DOI: 10.38146/bsz-ajia.2026.v74.i8.pp2253-2271

A Mátrixtól Dantéig – isteni színjáték az online csalások világában
Az online csalások elleni fellépés új rendészeti modelljei

From the Matrix to Dante – Divine Comedy in the World of Online Fraud
New Law Enforcement Models Against Online Fraud

Nagy Ágnes
bűnügyi rendőrfőkapitány-helyettes, rendőrségi főtanácsos, rendőr ezredes
Győr-Moson-Sopron Vármegyei Rendőr-főkapitányság
nagyagnes@gyor.police.hu

Absztrakt

Cél: A tanulmány célja annak bemutatása, hogy az online csalások elleni fellépés miként alakította át a kriminalisztikai gondolkodást, milyen új rendészeti válaszok jelentek meg a digitális térben elkövetett bűncselekmények kezelésére, valamint hogyan kapcsolódik össze a technológiai fejlődés, a pszichológiai manipuláció és a modern bűnüldözési stratégia az online csalások elleni küzdelemben.

Módszertan: A szerző hazai és nemzetközi szakirodalom, valamint hazai jogszabályok alapján vizsgálta az online csalásokkal kapcsolatos új kriminalisztikai módszereket és a rendészeti válaszmechanizmusokat.

Megállapítások: A bűnözés szerkezetének átalakulása a rendészeti és kriminalisztikai gondolkodás megváltozását is magával hozta. A hagyományos nyomozási modellek mellett egyre inkább előtérbe kerültek a valós idejű adatfeldolgozáson, az országos koordináción, valamint a pénzügyi és digitális adatok gyors elemzésén alapuló rendszerek. A rendőrség által alkalmazott technikai és technológiai eszközök bővültek.

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás ideje: 2026. 03. 10. Átdolgozás: 2026. 04. 07. Elfogadás: 2026. 05. 21.

Érték: A tanulmány bemutatja az online térben elkövetett nyomozások kihívásait és nehézségeit, egyben azokat a rendszereket is, melyek az új kriminalisztikai módszerek alappilléreit jelenthetik, és komplex értékelést ad az aktuális helyzetről.

Kulcsszavak: kiberbűncselekmény, adathalászat, bűnelemzés, prevenció

Abstract

Aim: The aim of this study is to demonstrate how the fight against online fraud has transformed criminological thinking, what new law enforcement responses have emerged for addressing crimes committed in the digital environment, and how technological development, psychological manipulation, and modern law enforcement strategies are interconnected in combating online fraud.
Methodology: Based on Hungarian and international literature, as well as domestic legislation, the author examined new criminological methods related to online fraud and the corresponding law enforcement response mechanisms.
Findings: The transformation in the structure of crime has also brought changes to law enforcement and criminological thinking. In addition to traditional investigative models, systems based on real-time data processing, nationwide coordination, and the rapid analysis of financial and digital data have increasingly come to the forefront. The technical and technological tools applied by the Police have expanded.
Value: The study presents the challenges and difficulties of investigations conducted in the online environment, while also introducing systems that may constitute the fundamental pillars of new criminological methods and providing a comprehensive assessment of the current situation.

Keywords: cybercrime, phishing, crime analysis, prevention

Bevezetés

„*Mi a valóság? Honnan tudod meghatározni, mi a valóság?”*[1]
(Morpheus a Mátrix című filmből)

A digitalizáció térnyerésével párhuzamosan a bűnözés szerkezete és működési mechanizmusa is jelentős változáson ment keresztül. Az online tér mára nem csupán kommunikációs és gazdasági platformként funkcionál, hanem olyan

1 “What is real? How do you define real?” – The Matrix – Morpheus.

sajátos bűnelkövetési közeggé vált, amelyben a klasszikus fizikai jelenlétet egyre inkább felváltja a virtuális megtévesztés, az anonimitás és a pszichológiai manipuláció.

A kibertérben megvalósuló csalási módszerek jelentős része nem az informatikai rendszerek közvetlen feltörésére, hanem az emberek felépített, irányított kommunikáció során történő befolyásolására épülnek. A modern online csalások sajátossága ugyanis éppen abban rejlik, hogy a sértett gyakran nem külső kényszer hatására, hanem egy mesterségesen felépített, valósnak tűnő digitális környezetben hozza meg döntését.

E jelenség sajátos párhuzamba állítható a *Mátrix* című film világával, amelyben a szereplők érzékelése és valóságértelmezése manipulált rendszeren keresztül történik. Az online csalások elkövetői hasonló módon építenek fel olyan hamis bizalmi környezetet, amelyben a sértett számára a megtévesztés sokszor csak a károkozás bekövetkezése után válik felismerhetővé. A digitális térben megjelenő manipulációs technikák – különösen a social engineering módszerek – ezért már nem kizárólag informatikai, hanem kriminalisztikai, pszichológiai és társadalmi kérdésként is értelmezhetők.

A kibertérben megvalósuló csalások rendszere ugyanakkor egy másik kulturális párhuzamot is felidézhet. Dante: *Isteni színjáték* című művében az alvilág fokozatos, egyre mélyebb körei jelennek meg, ahol az ember saját döntéseinek és megtévesztéseinek következményeivel szembesül. Az online csalások világában hasonlóan egymásra épülő, komplex elkövetési formák figyelhetők meg: az adathalász támadásoktól a romantikus csalásokon át a banki visszaélésekig olyan többlépcsős megtévesztési folyamatok alakultak ki, amelyek a sértettek számára sok esetben csak utólag válnak átláthatóvá.

A jelenség társadalmi veszélyességét jól mutatja, hogy a rendőri eljárásban regisztrált online csalások száma az elmúlt években jelentős növekedést mutatott. Az Országos Rendőr-főkapitányság adatai szerint az online csalások száma a 2019-ben rögzített 4912 esetről néhány év alatt több mint kétszeresére emelkedett, míg 2022-ben az előző évhez viszonyítva 79,52%-os növekedés volt tapasztalható. 2023 első nyolc hónapjában már 7483 online csalást regisztráltak a hatóságok. Az információs rendszer felhasználásával elkövetett csalások száma szintén folyamatos emelkedést mutatott, amely jól érzékelteti a bűnözés digitális térbe történő áthelyeződését (ORFK, 2023).

A nemzetközi trendek ugyancsak azt mutatják, hogy a kibertérben elkövetett vagyon elleni bűncselekmények egyre inkább meghatározó részét képezik a szervezett és transznacionális bűnözésnek. Az Europol 2023. évi Internet Organised Crime Threat Assessment (IOCTA) jelentése szerint az online csalások és a social engineering technikák alkalmazása az európai kiberbűnözés egyik

legdinamikusabban fejlődő területévé vált, különös tekintettel a pénzügyi tranzakciókhoz kapcsolódó megtévesztési módszerekre (URL1). Az Európai Unió Kiberbiztonsági Ügynöksége 2023-as fenyegetettségi jelentése külön hangsúlyozza, hogy a modern kibertámadások jelentős része már nem technikai sérülékenységekre, hanem az emberi tényező manipulációjára épül (URL2).

A rendőrség online térben elkövetett csalások elleni fellépésének részeként jött létre a Digitális Adatelemző és Nyomozástámogató Rendszer (DANTE), mely olyan – az országos koordinációt támogató – informatikai alkalmazás, amely a hét minden napján 24 órában végzi a bankoktól beérkező adatok centralizált irányítását, s aminek célja az online csalásokhoz kapcsolódó gyanús tranzakciók gyors kezelése, az összefüggések feltárása és a sértetti kármegtérülés elősegítése. A rendszer a Nemzeti Adó- és Vámhivatal (NAV) Pénzmosás és Terrorizmusfinanszírozás Elleni Irodájával (PEI) együttműködésben, országos koordinációs modell alapján működik.

Az online csalások kriminalisztikai sajátosságai

A digitális technológia fejlődésével párhuzamosan a vagyon elleni bűncselekmények egy része fokozatosan áthelyeződött az online térbe, amely a nyomozások során új kihívásokat eredményezett.

A bűncselekmény kriminalisztikai sajátosságai közül kiemelt jelentőséggel bír az úgynevezett social engineering módszerek térnyerése. A szakirodalom a social engineering fogalma alatt olyan manipulációs technikákat ért, amelyek során az elkövetők nem elsősorban technikai sérülékenységeket használnak ki, hanem az emberi bizalomra, félelemre, sürgetésre vagy megtévesztésre építenek. Christopher Hadnagy (2010) meghatározása szerint a social engineering lényegében „az emberi befolyásolás művészete”, amelynek célja, hogy az áldozat önként adjon át bizalmas információkat, vagy hajtson végre számára hátrányos műveleteket.

A modern online csalások jelentős részében az elkövetők banki ügyintézőnek, hivatalos szerv képviselőjének vagy szolgáltatónak adják ki magukat, és olyan kommunikációs helyzetet teremtenek, amelyben a sértett valósnak érzékeli az elkövető által közölt információkat. A módszer különösen veszélyes abból a szempontból, hogy a vagyoni hátrányt okozó tranzakciót sok esetben maga a sértett hajtja végre, abban a meggyőződésben, hogy saját pénzügyi biztonságát védi. Az online csalások kriminalisztikai jellemzője még a rendkívül rövid reakcióidő. A digitális pénzügyi tranzakciók sajátossága, hogy a megszerzett pénzösszegek akár perceken belül több pénzügyi szolgáltatón, köztes

számlán vagy nemzetközi tranzakciós láncolaton keresztül továbbításra kerülhetnek. Ez a körülmény jelentősen csökkenti a hagyományos nyomozási mechanizmusok hatékonyságát, és új típusú, valós idejű rendészeti reagálást tesz szükségessé. A problémát tovább súlyosbítja, hogy az online csalások sok esetben nemzetközi infrastruktúrára épülnek. Az elkövetők külföldi szervereket, anonim kommunikációs platformokat, valamint kriptovaluta-alapú megoldásokat alkalmaznak, amely jelentősen megnehezíti az eljáró hatóságok feladatát. Az Europol IOCTA 2025. évi jelentése szerint az online pénzügyi csalások, az adatlopások és a social engineering technikák továbbra is az európai kiberbűnözés legdinamikusabban fejlődő területei közé tartoznak (URL1). A digitális térben elkövetett csalások elleni fellépés során fokozatosan nyilvánvalóvá vált, hogy a hagyományos, területileg elkülönülő és jellemzően ügycentrikus nyomozási modellek önmagukban már nem képesek hatékony választ adni az online bűnözés dinamikus működésére. Az online csalások jelentős része ugyanis nem izolált cselekményként jelenik meg, hanem országos vagy nemzetközi szinten működő, többszereplős elkövetői struktúrákhoz kapcsolódik, amelyekben ugyanazon bankszámlák, IP-címek, telefonszámok vagy kommunikációs mintázatok akár több száz büntetőeljárásban is megjelenhetnek.

A kriminalisztikai gyakorlatban ezért felértékelődött az adatkapcsolatok gyors felismerése, az előzménykutatás, valamint a különböző büntetőeljárások közötti összefüggések valós idejű feltárása. A digitális környezetben keletkező adatmennyiség olyan mértékűvé vált, amely a hagyományos manuális feldolgozási módszerekkel már csak korlátozottan volt kezelhető. A nyomozások eredményességét ezért egyre inkább meghatározta az, hogy az eljáró hatóság milyen gyorsan képes felismerni a sorozatjellegre utaló kapcsolatokat, valamint azonosítani azokat a pénzügyi és kommunikációs csomópontokat, amelyek az elkövetői hálózat működésében központi szerepet töltenek be (Fenyvesi, 2004).

Így a hagyományos nyomozási szemlélet mellett fokozatosan megjelent az adatvezérelt, koordinált és elemzésalapú rendészeti működés igénye, amely már nem kizárólag az elkövető azonosítására, hanem a sértetti vagyon gyors biztosítására és a tranzakciós láncolatok megszakítására is fókuszál. Az online csalások nyomozása során különösen jelentős szerepet kapott a pénzügyi adatok elemzése. A digitális pénzforgalom sajátossága, hogy az elkövetők gyakran többlépcsős tranzakciós láncolatokat alkalmaznak, amelyek célja a pénz eredetének és útvonalának elfedése. A sértetti összegek rövid időn belül több számlán, pénzügyi szolgáltatón, vagy akár különböző országokon keresztül mozoghatnak, amely jelentősen megnehezíti a hagyományos eszközökkel történő felderítést.

A Mátrix Projekt és a DANTE mint új rendészeti válaszmodell

A digitális adatkapcsolatok elemzésére épülő rendészeti szemlélet a gyakorlatban fokozatosan egy új működési modell kialakulását eredményezte. Az online csalásokkal összefüggő ügyekben egyre nyilvánvalóbbá vált, hogy az egyes büntetőeljárásokban keletkező adatok önmagukban sok esetben nem hordoznak elegendő információt az elkövetői struktúrák feltárásához. A különböző ügyekben megjelenő bankszámlák, telefonszámok, IP-címek, eszközazonosítók vagy kommunikációs mintázatok azonban már lehetőséget biztosíthatnak olyan összefüggések felismerésére, amelyek túlmutatnak az adott nyomozás keretein. Az online csalások számának folyamatos emelkedése a hazai rendészeti szervek részéről is új szemléletű válaszmechanizmusok kialakítását tette szükségessé. A növekvő fenyegetettségre reagálva a rendőrség 2023. október 1-jén indította el a Mátrix Projektet, amelynek célja az online csalások elleni fellépés hatékonyságának növelése, az elkövetői körök gyorsabb azonosítása, valamint az országos koordináció erősítése volt. A projekt egyik legfontosabb elemeként létrejött a Kiber300 elnevezésű országos kibernyomozó egység, amelynek feladata az online csalásokkal kapcsolatos eljárások támogatása, az elkövetői hálózatok felszámolása, valamint a nyomozók speciális szakirányú képzése (Nagy, 2025).

A Mátrix Projekt elnevezése sajátos módon kapcsolódik a digitális tér megtévesztésre épülő jellegéhez. Az online csalások jelentős részében ugyanis az elkövetők olyan mesterséges kommunikációs és bizalmi környezetet hoznak létre, amelyben a sértett valósnak érzékeli az elkövető által közölt információkat. A kriminalisztikai fellépés egyik legnagyobb kihívása éppen ezen manipulációs minták felismerése, valamint a digitális térben megjelenő adatkapcsolatok gyors értelmezése és elemzése.

A digitális bűnözés elleni küzdelem során ezért felértékelődött az elemző-értékelő tevékenység szerepe, és azzal együtt megjelent az alkalmazható módszerek kiszélesítésének igénye. A kriminalisztikai gyakorlatban egyre hangsúlyosabbá vált az adatok közötti kapcsolatrendszerek maradéktalan feltárása, a sorozatjelleg felismerése, valamint az elkövetői hálózatok működési folyamatainak elemzése. A hagyományos bizonyítási szemlélet mellett megjelent az adatvezérelt nyomozás igénye, amely már nem kizárólag az egyedi cselekmény rekonstruálására, hanem az elkövetői struktúrák teljes működési rendszerének azonosítására is törekszik.

Az online csalások nyomozása során a digitális tranzakciók sebessége miatt a sértetti összegek biztosítására gyakran csak rendkívül szűk időintervallumban nyílik lehetőség. E körülmény a nyomozó hatóságok részéről olyan reagálási

képességet tesz szükségessé, amely alkalmas a pénzügyi információk azonnali értékelésére, a tranzakciós láncolatok feltérképezésére és a szükséges intézkedések gyors kezdeményezésére.

A pénzügyi információk szerepének növekedésével párhuzamosan a nyomozásokban egyre nagyobb jelentőséget kapott az együttműködés a pénzügyi szektor és a rendészeti szervek között. Az online csalások elleni fellépés során ugyanis a sértetti vagyon biztosításának lehetősége sok esetben azon múlik, hogy a pénzügyi szolgáltatók, az elemző szervezetek és a nyomozó hatóságok milyen gyorsan képesek információt cserélni egymással.

E szemléletváltozás a jogalkotás szintjén is megjelent. Az online csalások elleni fellépés érdekében szükséges törvények módosításáról szóló 2024. évi XVIII. törvény több ponton is olyan szabályozási környezet kialakítására törekedett, amely gyorsabb reagálási lehetőséget biztosít a pénzügyi visszaélések kezelésére. A módosítás alapján a pénzintézetek meghatározott esetekben kötelesek jelzést küldeni a NAV PEI részére, továbbá lehetőség nyílt a tranzakciós láncolatokban szereplő összegek ideiglenes felfüggesztésére is.[2]

A rendészeti gyakorlatban mindez fokozatosan egy olyan koordinált működési modell kialakulásához vezetett, amelyben a digitális adatelemzés, a pénzügyi információfeldolgozás és a valós idejű nyomozástámogatás már egymással szoros kapcsolatban jelenik meg. E folyamat egyik legjelentősebb hazai elemeként értékelhető a DANTE működése, amely az online csalásokkal összefüggő adatkapcsolatok gyors feldolgozására, valamint a büntetőeljárások közötti összefüggések feltárására épül.

A DANTE kriminalisztikai szerepe

A DANTE működési modelljének egyik legjelentősebb sajátossága, hogy a rendszer már nem kizárólag klasszikus ügykezelési logikára épül, hanem a digitális adatkapcsolatok folyamatos és országos szintű elemzésére. A rendszer működése során a NAV PEI által továbbított jelzésekhez kapcsolódó bankszámlaadatok, személyi adatok és szöveges információk előzménykutatása történik meg, amelynek eredményeként lehetőség nyílik az egyes büntetőeljárások közötti összefüggések gyors felismerésére.

A működési mechanizmus kriminalisztikai szempontból különösen azért bír jelentőséggel, mert az online csalások jelentős része sorozatjellegű elkövetési struktúrához kapcsolódik, és az esetek közötti összefüggések (kedvezményezetti

2 2024. évi XVIII. törvény az online csalások elleni fellépés érdekében szükséges törvények és egyéb büntetőjogi tárgyú törvények módosításáról, 29. §.

bankszámlák, telefonszámok, IP-címek, kommunikációs mintázatok) a hagyományos nyomozási eszközök alkalmazásával sok esetben rejtve maradhatnak, mivel az egyes eljárások különböző nyomozó hatóságok előtt, eltérő időpontban és eltérő információs háttérrel jelennek meg.

A DANTE ezzel szemben lehetőséget biztosít arra, hogy a különböző ügyekben keletkező digitális nyomok országos szinten összevethetők legyenek. A program működésének egyik alapvető eleme ezért az előzménykutatás, amelynek során a rendelkezésre álló adatállományok alapján megállapíthatóvá válhat, hogy egy adott tranzakció, bankszámlaszám vagy személy szerepelt-e már korábbi büntetőeljárásokban.

A kriminalisztikai jelentőség ugyanakkor nem kizárólag az összefüggések feltárásában jelenik meg, hanem az időfaktor kezelésében is. Az online csalásokkal összefüggő tranzakciók esetében ugyanis gyakran csupán néhány órás időablak áll rendelkezésre ahhoz, hogy a nyomozó hatóságok a szükséges intézkedéseket megtegyék.

A rendszer működése ezzel lényegében egy új típusú digitális forrónyomos reagálási modell kialakulását eredményezte. Míg a klasszikus forrónyomos tevékenység jellemzően fizikai helyszínhez, személyhez vagy tárgyi bizonyítási eszközhöz kapcsolódik, addig az online csalások esetében a gyors reagálás középpontjába a digitális pénzmozgások, az elektronikus kommunikációs kapcsolatok és az adatkapcsolatok elemzése került. A DANTE fejlesztési céljai között ezért már kifejezetten megjelent a „kiemelt ügyekben forrónyomos tevékenység elemzői támogatása", valamint az „egyedi döntés alapján valós idejű műveleti támogató elemzés" biztosítása is.

A rendszer működése ugyanakkor túlmutat a technológiai fejlesztés kérdésén. A DANTE felállítása tekinthető a kriminalisztikai szemléletváltás egyik elemének is, hiszen az online csalások elleni fellépés során a hagyományos ügycentrikus megközelítést fokozatosan felváltja az adatkapcsolatokra, elemzési folyamatokra és országos koordinációra épülő működési modell (Fenyvesi, 2013).

A DANTE működésével összefüggésben a nyomozási struktúrában is érzékelhető változás következett be. Az online csalásokkal kapcsolatos eljárások során ugyanis egyre hangsúlyosabbá vált, hogy a digitális térben keletkező adatok önmagukban sok esetben nem értelmezhetők megfelelő kontextus nélkül. A bankszámlaadatok, IP-címek, kommunikációs kapcsolatok vagy eszközazonosítók csak akkor válnak valódi kriminalisztikai információvá, ha azok más ügyek adataival, pénzügyi tranzakciókkal vagy egyéb digitális nyomokkal összekapcsolhatók.

A digitális bizonyítás jellegzetessége és komplexitása miatt az online csalásokkal kapcsolatos nyomozásokban felértékelődött a digitális forenzika szerepe.

Eoghan Casey szerint (2011) a digitális bizonyítékok sajátossága, hogy azok egyszerre rendkívül sérülékenyek és rendkívül nagy információtartalommal rendelkeznek, ezért kezelésük speciális kriminalisztikai módszereket igényel. A digitális adatok elemzése során ugyanakkor nem csupán az elkövetési cselekmény rekonstruálása válik lehetővé, hanem az elkövetői kapcsolatrendszerek, kommunikációs mintázatok és tranzakciós hálózatok feltárása is.

A digitális környezetben keletkező nyomok sajátossága továbbá, hogy azok jelentős része rendkívül rövid ideig hozzáférhető. Az IP-címekhez kapcsolódó adatok, a tranzakciós információk, a kommunikációs metaadatok, vagy a különböző platformokon keletkező naplóállományok sok esetben csak korlátozott ideig állnak rendelkezésre. Ez a folyamat a kriminalisztikai gondolkodásban is szemléletváltást eredményezett. A hagyományos bizonyítási eszközök mellett felértékelődött az elemző-értékelő tevékenység, a hálózati kapcsolatok vizsgálata, valamint a digitális adatokból levonható következtetések jelentősége. Az online csalások elleni fellépés során ugyanis sok esetben nem egyetlen bűncselekmény rekonstruálása jelenti a legnagyobb kihívást, hanem az egymással összefüggő elkövetési folyamatok és tranzakciós láncolatok feltárása.

A kriminalisztikai tapasztalatok alapján az elkövetők gyakran ugyanazokat a kommunikációs sémákat, pénzügyi megoldásokat és technikai infrastruktúrákat alkalmazzák különböző sértettekkel szemben. Az ismétlődő mintázatok felismerése ezért nem csupán az adott ügy eredményes felderítését segítheti elő, hanem hozzájárulhat további bűncselekmények megelőzéséhez és az elkövetői hálózatok gyorsabb azonosításához is. A DANTE tehát nem kizárólag adminisztratív vagy informatikai támogató eszközként értelmezhető, hanem olyan komplex kriminalisztikai platformként, amely az online csalásokhoz kapcsolódó digitális nyomok összekapcsolását és elemzését teszi lehetővé. Az online csalásokkal összefüggő adatok országos szintű összevetése, a gyors előzménykutatás és a valós idejű tranzakcióelemzés ma már nem pusztán technológiai lehetőség, hanem a hatékony kriminalisztikai fellépés egyik alapvető feltétele.

Digitális nyomozás az online csalások elleni küzdelemben

A digitális bizonyítékok sajátosságai az online csalások nyomozása során a bizonyítási eljárások szerkezetét is jelentősen átalakították. A klasszikus kriminalisztikai szemléletben a bizonyítás középpontjában jellemzően a fizikai nyomok, tárgyi bizonyítási eszközök, tanúvallomások és helyszíni rekonstrukciók álltak, míg a kibertérben elkövetett bűncselekmények esetében a bizonyítás jelentős része elektronikus adatokhoz, digitális kommunikációhoz, tranzakciós információkhoz és metaadatokhoz kapcsolódik (Fenyvesi, Herke & Tremmel, 2022).

A digitális adatok sajátossága, hogy azok rendkívül könnyen módosíthatók, törölhetők vagy elrejthetők, ezért az ilyen típusú bizonyítékok biztosítása során kiemelt jelentősége van az adatok gyors rögzítésének és hiteles dokumentálásának. Eoghan Casey szerint (2011) a digitális bizonyítékok kezelésének egyik alapvető sajátossága, hogy az adatok sérülékenysége és változtathatósága miatt a bizonyítási láncolat (chain of custody) folyamatos biztosítása elengedhetetlen.

A digitális bizonyítás során nem kizárólag az adatok tartalma bír relevanciával, hanem azok keletkezési ideje, módosítási körülményei, valamint kapcsolati rendszere is. A kommunikációs metaadatok, IP-címek, eszközazonosítók vagy elektronikus tranzakciós adatok sok esetben elsősorban kapcsolatelemzési és összefüggés-feltárási funkciót töltenek be. A modern online csalások nyomozása során ezért a kriminalisztikai elemzés fókusza fokozatosan az izolált elkövetési cselekmények vizsgálatáról a kapcsolati hálózatok és tranzakciós struktúrák elemzésére helyeződött át (Jewkes & Yar, 2010).

Az online csalásokkal összefüggő nyomozások során különös jelentőséggel bírnak a pénzügyi tranzakciókhoz kapcsolódó adatok. Az Europol IOCTA 2025. évi jelentése szerint az online pénzügyi csalások esetében továbbra is meghatározó szerepet töltenek be a többlépcsős tranzakciós láncolatok, valamint az úgynevezett „money mule" hálózatok alkalmazása, amelyek célja a pénzeszközök eredetének elfedése és a nyomon követhetőség megnehezítése (URL1). A digitális pénzmozgások elemzésének jelentőségét a hazai kriminalisztikai szakirodalom is hangsúlyozza. Nyitrai Endre álláspontja szerint a pénzügyi profilalkotás és a hálózatkutatás a modern vagyonvisszaszerzési és online csalásokkal kapcsolatos nyomozások egyik meghatározó elemévé vált, mivel lehetőséget biztosít az elkövetői kapcsolatok, tranzakciós útvonalak és pénzügyi mintázatok feltárására (Nyitrai, 2023).

A digitális környezetben működő elkövetői struktúrák sajátossága, hogy azok sok esetben nem hierarchikus, hanem laza, hálózatszerű kapcsolatrendszerben működnek. Manuel Castells szerint (2010) az információs társadalom működésének egyik alapvető jellemzője a hálózati struktúrák dominanciája, amely a bűnözési formák szerveződésében is megjelenik. Az online csalások esetében ez különösen jól érzékelhető, mivel az elkövetők gyakran különböző országokban működő technikai, pénzügyi és kommunikációs infrastruktúrákat kapcsolnak össze. A digitális bűnözés hálózati jellegének erősödése a nyomozási módszerek szükségszerű fejlődésével járt. Az online csalásokkal összefüggő eljárások során ugyanis egyre gyakrabban jelentek meg olyan elkövetési formák, amelyekben az egyes szereplők feladatai elkülönülnek egymástól. A kriminalisztikai tapasztalatok alapján külön személyek foglalkoznak az adathalász kommunikációval, mások a pénzügyi tranzakciók lebonyolításával, míg egyes

szereplők kizárólag a pénzeszközök továbbításában vagy készpénzfelvételében vesznek részt. A digitális térben működő bűnözői struktúrák ezért sok esetben már nem klasszikus hierarchikus szervezetként, hanem decentralizált, rugalmas hálózati rendszerként működnek. A kriminalisztikai elemzés így egyre inkább túlmutat az egyedi elkövetési cselekmény vizsgálatán, és az elkövetői hálózat teljes működésének feltárására irányul.

A hálózatkutatás kriminalisztikai jelentőségét a hazai szakirodalom is hangsúlyozza. Nyitrai Endre szerint a pénzügyi profilalkotás és a hálózatkutatás alkalmazása lehetőséget biztosít arra, hogy a nyomozó hatóságok ne csupán az egyes pénzügyi műveleteket, hanem az azok mögött álló kapcsolati rendszereket és pénzügyi mintázatokat is feltárják. A szerző kiemeli, hogy a digitális pénzforgalom és az online kommunikáció elemzése során az összefüggések felismerése sok esetben nagyobb kriminalisztikai jelentőséggel bírhat, mint az egyedi bizonyítékok önálló vizsgálata. A digitális kapcsolatrendszerek elemzése során különösen jelentős szerepet kapott a nyílt forrású információgyűjtés (Open Source Intelligence – OSINT) is. A közösségi médiafelületek, online piacterek, nyilvánosan hozzáférhető adatbázisok és különböző digitális platformok olyan információforrásként jelenhetnek meg, amelyek segítségével az elkövetők kapcsolatrendszere, kommunikációs szokásai vagy pénzügyi aktivitása részben rekonstruálhatóvá válhat. A modern kriminalisztikai gyakorlatban ezért az OSINT-eszközök alkalmazása fokozatosan a digitális nyomozások egyik meghatározó elemévé vált (Baggili, Breitinger, & Moore, 2021).

A digitális nyomozások során külön jelentőséggel bír a bűnügyi hírszerzés is. Nyeste Péter és Szendrei Ferenc álláspontja szerint a modern bűnügyi hírszerzés elsődleges célja már nem kizárólag az egyedi bűncselekményekhez kapcsolódó információk megszerzése, hanem az elkövetői hálózatok, kapcsolati rendszerek és működési mintázatok feltárása (Nyeste & Szendrei, 2019). A szerzők rámutatnak arra is, hogy a digitális térben működő bűnözői csoportok esetében az adatkapcsolatok elemzésének és az információk gyors megosztásának óriási szerepe van.

Az online csalásokkal összefüggő nyomozások során a pénzügyi adatok elemzése mellett felértékelődött az elektronikus kommunikáció vizsgálata is. Casey szerint a digitális bizonyítékok egyik legfontosabb sajátossága, hogy azok nem izoláltan, hanem komplex adatkapcsolati rendszer részeként értelmezhetők. Az elektronikus levelezések, IP-címek, naplóállományok és kommunikációs kapcsolatok együttes vizsgálata ezért lehetőséget biztosíthat az elkövetői magatartás rekonstruálására, valamint a kapcsolati hálózatok feltárására. A mesterséges intelligencia fejlődése ugyanakkor új dimenziót nyitott az online csalások módszertanában is. Az Europol IOCTA 2025. évi jelentése szerint a generatív

mesterséges intelligencia alkalmazása jelentősen megkönnyíti a hitelesnek tűnő kommunikációs tartalmak, hamis digitális identitások és automatizált megtévesztő üzenetek előállítását (URL1). A deepfake-technológiák, hangutánzó rendszerek és mesterséges intelligenciával támogatott kommunikációs megoldások alkalmazása ezért a jövőben tovább növelheti az online csalások kriminalisztikai kihívásait.

A digitális nyomozási módszerek fejlődése mellett a kriminalisztikai gondolkodásban is érzékelhetővé vált egyfajta paradigmaváltás. A klasszikus bűnügyi szemléletben a nyomozás alapvetően reaktív jellegű volt, amely az elkövetett bűncselekmény utólagos felderítésére koncentrált. Az online csalások esetében azonban egyre hangsúlyosabbá vált a proaktív adatfeldolgozás, a tranzakciós mintázatok folyamatos monitorozása, valamint az előzetes kockázatelemzés szerepe. A digitális környezetben ugyanis a gyors reagálás sok esetben közvetlenül befolyásolhatja a sértetti vagyon megtérülésének lehetőségét.

A digitális térben megjelenő megtévesztési mechanizmusok összetettsége ugyanakkor nemcsak technológiai, hanem társadalmi és pszichológiai kihívást is jelent. Kollár Csaba kutatása rámutat arra is, hogy a csalók tudatosan építenek az áldozatok pszichológiai gyengeségeire, különösen a bizalomra és a gyors haszonszerzés reményére (Kollár, 2018). Az online csalások elleni fellépés eredményessége ezért hosszú távon nem kizárólag a nyomozási és technológiai képességeken múlik, hanem a digitális tudatosság fejlesztésén, a pénzügyi biztonsági ismeretek erősítésén, valamint az állami és társadalmi szereplők közötti együttműködésen is.

Az online csalások pszichológiai sajátosságai és a megelőzés lehetőségei

Az online csalások sajátossága, hogy az elkövetési mechanizmusok középpontjában sok esetben nem technikai rendszerek közvetlen támadása, hanem az emberi döntéshozatal befolyásolása áll. Jelentős része pszichológiai manipulációra, bizalomépítésre, sürgetésre vagy félelemkeltésre épül, amelynek célja, hogy a sértett önként hajtson végre az elkövető számára kedvező műveletet. A kibertérben megvalósuló megtévesztések ezért kriminalisztikai és informatikai kérdésen túl pszichológiai szempontból is vizsgálhatók. A social engineering módszerek egyik legfontosabb sajátossága, hogy azok tudatosan építenek az emberi viselkedés kiszámítható elemeire. Az online csalások során alkalmazott pszichológiai manipuláció sok esetben nem spontán folyamat, hanem előre megtervezett kommunikációs stratégia eredménye.

A kriminalisztikai tapasztalatok alapján az online csalások jelentős részében az elkövetők olyan érzelmi állapot kialakítására törekednek, amely gyors döntéshozatalra készteti a sértettet. A magukat banki ügyintézőnek vagy hatósági személynek kiadó elkövetők kommunikációjában gyakran jelenik meg a sürgetés, a fenyegetettség érzetének kialakítása vagy a pénzügyi veszteségtől való félelem hangsúlyozása. A romantikus csalások esetében ezzel szemben az érzelmi kötődés és a bizalmi kapcsolat kialakítása kerül előtérbe, amely hosszabb idő alatt, fokozatos manipuláció révén vezet a sértett befolyásolásához. A pszichológiai manipuláció sikerességében jelentős szerepet játszik a digitális kommunikáció sajátossága is. Az online térben a sértett sok esetben nem rendelkezik azokkal a nonverbális információkkal, amelyek személyes kommunikáció során segíthetnék a megtévesztés felismerését. A digitális környezetben ezért az elkövetők könnyebben alakíthatnak ki hitelesnek tűnő identitást, különösen akkor, ha kommunikációjukat hivatalos logók, hamis ügyfélszolgálati felületek, vagy mesterséges intelligencia segítségével generált tartalmak támogatják (URL1).

Az online csalások pszichológiai folyamatai szoros kapcsolatban állnak a modern információs társadalom működésével is. Castells szerint (2010) a hálózati társadalomban az információ és a kommunikáció válik a társadalmi működés egyik meghatározó elemévé, amely a manipulációs technikák fejlődésében is megjelenik. Az online csalások esetében ez különösen érzékelhető, mivel az elkövetők sok esetben a digitális kommunikáció gyorsaságát, tömegességét és személytelenségét használják ki.

Az online csalások pszichológiai sajátosságainak vizsgálata során a hazai szakirodalom is egyre hangsúlyosabban foglalkozik az emberi tényező szerepével. A magyar kutatások rámutatnak arra, hogy a modern online csalások eredményessége sok esetben nem elsősorban technológiai fölényből, hanem a sértettek pszichológiai befolyásolásából fakad. A digitális térben működő elkövetők tudatosan építenek a bizalomra, a félelemre, a sürgetésre, valamint az információs bizonytalanságra, amely jelentősen csökkentheti az áldozatok kritikai döntéshozatali képességét.

Krasznay Csaba szerint a kibertérben megvalósuló támadások jelentős része ma már nem klasszikus technikai támadásként, hanem pszichológiai manipulációként értelmezhető. A szerző kiemeli, hogy az emberi tényező sérülékenysége a modern kibervédelem egyik legkritikusabb pontjává vált, mivel a felhasználók döntései sok esetben könnyebben befolyásolhatók, mint a megfelelően védett informatikai rendszerek (Krasznay, 2015).

A magyar szakirodalom az online viktimizáció kérdésével összefüggésben is hangsúlyozza a pszichológiai tényezők jelentőségét. Parti Katalin rámutat arra, hogy a digitális tér sajátosságai – különösen az anonimitás, a fizikai távolság és

a személyes kontroll hiánya – jelentősen növelhetik a manipuláció sikerességét (Parti, 2019). Az online kommunikáció során a sértettek sok esetben olyan bizalmi helyzetbe kerülnek, amelyben hiányoznak a személyes interakciók során megszokott kontrollmechanizmusok és nonverbális visszajelzések.

A pszichológiai manipuláció szerepét hangsúlyozza Csepregi Sándor is, aki szerint a modern online csalások esetében az elkövetők tudatos kommunikációs stratégiákat alkalmaznak annak érdekében, hogy sürgető, fenyegető vagy hivatalosnak tűnő helyzetet alakítsanak ki (Csepregi, 2021). A szerző szerint az online térben a megtévesztés sikerességének egyik kulcsa az, hogy az elkövetők rövid idő alatt képesek érzelmi nyomást gyakorolni a sértettre, amely jelentősen csökkentheti a racionális döntéshozatal lehetőségét. A hazai kriminalisztikai szakirodalom a digitális tudatosság fejlesztésének jelentőségét is kiemeli. Fenyvesi Csaba álláspontja szerint a modern kriminalisztikai megelőzés már nem korlátozódhat kizárólag a klasszikus rendészeti eszközökre, hanem ki kell terjednie az információs és digitális biztonságtudatosság erősítésére is (Fenyvesi, 2014a). Az online csalások esetében ugyanis a megelőzés egyik legfontosabb eleme annak felismerése, hogy az elkövetők sok esetben nem technikai hibákat, hanem emberi döntési folyamatokat használnak ki. A magyar szakirodalom tehát egyértelműen arra mutat rá, hogy az online csalások elleni fellépés nem értelmezhető kizárólag technológiai vagy büntetőjogi kérdésként (Fenyvesi, 2016). A digitális megtévesztési mechanizmusok sikeressége szoros kapcsolatban áll az emberi pszichológia sajátosságaival, amely a kriminalisztikai elemzés és a prevenciós stratégia kialakítása során egyaránt meghatározó jelentőséggel bír (Fenyvesi, 2003).

A megelőzés szempontjából ezért az online csalások elleni fellépés nem korlátozódhat kizárólag represszív vagy technológiai eszközökre. Az Europol és az ENISA jelentései egyaránt hangsúlyozzák, hogy a digitális biztonságtudatosság fejlesztése a modern kibervédelem egyik legfontosabb eleme. A lakosság megfelelő tájékoztatása, a tipikus elkövetési módszerek ismertetése, valamint a pénzügyi biztonsági ismeretek erősítése közvetlenül hozzájárulhat az online áldozattá válás csökkentéséhez. A prevenciós szemlélet erősítésében Magyarországon kiemelt szerepet tölt be a KiberPajzs program, amely a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Kibervédelmi Intézet, a rendőrség, valamint további állami és piaci szereplők együttműködésével jött létre. A program elsődleges célja a lakosság digitális és pénzügyi biztonságtudatosságának fejlesztése, valamint az online csalásokkal kapcsolatos figyelemfelhívás erősítése. A kezdeményezés jelentősége abban áll, hogy az online csalások elleni fellépést komplex társadalmi problémaként értelmezi, amelynek kezelése nem kizárólag rendészeti vagy technológiai megoldásokat, hanem széles körű

edukációs és kommunikációs együttműködést is igényel. A program rendszeresen közzétesz tájékoztató anyagokat az aktuális online csalási módszerekről, különös tekintettel a banki adathalászatokra, a telefonos megtévesztésekre, a hamis befektetési ajánlatokra és a közösségimédia-felületeken megjelenő visszaélésekre. A KiberPajzs program prevenciós szemlélete különösen azért bír jelentőséggel, mert az online csalások jelentős részében maga a sértett hajtja végre a tranzakciót, így a bűncselekmények megelőzésének egyik legfontosabb eszköze a tudatos felhasználói magatartás kialakítása (URL3).

A prevenciós tevékenység a rendőrség működésében is egyre hangsúlyosabb szerepet kapott. Az online csalások elleni fellépés során a rendészeti szervek felismerték, hogy a gyors technológiai fejlődés és az elkövetési módszerek folyamatos változása miatt a hagyományos bűnmegelőzési formák önmagukban már nem elegendőek. Ennek megfelelően a rendőrség az elmúlt években több, kifejezetten az online csalások megelőzésére irányuló programot és kommunikációs kampányt indított. A Mátrix Projekt keretében külön hangsúlyt kapott a lakossági tájékoztatás, a tipikus online csalási módszerek ismertetése, valamint a digitális tudatosság fejlesztése. A rendőrség bűnmegelőzési kommunikációjában rendszeresen jelennek meg figyelemfelhívó kampányok a banki ügyintézőnek magukat kiadó elkövetőkről, az adathalász üzenetekről, a romantikus csalásokról, vagy az online piactereken megjelenő visszaélésekről. A prevenciós tevékenység jelentősége különösen abban áll, hogy az online csalások elleni fellépés során a rendészeti szervek már nem kizárólag represszív szereplőként jelennek meg, hanem a digitális biztonságtudatosság fejlesztésének aktív alakítóivá is váltak.

A kriminalisztikai megelőzés szempontjából különösen fontos annak felismerése, hogy az online csalások módszerei rendkívül gyorsan változnak. A mesterséges intelligencia alapú kommunikációs megoldások, deepfake-technológiák és automatizált megtévesztő rendszerek fejlődése miatt a digitális manipuláció egyre nehezebben felismerhető. Az online csalások elleni fellépés eredményessége ezért hosszú távon nem kizárólag a technológiai képességeken múlik, hanem a társadalmi tudatosság, a digitális kritikai gondolkodás és a prevenciós tevékenység fejlesztésén is (Fenyvesi, 2014b).

Összegzés

A tanulmányban rámutattam arra, hogy a digitális bűnözés fejlődése alapvetően alakította át a kriminalisztikai gondolkodást és a rendészeti működés szerkezetét. Az online csalások sajátosságai – különösen a valós idejű pénzügyi tranzakciók,

a nemzetközi infrastruktúra, valamint a hálózatszerű elkövetői struktúrák – szükségessé tették az adatvezérelt, koordinált és elemzésalapú nyomozási modellek kialakulását. A hagyományos ügycentrikus megközelítés mellett egyre hangsúlyosabbá vált a digitális adatkapcsolatok elemzése, az előzménykutatás, a hálózatelemzés, valamint a valós idejű reagálás képessége (Fenyvesi, 2015).

A Mátrix Projekt és a DANTE létrejötte, a digitális nyomozástámogatás, az országos koordináció, valamint a pénzügyi és kommunikációs adatkapcsolatok gyors elemzése olyan új rendészeti működési modellt eredményezett, amely már képes alkalmazkodni a kibertérben működő bűnözői struktúrák dinamikájához. A DANTE működése túlmutat egy technológiai fejlesztés keretein: olyan kriminalisztikai platformként értelmezhető, amely a digitális nyomok országos szintű összekapcsolásával új dimenziót nyitott az online csalások elleni fellépésben.

A tanulmány ugyanakkor arra is rámutatott, hogy az online csalások sikerességének egyik legfontosabb eleme továbbra is az emberi tényező.

Álláspontom szerint az online csalások elleni eredményes fellépés kizárólag komplex, többdimenziós megközelítés alkalmazásával valósítható meg. A represszív eszközök mellett elengedhetetlenné vált a digitális tudatosság fejlesztése, a pénzügyi biztonsági ismeretek erősítése, valamint az állami, rendészeti és pénzügyi szereplők közötti együttműködés további fejlesztése. A technológiai fejlődés, a mesterséges intelligencia és az automatizált megtévesztési módszerek térnyerése várhatóan tovább növeli majd az online csalások komplexitását, amely a kriminalisztika és a rendészet számára hosszú távon is folyamatos alkalmazkodási kényszert jelent.

Felhasznált irodalom

Baggili, I., Breitinger, F., & Moore, J. (2021). *Digital forensics and investigations*. Springer.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Castells, M. (2010). *The rise of the network society*. Wiley-Blackwell. https://doi.org/10.1002/9781444319514

Csepregi S. (2021). A social engineering szerepe a modern kibertámadásokban. *Hadmérnök*, 16(2), 95–104.

Fenyvesi Cs. (2003). *A kriminalisztikai verzió.* Kriminalisztikai tanulmányok. Dialóg Campus.

Fenyvesi Cs. (2004). A XXI. századi bűnüldözés-tudomány nemzetközi tendenciái. *Magyar Tudomány, 49*(6), 757–765.

Fenyvesi Cs. (2013). A kriminalisztika jövőbeli fejlesztési lehetőségei, kihívásai. *Pro Futuro, 3*(2), 42–61. https://doi.org/10.26521/Profuturo/2013/2/5507

Fenyvesi Cs. (2014a). *A kriminalisztika tendenciái.* Dialóg Campus Kiadó.
Fenyvesi Cs. (2014b). *Kriminalisztika – elmélet és gyakorlat*. Dialóg Campus.
Fenyvesi Cs. (2015). A kriminalisztika veszélyei. In Gaál Gy. & Hautzinger Z. (Szerk.), *Modernkori veszélyek rendészeti aspektusai.* Pécsi Határőr Tudományos Közlemények XVII. (pp. 115-126). Magyar Hadtudományi Társaság.
Fenyvesi Cs. (2016). A digitális adatok jelentősége a kriminalisztikában. *JURA, 1*(2), 50–59.
Fenyvesi Cs., Herke Cs. & Tremmel F. (2004). *Új magyar büntetőeljárás.* Dialóg Campus.
Fenyvesi Cs. (2017). *A kriminalisztika tendenciái: A bűnügyi nyomozás múltja, jelene, jövője*. Dialóg Campus.
Fenyvesi Cs. (2019a). A hatékony bűnüldöző értékjegyei a XXI. században. In Gaál Gy. & Hautzinger Z. (Szerk.), *A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Pécsi Határőr Tudományos Közlemények XXI.* (pp. 143–146). Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja.
Fenyvesi Cs. (2019b). Kriminalisztikai világtendenciák: Különös tekintettel a digitális felderítésre. In Mezei K. (Szerk.), *A bűnügyi tudományok és az informatika* (pp. 64–82). PTE ÁJK; MTA Társadalomtudományi Kutatóközpont.
Fenyvesi Cs. (2020). A kriminalisztika válaszai a társadalmi kihívásokra: A bűnüldözés fejlesztési lehetőségei. In Gaál Gy. & Hautzinger Z. (Szerk.), *A hadtudománytól a rendészettudományig: Társadalmi kihívások a nemzeti összetartozás évében. Pécsi Határőr Tudományos Közlemények XXII.* (pp. 211-225). Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja.
Fenyvesi Cs., Herke Cs., & Tremmel F. (Szerk.) (2022). *Kriminalisztika*. Ludovika Egyetemi Kiadó.
Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*, Wiley Publishing.
Jewkes, Y., & Yar, M. (Eds.). (2010). *Handbook of internet crime*. Willan Publishing.
Kollár Cs. (2018). A magyarországi online csalások fontosabb tulajdonságai: A 2013 és 2016 között elkövetett releváns bűnesetek elemzése. *Belügyi Szemle, 66*(10), 56–70. https://doi.org/10.38146/BSZ.2018.10.4
Krasznay Cs. (2015). *Kibervédelem a kibertérben*. HVG-ORAC.
Nagy, Á. (2025). Digital threats: Trust and manipulation in cyberspace. *Police Studies, 2025*(3–4), 92–105. https://doi.org/10.53304/PS.2025.3-4.08
Nyeste P., & Szendrei F. (2019). *A bűnügyi hírszerzés kézikönyve*. Dialóg Campus.
Nyitrai E. (2023). A pénzügyi profilalkotás és a hálózatkutatás szerepe a vagyonvisszaszerzésben. In Mátyás Sz. (Szerk.), *A vagyonvisszaszerzés kriminalisztikai és jogi vetületei* (pp. 157–173). Magyar Rendészettudományi Társaság.
Országos Rendőr-főkapitányság (2023). *Cselekvési terv a kiberbűnözés elleni harc rövidtávú és stratégiai célkitűzéseiről, a megelőzés és tájékoztatás lehetőségeiről*. Országos Rendőr-főkapitányság.
Parti K. (2019). Az online viktimizáció kriminológiai kérdései. In Virág Gy. (Szerk.), *Kriminológiai tanulmányok 56.* (pp. 145–158). Országos Kriminológiai Intézet.

A cikkben szereplő online hivatkozások

URL1: *Europol*: *Internet Organised Crime Threat Assessment (IOCTA) 2025,* https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

URL2: ENISA: *ENISA Threat Landscape 2023.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

URL3: *Kiberpajzs honlapja*. https://kiberpajzs.hu/a-kezdemenyezesrol

Alkalmazott jogszabályok

1994. évi XXXIV. törvény a Rendőrségről

2001. évi CIV. törvény a jogi személyekkel szemben alkalmazható büntetőjogi intézkedésekről

2012. évi C. törvény a Büntető Törvénykönyvről

2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről

2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról

2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

2017. évi XC. törvény a büntetőeljárásról

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

A cikk APA szabály szerinti hivatkozása

Nagy Á. (2026). A Mátrixtól Dantéig – isteni színjáték az online csalások világában. Az online csalások elleni fellépés új rendészeti modelljei. *Belügyi Szemle*, *74*(8), 2253–2271. https://doi.org/10.38146/bsz-ajia.2026.v74.i8.pp2253-2271

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Nagy Ágnes, aki a nagyagnes@gyor.police.hu e-mail címen érhető el.