TÓTH DÁVID

AZ IDENTITÁSLOPÁS KRIMINOLÓGIAI SAJÁTOSSÁGAI

1. Bevezetés

Az identitáslopás kezdeti formájában egy másik ember megszemélyesítése volt csalási szándékkal. A bűncselekmény előképére találunk példát a Bibliában Jákob és Ézsau történetében, ahol Izsák elsőszülött fia Ézsau egy tál lencsefőzelékért lemondott előjogairól Jákob javára, de erről apjuk nem szerzett tudomást. (Mózes 1. könyve 25,19–34) Később Jákob elment a már vak apjához, hogy megkapja az áldást az örökséghez. Ezt Ézsau ruháiban és kecskebőrben tette, hogy Izsák ne vegye észre a csalást. A számos történelmi példa között ki lehet még emelni John Aylmer történetét, aki az 1440-es években praktizált orvosként Angliában. 1449-ben elmenekült Franciaországba, mivel azzal vádolták, hogy megölte az asszonyát. Megközelítőleg egy évvel később visszatért Angliába Jack Cade álnéven. Aylmer elkezdett szervezni egy sereget a szakadárokból VI. Henrik király ellen. Ekkor azt állította, hogy ő John Mortimer, aki Richárd york-i herceg rokona. Aylmer serege legyőzte a királyi katonákat Kentnél. A kezdeti siker ellenére később a serege szétesett, végül Aylmert Kent Sheriffje ölte meg.[1]

A modern korban az identitáslopás az információtechnológia fejlődésével egyre nagyobb méreteket ölt világszerte. Ennek számos oka van. Egyrészt több személyes információ érhető el az interneten, mivel az emberek önként osztanak meg adatokat magukról a közösségi hálózatokon. Másrészt a kormányzati és üzleti szervek nagyméretű adatbázisokban tárolják az emberek személyes adatait. Harmadrészt az elkövetők az elérhető vagy feltörhető oldalakat, felhőszolgáltatásokat, számítógépeket folyamatosan támadják különböző technikákkal (mint pl.: hacking, vírusok küldésével) hogy hozzájussanak ezekhez a személyes adatokhoz. A kibertérben elkövetett bűncselekmények mellett nem szabad megfeledkezni a fizikai úton történő bűncselekményekről (lopás, csalás), amelyek szintén növelik e speciális bűnözési forma mértékét.

A tanulmány célja az identitáslopás kriminológiai sajátosságait feltárni, és ezzel kapcsolatban prevenciós javaslatokat megfogalmazni.

2. Az identitáslopás fogalma

Az identitáslopásnak az irodalomban nincs egységesen elfogadott definíciója. A külföldi szakirodalomban több elnevezést is használnak ugyanarra a jelenségre. Egyrészt szokták hívni identitáslopásnak (Identity theft, identitätsdiebstahl), amely inkább az Egyesült Államokban[2] és Németországban[3] terjedt el. Másrészt az Egyesült Királyságban[4] identitáscsalásként (identity fraud) aposztrofálják ezt a bűnözési formát.

---

[1] Hoffman, Sandra K. – McGinley, Tracy G.: Identity theft. ABC-CLIO, Santa Barbara, California, 2010. 6-7. o.

[2] Biegelman, Martin T.: Identity theft Handbook: detection, prevention and security. John Wiley and Sons, Inc, Hoboken, New Jersey. 2009. 2. o.

Charles M. Kahn és William Roberds szerint identitáslopásnak minősül más személyes adatainak csalási szándékkal történő használata.[5] Katie A. Farina definíciója a csalásra helyezi hangsúlyt: „Az egyén személyes adatainak csalási szándékkal történő használata."[6] Biegelman szerint – aki egy kézikönyvet írt a témában – az identitáslopás nem más, mint az emberek jó hírnevének és reputációjának lopása anyagi haszonszerzés végett.[7] Jogi meghatározásra is találunk példát az Egyesült Államokban. Az USA Kódexének (US Code) 18. Fejezetének 1028. § (7) pontja mondja ki, hogy

- aki szándékosan és jogellenesen
- átad, birtokol, vagy használ azonosító eszközöket,
- egy másik személyről,
- azzal a céllal, hogy – tettesként, bűnsegédként, vagy felbujtóként –
- jogellenes tevékenységet fejtsen ki,
- büntetendő a tagállami vagy a szövetségi jog szerint.

Ha közös nevezőre akarjuk hozni a fogalmi meghatározásokat, akkor az alábbi elemeket találjuk meg mindegyikben. Valamennyi definícióban található:

- elkövetési tárgy, ami az identitáshoz köthető információ.
- Büntetendő cselekmény, amely terjedhet a megszerzéstől a használaton át, a kereskedésig.
- Alanyi elem, ami tipikusan valamilyen célzatot tartalmaz (pl.: csalárd szándék)-
- Végül valamennyi szerző egyetért abban, hogy a bűncselekmény akkor valósul meg, ha az áldozat nem járult hozzák, hogy az adataihoz hozzáférjenek és azt használják.

A magyar Büntető Törvénykönyv nem bünteti önálló tényállás alatt, de az ezzel kapcsolatos magatartások több bűncselekményt (csalást, információs rendszer felhasználásával elkövetett csalást, személyes adattal visszaélést, okirattal visszaélést, közokirat-hamisítást, készpénz-helyettesítő fizetési eszközzel visszaélést) is megvalósíthatnak.

3. A személyazonosság-lopás megjelenési formái

Az identitáslopásnak több tipológiája van a jogirodalomban. Hoffman és McGinley felosztása azon alapszik, hogy mi ellen irányul a bűncselekmény. Ez alapján megkülönböztetnek személyes és üzleti identitáslopást.

A személyes identitáslopás esetén az egyén személyes adatait szerzik meg csalárd szándékkal. Rendszerint olyan jogellenes tevékenységek érdekében teszik ezt, mint a szolgáltatások jogosulatlan igénybevétele, áruk vételezése, pénz lopás az egyéb bűnözői

[3] Borges, Georg – Schwenk, Jörg et al.: Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte. Springer, Heidelberg. 2011. 9. o.

[4] Forrás: https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft (Letöltés ideje: 2019.06.10.)

[5] Kahn, Charles M. – Roberds, William: Credit and identity theft. In: Journal of Monetary Economics 55. 2008. 251. o.

[6] Farina, Katie A: Cyber Crime: Identity Theft. In: International Encyclopedia of the Social & Behavioral Sciences. 2015. 633. o.

[7] Biegelman: i.m. 2. o.

tevékenységének támogatására. Az elkövetési tárgyak körébe tartozik különösen az áldozat neve, lakcíme, telefonszáma, személyi igazolvány száma, bankkártya száma és ahhoz tartozó PIN-kód, biometrikus adatai, e-mail címe, anyja neve.

Üzleti identitáslopás elsősorban cégek, pénzügyi intézetek, bankok ellen irányulnak. Az elkövető célja változó, de leggyakrabban az anyagi haszonszerzés, illetve a vagyoni károkozás. Tipikusan az alábbi adatok megszerzésére irányul az identitáslopás: a cég neve, székhelye, telefonszáma, e-mail címe, logója, védjegye, bankszámlaszáma, adóazonosító száma.[8]

Egy többszerzős tanulmány[9] szerint az identitáslopástól meg kell különböztetni az identitás átvételt, amikor az elkövető egy létező személy identitását veszi át annak beleegyezése nélkül. További külön kategória még az identitás delegálás, ez akkor valósul meg, ha két vagy több személy megegyezik abban, hogy egymás személyazonosságát használhassák. Erre lehet példa, amikor vásárlók cserélik a hűségkártyáikat.

Egy cizelláltabb tipológia[10] szerint megkülönböztetünk vagyoni, egészségügyi, bűnügyi, szintetikus, és gyermek identitáslopást. Különleges kategóriaként említik még az ún. identitás klónozást.

- A személyazonosság-lopás egyik leggyakoribb formája a vagyoni, amikor az elkövető egy másik ember személyes adatait vagyoni haszonszerzés végett szerzi meg. Elsősorban bankszámla és a bankkártya adatok ellen irányul a bűncselekmény.
- Az Egyesült Államokban növekvő probléma az ún. egészségügyi identitáslopás. Az elkövetők kórházakat, és egészségügyi szolgáltatók szervereit támadják, hogy megszerezzék az áldozatok társadalombiztosítási számát. Az ellopott adatokkal ezt követően tudnak kereskedni a darkneten. Maga az elkövető is igénybe vehet jogtalanul az egészségügyi szolgáltatásokat. 2017-ben 300 egészégügyi szerv tett feljelentést az Egyesült Államokban arról, hogy feltörték az adattároló rendszerüket.[11]
- Bűnügyi identitáslopás esetén az elkövető a lopott személyi igazolvánnyal, jogosítvánnyal igazolja magát a büntetőeljárásban. Ebben az esetben fennállhat az a probléma, hogy csak évekkel később kerül felhasználásra a lopott személyazonosító okmány és a hatóságok ártatlan emberek (korábbi áldozatok) ellen indíthatnak eljárást. A magyar joggyakorlatban is felmerült ez a jelenség. A 2/2004 Büntető Jogegységi Határozat szerint, ha az elkövető az ellene indított büntetőeljárás során más létező személynek adja ki magát, és az ennek megfelelő adat kerül az ügyben eljáró hatóságok által készített közokiratba, akkor az elkövető megvalósítja a hamis vád bűncselekményét és az „intellektuális" közokirat-hamisítás bűntettét. Amennyiben az elkövető a személyazonosságának az igazolására más nevére szóló valódi közokiratot is felhasznál, a hamis vád bűntette és az „intellektuális" közokirat-hamisítás bűntette mellett a közokirat-hamisítás b) pontjának 3. fordulatát („más nevére szóló valódi közokiratot felhasznál") követi el. Relatíve újabb hasonló ügyek is voltak a magyar bíróságok előtt. A más nevére

[8] Hoffman – McGinley: i. m. 3-5. o.
[9] Koops, Bert Jaap, - Leenes, Ronald et. al.: A typology of identity-related crime. Conceptual, technical and legal issues. In: Information, Communication & Scoitey. 2009/1. 8. o.
[10] Manap, Nazura Abdul – Rahim, Anita Abdul – Taji, Hossein: Cyberspace Identity Theft: The Conceptual Framework. In: Mediterranean Journal of Social Sciences. Vol 6. No. 4. 2015. 600-602. o.
[11] Forrás: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (Letöltés ideje: 2019. 06. 16.)

szóló nem fényképes okiratok átadása esetén is megvalósul a közokirat-hamisítás.[12] Egy Kúria előtt záródó ügyben pedig az elkövetőt közokirat-hamisítás bűntettében [Btk. 342. § (1) bekezdés b) pont], valamint okirattal visszaélés vétségében [Btk. 346. § (1) bekezdés a) pont] találták bűnösnek, mivel szabálytalanul parkolt és az igazoltató rendőröknek a személyazonosítása céljából átadta a testvérének az útlevelét.[13]

- Szintetikus identitáslopásnál az elkövető egy vagy több valós információt társít egy másik személy vagy egy nem létező személy adataival, így létrehozva egy új szintetikus személyt. Ezt a technikát fel tudják használni például bankszámlák nyitásához vagy kölcsönfelvételhez. Különösen annak okozhat kárt, akinek a társadalombiztosítási számát lopják el. Ez is növekvő probléma az USA-ban. A banki ügyintézők nem tudják ellenőrizni azt, hogy meghatározott társadalombiztosítási számhoz milyen név társul, csak azt, hogy nyitottak e már korábban számlát vele.
- A gyermek identitáslopás a szintetikus személyazonosság-lopás egyik vállfajaként is tekinthető. Az elkövetők gyermekek és fiatalkorúak társadalombiztosítási számát próbálják megszerezni. A bűncselekmény lappangási ideje akár évekig is tarthat. Előfordulhat, hogy az áldozat, csak 18 évesen nyit bankszámlát, és addigra a társadalombiztosítási számához kapcsolódóan már tetemes adóssága van.
- Sajátos esetkör az identitás klónozás, amikor az elkövető nem csak egy, hanem minél több, lehetőleg valamennyi személyazonosító adatot próbál megszerezni, majd felhasználni. A bűnöző de facto leklónozza az áldozatot, ő nem lesz más, mint a sértett egy másik helyen, egy másik államban. A bűnelkövetők fő célja, hogy elrejtsék a saját identitásukat és új életet kezdhessenek. Történhet az identitás klónozás például munkavállalás, házasságkötés, gyermekvállalás céljából. Az elkövetők tipikusan illegális bevándorlók, vagy büntetett előéletű emberek.

4. Az identitáslopás technikái

A teljesség igénye nélkül csak gyakoribb elkövetési formákat ismertetek. Zeno Geradts szerint a felhasználók személyes adatainak és jelszavának kicsalása leggyakrabban adathalász e-mailekkel (phising) történik, amikor az elkövetők a bank nevében kérik az ügyfelet, hogy adják meg személyes adataikat. Ezeket általában könnyű kiszűrni, mert sokszor ingyenes e-mail címekről (gmail, hotmail) küldik.[14]

Az adathalász e-mailek tartalmazhatnak egy linket, amely elvezetheti a felhasználót egy leklónozott oldalra. Tipikusan bankok, illetve webáruházak oldalát másolják le, ahol az áldozat be tudja gépelni a személyes adatait. Ezt a jelenséget pharmingnak hívják a szakzsargonban.[15]

[12] BH2014. 234. II.
[13] Kúria Bfv.1695/2017/6
[14] Geradts Zeno: Identity theft. In: Siegel Jay - Saukko, Pekka (Szerk): Encyclopedia of Forensic Sciences, Second Edition. Academic Press, Amsterdam - Boston - Heidelberg - London - New York - Oxford - San Diego - San Francisco - Sydney - Tokyo. 2013. 419. o.
[15] Whitson, Jennifer – Haggerty, Kevin D.: Identity theft and the care of virtual self. In: Economy and Society 2008. 579. o.

A phising-hez hasonló elkövetési technika a smishing.[16] Az ilyen jellegű támadásoknál az elkövető elküld egy sms-t, amely tartalmaz egy linket egy hamis weboldalra ahol az áldozat meg tudja adni a személyes adatait. A bűnözők általában olyan tartalmú smseket küldenek, amelybe kérik a bankkártyaszámot, személyes adatokat, hogy megoldhassák az egyébként nem létező problémákat (pl.: hogy ne zárolják az ügyfél bankszámláját).

Arra is volt példa, hogy a bűnelkövetők felállítottak egy vezetéknélküli hálózatot (wifit), amelyre, ha a gyanútlan felhasználók csatlakoznak, veszélynek teszik ki személyes adataikat. Ez az ún. Wi-phising.[17]

A phisinghez szintén hasonló jelenség a vishing. Ilyenkor az elkövetők telefonhíváson keresztül, pszichológiai manipulációval (ún. social engineering) próbálják megszerezni a bankszámlákhoz kapcsolódó adatokat. Ebben az esetben nem a technológia, hanem az emberek hiszékenysége, naivitása, befolyásolhatósága lesz a támadó fő fegyvere.[18]

A fentiektől jellegzetesen tér el az ún. skimming. Ennek lényege, hogy az elkövetők bankautomaták (ATM) nyílására felszerelnek miniatűr adatrögzítő eszközöket és így szerzik meg a bankkártya adatainkat.[19]

Egy klasszikus technikája az identitáslopásnak a jogosulatlan behatolás (hacking). Erre volt példa a 2005-ben végrehajtott támadás a DSW cipőbolt hálózat ellen, melynek eredményeképpen 1.4 millió kártyaforgalmi adatot loptak el 108 boltól.[20]

5. Az áldozatoknak okozott károk

Az Egyesült Államokban a Javelin nevezetű közvéleménykutató cég 2019-es jelentése szerint 2018-ban az áldozatok száma 14.4 millió fő volt.[21] Empirikus viktimológiai kutatásokat végzett Reyns és Henson, arról, hogy az áldozatoknak milyen károkat okoztak az elkövetők. A Kanadai Általános Társadalmi Kérdőíven keresztül végzett felmérést a szerzőpáros a kanadai lakosságnál. Eredményeik szerint meghatározott rutinszerű online tevékenységek korrelatív módon növelik az identitáslopás bekövetkeztét.[22]

Az áldozatoknál jelentkező károkat az alábbiak szerint lehet csoportosítani:

- vagyoni károk,
- egészségügyi károk,
- szociális károk, és jogi károk.

[16] Tajpour, Atefeh – Ibrahim, Suhaimi – Zamani, Mazdak: Identity theft methods and fraud types. In: International Journal of Information Processing and Management 2013/7. 53. o.

[17] Uo.

[18] Biegelman: i. m. 37. o.

[19] Lásd bővebben Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozása. In: Kecskés Gábor (Szerk.) Doktori Műhelytanulmányok. Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, Győr. 2015. 252. o.

[20] Chawki, Mohamed – Wahab, S. Abdel Mohamed: Identity theft in cyberspace: issues and solutions. In: Lex Eletrconica 2006/1. 14. o.

[21] Forrás: https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt (letöltés ideje 2019.06.16.)

[22] Lásd bővebben: Reyns, Bradford W. – Henson, Billy: The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory In: International Journal of Offender Therapy and Comparative Criminology. 2015/1. 1. o

Mindenekelőtt a vagyonvesztés a leggyakoribb kár, amit elszenvednek széles körben az áldozatok. A Federal Trade Commission 2018-ban kiadott jelentése szerint 2017-ben az identitáslopással kapcsolatos csalások összesen 905 millió dollár kárt okoztak az áldozatoknak.[23]

Az egészégügyi károk első szintje, hogy az áldozatok érzelmi traumákon mehetnek keresztül, és a reviktimizációtól való félelem tovább növelheti a szorongást. A pszichológiai problémák később egyéb egészségügyi gondokat okozhatnak, így alvászavart, fejfájást, fáradékonyságot. A legnagyobb veszélyeket e tekintetben egészségügyi identitáslopás jelenti, mert a téves orvosi adatok után a „valódi" beteget félrediagnosztizálhatják és félrekezelhetik, amelynek eredménye akár halálos is lehet.

Szociális és jogi károk közé tartozik, ha az áldozatok ellen polgári illetve büntetőügyek indulnak, mivel nevükkel visszaéltek. Csökkenhet a jó hírnevük, és a társadalmi megbecsülésük. Amennyiben büntetőeljárás indul velük szemben, el kell viselniük az eljárási cselekményeket, (pl.: téves őrizetbe vételt, kihallgatásokat, és végső soron akár tevés elítélés, Justizmord is bekövetkezhet). Nemcsak a társadalom tagjai, hanem a közvetlen családi környezetük és megbélyegezheti az identitáslopás áldozatait.

Az identitáslopás áldozatainak jelentős része nem tesz feljelentést a történésekről. Harell tanulmánya szerint[24] az áldozatok 93%-a nem tett feljelentést a rendőrségnél. Az emberek többsége (68%-a) azért mulasztotta el a feljelentés megtételét, mert máshogyan oldották meg az ügyüket. A feljelentést mulasztók több, mint 12%-a gondolta azt, hogy a rendőrség nem képes rajtuk segíteni.

6. A bűnmegelőzés javaslatok

Véleményem szerint három szereplőnek van nagy szerepe a bűnmegelőzésben: az államnak, a pénzügyi szervezeteknek, és az egyéneknek.

Az állam feladata, hogy büntetendővé tegye az ezzel kapcsolatos bűncselekményeket (akár önálló tényállás alatt). A jogalkalmazó szerveknek, pedig érvényesíteni kell az állam büntetőigényét. Végezetül külföldön vannak modellek áldozatsegítő szolgálatokról, amelyek kifejezetten az identitáslopás áldozataival foglalkoznak. Az ilyen szolgálatokat többféleképpen meg lehet keresni, amelyek tanácsokat adnak, és segítenek a probléma megoldásában.[25]

Pénzügyi szervezeteknek számos feladata van, az identitáslopással összefüggésben az alábbiakat emelném ki:

- az ügyfelek adatainak zártan kezelése,
- törvények betartása,
- naprakész biztonsági rendszerek felállítása a potenciális támadásokkal szemben.

Az egyének számára számos hasznos tanácsot lehet megfogalmazni. Így például:

- a közösségi médiumokon minél kevesebb információt megosztani, és azt is csak a baráti körrel,
- személyazonosításra alkalmas dokumentumokról ne készítsünk fényképeket,
- bankkártya információt ne tároljunk online stb.

---

[23] Forrás: https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers (Letöltés ideje: 2019.06.15.)

[24] Erika Harell: Victims of identity theft, 2016. In: Bureau of Justice Statistics 2019/1. 13. o.

[25] https://victimsupportservices.org/help-for-victims/crime-types/identity-theft/ (Letöltés ideje: 2019.06.15.)

Amennyiben megtörtént a baj, az áldozatok részéről fontos, hogy proaktívak legyenek:

- tegyenek feljelentést,
- ha bankkártya adatokat loptak el, érdemes letiltani a kártyát és lefagyasztani a számlát,
- és felvenni a kapcsolatot a pénzügyi szervekkel, illetve az áldozatsegítő szolgálatokkal.

7. Összegzés

A személyazonosság-lopás és az ahhoz bűncselekmények nem ismernek határokat, ezért fontos egy összehangolt egységes államok közötti fellépés a bűnelkövetőkkel szemben. Ez különösen regionális szinten lehet hatékony. Ehhez szükséges egy harmonizált jogi szabályozás kell illetve a bűnügyi szerveknek összehangolt együttműködése. E tekintetben vannak pozitív fejlemények az Európai Unióban. Korábban már elfogadta az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról szóló irányelvet, mely foglalkozik a két kapcsolódó bűncselekménnyel a rendszert érintő jogellenes beavatkozással és az adatot érintő jogellenes beavatkozással. Újabb fejlemény, hogy az Európai Parlament és a Tanács elfogadta az 2019/73 irányelvet, ami megújítja az uniós szabályozást a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és hamisítás elleni küzdelem jogi eszköztárát.