TÓTH DÁVID

A PÉNZÜGYI IDENTITÁSLOPÁS AKTUÁLIS TRENDJEI

1. Bevezetés

A jelen kutatásomban a pénzügyi identitáslopás aktuális tendenciáit vizsgálom. A pénzügyi identitáslopás *(financial identity theft)* személyazonosság-lopás egyik fajtája, amely akkor valósul meg, ha valakinek a személyes, illetve pénzügyi adatait (például nevét, társadalombiztosítási számát vagy bankkártya adatait) ellopják, és ezt követően azokkal csalárd tevékenységeket valósítanak meg haszonszerzés céljából. A cselekmény alapvetően két fázisból tevődik össze. Első stádiumban a bűnelkövető különböző cselekményekkel (pl.: lopás, adathalászat, *skimming* stb.) a személyes, pénzügyi adatok jogellenes megszerzését törekszik megvalósítani. A második szakaszban pedig a megszerzett adatokkal való visszaélésszerű magatartásokat sorolhatjuk e jelenség alá. Utóbbira példa, ha valaki a jogosulatlanul más nevében hitelszámlát nyit meg, vagy más személy bankkártya adataival vásárol. A második fázisban megvalósuló magatartásokat szokták identitáscsalásnak is nevezni a szakirodalomban. Az elkövető tipikus célja a pénzügyi személyazonosság-lopásnál a vagyoni haszonszerzés. Lényeges hangsúlyozni, hogy ez a bűnözési forma csak akkor valósul meg, ha az áldozat személyes adatainak jogtalan megszerzése és azokkal való visszaélés az áldozat tudta vagy hozzájárulása nélkül történt meg.[1]

A magyar büntetőjogban jelenleg nem találunk speciális tényállást erre a kriminológiai fogalomra nézve. Tipikusan az alábbi tényállások megállapítására kerülhet sor pénzügyi identitáslopás esetén:

- készpénz-helyettesi fizetési eszközökkel kapcsolatos bűncselekmények,[2]
- személyes adattal visszaélés,[3]
- információs rendszer felhasználásával elkövetett csalás.

A bűncselekménynek az áldozatok szempontjából számos negatív következménye lehet, többek között anyagi károk, hitelképesség csökkenése, valamint további jogi nehézségek is előállhatnak.

A koronavírus okozta világjárvány és az ellene való védekezésként alkalmazott lezárások jelentős hatással voltak az emberek életére globálisan. Egyre több ember kényszerült otthon maradni, távmunkában végezni a munkáját, kommunikációt folytatni online térben emberekkel. Ezzel összefüggésben nőtt az emberek függősége az informatikai eszközöktől, és egyre több időt töltöttek a kibertérben. Ez a helyzet még inkább az online

[1] A szakirodalomban található meghatározásokról lásd még: Tóth Dávid: Személyiséglopás az interneten. Büntetőjogi Szemle 2020/1. 113-119. o.

[2] Gál István László: A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In: Polt, Péter (szerk.): Új Btk. kommentár: 7. kötet, Különös rész. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. Budapest. 2013. 193-224. o.

[3] Eszteri Dániel – Péterfalvi Attila: A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In: Görög Márta – Menyhárd Attila; Koltay, András (szerk.): A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE ÁJK, Budapest. 2017. 405-420. o.

világ felé irányította a bűnözőket. A válsághelyzetek mindig is új lehetőségeket teremtettek a bűnelkövetők számára, és ez a tendencia a pandémia idején is megmutatkozott.

2023 januárjában a Hootsuite jelentése[4] szerint az egyének átlagosan 6 óra 37 percet töltenek az interneten, vagyis közel egy napnak a harmadát. Miközben világszerte nő a népesség (2023 januárjában 8.01 milliárd fő), ezalatt az internethasználók száma és aránya is növekszik. Globálisan több mint 5.16 milliárd ember használja az internetet és a felhasználók jelentős része valamely közösségi médián is regisztrálva van.

A kiberbűnözés már a pandémia előtt is egy folyamatosan növekvő és aktuális probléma volt, ám a pandémia jelentős lökést adott ennek a társadalmi jelenségnek, tovább erősítve annak hatását. A pandémia okozta lezárások számos emberben szorongást, illetve a félelem szintjének emelkedését eredményezte, ez pedig növelte az esélyét annak, hogy átverések és csalások áldozataivá váljanak.[5]

2. Az identitáslopás kialakulásához vezető általános okok

Gupta[6] és mások végeztek kutatást arra vonatkozóan, hogy milyen tényezők vezettek az identitáslopás kialakulásához. Az alábbi faktorokat emelték ki:

- *Politikai és gazdasági tényezők*. A szerzők szerint a fejlődő országok gazdasági és politikai instabilitása növeli az identitáslopás esélyét. Erre példaként említik, amikor illegális bevándorlók hamis útleveleket használnak.
- *Társadalmi tényezők*. Az emberek kommunikációs szokásai és a személyes adatok hanyag kezelése szintén hozzájárul az identitáslopás megvalósulásához. A szerzők véleménye szerint az alacsony iskolázottság és a közösségi média felületek felelőtlen használata hozzájárul az identitáslopás terjedéséhez.
- *Technológiai tényezők*. Az internet és a digitális technológiák használata megkönnyíti az identitáslopást. Sokkal nagyobb mennyiségben érhetők el személyes adatok az interneten és a kifinomult bűnelkövetési technikákkal egyszerűbbé válik azok jogellenes megszerzése.[7]

3. A pénzügyi identitáslopás aktuális tendenciái

3.1. A pénzügyi identitáslopásra vonatkozó statisztikák a pandémia alatt

A pandémia komoly biztonsági kihívást jelentett a pénzügyi szervezeteknek és bankoknak is. Szükségessé vált az online bankolásnak a továbbfejlesztése és minél szélesebb körben történő alkalmazása a lezárások miatt. A távoli és online tranzakciók esetében az intézményeknek új biztonsági szabályokat és szoftvereket kellett alkalmazniuk az ügyfelek azonosítására. A kiberbűnözői csoportok pedig a biztonsági réseket keresték az online bankolást végző ügyfeleknél,[8] hiszen a bankkártya adatok jogellenes megszerzésével

[4] Forrás: https://wearesocial.com/uk/blog/2023/01/digital-2023/ (Letöltés ideje: 2023. 07. 02.)
[5] Marguerite DeLiema,– David Burnes – Lynn Langton: The Financial and Psychological Impact of Identity Theft Among Older Adults. In: Journal of Elder Abuse & Neglect 32, 2020/4-5. 343–362. o.
[6] Gupta, Chander Mohan – Devesh Kumar: Identity Theft: A Small Step Towards Big Financial Crimes. In: Journal of Financial Crime 27, 2020/3. 897-910. o.
[7] Uo.
[8] Ozik, Gideon – Sadka, Ronnie – Shen, Siy: Flattening the Illiquidity Curve: Retail Trading during the COVID-19 Lockdown. In: Journal of Financial and Quantitative Analysis 56, 2021/7. 2356-2388. o.

jelentős anyagi károkat tudnak okozni.[9] Wronka Cristoph ezt úgy összegzi, hogy a pénzügyi identitáslopás a járvány előtti állapotokhoz képest egyszerűbbé vált, a bűnelkövetők az online bankolásból eredő azonosítási nehézségeket ki tudták használni és okoztak számos esetben anyagi károkat.[10]

Ezeket a megállapításokat a statisztikai adatok is illusztrálják. Az elmúlt években több statisztikai kimutatás is napvilágot látott az identitáslopással összefüggésben. A Javelin stratégia vizsgálatai szerint a személyazonosság-lopás bűnözési formája 2020-ban a következő jellegzetességekkel volt leírható:

- A személyazonosság lopás által okozott károk a becslések alapján 43 milliárd USA dollárra voltak tehetőek 2020-ban. A bűnözők tipikusan hamis ajánlatokkal, adathalász e-mailekkel és telefonhívásokkal közvetlenül a fogyasztókat célozták meg.
- A személyazonosság-csalás áldozatainak száma 10 százalékkal 49 millióra főre csökkent, de átlagosan egy áldozatnak a vesztesége nőtt 42 százalékkal 1100 dollárra.
- Tipikus elkövetési technikák közé tartozott a phising, vishing, smishing és megszemélyesítés.
- A személyazonossággal kapcsolatos csalások leggyakoribb típusai a Covid-19 segélyhez, a munkanélküli segélyhez kapcsolódtak.[11]

Az ezt követő évről az Amerikai Szövetségi Kereskedelmi Bizottság (Federal Trade Comission, rövidítve: FTC) jelentése 2021-ről írt részletesen. A közleményük szerint 2.8 millió bejelentés érkezett az FTC felé. A csalások által okozott károk 70 százalékkal növekedtek az azt megelőző évhez képest, és a becslések alapján ennek számszerű mértéke 5.8 milliárd dollár volt. A jelentés szerint közel 1.4 millió bejelentés érkezett kifejezetten identitáslopással összefüggésben.[12]

A 2022-es évről is már több kutatás mutatott ki számokat az identitáslopással vonatkozásában. A tavalyi évben több mint 1 millió (pontosan 1 107 209) amerikai jelezte a hatóságok felé, hogy identitáslopással összefüggő támadás érte őt. Nominálisan a károk összértéke továbbra is hasonló volt, 43 milliárd dollárnyi kárt okoztak. Az ügyek 27 százaléka a pandémia idején közigazgatási dokumentumokhoz vagy juttatásokhoz kapcsolódtak. Georgia államában valósult meg a legtöbb személyazonosság-lopás. A 30 és 39 év közötti korosztály volt a leginkább érintve a bűncselekményekben. Az áldozatok jövedelmi viszonyait is elemezték, amely alapján 51 százalékuk évi 75 000 dollárnál több jövedelemmel rendelkezett, vagyis inkább a vagyonos társadalmi rétegeket célozták meg az elkövetők. Az áldozatok 14 százaléka jelentette, hogy az identitáslopás miatt több mint 10 000 dollárt vesztéséget szenvedtek.[13]

---

[9] Hawdon, James – Katalin, Parti – Thomas E. Dearden: Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment. In: American Journal of Criminal Justice 45, 2020/4. 546-562. o.

[10] Wronka, Christoph: Impact of COVID-19 on Financial Institutions: Navigating the Global Emerging Patterns of Financial Crime. In: Journal of Financial Crime 29, 2022/2. 476-490. o.

[11] Forrás: https://javelinstrategy.com/research/2020-identity-fraud-study-genesis-identity-fraud-crisis (Letöltés ideje: 2023.07.02)

[12] Forrás: https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 (Letöltés ideje: 2023.07 01.)

[13] Forrás: https://finmasters.com/identity-theft-statistics/ (Letöltés ideje: 2023.07.01.)

3.2. Az ún. Card-Not Present csalások

Európában is történtek analízisek az elmúlt időszak tendenciáiról. Az online térben bankkártyákkal történő visszaéléseket a szakirodalomban az ún. Card-Not-Present (CNP) csalásként aposztrofálják. Az ilyen típusú visszaélések többségbe kerültek az ATM vagy a fizikai térben megvalósuló bankkártya csalásokhoz képest. A kártya nélküli csalások értéke az Európai Unióban 2019-ben 4,3%-kal nőtt az előző évhez képest, elérve a 1,50 milliárd eurót. Ez az összeg a kártyás csalások teljes értékének 80%-át tette ki. A kártya nélküli csalások túlnyomó része határokon átnyúló tranzakciókhoz kapcsolódik, különösen az Európai Uniós Egységes Fizetési Térség (SEPA) területén belül. 2015 és 2019 között, a kártya nélküli csalások értéke 15,9%-kal nőtt,

Az Európai Központi Bank jelentése alapján összesen közel félmillió (pontosan 459,297) bankkártya csalással elkövetett eset érkezett be 2020-ban.[14] 2021-ben a CNP csalások viszont 12,1 százalékkal csökkentek 2020-hoz képest. A csalások által okozott károk mértéke összesen 1,28 milliárd eurót volt. Az erősített biztonsági előírások, például a megerősített ügyfélhitelesítés fontos szerepet játszott a CNP csalás csökkentésében a SEPA régióban. Bár az Európai Unióban csökkent a CNP csalások száma, az Európai Központi Bank jelentése kiemeli, hogy a jövőben továbbra is komoly kihívásokkal kell szembenézniük az online fizetési rendszerek fejlesztőinek. Ez szükséges ahhoz, hogy meg tudják előzni a potenciális jövőbeni bűncselekményeket. [15]

A CNP csalások ezen belül nagy mértékben kimagaslanak, 2021-ben már 87 százalékos aránnyal. Ezt követik a POS terminálokon végzett csalások 10-20 százalék között mozogva éves szinten és végül legkisebb arányban jönnek az ATM csalások.

Yenal és mások által végzett kutatásban rámutatnak, hogy a technológia jelentős szerepet játszik a CNP csalásokban. Az okostelefonok és a nyilvánosan hozzáférhető számítógépek különösen kockázatosak lehetnek ezen csalások szempontjából. Emelett azt is kiemelték, hogy számos esetben az elavult mobileszközök kevésbé védettek, mint a hagyományos számítógépek és a bűnözők könnyebben kihasználhatják ezen eszközöknél a biztonsági réseket. A rendszeres szoftverfrissítések segíthetnek az ilyen típusú csalások megelőzésében.[16]

4. Magyarországi statisztika

Mivel Magyarországon nincs külön tényállás az identitáslopás vonatkozásában, így nehéz pontos képet kapni annak volumenéről. A pénzügyi identitáslopással összefüggő bűncselekményekről az alábbiakat emeltem ki:

[14] Forrás: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html (Letöltés ideje: 2023.07.01.)
[15] Uo.
[16] Akdemir, Naci, – Serkan Yenal: Card-not-Present Fraud Victimization: A Routine Activities Approach to Understand the Risk Factors. In: Güvenlik Bilimleri Dergisi 9., 2020/1. 243-268. o.

bűncselekmények száma / év	2019	2020	2021	2022
Készpénz-helyettesítő fizetési eszköz hamisítása	52	784	1	12
Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése	1	0	0	0
Készpénz-helyettesítő fizetési eszközzel visszaélés	246	218	134	136
Személyes adattal visszaélés	1478	942	1078	2185
Információs rendszer felhasználásával elkövetett csalás	2624	3400	2681	4084

1. sz. táblázat: A pénzügyi identitáslopással összefüggő bűncselekmények éves statisztikája[17]

Amióta a készpénz-helyettesítő fizetési eszközzel visszaélés szubszidiárius viszonyban áll az információs rendszer felhasználásával elkövetett csalással, azóta utóbbi nagyobb számban fordul elő a bűnügyi statisztikákban. 2022-ben több, mint duplájára nőtt a személyes adattal visszaélések száma, ami szignifikánsnak tekinthető. Viszonylag nagy emelkedését láthatunk az információs rendszer felhasználásával elkövetett csalások vonatkozásában is. Nem szabad megfeledkeznünk a számok kapcsán, hogy az online térben megvalósuló bűncselekmények esetén magasfokú látencia a jellemző és ez különösen igaz az identitáslopással összefüggő bűncselekmények kapcsán.

5. Az identitáslopás potenciális kihívásai a jövőben: deepfake, morphing

Az identitáslopás új veszélyességi szintre emelkedhet a jövőben a mesterséges intelligencia dinamikus fejlődésével összefüggésben, amely segítségével már nem csak az azonosító adatok, hanem maguk a személyek is hamisíthatók lesznek. Ilyen technikát alkalmazhatnak

[17] Forrás: https://bsr.bm.hu/Document (Letöltés ideje: 2023.07.02.)

a Deepfake és a morphing során. Mindkettő a digitális képek vagy videók manipulálására használt technikák, de más-más módon működnek, és más-más célokra használják őket.

Az Oxfordi kéziszótár definíciója szerint a „deepfake" egy olyan technológia, amely digitálisan módosítja egy személy videón megjelenő külső jegyeit, hogy az illető úgy tűnjön, mintha egy másik személy lenne. Emellett ide sorolható az is, ha valakinek a hangját „lopják el" s azzal generálnak hamis hangfelvételeket. A deepfake videók vagy hangfelvételek létrehozásához mesterséges intelligenciát alkalmaznak, annak is a mélytanulásnak nevezett technológiáját, hogy hamis eseményekről készült képeket hozzanak létre, vagy meglévő videofelvételeket manipuláljanak. A „mélyhamisítások" azt a látszatot kelthetik, mintha valaki olyasmit mondott vagy tett volna, amit valóságban nem. Ezt úgy érik el, hogy egy gépi tanulási modellt nagy mennyiségű vizuális adaton (pl.: egy személy arcáról készült képeken vagy videókon) keresztül betanítják a mesterséges intelligenciát, majd a modell segítségével olyan új képeket vagy videókat hoznak létre, amelyek utánozzák a képzési adatokból tanult megjelenést és viselkedést.

A morphing ezzel szemben egy olyan technika, amely egy adott képnek egy másik képbe történő átalakítását vagy beolvasztását jelenti. Az arcok esetében általában két vagy több különböző arcot vesznek alapul, és azokat összemossák, hogy egy olyan összetett képet hozzanak létre, amely osztozik az eredeti képek jellemzőivel. Ez a folyamat két lépésből áll: először az ún. „warping" lépésben a kép formáját megváltoztatják, hogy az illeszkedjen a másik kép formájához. Ezután az ún. „cross-dissolving" lépésben a két kép színeit összekeverik, hogy a végeredmény egy sima átmenet legyen, amelyben az egyik arc mintha átalakulna a másik arccá. Ez a technika lehetővé teszi, hogy két különböző arcot összeolvasszanak egyetlen képpé, ami mindkét eredeti arc jellemzőit hordozza.[18]

A deepfake-hez kapcsolódó bűncselekmények egyik figyelemre méltó példája volt az az eset, amikor a támadók 2019 szeptemberében egy brit székhelyű energiavállalat vezérigazgatójának a hangját használták fel. A támadók felvették a kapcsolatot a cég ügyvezető igazgatójával. Az elkövetés során egy mesterséges intelligencia által generált hangot használtak, amely szinte teljesen megegyezett a valódi vezérigazgató hangjával. Az ügyvezetőtől azt kérték, hogy 243 000 dollárt utaljon át sürgősen a megadott számlaszámra. Az ügyvezető ennek eleget is tett. A pénzt egy magyarországi számlára utalták, majd ezután továbbutalták Mexikóba, illetve más helyekre, ezzel megnehezítve az azonosításukat. Az eset csalárd jellegét már csak későn fedezték fel, így a pénzt nem sikerült visszaszerezni. Ebben az ügyben egyszerre alkalmazásra került a deepfake technológia, a pszichológiai manipuláció (social engineering) és az identitáslopás. [19]

6. Összegezés

A COVID-19 világjárvány és az abból eredő korlátozási intézkedések miatt megnőtt azoknak a száma, akik több időt töltenek az online térben, és nőtt az emberek függősége az internettől. Az online aktivitás növekedése új lehetőséget teremtett a kiberbűnözők számára mivel több a potenciális áldozat.

A pandémia alatt a pénzügyi szervezetek és bankok számára komoly biztonsági kihívást jelentett az online bankolás széleskörű alkalmazása. Az intézményeknek új

[18] Agarwala, Akshay, és Nalini Rathab: Manipulating Faces for Identity Theft via Morphing and Deepfake: Digital Privacy. In: Deep Learning, vol. 48, 2023, 223. o.

[19] Forrás: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company (Letöltés ideje: 2023.07.02.)

biztonsági szabályokat és szoftvereket kellett alkalmazniuk az ügyfelek azonosítására. A statisztikák alapján az identitáscsalások által okozott károk jelentősen növekedtek az előző évekhez képest. A pénzügyi személyazonosság-lopás számos veszélyessége abban áll, hogy jelentős anyagi károkat, illetve jogi problémákat tud okozni az áldozatok számára.

A fizikai térben megvalósuló bankkártya visszaélések száma mára már elenyésző a CNP csalásokhoz képest. Ezek megelőzésében fontos szerepe van a biztonsági fejlesztéseknek, frissítéseknek, illetve a felhasználó tájékoztatásnak. Fontos, hogy a felhasználók tisztában legyenek a potenciális veszélyekkel, és megértsék, hogyan védhetik meg magukat a pénzügyi identitáslopás online formáitól és technikáitól mint, például a phishing, vishing, smishing.

Meglátásom szerint célszerű a jövőre nézve speciális tényállásban szabályozni az identitáslopás bűncselekményét külföldi modellek alapján.[20]

[20] Tóth Dávid: Az identitáslopás szabályozása angolszász államokban. In: Baráth, Noémi Emőke; Mezei, József (szerk.) Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével 2020. Doktoranduszok Országos Szövetsége, Budapest, 2020. 228-237. o.