NAGY ZOLTÁN ANDRÁS

A CSALÁS-JELLEGŰ CSELEKMÉNYEK AZ E-KERESKEDELEM KÖRÉBEN

1. Bevezetés

A katonai kutatás alapvetően a kommunikáció céljára hívta életre az internetet,[1] mely közel 30 évig az Egyesült Államok honvédelmi minisztériumának fennhatósága alatt működött a funkció bővülését követő különböző elnevezésekkel. Az 1980-as években a számítógépes hálózat megjelent Nyugat-Európában is, ez már a globalizálódás kezdete volt, igaz az európai és észak-amerikai hadseregeket kötötte össze. Az 1990-es évektől engedélyezték a hálózat kereskedelmi célú, egyszersmind civil hasznosítását.

1992-ben J.H. Snider and Terra Ziporyn szerzőpáros kiadta a „Future Shop: How New Technologies Will Change the Way We Shop and What We Buy" című könyvét. 1994-ben megjelent az első cég Pizza Hut. Közzétették az első banner hirdetéseket a hotwired.com honlapján. Az egyik a Zima nevű üdítőitalt, a másik az AT&T szolgáltatásait hirdette.1995-ben Amazon.com is megnyitotta virtuális áruházát, nem sokkal később az eBay is 1996-ban életre hívták az első netbankot NETBank nevén, amely 2007-ben zárta be „kapuját". Az első „fecskék" után ma már tömegesen találunk üzleti – kereskedelmi tevékenység folytatására szakosodott web-oldalt. A bevezetőben néhány fogalom tisztázása fontos.

Az elektronikus üzletvitel (electronic business, röviden: e-business) a számítógépes hálózatokon bonyolított gazdasági tevékenységek összessége. Tágabb fogalom, mint az elektronikus kereskedelem (electronic commerce, röviden e-commerce), mert magában foglalja a marketinget, a munkaügyi teendőket, a vevő tájékoztatást, a logisztikai és további feladatok végrehajtását. Az e-business területei a következők:

[1] Az internet (Internetworking System – hálózatok hálózata rövidítés). A szovjet szputnyik 1957-es sikeres fellövését követően kitört az USA-ban az ún. „szputnyik-sokk". Ezt ellensúlyozandó, többirányú fejlesztésbe kezdtek. Ezek egyike volt az, hogy a hadserege vezetésének megbénítását megakadályozandó, több vezetési pontot alakítottak ki. Ezeket földalatti kábellel kötöttek össze. Majd egyre több katonai és civil kutatóintézet és egyetem csatlakozott a hálózatra, míg végül szétvált a katonai és civil hálózatra, amely utóbbit 1993-tól lehet szabadon használni.

Business to business (röviden: B2B): az eladó is vállalat, vállalkozás (szervezet), és a vevő is vállalat, vállalkozás (szervezet). Két vagy több cég, intézmény között létrejövő elektronikus marketing, logisztikai, értékesítési és egyéb relációk. Legjellemzőbb területei a nagykereskedő és kiskereskedő között kereskedelmi kapcsolat, illetve a vállalkozások egymás között kötött üzleti célú megállapodásai, azok teljesítése, marketing folytatása stb.

Business to consumer (B2C): a vállalat, vállalkozás a fogyasztó felé fordul áru-, szolgáltatás nyújtása, marketing (reklám, kérdőív, nyereményjáték formájában is), kommunikáció és egyéb üzleti célból.

Cwonsumer to business (C2B): a fogyasztó keresi a vállalkozásokat, vállalatokat, áruvásárlás, szolgáltatás rendelése, igénybe vétele (web-shopok, utazási irodák, autóbérlés stb.) céljából.

Consumer to consumer (C2C): a fogyasztó a fogyasztóval áll üzleti, kereskedelmi kapcsolatban, például second hand oldalakon, vásárok hirdetésével, egyéni eladásokkal.

Léteznek aztán további relációk:

Az e-businessbe a kormányzat, önkormányzat, államigazgatás is beléphet, pl. koncessziós pályázatok, közbeszerzések kiírása, állami megrendelések stb. (A2B), koncessziós-, közbeszerzési pályázatok benyújtása, állami megrendelések teljesítése stb. (B2A), adó-, vám-, illeték kiszabása, beszedése (A2C, A2B), fizetése, hivatalos okiratok intézése, ellenértékük megfizetése céljából (B2A, C2B).

Továbbá – sajnos, realitás – a Criminals to Criminals (C2C) viszonylat is, a külön kliens programmal elérhető Darkneten virtuális valutáért fegyverek, hamis okiratok, pornográf-, pedofil fotók, videók, az e-mail-címek, személyes adatok, kábítószer és más tárgyak, eszközök adásvétele, a botnetek, a bérgyilkosság bérlése, bűnözők, terroristák titkolt kommunikációja és más ügyletek.

Az elektronikus üzletvitelnek része az elektronikus kereskedelem, amely a távollévők között, elektronikus eszközök által tett olyan jogilag releváns cselekményeket foglalja magában, amelyek egyedileg meghatározható jogalanyok között polgári jogi jellegű jogviszonyt hoznak létre, feltéve, hogy a jogszabály az elektronikus kereskedelemre vonatkozó rendelkezések alkalmazását nem zárja ki.[2] E teljeskörű, absztrakt definícióból kiszűrhető, hogy az e-kereskedelem a polgárjogi szabályok szerinti zajló eladó és vevő közötti adásvételre, szolgáltatás nyújtására koncentrál.

Az e-kereskedelem nem korlátozódik a számítógépes hálózatokon (interneten, extraneten, intraneten) folyó kereskedelmi tevékenységekre, idetartoznak a külön-

[2] KONDRICSZ Péter – TÍMÁR András: Az elektronikus kereskedelem jogi kérdései. Budapest, KJK-Kerszöv. Jogi és Üzleti Kiadó, 2000. 71. o.

böző automaták (a jegykiadó automatáktól az édességet, üdítőket áruló automatákig), a mobiltelefonon közvetlenül vagy valamely applikáción keresztül történő áru-, szolgáltatásrendelés és fizetés.

Jelen fejezetünk az interneten zajló kereskedésre fókuszál.

2. Az e-kereskedelemmel összefüggő csalás-jellegű tevékenységek típusai

2.1. A megtévesztő tartalomközlésekkel megvalósuló csalás-jellegű tevékenységek[3]

Az internet weboldalain, az elektronikus hirdetőtáblákon (bulletin boards), hírcsoportban (news-groups), a különböző közösségi oldalakon, a Twitteren, Messengeren, chat-oldalakon, saját weboldalon, más weboldalak fórum rovataiban, az FTP-, a goopher-, a telnet-hálózatokon, az intra-, és az extraneten tehetők közzé árut, szolgáltatást hirdető tartalmak, szövegben, képben, valamint ezekhez csatolt audió-, vagy videofájlban. Továbbá küldhetők közlések, hirdetések[4] egy meghatározott személynek, illetve korlátlan számú személynek elektronikus levélben (e-mailben). E számos közlésre alkalmas oldalon egyaránt olvashatók – csak az üzleti – kereskedelmi tartalmakat tekintve – valódi és megtévesztő információk.

2.1.1. A csaláshoz (Btk. 373.§) legközelebb álló tartalomközléssel elkövethető bűncselekmény a Btk. 412. §-ba ütköző és e szakasz szerint minősülő „piramisjáték szervezése" bűncselekmény. A „szervezés", mint elkövetési magatartás felölheti a számítógépes hálózaton történő jellemzőn írásbeli tájékoztatást (pl. a szabályok ismertetését, a kis befektetéssel nagy nyereséget hozó megtévesztő ígéretet stb.), ami – implicite – felhívást, mint verbális előkészületi magatartás, vagy ha sikeres a felhívás, akkor az rábírás, mint felbujtói magatartás.

Nem csupán a piramisjáték kezdeményezője tekintendő szervezőnek, hanem azok is, akik újabb személyeket szerveznek be a játékba, azaz, akik megosztják a piramisjátékra vonatkozó tartalmakat, kivéve azon felhasználókat, akik a játéktól való tartózkodásra hívják a figyelmet, akik leleplezik a játék valódi természetét.

[3] Nagy Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1. 1992/1. 22-26. o.

[4] Nagy Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. Belügyi Szemle 2018/7-8. 87. o.

2.1.2. Megtévesztő tartalomközlés vonatkozhat továbbá egyfelől rossz minőségű termékre is.[5] A rossz minőség fogalmát a Büntető törvénykönyv egy speciális – csak e szakaszra releváns – értelmező rendelkezésben határozza meg, melynek értelmében: rossz minőségű a termék, „ha a jogszabályban vagy az Európai Unió közvetlenül alkalmazandó jogi aktusában előírt biztonságossági vagy minőségi követelményeknek nem felel meg, ilyen előírás hiányában akkor, ha a termék rendeltetésszerűen nem használható, vagy használhatósága jelentős mértékben csökkent." (Btk. 415.§ (6) bekezdése).

Ha a forgalomba hozatal megtörténik, akkor a tevékenység a Btk. 415.§ (1) bekezdésébe ütköző és egyéb minősítő körülmények hiányában ugyanezen bekezdés szerint minősülő rossz minőségű termék forgalomba hozatal bűncselekménye valósul meg.[6]

Ugyanakkor a termék számítógépes hálózaton történő felkínálása megvételre a bűncselekmény előkészületi cselekményének (Btk. 415.§ (3) bekezdés) minősül.

A jogalkotó a fogyasztói érdekek védelme, a termékek minőségbiztosításának fontossága miatt a gondatlan bűnelkövetést is szankcionálja (Btk. 415.§ (4) bekezdés).

Ugyanakkor a forgalmazás felhívója büntetlenségét biztosítja a törvényhozó, ha mihelyt tudomást szerez a termék rossz minőségéről, mindent megtesz azért, hogy a rossz minőségű termék a birtokába visszakerüljön (Btk. 415.§ (5) bekezdése).

Mivel megtévesztő tartalomközléssel valósul meg a rossz minőségű termék forgalomba hozatala, így – értelemszerűen – a csalás (Btk. 373.§) bűncselekményéhez való viszonyát tisztáznunk kell. A rossz minőségű termék forgalomba hozatala bűncselekmény tárgyi oldalán eredményt, in concreto kárt nem határoz meg a törvényhozó a tényállásban, míg a csalás bűncselekménye tárgyi oldalán a kár tényállási elem. Ha azonban a jogsértő cselekmény elkövetésével kár is keletkezik, és a csalás büntetési tétele az adott esetben magasabb, a konszumpció elve alapján kizárólag csalás megállapítására kerülhet sor.[7]

Még egy megjegyzés, amennyiben a rossz minőségű termék egyben olyan termék, amely az adott közfogyasztási cikk vonatkozásában valamilyen rendellenességet mutat (pl. megromlott, a gyártási technológia miatt vagy tárolása során vált rendellenessé), és ezzel egészségre is káros, akkor ártalmas közfogyasztási cikkel visszaélés bűncselekményt (Btk. 189. §) kell felhívni. Megjegyzendő, hogy ennek

[5] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. Budapest, KJK-Kerszöv., 2002. 193-200. o.

[6] Lásd ehhez Szathmáry Zoltán: A hamis termékek forgalmazásával elkövetett iparjogvédelmi jogok bizonyításának nehézségei. Ügyészek Lapja 2015/2. 5-15. o.

[7] Tóth Mihály: Rossz minőségű termék forgalomba hozatala. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014. 569-571. o.

a bűncselekménynek nincs előkészülete, így e bűncselekmény csak a forgalomba hozatallal jön létre (Btk. 189.§ (2) bekezdése).

2.1.3. Másfelől az áru valamely „lényeges tulajdonságai" tekintetében is lehet megtévesztő a tartalomközlés.[8]

Ez esetben a Btk. 417.§ (2) bekezdése szerint minősülő és ugyanezen szakasz szerint büntetendő fogyasztók megtévesztése bűncselekmény jön szóba. E bekezdésben a bűncselekmény elkövetési magatartása, jelesül a „megtévesztésre alkalmas tájékoztatás" számítógépes környezetben is releváns lehet. A lényeges tulajdonság absztrakt fogalmát egy speciális értelmező rendelkezés részletezi:

– az áru összetétele, műszaki jellemzői és az árunak az adott célra való alkalmassága,
– az áru eredete, származási helye,
– az áru tesztelése, ellenőrzöttsége vagy annak eredménye (Btk. 417. (4) bekezdése).

A bűncselekmény súlyosabban minősül, és akár három évig terjedő szabadságvesztéssel is büntetendő, ha az áru egészségre vagy környezetre gyakorolt hatásával, veszélyességével, kockázataival vagy biztonságosságával kapcsolatos jellemzőivel összefüggésben követik el.

A fogyasztók megtévesztése bűncselekmény tényállásban esetleges tárgyi elemként szerepel a hely, in concreto a „nagy nyilvánosság". A magyar büntetőjogban az 1999. CXX. törvény a nagy nyilvánosság fogalmát kiterjesztette az elektronikus hírközlési hálózatokra is, így a számítógépes hálózatok is ideértendők. A nagy nyilvánosság jelen fogalma a Btk. értelmező rendelkezésének 22. pontjában olvasható, – természetesen – az elektronikus hírközlő hálózat fogalmával együtt. Így a fogyasztók megtévesztése bűncselekménye ide idézett alapesete (2) bekezdése is csak akkor valósul meg, ha azt nagy nyilvánosság előtt, pl. számítógépes hálózatokon keresztül követik el.

2.1.4. Az áru eredetére vonatkozó hamis vagy csupán részben valódi tartalomközlés is megvalósíthat bűncselekményt, ha a vámellenőrzés alól elvont nem közösségi árut, jövedéki adózás alól elvont terméket, vagy lopásból, sikkasztásból, csalásból, hűtlen kezelésből, rablásból, kifosztásból, zsarolásból, jogtalan elsajátításból vagy orgazdaságból származó dolgot kínálnak eladásra. Amennyiben az eladó a dolog az elkövető birtokában van, és ezért tudja az árut értékesíteni, akkor orgazdaságért

[8] Tóth (2002): i.m. 219-228. o. Tóth Mihály: Fogyasztók megtévesztése. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014. 572-575. o.

(Btk. 379.§) felel, amennyiben nincs a bűncselekményből származó dolog a birtokában, de tud arról, hogy lelhető fel vagy rendelésre elérhetővé válik, akkor bűnpártolásért (Btk. 282.§) felel az elkövető.

Az orgazdaság elkövetési tárgyai egyfelől a közösségi áruk, melyek:

– olyan áruk, amelyeket teljes egészében a Közösség vámterületén állítottak elő/jöttek létre (és nem tartalmaznak harmadik országból importált árukat),
– olyan harmadik országból importált áruk, amelyeket szabad forgalomba bocsátottak,
– olyan áruk, amelyet vagy harmadik országból importált és szabad forgalomba bocsátott árukból, vagy a Közösség területén létrejött/előállított árukból és harmadik országból importált és szabad forgalomba bocsátott árukból állítottak elő/jöttek létre.

A nem közösségi áruk tehát, olyan áruk, amelyek eltérnek a közösségi áruktól.

Másfelől a jövedéki termékek, mint elkövetési tárgyak:

– az ásványolaj,
– az alkoholtermék,
– a sör,
– a bor,
– a pezsgő,
– a köztes alkoholtermék,
– a dohánygyártmány.[9]

A teljesség igényével: ha a jövedéki termék az elkövető birtokában van, és értékesíti az árut, akkor költségvetési csalást (Btk. 396.§) követi el, azonban, ha az elkövető nincs a jövedéki termék birtokában, de tud arról, hogy az hol lelhető fel vagy rendelésére elérhetővé válik, akkor bűnpártolásért (Btk. 282.§) felel.

2.1.5. Megtévesztő tartalomközlés lehet olyan termékre vonatkozóan, amely a termék valódi mivoltát, tulajdonságait részben vagy egészben leplezi. E körbe tartozhatnak a jogszabályokban tiltott termékek.

A termék kábítószernek minősülő elegy, szer, tabletta stb. összetételének elhallgatásával megtéveszti az érdeklődő felhasználót, akkor a kábítószert áruló személy, ha a kábítószert forgalomba hozta, akkor a Btk. 176.§ (1) bekezdésébe ütköző és egyéb minősítő körülmények hiányában e bekezdés szerint büntetendő kábítószer-

[9] 2003. évi CXXVII. törvény a jövedéki adóról és a jövedéki termékek forgalmazásának különös szabályairól 3.§ (2) bekezdés

kereskedelem bűntettét követi el. Amennyiben a forgalomba hozatal nem valósult meg, akkor pedig a bűncselekmény előkészülete (Btk. 176.§ (6) bekezdés) valósul meg. Továbbá a kábítószer forgalomba hozatalához szükséges számítógépes háttér biztosítója delictum sui generis bűnsegédként felel (Btk. 176.§ (4).

Hasonló a szabályozás az új pszichoaktív anyag forgalmazása esetén (Btk. 184.§ (1) bekezdés). Tehát büntetendő a dizájner drogok forgalmazásának előkészülete (Btk. 184.§ (6) bekezdése), és a forgalmazáshoz nyújtott delictum sui generis bűnsegély is (Btk. 184.§ (4) bekezdése).

A doppingszerek[10] esetében a Büntető Törvénykönyv a forgalmazói magatartásokat rendeli büntetni (Btk. 185.§ (2) bekezdése). Szankcionált a forgalmazás előkészülete is (Btk. 185.§ (4) bekezdés).

A fenti tilalmakhoz hasonló a hamis, hamisított vagy Magyarországon nem engedélyezett egészségügyi termékek forgalmazása büntetni rendeltsége (Btk. 186.§ (1) bekezdés). Úgyszintén tiltott a forgalmazás előkészülete is (Btk. 186.§ (4a) bekezdés).

Ezekben az esetekben bár lehet megtévesztő a tartalomközlés a termék tulajdonságára, összetételére, más jellemzőjére vonatkozóan, sőt a potenciális fogyasztók tévedésbe ejtésének vagyoni haszonszerzési célja is lehet, de ez nem csalásként (Btk. 373.§) értékelendők, hanem a fentebb említett tényállások hívandók fel.

2.1.6. Ismert olyan megtévesztő és haszonszerzési célú tartalomközlés, amely nem bűncselekmény, mivel előkészülete nincs, kísérleti szakaszba lépése pedig látens marad, és csak a befejezett bűncselekmény észlelhető.

Az internetes pénzügyi visszaélések közül a leghíresebb-leghírhedtebb az ún. nigériai levelek („Advance Fee Fraud", vagy „419 Fraud" [Four-One-Nine], – a 419-es szám a nigériai büntető törvénykönyv idevonatkozó rendelkezésének a száma) néven elhíresült csalássorozat.

Lényege az, hogy a gyanútlan felhasználó saját e-mail címére kap egy levelet, amelyben egy magas rangú nigériai hivatalnok, kormánytag stb. leszármazója a gyanútlan felhasználónak (egy szívhez szóló levélben) arról panaszkodik, hogy apja halála után a családi vagyont zárolták, és annyi pénze sincs, hogy az ügyvédi, és egyéb díjakat, – amelynek fejében a vagyont vissza tudná szerezni – kifizesse. Így pénzt kér egy nigériai bankszámlára. Természetesen a visszaszerzett vagyonból busásan „kárpótolná" a neki segítőt.[11]

Ezekhez hasonló a nemrégiben feltűnt és talán most is „játszott" holland lottó. Ebben az esetben a gyanútlan felhasználó szintén a saját e-mail címére kap egy levelet,

[10] Lásd bővebben: Nagy Zoltán András: Sport és büntetőjog. Pécs, Kódex Nyomda, 2014.
[11] http://www.webmutato.hu/webmix/uzlet/vigyazat.htm [2018.03.31.]

amelyben közlik vele, hogy nyert Hollandiában a lottójátékon, ám a nyeremény átvétele előtt ki kellene fizetni a nyereményadót, meg valamilyen járulékos költséget. Tehát a megtévesztés abban áll, hogy nyereményt ígérnek bizonyos pénzösszeg megelőlegezését követően.[12] Már spanyol, sőt svájci lottóként is ismert ugyanez a szisztéma.

Újabb hasonló próbálkozás volt, amikor a „nigériai levelek" példáját követve a Dél-Afrikai Köztársaságból érkeztek megkeresések magyar felhasználókhoz.[13]

Mivel a csalás bűncselekményének (Btk. 375.§) az előkészülete kívül esik a büntetni rendeltségen, így ezek a megtévesztő tartalomközlések legfeljebb erkölcsileg helyteleníthetők, hiszen csupán a megtévesztésből nem keletkezhet kár.[14]

2.2. A tranzakció során megvalósuló megtévesztések

Az e-kereskedelem folytatásához – általában – e-boltok „nyitása" szükséges feltétel. Az ügylet távollévők között köttetnek.[15] A tranzakcióra a távollévők között kötött szerződés külön szabályai irányadók. Ennek egyik legfontosabb szabálya fogyasztó elállásának a lehetősége. A felhasználó egyoldalúan visszaléphet és a termék visszaküldése esetén követelheti a kereskedőtől az általa kifizetett összeg visszatérítését.[16] Az elállási jog kompenzálja azt, hogy a vásárlás előtt nem volt lehetőségünk a termék megvizsgálására, kipróbálására, illetve üzembe helyezésére.

Az e-boltokban történő vásárlás előtt a felhasználónak regisztrálnia kell egy azonosítóval és egy jelszóval, majd ezen adatokkal tud belépni az e-boltba. Ott a kiválasztott árut egy virtuális kosárba helyezi, majd kiválasztja a szállítási címet (a felhasználó lakcímére, a pick-pontra vagy az értékesítőhelyre), majd a fizetés módját (utánvéttel a teljesítés helyén, bankkártyával on-line, átutalással, az eladó valós térbeli telephelyén, raktárában, készpénzzel vagy kártyával stb.), majd a vevő a regisztráció során megadott e-mail címre, telefonra stb. kap egy visszaigazolást a vásárlásról.

Az e-boltok virtuális áruházak[17], amelyeknek több előnyét már megtapasztalhattuk és fejlődésüknek is emiatt töretlen:

---

[12] http://index.hu/tech/jog/holland0902/ [2018.03.31.]

[13] Lásd Clough, Jonathan: Principles of cybercrime. Second Edition. Cambridge University Press, 2015. 209-212. o.

[14] Erdősy Emil – Földvári József – Tóth Mihály: Magyar Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2004. 507. o.

[15] 45/2014. (II. 26.) Korm. rendelet III. fejezete

[16] 45/2014. (II. 26.) Korm. rendelet III. 24. §

[17] Érdekességként megemlítendő, hogy a webáruházakra nézve veszélyt jelenthetnek az ún. DDoS-támadások, melyek jelentős bevételkiesést és presztízs veszteséget eredményezhetnek a támadással érintett cégnél. Lásd Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 70. o.

– A valós térbeli üzleti lehetőségekkel szemben a teljes választék prezentálható.
– Nélkülözhető egy üzlet-, irodahálózatot fenntartása, elegendő egy raktáráruház, központi irodára, esetleg elég egy logisztikailag jól szervezett hálózat részének lenni, ahol közvetítő tevékenység is folytatható, kevesebb élőmunka szükséges a tevékenységhez.
– Költséghatékony, ami olcsóbb árakat is jelenthet, pontosabban jelenthetne, ha a szállítási költségek nem drágítanák meg az értékesítést.
– Mivel nincsenek üzletei a vállalkozásnak, nem kell azokat folyamatosan feltölteni, így az állandó szállítások hiányában ez az értékesítési forma egyben környezetbarát is.
– Gyakorlatilag non-stop „nyitva tartással" működnek az e-boltok.
– Mivel a Föld minden tájékán működnek e-boltok, így a vevő előtt megnyílik az egész világ.
– Gyors üzletkötés lehetősége adott („one click order").
– A vállalkozás számára a reklám lehetőség saját web-oldalán korlátlan, ezt segíthetik linkek, nyereményjátékok stb.
– A vállalkozás a piackutatáshoz, marketing tevékenységének eredményesebbé, sikeresebbé teheti saját felhasználású kérdőíve elérhetőségével web-oldalán.
– A vevőnél a kényelmi szempontok elvitathatatlanok, karos székből választhat és házhoz szállítják az általa rendelt árukat.
– Tegyük hozzá nem kevés malíciával, hogy az is előnye az e-boltoknak, – mivel fizikailag nincsenek jelen a vevők, – így nem lopnak, nem lophatnak a boltból, ami ugyebár a valós térbeli boltoknál, üzleteknél reális veszély.

Az e-boltok térhódításukkal ma még kiegészítik a valós térben található kereskedelmi egységeket, és biztosak lehetünk abban, hogy nem is szoríthatja ki azokat, hiszen vannak olyan hátrányai az e-boltoknak, amelyeket nem lehet kiküszöbölni.

– A vevő nem kerül fizikai kapcsolatba az általa kinézet vagy választott termékkel, így (cipők, ruhadarabok nem próbálhatók fel, használt gépjármű vétele kifejezetten „zsákbamacska").
– Hátrány az is, hogy az értékesítés során a vevő és az eladó közötti kontextus személytelen, elmarad az eladó segítőkészsége, rábeszélése"
– Nem minden áruféleség értékesíthető, illetve értékesíthető a vevő számára biztonsággal (pl. a törékeny áruk), továbbá frissensült élelmiszerek (pl. pizza, egyéb péksütemény), ha a vevő frissen is kívánja elfogyasztani, aki az eladónak és megrendelőnek időben – viszonylag – közel kell lenniük egymáshoz.

A veszélyek az e-kereskedelem hátrányaiban rejlenek. Az eladó oldalán jelentkező gond az, hogy nem kerül fizikai kapcsolatba a vevővel és a vevő bankkártyájával. Egyfelől nem lehet biztos abban, hogy a megrendelő valós személy-e vagy valós e-mail-címmel regisztrált-e. Másfelől az eladó a vevő által használt bankkártyával sem érintkezik, és szintén nem lehet biztos abban, hogy a bankkártya, mivel fizettek, valódi-e és, ha valódi is a tényleges kártyabirtokosé vagy sem.

A vevő is aggódhat azért, hogy megkapja-e az árut, illetőleg az áru az-e, amit rendelt, az áru nem bűncselekményből származik-e, nem szenved-e más jogi vagy minőségi fogyatékosságban.

Az üzletkötés gyorsasága és egyszerűsége iránt igényt kell a biztonság követelményével összeegyeztetni.

2.2.1. Card-present csalás[18]

Hazánk pénzügyi történetéből – gazdasági fejletlensége miatt – a „csekk-korszak" kimarad és a fejlett piacgazdaságok technikai evolúciójában a bankkártyák korszakába csöppent. Először 1988-ban jelent meg az első, még devizaszámlához kapcsolt, egy évvel később a csekkhez kötött kártya. Ugyanebben az évben került forgalomba az első ún. ATM – kártya is.

Ma Magyarországon hét és félmillió körüli különféle banki műveletek végrehajtására szolgáló bankkártya,[19] valamint több százezer nem a bankok által kibocsátott plasztiklapok kerülnek forgalomba, így az American Express (Amex)-kártyái, valamint olajtársaságok üzemanyagkártyái, kereskedelmi egységek kártyái stb.

A bankkártyák funkciói folyó-számlakezelés, készpénzfelvétel automatából vagy a pénztárból, készpénz nélküli vásárlás, átutalás, vásárlás az interneten keresztül, hitelfelvétel, csekkgarancia stb. Sőt, – saját tapasztalatból merítve – az Egyesült Királyságban a kártyával történő vásárlás helyén pénzfelvételre is van mód (ez az ún. cash – back funkció), azonban e szolgáltatás hazánkban még ismeretlen.

A legkülönfélébb kereskedelmi, vendéglátó, idegenforgalmi helyek, amelyek vállalják a bankok által kibocsátott kártyák elfogadását ezzel az ügyfél számára lehetővé teszik a készpénz nélküli vásárlást vagy szolgáltatás igénybe vételét. A plasztiklap mára munkahelyi-, uszoda-, könyvtár-, golf- és jachtklub, stb. belépő, többféle

[18] Lásd részletesen: Mezei Kitti – Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 297-308. o.; valamint Ambrus István – Deák Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2. 85-103. o.

[19] http://www.klikkbank.hu/lakossagi/20051026mar75.html [2017.09.30.]

törzsvásárlói (sőt multi-) kártya. Nem kicsiny feladatot ró ránk az egyre növekvő számú különböző azonosítók (PIN-kódok, jelszavak stb.) megjegyzése vagy legalábbis annak azonnali ismerete, hogy hová írtuk fel.

A készpénzkímélő kártyák elvitathatatlan előnyei, amelyek tények (pl. kényelmes, prompt nagyobb vásárlások lehetősége stb.) mellett inkább a pénzintézetek és a munkáltatók járnak jól a fizetések bankszámlára történő utalással. Tényszerűen, a pénzintézetek azért, mert a kártyaszámlára történő munkabér átutalással, pótlólagos forráshoz jutnak havonta, hiszen a számlára utalt pénzt nem egyszerre, hanem többszöri alkalommal veszik le az ügyfelek, továbbá azzal, hogy a kártyabirtokosok sokszor nem merítik ki számlájuk egyenlegét (marad néhány száz-, néhány ezer forint a több millió kártyabirtokos számláján). Ezentúl valamennyi bankműveletért, így általában a 2-nél többszöri pénzlevételért, számlavezetésért, átutalásért, átvezetésért pénzkezelési és egyéb költségeket számolnak fel, amelyek tisztes nagyságrendet is elérhetnek. De jól járnak a munkáltatók, mert megmenekülnek a pénzkivétellel, pénzőrzéssel, és a kézi kifizetéssel összefüggő költségektől.

Az ügyfelek járnak a legrosszabbul, mivel a bankkártya őrzése, továbbá a bankkártyák használatához „sok kicsi, sokba kerül" költségek őket terhelik. Nagy valószínűséggel a közszférában senki nem kapja kézhez a jogszabályban, vagy munkaszerződésben meghatározott bruttó bérből következő nettó bért, csak a banki költségekkel csökkentett nettó bért. Bár a munkáltatók a bankkártya költségek ellensúlyozására törekednek egy minimális összeggel, amely az ügyfelek banki veszteségeinek csupán kis részét fedezik.

Reális probléma az is, hogy a bankkártya elvesztése, ellopása jóval nagyobb kárt okozhat[20] az ügyfél számára, mintha a pénztárcáját elhagyta vagy ellopták volna őrizetéből. A bankkártyán ugyanis az egész havi bevételünk szerepel, míg pénztárcánkban általában az aktuális áruvásárlás, vagy szolgáltatás igénybevételének becsült költsége van némi rátartással, és nem az egész havi fizetésünk egyszerre. Napjainkban jellemzően a „kisemberek" viselik mások gazdagodásának, multik és a politika erőteljes, önös érdekérvényesítésének, a rossz gazdasági, politikai döntéseknek káros következményeit, és tőlük várják, hogy feláldozzák életüket a gazdasági, politikai érdekekért, terület- vagy energiaforrás szerzéséért.

A bankkártyák számának és a velük végzett műveletek elterjedésével egy időben a kártyákkal történő visszaélések lehetőségei folyamatosan bővülnek. A bankkártyák biztonsági rendszere mindig is a bűnözők sikeres módszerei mögött marad, ami általában természetes folyamat.

[20] Például külön érdekesség, hogy sor került a rendőrségi állomány ismereteinek a vizsgálatára a készpénz-helyettesítő fizetési eszközök használatával kapcsolatban. Lásd bővebben: SIMON Béla: A rendőrségi állomány felkészültsége a kiberbűnözésre. Hadtudományi Szemle 2018/1. 394-396. o.

A kártyakibocsátók ennek megakadályozására több- és eltérő fokozatú biztonsági megoldásokat dolgoztak ki, és alkalmaznak:

- A kártyakibocsátó által használt nemzetközi logo (EC/MC, Visa).
- A kártyán levő dombornyomás és annak valódisága. Több elektronikus kártyán nincs dombornyomás (pl. Cirrus, VISA Electron, internetes vásárlásra kibocsátott).
- Bonyolult kártyaszám alkalmazása: meghatározott számkombinációk (bank, ügyfél, kártyatípus stb.) találhatók a kártyákon. A Mastercard kártyaszáma 16 számból áll, és 51, 52, 53, 54, vagy 55-tel kezdődik. A Visa kártyaszámok 13 vagy 16 számjegyből állnak, és 4-sel kezdődnek. Az American Express kártyaszáma 15 számból áll és 34 vagy 37 a kezdete. A Diners Club kártyaszáma 14 számból áll, és 30, 36, vagy 38 a kezdete. A VISA kártyaszám első négy számjegyét a szám alatt vagy felett nyomtatva is megismétlik, míg a Mastercardon, a hátlapon, az aláírási panelben is jelzi a kártyaszámot.
- Egyedi PIN-kód generálása vagy választása. E PIN-kódok különböző jogellenes (megtévesztés mint például a social engineering technikák alkalmazása), erőszakos cselekményekkel (kényszer, fenyegetés, zsarolás stb.) kikényszeríthetők a kártyabirtokostól.[21]
- Hologramos jelek alkalmazása.
- Csak UV-lámpával látható jelzések.
- A megjelölt lejárati dátum megakadályozza, hogy a kártyát érvényességi idején túl is használják.
- A kártya hátoldalán szereplő aláírás.
- Először a videókazetták mágnesszalagja méretével teljesen megegyező mágnesszalag alkalmazása adatrögzítésre, amely gyerekjátékká tette a bankkártya klónozását, a mágnesszalagon szereplő adatok „ellopását". Ezt a nagyon amatőr technikai megoldást váltotta fel a chip, majd nagyon rövid időn belül a biometrikus azonosítás bevezetése.
- Online kapcsolat kiépítése a kártyakibocsátók- és az elfogadóhelyek között, ezzel online tranzakciók lebonyolítása, amellyel legalább az offline csalás lehetőségeit szűrhetik ki.
- Azonnali SMS-értesítés a bankkártyával történő fizetésről.
- A kártyahasználat identifikálása, amellyel a szokatlan tranzakciók kiszűrhetők.
- A gyanús ügyfelek nyilvántartása, kizárása a kártyatársaságoknál, bankoknál.

[21] Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 243. o.

A kereskedelmi és a vendéglátóhelyeken történt vásárláskor a kártyabirtokos aláírásával hitelesíti a kártyával történő vásárlást. Vajon ellenőrzik-e minden esetben a kereskedők az aláírást, és ki tudják-e szűrni a hamis aláírásokat? Sajnálatosan, nem minden esetben győződnek meg arról, hogy a kártyán, illetőleg a vásárlást igazoló blokkon hasonlít-e az aláírás. Általában a lehúzást követően gyorsan visszaadják a vásárlónak, és sok esetben a tranzakció vége előtt már a következő vásárló áruit olvassák be a pénztárgépbe.

A kis értékű, Magyarországon az 5 000 forintos vásárlási limitig nem szükséges PIN-kód begépelése a terminálba, ami kényelmi szolgáltatás, ám visszaélés esetén a biztonság ezzel nullára csökkent.

Jelen tanulmányunk csak a bankkártyával fizetéssel összefüggő visszaélésekre koncentrál,[22] így kimaradnak az ATM-elleni támadások különböző fajtái és lehetőségei (közvetlen pénzszerzés, a bankkártya fizikai megszerzése illetőleg a bankkártyán található elektronikus adatok megismerése stb.).

Kártyaelfogadással kapcsolatos potenciális visszaélések:

- Kártyaelfogadás fiktív (ál-) üzletben. Az elkövetők hamis, hamisított okiratokkal olyan kereskedelmi üzletet nyitnak, amelyek bankokkal szerződést kötnek kártyaelfogadásra. Néhány heti vagy havi forgalom után, bevárva a banktól átutalt összegeket az álkereskedők megszüntetik vállalkozásukat.
- Az engedélyeztetéshez szükséges szigorú szabályok szűrhetik ki a csalókat.
- „Csalárd összejátszás" a jogosulatlan vásárlókkal: a kereskedő tudva arról, hogy hamis, hamisított vagy lopott kártyát használnak fel, elfogadja azt és igazolja a vásárlást. Nyilván a kereskedő „tévedésére", „tökéletesnek látszó hamis bankkártyára" hivatkozva hárítaná el a felelősségét.
- A kártyalehúzások megtöbbszörözése. Ebben az esetben „fizetéskor" a vásárolt összeg többszörösével terheli meg a vevő kártyaszámláját. A kártyabirtokos, ha kiadta a kezéből a bankkártyáját pl. elegáns étteremben, benzinkútnál akkor szembesülhet azzal, hogy kártyáját többször lehúzták, illetve a kártya hátoldalán levő titkos kódot lemásolták.
- A fizetésről szóló azonnali SMS-értesítés rögtön jelzi, ha a kártyát többször lehúzták.
- A kártya adatainak lemásolása ellen csak úgy védekezhetünk, ha a kártyát ki sem adjuk kezünkből, még fizetéskor sem.

[22] Goodman, Marc: Future Crimes. London, Transworld Publishers, Corgi Book, 2016. 302-303. o. Senker, Cath: Cybercrime and the Darknet. London, Arcturus Holdings Ltd., 2017. 42-43. o. Nagy Zoltán András: Bűncselekmények, számítógépes környezetben. Budapest, Ad-Librum, 2009. 153-173. o.

– A kártyalehúzás többszörözése abból a célból, hogy a kártyán szereplő adatokat megismerjék („klónozás", „korábban stemplizés").

A kártya-felhasználás során megvalósítható visszaélések:
– A kártyabirtokos visszaélései között korábban volt gyakori a fedezettúllépés: a kártyabirtokos szándékosan többet költ, mint amennyi a kártyaszámláján van. Csak offline terminálon keresztül történő vásárlásnál valósítható meg.
– Más személy kártyájával megvalósítható visszaélések:
– Elvesztett vagy ellopott bankkártyákkal a PIN-kód hiányában kis értékű vásárlásokkal az eredeti kártyabirtokosnak kárt okozó visszaélés, sőt a PIN-kód ismeretében még nagyobb anyagi kár okozható, a bankkártya letiltásáig.
– Hamis vagy hamisított kártyák használata esetén egy már létező kártyáról készített az «klónozott" kártyával történik a fizetés, ebben társ lehet a kereskedő is. Vagy még azelőtt, mielőtt a bankkártya birtokos átvette volna a kereskedelmi banktól a kártyáját klónozták a banki munkatárssal összejátszó elkövetők. A bankkártya szigorú zárt borítékban történő csomagolása ez utóbbit kiszűri.

2.2.2. A card-not-present csalás

E csalási formáról akkor beszélünk, amikor a tranzakciónál nincs jelen a kártya.[23] Az online, a telefonon, mobiltelefon applikációján keresztül történő áru- vagy szolgáltatás rendelés kifizetésénél nincs jelen a bankkártya.

A veszélye – tehát abban van –, hogy az eladó nem vizsgálhatja a bankkártya tulajdonosát, a bankkártya valósnak tűnik, hiszen fizetéskor a bankkártya validitását ellenőrzi a befogadó bank rendszere. Bár a bankkártya lehet klónozott is.

A bankkártya ma már multifaktoros védelme (elektronikus és biometrikus azonosítók, a tranzakciók és az identitás összekapcsolása, figyelemmel kísérése és más megoldások) sem nyújtanak teljeskörű biztonságát a card-not-present csalások ellen.

A bankkártya érvényességét a kártyabirtokos neve, a kártyaszám, a kártya hátoldalán található háromjegyű biztonsági kód jelzi elsősorban. A bankkártya eme azonosítóinak jogellenes megszerzése történhet:
– adathalászat által (hamis banki oldalon történő adatközléssel, hamis tartalomközlő e-mailben – stb.),

[23] Europol: Internet Organised Cybercrime Threat Assessment 2016. 29-30. o. https://www.europol.europa.eu/iocta/2016/ [2018.05.20.] Europol: Internet Organised Cybercrime Threat Assessment 2017. 43-44. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 [2018.05.20.] https://www.investopedia.com/terms/c/cardnot-present-fraud.asp [2018.05.20.]

– korábbi tranzakciók esetében az adatok online kifürkészése által,
– korábbi tranzakciót követően a tisztességtelen dolgozók által,
– a bankkártyával fizikai kapcsolatba került személyek által.

A bankkártya használat bizalmasságát, titkosságát veszélyezteti a nyílt Wi-Fi vagy az általában a nem védett mobiltelefonok applikációinak a használata.

Az internet alvilágában a bankkártya adatoknak hatalmas értékük van. A kártyabirtokosnak nagy károkat okozhatnak. A bűnözők saját kényük-kedvük szerint költhetik a kártyabirtokos pénzét (megélhetésükre, kábítószerekre, hamis okmányokra, fegyverre, egy további bűncselekmény fizikai előkészületeire stb.).

A card-not-present csalás a Btk. 375.§-ba ütközik és az értékhatár megfelelő bekezdése szerint információs rendszer felhasználásával elkövetett csalásnak[24] minősül.

Érdemes továbbá megjegyezni, hogy bankkártyákkal kapcsolatos bűncselekmények tényleges károsultjai – s így sértettjei – a bankkártyákat kibocsátó pénzintézetek, azonban ők általában megtérítik egyből a bankkártya tulajdonosának a kárát, amennyiben nem volt neki felróható a bűncselekmény elkövetése.[25]

2.2.3. Az aukciós csalások, avagy átverések az árverésen

Az internetes aukciós oldalakon[26] a felhasználók licitálás útján tudnak vásárolni.[27] A licitálás lehetősége akkor nyílik meg az érdeklődő felhasználók előtt, ha azok regisztráltak az adott aukciós oldalra. Ha az online árverési oldalon regisztrálunk, egyrészt szerződéses jogviszonyba kerülünk az árverési oldal üzemeltetőjével, amely a regisztrációnk alapján az oldalon nyújtott szolgáltatásokhoz (aukción való részvétel, termékek árverésre való meghirdetése, a weboldal eléréséhez stb.) való hozzáférést biztosít. Az adott termék licitálásakor, és az árverés lezárását követően a termék eladójával kerülünk jogviszonyba. A szerződés nem – vagy hibás teljesítése miatt igényünket a termék eladójával szemben lehet érvényesíteni.

Az aukciós oldalakon, az eladó általában egyaránt megjelenhet a B2C és C2C relációjú kereskedelem. A vállalkozások, üzleti szféra számára több előnyt jelenthet, nevük, termékeik ismertté tehetők, az elfekvő, eladatlan készletek kiárusíthatók. Nyilván nagyobb tételben történő értékesítés nem igazán várható.

[24] Lásd ehhez: Kondorosi András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2. 73-75. o.

[25] BH 2004.11.452.; valamint Szabó Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6. 50.

[26] Lásd bővebben: Vincze Gabriella Anita: A digitális kor „gyermekei": az internetes aukciós oldalak és jogi problémáik. Magyar Jog 2016/7-8. 471-477. o.

[27] Bártfai Barnabás: Az internet lehetőségei. Budapest, BBS-Info.2008. 98-116.o.

Az eladó aukcióként felkínálja az értékesíteni kívánt tárgyat, amire az érdeklődő felhasználók licitálhatnak.

Az aukció éppúgy lehet sikertelen, mint sikeres. Sikertelen az aukció, ha az eladó visszavonja az áruját a licitálástól, vagy ha az eladó úgy gondolja, hogy a felkínált árak nem érik el az eladó által megkívánt árat, ami lehet az eredetinél akár kevesebb is, ha az eladó így dönt.

Sikeres a licitálás, ha a termék elkel az eladónak megfelel a vevő által felkínált ár. Általában a legjobb ajánlatot tevő vevő nyeri a licitálást. A sikeres aukciót követően az aukciós oldal üzemeltetője automatikus üzenetben közli a vevővel az eladó, az eladóval a vevő regisztrációkor megadott elérhetőségét. Az ügyletet a vevő és az eladó önállóan bonyolítja le.

A sikeres ügyletkötést követően az eladó jutalékot fizet az aukciós oldal üzemeltetőjének.

A sikeres ügyletkötést követően szükség van az eladónak a vevő, a vevőnek az eladó értékelésére. Ennek azért van jelentősége, hogy az értékelésből kitűnjön menynyire megbízható az adott partner, akár eladó, akár vevő oldalon.

A licitálásnak kétféle formája lehet:

– fixáras eladás, ebben az esetben alkudni sem lehet,
– meghatározott licitösszegről induló licitálás: a termék reális árához közeli vagy a licitálás során általában a reális ár körüli ár; vagy szándékosan eltérített, túl magas vagy túl alacsony ár (pl. a túl alacsony ár egyik speciális esete az 1 forintól induló ár).

A licitáló a kiválasztott tárgyat megtekintheti fényképen, elolvashatja róla a rövid ismertetőt, és ennek ismeretében licitálhat, órák, napok elteltével, akár többször is.

a) Csalás az aukció idején:

Nézzünk az árverésen történő átverések tipikus eseteit:

– Shill-csalás: ebben az esetben a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga az eladó – hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Kockázat nincs, hiszen, ha a shill-re marad az áru, nem történik semmi.
– Shield-csalás: ebben az esetben is a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga a vevő – hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Majd amikor a legmagasabb árral a shield magára marad, akkor alacsonyabb árért átengedi az igazi licitálóra.
– Mind a shill-, mind a shield-csalások szervezett elkövetést tételeznek fel.

b) Csalás az aukciót követően:[28]

A sikeres licitálást követően a nyertes vevő a vételár kiegyenlítését követően:

- Hamis, vagy (a licitálásra felkínált tárgyhoz képest) gyenge minőségű árut kap (Ptk. 6. könyv XXII. fejezet: A szerződésszegés általános szabályai).
- Egyáltalán nem kapja meg a kifizetett árut a vevő (csalás, Btk. 373.§).
- Bűncselekményből származó dolgot értékesített (orgazdaság, Btk. 379.§).

Az első két eset jórészt kivédhető, ha a licitáláson nyertes a postai utánvéttel történik az áru kifizetése, majd átvétele. Más kérdés, hogy az aukciós szabályzat megengedi-e az utánvétes áruvásárlást, vagy azonnal, bankkártyával történő kiegyenlítéséhez ragaszkodnak a licitálást szervezők.

Az orgazdaság a laikus számára is sokszor fel sem tűnik, fel sem tűnhet, fel nem tűnik. Esetleg a fizikai erőszakot mutató nyomsérülések, eredeti csomagolás hiánya (bár ez utóbbi a second-hand termékek esetében jellemző), akár a médiából is ismert (pl. körözött) tárgy, festmény, netán egy harmadik személy neve szerepel a tárgyakon stb. jelezhetik, hogy az áru vélhetően bűncselekményből származik.

c) Jutalék-csalás: az aukciónak és más second-hand értékesítési lehetőséget (tárhelyet, az eladó és vevők kölcsönös elérhetőségét stb.) biztosító vállalkozások a tranzakciókból meghatározott jutalékot szednek be, amely tevékenységük fenntarthatóságához járulnak hozzá.

Jutalék-csalás esetén az eladó vagy elhallgatja terméke sikeres értékesítését, vagy megpróbál „eltűnni" az aukciós – oldal látóköréből.

Az aukciós oldalak regisztrációval, majd ez alapján valós térbeli címre történő levél küldésével és válaszolási kötelezettséggel igyekeznek kiszűrni azokat, akik jutalék- vagy más csalási cselekményre használnák fel a C2C relációt.

d) Megtévesztő aukció adathalászat céljával:

Az aukcióra történő benevezés szokatlan formája az ún. 1 forintos aukció. A vevő 1 forintot köt ki a licitálás (vélhetően) elején, amikor az áruját megjeleníti a web-oldalon. Nem kétséges, kiváló reklámfogás, hiszen felkelti az érdeklődést és mintegy mézesmadzag az érdeklődő felhasználókban. Azt a téves képzetet keltheti, hogy a termék milyen olcsón beszerezhető, mert, ha történik is licitálás, még akkor is lehet, hogy nagyon olcsón megszerezhető az a termék.

Az átverés az árverésen a következő, bár úgy tűnik, hogy létrejön az alku (akár 1 forinton, akár egy másik összeggel) és ekkor az eladó megismeri a vevőt, megkapja a vevő elérhetőségét (e-mail cím, más azonosítók), majd az e-kereskedelem során

[28] Gercke, Marco: Understanding cybercrime: phenomena, challenges and legal response, Geneva, ITU. 2012. 30. o.

nem tiltott módon az eladó visszalép[29] (mert meggondolja magát, kitalál egy fals indokot stb.).

Az üzlet így nem jön létre, ám az eladó a vevő adatait már megszerezte.

A csalások formáiról tájékoztatást kapunk az aukciós oldalakon.

3. Esettanulmány: egy sikeresen felderített aukciós csalás

Lásunk egy sikeresen felderített összetett aukciós csalás bűncselekményt:[30] 2009. január feljelentés az egyik budapesti, kerületi rendőrkapitányságon: a sértett az aukciós online piactéren vásárolt két 25 ezer értékben vásárolt bőrdzsekit nem kapta meg. A hatósági az alábbi intézkedéseket rendelte el:

Megkeresés (1): az aukciós piactér felé:

– a gyanúsított(ak) regisztrációs adatai,
– belépési IP címek,
– eladott termékek, vásárlók (sértettek) adatai.

Megkeresés (2):

– az internetszolgáltató (hozzáférést biztosító szolgáltató) felé,
– 3 olyan bank felé, ahonnan az eladótól az ún. ellenőrző utalások érkeztek az online piactér számlájára.

Házkutatás a gyanúsítottnál:

– számítógép nem került elő (talán „készült" a gyanúsított?),
– előkerültek a 3 bank papírjain további 7 bank papírjai.
– Megkeresés (3): az online piactér felé a pénzutalások érkezhettek-e ezekből a bankokból?

Szembesítés azzal a sértettel, akitől a pénzt átvette: eredményes volt.

Az online piactér további felhasználóneveket azonosított, tehát több néven árultak 10 nevet felhasználó sikerült azonosítani.

Ugyanakkor gyanúsak voltak az eladóról szóló értékelések. Az egyik „vevő" többször több néven futó, de ugyanattól az „eladótól" vásárolt és pozitíve értékelte a tevékenységét (gyors, megbízható, korrekt, segítőkész stb.). A naplózott értékelések áttekintésekor: 33 pozitív értékelés érkezett két „vevőtől", ugyanazon, bár több néven szereplő „eladóról", pl. olyankor is, amikor a tranzakció még meg sem történt,

[29] 45/2014. (II. 26.) Korm. rendelet nem tiltja ezt a lehetőséget.

[30] Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Budapest, Allegoup Kft. 2012. 8/1 – 8/7. o.

időben meg sem történhetett. Jutalék csalás gyanúja is felmerült: az eladó, a később „gyanúsított" nagy értékű számítógépeket árult a különböző online piactéren. Az eladó a regisztrációkor többek között a hamis neveken, hamis címeket adott meg. Minden név, nyilván nem véletlenül gyakori magyar név volt. Balszerencséjére vagy épp ellenkezőleg, hogy valódinak tűnjön az eladó, az egyik valós lakcímen valóban lakott egy felhasznált nevű személy, aki rendszeresen kapott felszólításokat, hogy az eladott terméke után a jutalékot fizesse be.

A címzett egy idő után megelégelte a felszólításokat és feljelentést tett a rendőrségen. A nyomozás során az IP-cím alapján azonosították az ismerősét, aki beismerő vallomást tett és így jutottak el a számítógépeket eladó gyanúsítotthoz. A nyomozás során az IP-cím alapján azonosították az ismerősét, aki beismerő vallomást tett és így jutottak el a számítógépeket eladó gyanúsítotthoz.

Illetékességi kérdések a büntetőeljárás során:

A csalás bűncselekménye kapcsán: a vételár kifizetése ellenére sem küldte az árut (telefont) az eladó. K-i bíróság (mint a sértett lakhelye) az egyik budapesti kerületi bírósághoz, mivel a szolgáltató székhelye, bankszámlája itt volt, a megtévesztő hirdetést itt adták fel. A kerületi bíróság az ügyet áttette Z-i bírósághoz, mivel a pénzutalás itt történt, hivatkozva a BH 2009. 317. döntésre, amely szerint csalás esetében a károkozó magatartás kifejtésének helye is megalapozhatja a bíróság illetékességét. A BH 2011. 332 sz. ítélet szerint „a megtévesztés akkor történt, amikor a sértett az interneten szembesült a vádlott megtévesztő szándékkal internetre feltett és azáltal közvetített eladási ajánlatával. Ehhez képest a károkozó magatartás kifejtése (pénzátutalás) és az eredmény bekövetkezte is értelemszerűen a sértett lakóhelyén történt. Ekként valamennyi esetben ez az elkövetés helye."

Kriminálmetodikai szempontból „állatorvosi ló" ez az eset:

- több sértett lehet; üzletszerűség gyanúja,
- sértettek az ország különböző pontjain lakhatnak,
- megkeresések szükségesek: az aukciós oldalt üzemeltető felé; pénzintézet(ek); a hozzáférést biztosító szolgáltatók felé; a mobilszolgáltatók felé (regisztrációs adat); vagy más irányba is pl. posta (kézbesítés adataira vonatkozóan).
- többféle (egymással általában összefüggő) bűncselekményre kell figyelni; csalás, okirati
- bűncselekmények, gondatlan pénzmosás, orgazdaság stb.
- több bűncselekmény valószínűsíti a több elkövetőt.

Nyílt forrású információgyűjtés (OSINT) fontossága az interneten[31]:

– Az elkövető(k) irányában: A regisztrációkor megadott adatok ellenőrzése: név, lakcím, telefonszám, e-mail cím stb. A vásárlási értesítőben megadott adatok: név, lakcím, bankszámla szám, telefonszám stb. Az ellenőrző utalások adatai: számlaszám, utalást teljesítő neve stb.
– Tanúk, sértettek irányában: az eladóval történő kapcsolattartás formáira: telefonszámok, e-mail címek, posta leveleken, levelezőlapokon szereplő címek, személyes találkozások stb.
– Milyen számlára, milyen névre, mikor, mennyi pénzt utaltak a bankok.

Egyéb, a nyomozás során felmerült adatok ellenőrzése:

– a megkeresésekre érkezett adatok, információk ellenőrzése, azok segítségével további
– megkeresések, ellenőrzések, sértettek, tanúk stb.
– Facebookon, Twitteren: kép, név, cím, e-mail, ismerősök, baráti kör, érdeklődési köre,
– aktuális fizikai kinézete, tartózkodás helye, gépkocsija, szórakozási szokásai, törzshelyei stb.
– Google: mit csinál, mit keres, mit akar venni, hová akar utazni, szórakozni menni stb.

Felhasznált Irodalom

Ambrus István – Deák Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2.

Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Budapest, Allegoup Kft. 2012.

Bártfai Barnabás: Az internet lehetőségei. Budapest, BBS-Info. 2008.

Clough, Jonathan: Principles of cybercrime. Second Edition. Cambridge University Press, 2015.

Erdősy Emil – Földvári József – Tóth Mihály: Magyar Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2004.

Europol: Internet Organised Cybercrime Threat Assessment 2016.

Europol: Internet Organised Cybercrime Threat Assessment 2017.

[31] Lásd Herédi István: Nyílt forrású adatgyűjtés az interneten. Belügyi Szemle 2018/7-8. 106-116. o.

GERCKE, Marco: Understanding cybercrime: phenomena, challenges and legal response, Geneva, ITU. 2012.
GOODMAN, Marc: Future Crimes. London, Transworld Publishers, Corgi Book, 2016.
GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
HERÉDI István: Nyílt forrású adatgyűjtés az interneten. Belügyi Szemle 2018/7-8.
KONDOROSI András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2.
KONDRICSZ Péter – TÍMÁR András: Az elektronikus kereskedelem jogi kérdései. Budapest, KJK-Kerszöv. Jogi és Üzleti Kiadó, 2000.
MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.
NAGY Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. Belügyi Szemle 2018/7-8.
NAGY Zoltán András: Bűncselekmények, számítógépes környezetben. Budapest, Ad-Librum, 2009.
NAGY Zoltán András: Sport és büntetőjog. Pécs, Kódex Nyomda, 2014.
NAGY Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1. 1992/1.
SENKER, Cath: Cybercrime and the Darknet. London, Arcturus Holdings Ltd., 2017.
SIMON Béla: A rendőrségi állomány felkészültsége a kiberbűnözésre. Hadtudományi Szemle 2018/1.
SZABÓ Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6.
SZATHMÁRY Zoltán: A hamis termékek forgalmazásával elkövetett iparjogvédelmi jogok bizonyításának nehézségei. Ügyészek Lapja 2015/2.
TÓTH Mihály: Fogyasztók megtévesztése. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014.
TÓTH Mihály: Rossz minőségű termék forgalomba hozatala. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014.
TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. Budapest, KJK-Kerszöv., 2002.
VINCZE Gabriella Anita: A digitális kor „gyermekei": az internetes aukciós oldalak és jogi problémáik. Magyar Jog 2016/7-8.