoznak. Teljes és részletes metodikai leírások, ehhez kapcsolódó tanácsok érhetők el, amelyek alapján alapfokú számítástechnikai ismeretekkel lehet bűncselekményeket véghez vinni.

A Magyar Nemzeti Bank által vezetett statisztika szerint a 2024. év III. negyedévében az elektronikus pénzforgalomhoz kötődő visszaélések kapcsán az ügyfélre terhelt károsszeg elérte a mindösszesen közel 5 milliárd forintot[40] (*Az elektronikus pénzforgalomhoz kötődő visszaélések kapcsán lekönyvelt kár megoszlása az ügyfelek és a pénzforgalmi szolgáltatók közt* 2024). Ezzel szemben a pénzforgalmi szolgáltató által viselt kár „csupán" 140 millió forint volt. Fontos leszögezni, hogy a hivatkozott károsszegek nem kizárólag a social engineering útján megvalósuló bűncselekményeket tükrözik, de a Pft. IX. fejezetében meghatározott kárfelelősségi szabályokból – miszerint az ügyfél felel a kárért a súlyosan gondatlan magatartás tanúsítása esetén – már következtetni lehet, hogy a közel 5 milliárd forintos károsszegben jelentős mértékben van jelen a pszichológiai manipuláción alapuló adathalászattal okozott kár. Ellenőrizve ezt a feltevést, a tárgyi statisztika szerint a jelen bekezdésben hivatkozott 5 milliárd forintból körülbelül 2,2 milliárd forintért felelős a social engineering, de ugyanitt az is kiolvasható, hogy a 2023. év I. negyedévéhez képest 2024 III. negyedévére, tehát szűk két éven belül több mint négyszeresére nőtt a pszichológiai manipuláción vagy megtévesztésen alapuló, elektronikus pénzforgalomban bekövetkezett sikeres visszaélések által okozott kár (*Az elektronikus pénzforgalomban bekövetkezett sikeres visszaélések* 2024).

Hogyan lehetne hatékonyabb a bűnmegelőzés? Egyrészt a meglévő tudatosságépítő anyagok és figyelemfelhívó információk célközönséghez történő eljuttatása terén lehet fejlődési potenciál. Az idősebb generáció tagjai nem feltétlenül az online térből tájékozódnak, inkább a hagyományos médiafelületeket (televízió) követik. Gondoljunk bele, hogy a Covid-járvány idején a köztelevízióban folyamatosan sugárzott tartalom következtében kis túlzással nem volt olyan, aki ne tudta volna a helyes kézmosás szabályait (más kérdés, hogy alkalmazta-e). Másrészt a felnövekvő generációk, a gyermekek vonatkozásában megfordítható lenne a modern technológiák használata és a használati tudatosság kialakulásának időbeli sorrendje. A Nemzeti Alaptanterv részeként, a kibertudatossággal foglalkozó összetett tantárgy oktatása indokolt lehet már általános iskolás kortól azzal, hogy annak egyik tematikus eleme lehet a kiberbiztonsággal, ezen belül online fizetésekkel kapcsolatos ismeretek megszerzése. Nemzetközi kitekintésben találhatunk ez irányú törekvéseket és példákat. Dél-Ausztráliában középiskolás diákok számára a tanterv reformjának részeként idén vezették be az online biztonságról és a közösségi média veszélyeiről szóló tantárgyat (Government of South Australia 2024), míg Vietnámban már a 2021/22-es tanévtől kezdve valamennyi állami iskolában a védelem és biztonság elnevezésű tantárgy keretében oktatják a kiberbiztonságot (VNA/VNP 2021). Észtország egy 2007-ben sérelmére végrehajtott komplex kibertámadást[41] követően kiberbiztonság szempontjából a világ egyik legerősebb oktatási rendszerét építette ki egészen az óvodáskortól kezdődően az egyetemi tanulmányokig bezárólag (*Cyber security education in Estonia: from kindergarten to NATO Cyber Defence Centre* 2022).

Végül ne feledkezzünk meg arról, hogy a szolgáltatói szektornak (is) elemi érdeke, hogy még előkészületi vagy kísérleti szakban szűrje ki a csalárd pénzügyi tranzakciókat.

[40] Pontosan 4 856 850 830 forint.

[41] A támadássorozat következtében a kormányzati és pénzügyi szektor, valamint az online média szinte teljes palettája vált elérhetetlenné.

Ezt jellemzően a felhasználói szokásokon alapuló és a mesterséges intelligencia által elemzett adatok segítségével végzik. Ilyen, a felhasználó szokásos tevékenységi sablonjától eltérő, csalárd műveletre utaló adat lehet: az eltérő eszközről történő belépés vagy belépés rövid időn belül eltérő eszközökről; a belépés ismeretlen vagy gyanús IP-címről; a felhasználói profiladatok hirtelen megváltoztatása; a belépés távoli földrajzi helyről; a rövid időn belüli sorozatos alacsony összegű tranzakciók; a sorozatos belépési kísérletek (Berger 2024).

Konklúzió

Összegzésképpen megállapítható, hogy a kibertérben az elkövetők az anonimitást biztosító és konspirációs eszközök alkalmazásával, valamint a fragmentált földrajzi lefedettségű nemzetközi jogi szabályozás révén, továbbá geopolitikai okokból eredően a jelenlegi nem egységes nemzetközi bűnügyi együttműködést biztosító környezetben helyzeti előnyből indulnak.

Kiemelt problémakörként azonosítható a fentieken túl a felgyorsult technológiai fejlődés, amelyet nehezen követnek le mind a jogi szabályozók, mind a rendészeti képességek. Valamint a bűnüldözési kapacitás korlátozottsága, amit főként a bűnmegelőzés eredményességével lehet(ne) ellensúlyozni.

Számomra mindebből az következik, hogy az online fizetésekkel kapcsolatos visszaélések területén (is) a reaktív helyett proaktív, a szolgáltatókkal magas szinten együttműködő bűnüldözési modellnek kell(ene) érvényesülnie.

Írásom célja ezáltal olyan tényezők és összefüggések szemleszerű felvillantása, amelyek kihatással vannak az elkövetői és bűnüldözői oldal közti egyensúlyra vagy fegyveregyenlőségre.

A kibertér mint bizonyos értelemben fizikai és virtuális határok nélküli[42] dinamikusan változó halmaz – a fizikai térrel szemben – kevésbé alkalmas a viszonylagos meghatározásokra (ezáltal különféle beazonosításokra). A jog hagyományosan kialakult fogalomrendszere, mint például a (területi, személyi, tárgyi) hatály, a személyiségi jogok, vagy éppen a kikényszeríthetőség teljesen másképpen értelmezhetők és érvényesíthetők. De máshogyan kell-e felderítést/nyomozást végezni, vagy bűnmegelőzési tevékenységet folytatni? A kibertér tágan vett történései mindenképpen kivetülnek az általunk ismert fizikai térben? Kutatásomban – fókuszálva az online fizetésekkel kapcsolatos visszaélésekre – többek közt ezen kérdéseket kívánom körüljárni.

Befejezésképpen ideillőnek tartok megosztani egy jogászberkekben jól ismert anekdotát és az anekdota jelen korra aktualizált átiratát: Pólay Elemér[43] jogászprofesszor egyetemi előadásán megkérdezte diákjait: ha kinéznek az ablakon, mit látnak? Sokféle választ kapott, de a legfrappánsabbat végül ő maga adta: „Ott (szerk.: odakint) jogalanyok és jogtárgyak vannak."

[42] Itt jegyzendő meg, hogy közismert becslések szerint a kibertéren belül a nyíltan elérhető úgynevezett surface web nagyjából 5%, míg az általános keresők által nem indexált tartalmat reprezentáló Deepweb és a sokszorosan titkosított Darknet együttesen körülbelül 95% „teret" foglal el.

[43] Pólay Elemér 1949-től 1985-ig a Szegedi Tudományegyetem Állam- és Jogtudományi Karának nemzetközileg elismert vezető professzora.

Amennyiben rendőr hallgatók részére tennék fel a kérdést, hogy mit látnak, ha „körülnéznek” az interneten, Pólay Elemér nyomán válaszuk így hangzana: Sértetteket és (bűn)elkövetőket!

Felhasznált irodalom

A fizetési kártyák száma a negyedév végén (2024. szeptember 30.). A szerző adatigénylése a Magyar Nemzeti Banktól.

Az elektronikus pénzforgalomban bekövetkezett sikeres visszaélések (2024. szeptember 30.). A szerző adatigénylése a Magyar Nemzeti Banktól.

Az elektronikus pénzforgalomhoz kötődő visszaélések kapcsán lekönyvelt kár megoszlása az ügyfelek és a pénzforgalmi szolgáltatók közt (2024. szeptember 30.). A szerző adatigénylése a Magyar Nemzeti Banktól.

Berger, Burkhard (2024): *How to Use Behavioral Analytics to Understand & Prevent Fraud*. Online: https://www.chargeflow.io/blog/use-behavioral-analytics-prevent-fraud

Cyber Security Education in Estonia: From Kindergarten to NATO Cyber Defence Centre (2022). *E-Estonia,* 2022. március 16. Online: https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/

Európai Tanács (2024): *A pénzmosás elleni küzdelem: a Tanács jogszabálycsomagot fogadott el*. Online: https://www.consilium.europa.eu/hu/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/

Europol (2024): *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2813/442713

FBI (2024): *FBI Releases Internet Crime Report*. Online: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report

Government of South Australia (2024): *South Australian Students to Learn About Dangers of Social Media*. Online: https://www.education.sa.gov.au/department/media-centre/our-news/south-australian-students-to-learn-about-dangers-of-social-media

Interpol [é. n.]: *Social Engineering Scams*. Online: https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams

KSH (2024): *Internethasználók aránya [a 16–74 éves népesség százalékában]*. Online: https://www.ksh.hu/stadat_files/ikt/hu/ikt0029.html

Leukfeldt, E. Rutger – Lavorgna, Anita – Kleemans, Edward R. (2017): Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research,* 23, 287–300. Online: https://doi.org/10.1007/s10610-016-9332-z

Magony Gellért (2023): *In Too Deep(fake) – Suggestions on How to Avoid Harmful Social Influences of Deepfakes*. Online: https://constitutionaldiscourse.com/gellert-magony-in-too-deepfake-suggestions-on-how-to-avoid-harmful-social-influences-of-deepfakes/

Marek, Lynne (2025): Card Fraud Losses Will Increase Over Next Decade. *Payments Dive,* 2025. január 15. Online: https://www.paymentsdive.com/news/payments-fraud-losses-prevention-nilson-outlook/737440/

Mátyás Szabolcs (2018): A szervezett bűnözés kriminálgeográfiai vizsgálata. In Frigyer László (szerk.): *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információáramlási szempontból.* I. kötet. Budapest: Nemzeti Közszolgálati Egyetem, 134–168.

Mbungu Kala, Emile (2024): Influence of Online Platforms on Criminal Behavior. *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE),* 10(1), 25–37. Online: https://doi.org/10.20431/2349-4859.1001004

Mezei Kitti (2020): *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest: L'Harmattan.

MTI (2022): Itt a nagy kutatás: kiderült, hogy mire használják a magyarok az okostelefonjukat. *Portfolio,* 2022. május 27. Online: https://www.portfolio.hu/uzlet/20220527/itt-a-nagy-kutatas-kiderult-hogy-mire-hasznaljak-a-magyarok-az-okostelefonjukat-547345

NMHH (2023): *Internethasználati szokások, digitális média- és tartalomfogyasztás.* Online: https://nmhh.hu/cikk/235951/Internethasznalati_szokasok_digitalis_media_es_tartalomfogyasztas

Peersman, Claudia et al. (2022): *Understanding Motivations and Characteristics of Financially-Motivated Cybercriminals.* Online: https://doi.org/10.48550/arXiv.2203.08642

Van Hardeveld, Gert Jan – Webber, Craig – O'Hara, Kieron (2017): Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist,* 61(11), 1244–1266. Online: https://doi.org/10.1177/0002764217734271

VNA/VNP (2021): Cybersecurity to Be Included in High School Curriculum. *Báo Ảnh Việt Nam,* 2021. január 20. Online: https://vietnam.vnanet.vn/english/print/cybersecurity-to-be-included-in-high-school-curriculum-251227.html

Jogi források

1994. évi XXXIV. törvény a Rendőrségről

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról

2012. évi C. törvény a Büntető Törvénykönyvről

2017. évi XC. törvény a büntetőeljárásról

2024. évi XVIII. törvény az online csalások elleni fellépés érdekében szükséges törvények és egyéb büntetőjogi tárgyú törvények módosításáról

A Kúria Bvf.I.830/2017 számú határozata

Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2019/713 (2019. április 17.) irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról

Az Európai Parlament és a Tanács (EU) 2023/1113 rendelete (2023. május 31.) a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az (EU) 2015/849 irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról

Az Európai Parlament és a Tanács irányelve a belső piaci pénzforgalmi szolgáltatásokról és elektronikuspénz-szolgáltatásokról, a 98/26/EK irányelv módosításáról, valamint az (EU) 2015/2366 és a 2009/110/EK irányelv hatályon kívül helyezéséről (javaslat, Brüsszel, 2023. július 28.)

Az Európai Parlament és a Tanács rendelete a belső piaci pénzforgalmi szolgáltatásokról és az 1093/2010/EU rendelet módosításáról (javaslat, Brüsszel, 2023. június 28.)