Tóth Dávid*

Személyiséglopás az interneten

1. Bevezetés

A személyiséglopás 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.[1]

A modern korban a személyiséglopás 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.

Tom Arnold már 2000-ben megfogalmazta, hogy a személyiséglopás az internetesbűnözés egyik leggyakoribb formája lehet, amely nem ismer határokat és globális méreteket fog ölteni.[2]

2. A személyiséglopás definíciója

2.1. A személyiséglopás meghatározása a szakirodalomban

2.1.1. Külföldi szakirodalmi meghatározások

A személyiséglopásnak 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[3] és Németországban[4] terjedt el. Másrészt az Egyesült Királyságban[5] identitáscsalásként *(identity fraud)* aposztrofálják ezt a bűnözési formát, mivel ott a törvényi szabályozás nem határozza meg speciális tényállásban, hanem a csalás körében értékeli a 2006-os csalási törvény *(Fraud Act 2006).*[6]

Charles M. Kahn és William Roberds szerint identitáslopásnak minősül más személyes adatainak csalási szándékkal történő használata.[7] Katie A. Farina definíciója a csalásra helyezi hangsúlyt: *„Az egyén személyes adatainak csalási szándékkal történő használata."*[8]

Hasonlóan fogalmaz kanadai szerzőpáros Lawson és Lawford. Az identitáslopás nézetük szerint, egy má-

* PhD, adjunktus, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Kriminológiai és Büntetés-végrehajtási Jogi Tanszék.

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

[2] Arnold, Tom: Internet Identity Theft. A Tragedy for Victims. A White Paper from the Technology Working Group, eBusiness Division, SIIA Project. 2000. 4. o.

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

[4] Borges, G. – Schwenk J. – Stuckenberg C. – Wegener, C.: Identitätsdiebstahl und identitätsmissbrauch im Internet. Rechtliche und technische Aspekte. Springer, Heidelberg–Dordrecht–London–New York. 2011. 9. o.

[5] https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft (letöltés ideje: 2019. 06. 10.)

[6] Alisdair A. Gillespie: Cybercrime. Key Issues and Debates. Routledge, New York. 2016. 145. o.

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

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

sik ember személyes információinak a jogellenes összegyűjtése és csalárd szándékú használata. Az elkövetők elsődleges célja a vagyoni haszonszerzés. Személyes adatokat számos módon megszerezhetik, így például:

- pénztárcák, laptopok, bankkártyák, winchesterek lopásával,
- számítógépes adattárolók feltörésével az interneten keresztül, vagy
- csalárd módon internetszolgáltatónak álcázva magukat látszólag piackutatás céljából.[9]

Biegelman szerint – aki egy kézikönyvet írt a témában – az identitáslopás nem más, mint az emberek jó hírnevének és reputációjának lopása anyagi haszonszerzés végett.[10]

Egy identitáslopással foglalkozó német könyv szerzői szerint az identitáslopás lényege a személyazonosság jogellenes megszerzése. Meghatározásuk szerint önmagában egy személyes adat (pl.: a bankkártyaszám) megszerzése még nem minősül identitáslopásnak, csak akkor, ha az adatösszesség (a bankkártyaszám mellett a név, lejárati szám) alkalmas a személy azonosítására.[11] Az identitáslopástól meg kell különböztetni az identitás-visszaélést *(identitätmissbrauch)*, amely alatt a személyes adatok csalárd módon történő használatát értik.[12]

2.1.2. Magyar szakirodalmi meghatározások

A külföldi elnevezésekhez hasonlóan, hazánkban is több szakkifejezés jelent meg. Eszteri Dániel és Máté István Zsolt közös tanulmányában az identitáslopás terminust használja a virtuális valóságot szimuláló *„Second Life"* nevezetű szoftverben elkövetett deliktumok kapcsán.[13] Hámori is ezt a szakkifejezést használja, és a definíciójának középpontjában a személyes adatok jogellenes megszerzése áll: *„egy személy adatainak (név, születési év, lakcím, hitelkártya-azonosító, tajszám és más személyes adatok, illegális eltulajdonítása azzal a céllal, hogy azokat különféle tranzakciókban anyagi előnyszerzésre használják az autóbérléstől a bankhitel felvételéig."*[14]

Haig Zsolt a fentivel ellentétben személyiséglopás terminológiát alkalmazza. Scwhartau könyvére[15] hivatkozva a személyiséglopást az információs hadviselés, azon belül a személyes információs hadviselés kategóriájába sorolja. A bűncselekmény megvalósulása esetén az áldozatuk anyagi és emberi méltóságot érintő károkat szenvedhetnek.[16]

Sorbán Kinga a személyazonosság-lopás szakkifejezést használja.[17] Szerinte ennek a bűnözési formának két mozzanata van. Az első fázisban a bűnelkövető eltulajdonítja az áldozat személyes adatait (pl.: tajszámát). A második fázis az adatok visszaélésszerű használatáról szól. Rámutat, hogy a magyar Büntető Törvénykönyv nem tartalmaz speciális tényállást, és véleménye szerint erre nincs is szükség, mert az ezzel kapcsolatos magatartások beilleszthetők már meglévő tényállásokba (pl.: személyes adattal visszaélésnek minősülhet).[18]

Meglátásom szerint valamennyi szakkifejezés helytálló, és nem lehet ezek között rangsorolni.

2.2. Az identitáslopás jogi meghatározása

Az identitáslopás az egyik leggyakoribb bűnözési forma az Egyesült Államokban. Nem véletlen, hogy az USA volt az első állam a világon, amely speciális tényállásban határozta meg a személyiséglopás fogalmát.[19] 1998-ban egy módosítótörvény *(Identity Theft and Assumption Deterrence Act[20])* emelte be a deliktumot a Kódexbe. A módosítás előtt csak az okirat-hamisításnak minősült az ellopott adatokkal történő hamis okirat készítése, de a személyazonosságra vonatkozó adattal való visszaélés még nem valósított meg önmagában bűncselekményt. A módosítás célja volt, hogy az identitással kapcsolatos visszaéléseket szövetségi szinten is büntetőjogi fenyegetettség alá vonja, amely szélesebb nyomozási eszközöket biztosított a rendőri szerveknek. Célkitűzés volt továbbá, hogy ne csak az anyagi károkozást rendeljék büntetni, hanem egyéb az identitáslopással kapcsolatos személyiségijogsérelmet is. Emellett a törvény magasabb büntetési tételt írt elő, mint a korábbi szerteágazó tényállásoknál, amely növelheti a váderedményességet és a vádalkut számát, ami – a beismerő vallomások miatt – felgyorsítja a büntetőeljárást.[21]

Jelenleg a kodifikált törvénykönyv 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.

[9] Lásd bővebben: Lawson Philippa – Lawford, John: Identity theft: the need for better consumer protection. Public Interest Advocacy Centre. 2003. 3–19. o.

[10] Biegelman, i. m. 2. o.

[11] Borges et al., i. m. 11. o.

[12] Busch, Christoph: Biometrie und Identitätsdiebstahl. In: Datenschutz und Datensicherheit – DuD. 2009/5. 317. o.

[13] Lásd bővebben: Eszteri Dániel – Máté István Zsolt: Identitáslopás a virtuális világban. In: Belügyi Szemle 2017/3. 79–107. o.

[14] Hámori Balázs: Bizalom, jóhírnév és identitás az elektronikus piacokon. In: Közgazdasági Szemle 2004/9. 832–848.

[15] Schwartau, Winn: Information warfare. Kindle e-book edition. Interpact Press Inc, New York. 2010. hely: 163.

[16] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. In: Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata. 2011/1–2. 14. o.

[17] Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. In: Themis: 2015/1. 343–375. o.

[18] Sorbán: i. m. 369–370. o.

[19] Samaha, Joel: Criminal law. Ninth edition.Thomson Wadsworth Publisher, USA, Belmont. 2008. 393.o.

[20] https://www.ftc.gov/node/119459 (letöltés ideje: 2019. 09. 20.)

[21] Borges et. al. i. m. 337–338. o.

Azonosításra alkalmas eszköznek minősül a törvény szerint bármilyen név vagy azonosítószám, amely egy meghatározott személy azonosságát bizonyítja. Különösen idetartozik az egyén:

- neve, társadalombiztosítási száma, születési dátuma, államilag kibocsátott járművezetési engedélye, vagy a gépjármű rendszáma, külföldi regisztrációs száma, útlevél száma, munkavállalói vagy adóazonosító száma;
- egyedi biometrikus adatai, mint az ujjlenyomata, hanglenyomata, retina- vagy íriszképe, vagy egyéb egyedi fizikai megkülönböztető jegye;
- egyedi elektronikus azonosító száma, címe, vagy irányítószáma; vagy
- telekommunikációs azonosító információja vagy azonosító eszköze.[22]

A törvény csak példálózó felsorolást tartalmaz.

A kódex nemcsak a hagyományos fizikai úton tárolt okmányokat védi, hanem a személyazonosságot tartalmazó elektronikus adattározókat is. Annak ellenére, hogy a törvény fejezetének címében identitáslopás szerepel, a személyazonosságra vonatkozó adat jogellenes megszerzését nem rendeli büntetni, csak az azt követő magatartásokat, így a birtoklást, átadást vagy használatot. Az 1028. szakasz védi emellett a szabadon elérhető adatokat is, függetlenül attól, hogy a személyazonosságra vonatkozó interneten érhető-e el, vagy mondjuk szemeteskukából. A leggyakrabban az elkövetők bankkártyák, hitelkártyák számát, automatákhoz használt PIN-kódot, vagy társadalombiztosítási számokat próbálnak megszerezni.[23]

A személyazonosságra vonatkozó adatok összegyűjtése számítógépes csalásnak minősülhet a kódex 1030. § szerint. A paragrafus szerint büntetendő például a védett adatokhoz történő jogellenes hozzáférése, vagy a kémprogrammokkal történő jelszó és bankkártyaszám megszerzése. A szabályozás megfelel az ún. Cybercrime Egyezménynek,[24] amelyet az Egyesült 2001-ben írt alá, 2006-ban ratifikált és 2007. január 1-jén hatályba is lépett. Az 1030. szakasz egy átfogó Bűnmegelőzési Törvénnyel *(Comprehensive Crime Control Act)* került megszövegezésre, és 1986-ban a Számítógépes Csalás és Visszaélés Törvénnyel *(Computer Fraud and Abuse Act)* került bővítésre. A legutóbbi jogfejlesztést a 2008-ban elfogadott módosító törvény valósította meg *(Identity Theft Enforcement and Restitution Act of September 2008)*. Ez a törvény pontosította és bővítette a joghatósági jogkörét a bűnüldöző szerveknek. Lényegében megkönnyítette a nyomozó szervek számára, hogy a számítógépes úton elkövetett identitás tolvajokkal szemben eljárjanak. Emellett meghatározza a kiberbűncselekmények áldozatát, és előírja, hogy kártérítési összeggel kell őket kárpótolni.[25]

A személyiséglopás jogkövetkezménye akár harmincévi szabadságvesztés is lehet amennyiben terrorizmus összefüggő bűncselekményről van szó. Az identitáslopást azért is büntetik nagy súllyal, mert sok esetben terrorizmus finanszírozására is alkalmas lehet.[26] Az amerikai jog a személyiséglopás kísérletét is büntetni rendeli azonos büntetési tétellel. A szövetségi joggyakorlat a büntetés kiszabásánál figyelembe veszi az áldozatok számát, az elkövetési tárgyat. A büntetéskiszabásnál szempont lehet még az adatok megszerzésének a módja. Súlyosabban minősülhet a bűncselekmény amennyiben, az adatokat jogellenes behatolással (hacking) szerezték meg. Végül rendszerint számításba veszik, hogy milyen kárt szenvedtek az áldozatok az identitáslopás miatt. Ez magában foglalja a pénzügyi károkat, a jó hírnév megsértését.[27]

3. A személyiséglopás fajtái

A személyiséglopás 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, pénzlopás az egyéb bűnözői 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.[28]

Egy többszerzős tanulmány[29] szerint az identitáslo-

[22] https://www.law.cornell.edu/uscode/text/18/1028 (letöltés ideje: 2019. 08. 20.)

[23] Borges et. al. i. m. 338–339. o.

[24] Az Európa Tanács égisze alatt Budapesten elfogadott, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezmény.

[25] Borges et. al. i. m. 339–340. o.

[26] A terrorizmus finanszírozásáról lásd bővebben: Gál István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. In: Szakmai Szemle: A katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata. 2012/1 8. 5–15. o. Gál István László: A XXI. század új bűncselekmény-típusa: a terrorizmus finanszírozása. Rendészeti Szemle: Az Igazságügyi és Rendészeti Minisztérium Szakmai, Tudományos Folyóirata. 2009/6. 61–90. o.

[27] https://www.comparitech.com/identity-theft-protection/identity-theft-assumption-deterrence-act/ (letöltés ideje: 2019. 09. 02.)

[28] Hoffman–McGinley: i. m. 3–5. o.

[29] 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.

pástól meg kell különböztetni az identitásátvételt, amikor az elkövető egy létező személy identitását veszi át annak beleegyezése nélkül. Továbbá külön kategória még az identitásdelegálás, 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[30] szerint megkülönböztetünk vagyoni, egészségügyi, bűnügyi, szintetikus és gyermekidentitás-lopást. Különleges kategóriaként említik még az ún. identitásklónozást.

- 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 bankkártyaadatok 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 dark neten. Maga az elkövető is igénybe vehet jogtalanul az egészségügyi szolgáltatásokat. 2017-ben 300 egészségügyi szerv tett feljelentést az Egyesült Államokban arról, hogy feltörték az adattároló rendszerüket.[31]
- Bűnügyi személyiséglopás 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 BJE 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 szóló nem fényképes okiratok átadása esetén is megvalósul a közokirat-hamisítás.[32] 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.[33]
- Szintetikus személyiséglopás 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 gyermekidentitás-lopás a szintetikus személyazonosság-lopás egyik válfajaként 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 identitásklónozás, amikor az elkövető nemcsak 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 identitásklónozás például munkavállalás, házasságkötés, gyermekvállalás céljából. Az elkövetők tipikusan illegális bevándorlók vagy büntetett előéletű emberek.

4. A személyiséglopás technikái az interneten

4.1. Phising

A teljesség igénye nélkül csak gyakoribb elkövetési technikákat ismertem. 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.[34]

[30] 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.

[31] https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (letöltés ideje: 2019. 06. 16.)

[32] BH 2014.234.II.

[33] Kúria Bfv.1695/2017/6.

[34] Geradts Zeno: Identity theft. In: Siegel Jay – Saukko, Pekka (szerk): Encyclopedia of Forensic Sciences, Second Edition. Academic Press, Amster-

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.[35]

4.2. Smishing

A phisinghez hasonló elkövetési technika a smishing.[36] 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 sms-eket küldenek, amelybe kérik a bankkártyaszámot, személyes adatokat, hogy megoldhassák az egyébként nem létező problémákat (pl.: hogy ne zárolják az ügyfél bankszámláját).

4.3. Wi-phising

Arra is volt példa, hogy a bűnelkövetők felállítottak egy vezeték nélküli hálózatot (wifit), amelyre, ha a gyanútlan felhasználók csatlakoznak, veszélynek teszik ki személyes adataikat. Ez az ún. Wi-phising.[37]

4.4. Skimming

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 bankkártyaadatainkat.[38]

4.5. Hacking

Egy klasszikus technikája az identitáslopásnak a jogosulatlan behatolás (hacking). Erre volt példa a 2005-ben végrehajtott támadás a DSW cipőbolthálózat ellen, melynek eredményeképpen 1,4 millió kártyaforgalmi adatot loptak el 108 boltól.[39]

4.6. Cybersquatting

Vitatott, hogy személyiséglopásnak minősül-e az ún. cybersquatting jelensége.[40] Cybersquatting esetében az elkövetők regisztrálnak egy domainnevet, egy meglévő védjegy vagy híres személy nevével. Az elkövetők arra számítanak, hogy a jövőben a meghatározott egyénnek, vagy üzleti cégnek szüksége lesz, majd erre a domainre, és ahhoz, hogy ezt megszerezzék, ki kell vásárolniuk az elkövetőktől, jóval magasabb összegért, mint az eredeti regisztrációs díj. Kérdés, hogy ez személyiséglopásnak minősül-e, vagy csak egy rosszhiszemű magatartásnak. Gatsik szerint, ez gyakorlatilag egy álcázott identitáslopás. Véleménye szerint ennek a cselekménynek hasonló hatásai vannak, így:

- csorbulhat egy személy hírneve, becsülete,
- anyagi károkat okoznak,
- visszaélnek egy személy nevével.

Példaként említi, amikor visszaéltek Sharon Stone és Walt Disney nevével. Létrehoztak egy sharonstone.com és egy dosney.com weboldalt, ahol pornográf tartalmakat tettek közzé, ezzel azt a látszatot keltve, hogy ők támogatják a szexipart.[41]

5. Az áldozatoknak okozott károk

Az Egyesült Államokban a Javelin nevezetű közvélemény-kutató cég 2019-es jelentése szerint 2018-ban az áldozatok száma 14,4 millió fő volt.[42] 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.[43]

A személyes adatok jogellenes hozzáférése nem csak anyagi szempontból viseli meg az áldozatokat. Johnson tanulmánya szerint évente több mint 9 millió áldozatnak átlagosan 1400 dollárt kell költeniük egy 2-4 évig terjedő időszakban, 600 órát eltöltve, hogy tisztázzák a nevüket.[44] Továbbá az FDA szerint elveszíthetik az állásukat, nehezebben juthatnak új álláshoz, elutasíthatják kölcsön- vagy hiteligénylésük, ingatlanukat, gépjárművüket, és még le is tartóztathatják őket, olyan cselekményért, amit el sem követtek.[45] Szélsőséges ügyek is vannak, például egy korábbi kémia szakon végzett

dam–Boston–Heidelberg–London–New York–Oxford–San Diego–San Francisco–Sydney–Tokyo. 2013. 419. o.

[35] Whitson, Jennifer – Haggerty, Kevin D.: Identity theft and the care of virtual self. In: Economy and Society 2008. 579. o.

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

[37] Uo.

[38] 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. 226–237. o.

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

[40] Gatsik, Jonathan H.: Cybersquatting: Identity theft in disguise. Im: Suffolk University Law Review. 2001/2. 277–302. o.

[41] Gatsik, Jonathan H.: Cybersquatting: Identity theft in disguise. Im: Suffolk University Law Review. 2001/2. 297–299. o.

[42] https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt (letöltés ideje: 2019. 06. 16.)

[43] 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.

[44] Johnson, Vincent R.: Cybersecurity, identity theft and the limits of tort liability. In: South Carolina Law Review. Vol. 57. 2005. 257. o.

[45] Samaha, i. m. 393. o.

hallgató talált egy biztonsági rést egy kereskedelmi weboldalon és váltságdíjat követelt a cégtől, azért cserébe, hogy ne lopja el a személyes adatokat.[46]

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.[47]

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.

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

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

7. Összegzés

A személyiséglopás és az ahhoz hasonló 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, 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 a 2019/73 irányelvet, ami megújítja az uniós szabályozást a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és hamisítás elleni küzdelem jogi eszköztárát.

Felhasznált irodalom jegyzéke

- Alisdair A. Gillespie: Cybercrime. Key Issues and Debates. Routledge, New York. 2016.
- Arnold, Tom: Internet Identity Theft. A Tragedy for Victims. A White Paper from the Technology Working Group, eBusiness Division, SIIA Project. 2000.
- Biegelman, Martin T.: Identity theft Handbook: detection, prevention and security. John Wiley and Sons, Inc, Hoboken, New Jersey. 2009.
- Borges, G. – Schwenk, J. – Stuckenberg, C. – Wegener, C.: Identitätsdiebstahl und identitätsmissbrauch im Internet. Rechtliche und technische Aspekte. Springer, Heidelberg–Dordrecht–London–New York. 2011.
- Busch, Christoph: Biometrie und Identitätsdiebstahl. In: Datenschutz und Datensicherheit – DuD. 2009/5. 317–317. o.
- Chawki, Mohamed – Wahab, S. Abdel Mohamed: Identity theft in cyberspace: issues and solutions. In: Lex Eletrconica 2006/1. 595–605. o.
- Eszteri Dániel – Máté István Zsolt: Identitáslopás a virtuális világban. In: Belügyi Szemle 2017/3. 79–107. o.
- Gál István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. In: Szakmai Szemle: A katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata. 2012/1 8. 5–15. o.
- Gál István László: A XXI. század új bűncselekménytípusa: a terrorizmus finanszírozása. Rendészeti Szemle: Az Igazságügyi és Rendészeti Minisztérium Szakmai, Tudományos Folyóirata. 2009/6. 61-90. o.
- Farina, Katie A: Cyber Crime: Identity Theft. In: International Encyclopedia of the Social & Behavioral Sciences. 2015. 633–637. o.
- Gatsik, Jonathan H.: Cybersquatting: Identity theft in disguise. Im: Suffolk University Law Review. 2001/2. 277–302. o.
- 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. 419–422. o.

[46] Rustad, Michael L.: Private enforcement of cybercrime on the electronic frontier. In: Southern California Interdisciplinary Law Journal. 2001/11. 63. o.

[47] https://victimsupportservices.org/help-for-victims/crime-types/identity-theft/ (letöltés ideje: 2019. 06. 15.)

- Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. In: Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata. 2011/1-2. 12–28. o.
- Hámori Balázs: Bizalom, jóhírnév és identitás az elektronikus piacokon. In: Közgazdasági Szemle 2004/9. 832–848.
- Hoffman, Sandra K. – McGinley, Tracy G.: Identity theft. ABC-CLIO, Santa Barbara, California, 2010.
- Johnson, Vincent R.: Cybersecurity, identity theft and the limits of tort liability. In: South Carolina Law Review. Vol. 57. 2005. 257. o.
- Kahn, Charles M. – Roberds, William: Credit and identity theft. In: Journal of Monetary Economics 55. 2008. 251–264. o.
- Koops, Bert Jaap, – Leenes, Ronald et. al: A typology of identity-related crime. Conceptual, technical and legal issues. In: Information, Communication & Scoitey. 2009/1. 1–24. o.
- Lawson, Philippa – Lawford, John: Identity theft: the need for better consumer protection. Public Interest Advocacy Centre. 2003.
- 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. 595–605. o.
- 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. 1–21. o
- Rustad, Michael L.: Private enforcement of cybercrime on the electronic frontier. In: Southern California Interdisciplinary Law Journal. 2001/11. 63–116. o.
- Samaha, Joel: Criminal law. Ninth edition.Thomson Wadsworth Publisher, USA, Belmont. 2008.
- Schwartau, Winn: Information warfare. Kindle e-book edition. Interpact Press Inc, New York. 2010.
- Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. In: Themis: 2015/1. 343–375. o.
- Tajpour, Atefeh – Ibrahim, Suhaimi – Zamani, Mazdak: Identity theft methods and fraud types. In: International Journal of Information Processing and Management 2013/7. 51–58. o.
- 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. 226–237. o.
- Whitson, Jennifer – Haggerty, Kevin D.: Identity theft and the care of virtual self. In: Economy and Society 2008. 572–594. o.

Felhasznált internetes hivatkozások

- https://victimsupportservices.org/help-for-victims/crime-types/identity-theft/ (letöltés ideje: 2019. 06. 15.)
- https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft (letöltés ideje: 2019. 06. 10.)
- https://www.comparitech.com/identity-theft-protection/identity-theft-assumption-deterrence-act/ (letöltés ideje: 2019. 09. 02.)+
- https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (letöltés ideje: 2019. 06. 16.)
- https://www.ftc.gov/node/119459 (letöltés ideje: 2019. 09. 20.)
- https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt (letöltés ideje: 2019. 06. 16.)
- https://www.law.cornell.edu/uscode/text/18/1028 (letöltés ideje: 2019. 08. 20.)