Magyar Rendészet 2025/3. 147–168.
DOI: 10.32577/MR.2025.3.9

RENDÉSZETTUDOMÁNY

Prediktív bűnmegelőzés a kiberbűnözés ellen

Egy MI-alapú szoftver fejlesztésének indokoltsága és lehetőségei

Predictive Crime Prevention against Cybercrime

Justification and Possibilities for Developing AI-Based Software

ÁRPÁS Béla,[1] GYARAKI Réka,[2] PRISKI Zsanett[3]

Cél: A tanulmány középpontjában egy olyan mesterségesintelligencia- (MI-) alapú innovatív szoftver koncepciója áll, amely az online térben elkövetett bűncselekmények prediktív megelőzését célozza meg. A kiberbűnözés jelentős térnyerésével párhuzamosan megnőtt az igény olyan proaktív, technológiai eszközök iránt, amelyek nem csupán a bűncselekmények utólagos felderítésére, hanem azok hatékony megelőzésére is alkalmasak. A tanulmány arra a komplex kérdésre keresi a választ, hogy lehetséges-e egy olyan adaptív rendszer fejlesztése, amely képes valós időben azonosítani azokat a felhasználókat, akik online magatartásuk alapján magasabb viktimizációs kockázati indexszel rendelkeznek.

Módszertan: A kutatás során átfogó, interdiszciplináris megközelítéssel, prediktív rendészeti és kockázatelemzési modellek alapján dolgoztunk ki egy koncepcionális keretrendszert. A módszertan alapját a meglévő MI-alapú szoftverek összehasonlító elemzése, a SWOT-analízis, a reprezentativitás biztosítására vonatkozó kutatásmódszertani elvek és az adatvédelmi kérdések részletes tanulmányozása adják.

[1] R. alezredes, mesteroktató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnügyi és Gazdaságvédelmi Tanszék, e-mail: arpas.bela@uni-nke.hu

[2] PhD, LL.M, r. őrnagy, adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kiberbűnözés Elleni Tanszék, e-mail: gyaraki.reka@uni-nke.hu

[3] R. tisztjelölt, hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnügyi alapképzési szak kibernyomozó szakirány, e-mail: priski.zsanett@stud.uni-nke.hu

Megállapítások: A kutatás rámutatott, hogy egy intelligens szoftver képes lehet az online jelenlét kockázati tényezőinek azonosítására, és a felhasználói viselkedés mintázatai alapján személyre szabott prevenciós javaslatokat nyújtani. Ez jelentősen elősegítheti a tudatos internethasználatot, és hatékonyabbá teheti a bűnmegelőzési stratégiákat.

Érték: A tanulmány eredményei alapján egyértelműen elmondható, hogy az MI-alapú, prediktív szoftverek jelentős szerepet tölthetnek be a jövő rendészeti stratégiáiban. A jövőbeli kutatási irányok prioritásai között szerepel a gyakorlati implementáció, a normatív keretrendszer fejlesztése és az etikai aspektusok szisztematikus integrálása.

Kulcsszavak: szervezett bűnözés, kiberbűnözés, prediktív bűnmegelőzés, kockázatelemzés, adatvédelem, információbiztonság, mesterséges intelligencia

Aim: The study focuses on the concept of an innovative artificial intelligence (AI)-based software for predictive prevention of crime in the online space. The significant rise of cybercrime has been accompanied by an increased demand for proactive technological tools that are not only capable of detecting crimes after the fact, but also of effectively preventing them. This study addresses the complex question of whether it is possible to develop an adaptive system that can identify in real time users who have a higher risk of victimisation based on their online behaviour.

Methodology: A conceptual framework was developed using a comprehensive, interdisciplinary approach based on predictive policing and risk analysis models. The methodology is based on a comparative analysis of existing AI-based software, a SWOT analysis, research methodological principles to ensure representativeness, and a detailed study of privacy issues.

Findings: Research has shown that intelligent software can identify risk factors for online presence and provide personalised prevention recommendations based on user behaviour patterns. This could significantly promote conscious internet use and make crime prevention strategies more effective.

Value: Based on the results of the study, it is clear that AI-based predictive software can play a significant role in future law enforcement strategies. Priorities for future research directions include practical implementation, the development of a normative framework and the systematic integration of ethical aspects.

Keywords: organised crime, cybercrime, predictive crime prevention, risk analysis, data protection, information security, artificial intelligence

Bevezetés

A 21. század első negyedét a negyedik, sőt olykor az ötödik ipari forradalom évtizedeiként említjük, éljük meg. Ez az időszak nemcsak az előre mutató *technikai, technológiai* és társadalmi fejlődés jegyében telik, hanem magában hordozza azt a veszélyt is, hogy a *deviáns körök*, így különösen a bűnelkövetői hálózatok is kihasználják a legújabb technológiákat és a legkorszerűbb technikai eszközöket a bűnös céljaik eléréséhez. Ahogyan azt tanulmányunkban majdan hangsúlyozzuk, különösen igaz ez a szervezett bűnözésre, amely folyamatosan alkalmazkodik a technológiai és társadalmi változásokhoz. Ez evidenciaként teszi szükségessé a rendészeti szervek számára is az egyre korszerűbb, innovatív eszközök alkalmazását. Ezt a szükségszerűséget tovább erősíti a modern társadalmak – már a büntető anyagi jogban is markánsan megjelenő – azon elvárása, amely a reagáló jellegű bűnüldözés felől egyre inkább a preventív rendészet felé tolódik, különösen a súlyos bűncselekmények, illetve a szervezett bűnözés vonatkozásában.

Tanulmányunk célja, hogy bemutassa a bűnmegelőzés – így különösen a modern kori szervezett bűnözéssel szembeni fellépés – egyik lehetséges szegmensét, a prediktív rendészetet, aminek jelentősége ugyan megosztja a szakembereket, de optimális esetben az alkalmazása új lehetőségeket kínálhat a bűnözési mintázatok azonosítására és a célzott, hatékony rendészeti intézkedések bevezetésére.

A szervezett bűnözés fogalma és jellemzői

A szervezett bűnözés rendszere évszázadokon és kontinenseken átnyúló kriminalisztikai jelenség, amely dinamikusan alkalmazkodik az adott korban mutatkozó bűnmegelőzési és bűnüldözési gyengeséghez. Sok esetben komplex és párhuzamos struktúrákat hoz létre az államhatalmi rendszerekkel szemben, és sajnos alkalmanként azokkal, vagy legalábbis azok egyes tagjaival együttműködve is.

Dános Valér megfogalmazásában (Dános 1999): „A szervezett bűnözés egy adott társadalom összbűnözésének sajátos alstruktúrája, amelyet azoknak a hivatásos bűnözőknek a bűncselekményei képeznek, akik valamely bűnöző társulás tagjaként (vezetőjeként) tervszerűen, tagolt munkamegosztás és magas fokú konspiráció mellett valósítják meg bűncselekményeiket."

A szervezett bűnözésnek fontos jellemzője a már említett dinamizmus, hiszen mind szerkezetében, mind pedig az egyes szervezetek által megvalósuló bűncselekményekben megfigyelhető a szinte folyamatos változás. Leon C. Megginson, a Louisianai Állami Egyetem menedzsment- és marketingprofesszora 1963-ban tartott előadásában kifejtette, hogy „Charles Darwin Fajok eredete című műve szerint nem a legintelligensebb fajok, és nem is a legerősebbek maradnak életben, hanem azok, amelyek a legjobban képesek alkalmazkodni és igazodni ahhoz a változó környezethez, amelyben találják magukat" (Megginson 1963). A szervezett bűnözés e tekintetben rendkívül organikus lénynek tekinthető. Folyamatosan alkalmazkodik az adott korban és helyen meglévő társadalmi, gazdasági, jogi és politikai berendezkedéshez. Emellett a szervezett bűnözés komplexitás is, amely a rendkívül szerteágazó tevékenységi körében jelenik meg. A klasszikusan

szervezett bűnözéshez köthető bűncselekmények például a zsarolás, az emberölés, a kábítószer-kereskedelem, a prostitúció. Emellett a szervezett bűnözés rendkívüli rugalmasságot mutatva, nem csupán a jogi és esetleges hatósági hiátusokat használja ki, hanem azon már jóval túlmutatva lépést tart a technológiai fejlődéssel is. Az olyan újonnan megjelent elkövetési módok, mint amilyen az online csalás, mellett megfigyelhető, hogy az elkövetők a korábban pönalizált deliktumokat új, illetve folyamatosan megújuló elkövetési módszerekkel valósítják meg. Ez a kettős folyamat tekinthető egyfajta kriminalisztikai evolúciónak. Éppen ezért a szervezett bűnözés elleni küzdelem minden korban és lokációban komoly kihívást jelent nemcsak a jogalkalmazók, hanem az igazságszolgáltatás, illetve a közigazgatás egésze számára, jelentősen túlmutatva ezzel a rendészet területén.

A szervezett bűnözés megjelenése és fejlődése Magyarországon

Hazánkban a szervezett bűnözés titkolva, sőt, hivatalosan tagadva – szoros összefüggésben az akkor még lassú társadalmi-gazdasági átalakulásokkal –, először az 1970-es években jelent meg. Ebben az időben Magyarország kapui a Nyugat felé kezdtek megnyílni, s az addigi kvázi zárt világunkba a külföldiek – a valutájuk mellett – magukkal hozták új bűnelkövetési módszereiket is. Ebben az időszakban erősödött az illegális árucsempészet, s kezdett elterjedtté válni a hengerzár mechanikai törésén alapuló lakásbetörés, vagyis a „lengyel módszer", majd a technikailag kifinomultabb „csehszlovák módszer", amely már az úgynevezett zárfésű alkalmazásával, roncsolásmentesen tette lehetővé az ingatlanokba való behatolást (Csiba–Bodor 1983). A bűnözés fejlődésével – attól függetlenül, de azzal párhuzamosan – élénkült a gazdaság, kezdett kialakulni a magánszektor. A jövedelmek és a vagyoni viszonyok differenciálódása kedvező feltételeket teremtett a szervezett bűnözés megjelenéséhez, egyes bűnszervezetek kialakulásához. A tehetősebb rétegek vagyonuk jelentősebb részét likvid tőkében (készpénzben, nemesfémekben, műkincsekben) tartották, jellemzően a legminimálisabb vagyonvédelmi eszközök nélkül, amely tényezők összessége ideális célponttá tette őket a betörők számára. Az 1980-as évekre a betörések már egészen szervezetté váltak. Kialakult a feladatmegosztás: tippadók, az orgazdák, az elkövetői kör által biztosított védők megjelenésével a betöréses lopás több elkövetős, szervezett bűnelkövetéssé alakult. Ebből a társadalom szinte semmit sem érzékelt, hiszen a hivatalos, állami kommunikáció tagadta a jelenség létezését. Azonban a rendszerváltás után a bűnözés cáfolhatatlanul magasabb szintre lépett. 1988-ban írt tanulmányában Dános Valér már tényként írta le a budapesti szervezett bűnözés létezését. Az 1980 és 1986 között végzett kutatásának eredménye szerint a szervezett bűnözésben érintettek száma Budapesten 800–1000 fő közé volt tehető (Dános 1988). A bűnszervezetek vezetőinek jelentős mértékű tőkefelhalmozása szükségessé tette a vagyonuk legalizálását, amely egyet jelentett a pénzmosás megjelenésével, vagyis az illegális vagyon legális gazdasági életbe való átforgatásával. Ez a fajta bűnelkövetés mindenképpen további fejlődésének tekinthető, hiszen addig a „fehér galléros" szervezett bűnözés jellemzően csak a hivatali visszaélésekben, illetve a sikkasztásban merült ki.

A rendszerváltással járó társadalmi és gazdasági átalakulás, a privatizáció, a liberalizálódó piacgazdaság, valamint a szabályozási zavarok további lehetőséget adtak

a szervezett bűnözés megerősödésére. Emellett a bűnüldöző szervek nem voltak felkészülve a gyorsan változó társadalmi és gazdasági környezet kihívásaira, ami ideális környezetet teremtett a szervezett bűnözés hazai térnyeréséhez (Kerezsi 2001; Vókó 2004). Ebben az időszakban alakultak ki azok a bűnszervezetek, amelyek már a klasszikus, maffiaszerű jellemzőkkel bírtak: hierarchikus felépítés, területi ellenőrzés, gazdasági érdekeltségek és célzott korrupció. 1988 és 1991 között az ismertté vált bűncselekmények száma 2,4-szeresére nőtt (Patkós–Tóth 2012). Ekkor jelentek meg először az olyan klasszikus maffiamódszerek, mint amilyen a zsarolás, a védelmi pénzek szedése, a leszámolások, ideértve a megrendelésre elkövetett gyilkosságokat is (Vókó 2004). A korszak jellegzetes illegálisjövedelem-forrása az úgynevezett olajszőkítés volt, amely olyan jelentős profitot termelt a szervezett bűnözők számára, hogy az azzal kapcsolatos belső, illetve szervezetek közti konfliktusok már életeket is követeltek. Ekkor vetették meg a lábukat hazánkban az orosz, ukrán és balkáni szervezett bűnözői csoportok is (Kis-Benedek 2003; Szabó 2008). Az egyes bűnszervezetek közötti konfliktusok, leszámolások súlyos társadalmi nyugtalanságot keltettek. A mélypont az 1998. július 2-án fényes nappal, Budapest belvárosában végrehajtott „Aranykéz utcai robbantás" volt, amely már a civil lakosságot is érintette az áldozatok személyében is. Ekkorra a szervezett bűnözés már nem csupán rendészeti vagy bűnüldözési probléma volt, hanem komplex társadalmi veszélyforrás, amely képes volt rombolni a közbizalmat és akadályozni a demokratikus intézményrendszerek működését, és aláásni az állami szuverenitást. A társadalom „telítődött a bűnnel". Az állam – reagálva a kialakult helyzetre – hathatós lépéseket tett a szervezett bűnözés felszámolására. Stabilizálta és átláthatóvá tette a jogi környezetet, megerősítette a rendőrséget és a nemzetbiztonsági szolgálatokat. Létrehozta a szervezett bűnözés elleni küzdelemre szakosodott, állandó struktúrával működő – bár időközben többször áthelyezett, átszervezett, átnevezett – felderítő egységet, amely ma a Készenléti Rendőrségen belül Nemzeti Nyomozó Iroda néven működik.

A digitalizáció és a kiberbűnözés térnyerése

A millenniumra nagyjából végbementek, lezajlottak azok a folyamatok, amelyek az erőszakhullámot generálták. Ekkor azonban új időszak, a negyedik, globális ipari forradalom kezdődött, pontosabban a már zajló digitalizáció jelentősen felerősödött – az internet, a mobiltelefon, a mobiltelefonnal elérhető internet előretörése által. Ez alapjaiban alakította át az emberek mindennapjait. A virtuális világ rohamléptékű fejlődése, egyszerű, olcsó és elérhető közelsége, az okoseszközök (IoT) és online platformok tömeges elterjedése hozzájárult ahhoz, hogy a felhasználók egyre több tevékenységet egyre szélesebb körben a virtuális térben végezzenek. Ma már a hírfogyasztás, a tanulás, a szórakozás, a kommunikáció, a vásárlás, valamint a banki és hivatalos ügyintézés is nagyrészt online térben zajlik. A 2019 év végén kitört SARS-CoV-2-vírus okozta világjárvány, illetve ennek kezelése érdekében elrendelt lezárások okán a digitalizálódás folyamata felgyorsult. Rendkívül rövid idő alatt jelentős mértékben kiszélesedett az online világban való mindennapi élet. A lezajlott, és ma is zajló, folyamat nem csupán a technológiai fejlődés eredménye, hanem társadalmi

és kulturális átalakulások indikátora is, ami új normákat, lehetőségeket és nem utolsósorban ma még – a biztonságtudatosság hiányában – jelentős kockázatokat teremt a felhasználók számára.

A digitális evolúció során, azzal párhuzamosan a bűnözők is adaptálódtak az online tér nyújtotta lehetőségekhez. A bűnelkövető egyén szempontjából az internet adta deindividualizáció (az elszemélytelenedés, az online anonimitás miatt) (Birch 2010), az erkölcsi kikapcsolás *(moral disengagement)* (Concha-Salgado et al. 2022) és az ezek eredményeként megjelenő online gátlástalanság mind elősegítik az egyébként teljes mértékben profitorientált bűncselekmények elkövetését. Ennek megfelelően a virtuális környezet nem korlátozta, hanem újabb lehetőséget teremtve kiterjesztette az illegális tevékenységek körét nemcsak földrajzilag, hanem szervezettség tekintetében is. Az internet egyfelől új színteret biztosít az egyes elkövetők, a kisebb bűnözői csoportok, valamint a tradicionális szervezett bűnözői csoportok számára, hogy a klasszikus – illegális – tevékenységeiket a digitális tér felhasználásával folytathassák. Emellett az internet lehetőséget teremtett új típusú, kifejezetten kiberbűncselekmények elkövetésére specializálódott szervezett bűnözői csoportok kialakulására és működésére is. Számos, szervezettséget mutató bűnözői csoport alakult kifejezetten az online tér adta lehetőségekre specializálva magát. Meg kell jegyezni, hogy az online térben megjelenő szervezett bűnözés struktúrája nem mutat teljes azonosságot a valós térben meglévő, tradicionális bűnszervezetekkel. A kibertérben működő szervezett bűnözői csoportok tipológiájának feltárásával Michael McGuire a brit Surrey Egyetem docense foglalkozott. McGuire kutatásai szerint a kiberbűnözés túlnyomó többsége – az esetek mintegy 80%-ában – szervezett keretek között zajlik, ugyanakkor az online térben megjelenő bűnszervezetek jelentős eltérést mutatnak a hagyományos, hierarchikus struktúráktól. A digitális környezet új típusú, rugalmasabb és decentralizáltabb szerveződéseket hozott létre, amelyek sokszor ideiglenes vagy célorientált együttműködéseken alapulnak. McGuire két fő online működésű csoporttípust különít el: a *swarm* és a *hub* modelleket. A *swarm* típus decentralizált, spontán módon szerveződő csoportokat takar, amelyek közös ideológiai vagy politikai célok mentén működnek, explicit hierarchia nélkül. Ezek a csoportok jellemzően hacktivista tevékenységeket folytatnak; ide tartozik például az Anonymous csoport. Ezzel szemben a *hub* típusú csoportok már strukturáltabbak és centralizáltabbak: egyes kulcsfontosságú szereplők (vezetők, technikai szakértők) köré épülnek, akik a működés irányítását végzik. Ezek a csoportok gyakran részt vesznek adathalászkampányokban, kártékony szoftverek terjesztésében, vagy működtetik az online feketepiacokat (McGuire 2012). A digitális környezetben való működés lehetővé teszi e csoportok számára a gyors alkalmazkodást, a transznacionális jelenlétet és a folyamatos újraszerveződést, ami különösen megnehezíti a hatóságok számára a felderítést.

A fent vázolt körülmények tették lehetővé az online térben elkövetett bűncselekmények számának radikális növekedését. A probléma súlyosságát mutatja, hogy az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája (Federal Bureau of Investigation, FBI) 2000 májusában fel kellett állítsa az Internet Crime Complaint Centert (Internetes Bűnügyi Panaszkezelő Központ) azzal a céllal, hogy az online csalásokkal és más kiberbűncselekményekkel, például hackeléssel, gazdasági kémkedéssel, zsarolással, pénzmosással és szellemi tulajdon elleni jogsértésekkel kapcsolatos

panaszokat fogadja. A Panaszkezelő Központ 2023-as jelentése szerint – évről évre növekvő mértékű – összesen 3,79 millió bejelentést kezelt, amelyek mögött összesen 37,4 Mrd dollár anyagi kár volt (Federal Bureau of Investigation 2023).

A kiberbűnözés elleni védekezés és prevenció Magyarországon

Magyarországon a 2001-ben aláírt Számítógépes bűnözésről szóló egyezmény (Convention of Cybercrime) 2004-ben lépett hatályba, amely fokozatosan került be a Büntető törvénykönyvbe és a büntetőeljárásról szóló törvénybe is. Az Európai Unió a kibertér veszélyeinek rohamos előretörése miatt több rendeletet és irányelvet is megalkotott, amit több-kevesebb sikerrel sikerült is implementálnunk, így az utolsók között megszületett a *Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény* és annak végrehajtási rendeletei, valamint az új *Kiberbiztonsági Stratégiánk* [1089/2025. (III. 31.) Kormányhatározat], amelyek megjelenése már nagyon szükséges volt.

A Parlament, készülve a virtuális térhódítással megjelenő problémákra, 2013-ban – Magyarország Biztonsági Stratégiája, a Nemzeti Kiberbiztonsági Stratégia, valamint az Európai Unió kiberbiztonsági stratégiája alapján – megalkotta *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt* (Ibtv.). A szabályozás 2013. július 1-jén lépett hatályba, és céljául a nemzeti elektronikus adatvagyon, valamint az állami és önkormányzati információs rendszerek védelmének erősítését tűzte ki. Az Ibtv. kiemelte, hogy az elektronikus rendszerek biztonságáért elsősorban az üzemeltető szervek felelnek. A törvény alapján jött létre a hazai kibervédelmi szervezetrendszer, amelynek feladata az állami szervek információbiztonsági tevékenységének támogatása, ellenőrzése és a biztonságtudatosság növelése. Az Ibtv. 2015. évi módosítása után a Nemzetbiztonsági Szakszolgálat (NBSZ) fontos feladatot kapott, 2015. október 1-jén megalakult a *Nemzeti Kibervédelmi Intézet (NKI)*[4]. Ez az intézményi átalakítás a kibervédelem hatékonyabb központosítását és szakmai színvonalának emelését szolgálta (NBSZ 2016).

A jogszabályi változások szükségességét jól mutatják többek között a Mastercard Cyber Insights által gyűjtött adatok, amelyek szerint a 2020–2023-as időszakban hazánkban – ahogy más közép- és kelet-európai országokban is – konzekvensen leginkább a közszférát ér támadás, majd a technológiai ipart és pénzügyi szférát, mindamellett magánszemélyeket ér a legnagyobb mértékű anyagi kár. Az elkövetési módszerek közül leginkább a *malware* (kártevő szoftver rendszerbe juttatása, adatlopás) és a *ransomware* (titkosító, kártevő program telepítése, majd zsarolás) támadás, de már jelentős mértékű a *reconnaissance,* vagyis a támadások előkészítése is (Mastercard 2025).

A Magyar Nemzeti Bank kimutatása szerint (MNB [é. n.]) 2020. I. negyedéve és 2024. IV. negyedéve között az elektronikus pénzforgalomban bekövetkezett közel 42 000 visszaélés kapcsán keletkezett kár meghaladta az 53,5 milliárd forintot (BSR [é. n.]).

[4] A Nemzeti Kibervédelmi Intézet neve 2025. október 1-jétől Nemzeti Kiberbiztonsági Intézetre változott.

Barabás és Koplányi 2023-as kutatásának eredménye azt mutatta, hogy Magyarországon az online áldozattá válás nagyobb gyakorisága figyelhető meg az offline cselekményekhez képest (30,7% és 21%) (Barabás–Koplányi 2023).

Mindezen jelenségek rávilágítanak arra, hogy az információs társadalom, és különösen az internet, noha számos gazdasági, kulturális és társadalmi előnyt biztosít, komoly kockázatokat is rejt magában. A kiberbűnözés, pontosabban az online tér felhasználásával elkövetett bűncselekmények professzionalizálódása jelentős kihívást jelent biztonsági szempontból.

A Magyar Nemzeti Bank, a Magyar Bankszövetség, az Országos Rendőr-főkapitányság, a Nemzeti Kibervédelmi Intézet és a Nemzeti Média- és Hírközlési Hatóság 2022 őszén megkezdte a KiberPajzs kampányt, amelyhez később további szervek – köztük az Igazságügyi Minisztérium, a Szabályozott Tevékenységek Felügyeleti Hatósága, az Államkincstár és a Nemzeti Védelmi Szolgálat – csatlakoztak. A kezdeményezés fő célja a lakosság pénzügyi digitális tudatosságának növelése, a kockázatok ismertetése és a biztonságos online magatartás népszerűsítése (*Az MNB kezdeményezése a kiberbiztonságért* 2022).

A Rendőrség 2023 őszén az online bűncselekmények visszaszorítása és felderítése érdekében megalkotta a Mátrix projektet. A program szerves része az Országos Rendőr-főkapitányság Bűnügyi Főigazgatóságán belül létrehozott Kiberstratégai Osztály, amely a programba delegált, a területi szerveknél szolgálatot teljesítő, közel 300 szakember munkáját és az általuk folytatott nyomozásokat koordinálja. A Nemzeti Közszolgálati Egyetem Rendészettudományi Karán 2024 nyarán önálló szervezeti egységként jött létre a korábban más szervezeti keretben működő Kiberbűnözés Elleni Tanszék.

Mára kissé megtorpanni látszó, de még mindig jelentős bűnügyi számokat és rendkívüli károkat mutató statisztikai adatok alapján szélmalomharcnak tűnik a küzdelem. Az online kockázatok hatékony kezelése, felismerése és megelőzése olyan komplex, interdiszciplináris megközelítést igényel, amelyben a bűnüldözési fellépés, a technológiai védelem mellett kiemelt szerepet kell kapnia a társadalmi szintű biztonságtudatosság erősítésének. Ennek érdekében szükséges az állami, gazdasági és civil szereplők összehangolt együttműködése, valamint a felhasználók digitális kompetenciáinak, biztonságtudatosságának folyamatos fejlesztése.

Alapgondolat

A Nemzeti Közszolgálati Egyetem vezetőségének, hallgatóinak, oktatóinak a figyelme is ide irányult. Azt láttuk, hogy kialakultak a felderítési eszközök, a bűnüldözés felvette a harcot az online tér segítségével elkövetésre kerülő bűncselekményekkel szemben, azonban a proaktív és preventív rendészet továbbra sem tekinthető hatékonynak e téren.

Az egyetemi közös gondolkodás során kialakult egy ötlet. A rendészettudomány szerteágazó diszciplínái arra sarkallták a szerzőket, hogy ötvözzék a kockázatelemzés, a prediktív rendészet és a bűnmegelőzés amúgy egymástól távol nem lévő területét az online

tér felhasználásával elkövetett, pontosabban elkövetendő bűncselekmények megelőzése érdekében.

Az alapgondolat abból indult, hogy van-e, és amennyiben nincs, lehetséges-e egy olyan programot készíteni, amely az online térben prediktíven előre jelezheti a potenciális áldozatoknak, hogy veszélyben vannak, lehetnek, annak következtében, hogy milyen jellegű magatartások jellemzik az online térben végzett jelenlétüket. Fontos, hogy az alapkoncepcióhoz olyan már létező és meglévő technikákat és módszereket rendeljünk, amelyek lehetővé teszik, hogy megfoghatóvá váljon a gondolat gyakorlati alkalmazáshoz.

A kockázatelemzés

A kockázatelemzés empirikus megközelítést jelent, amelynek célja azoknak a potenciális kockázatoknak, veszélyeknek az identifikálása, értékelése és kezelése, amelyek negatívan befolyásolhatják a vizsgált szervezet, projekt vagy tevékenység eredményességét. A folyamat vége ideális esetben a megfelelő válaszintézkedések kidolgozása, illetve azoknak a visszakommunikálása. Ezeknek az analíziseknek az elsődleges célja kettős: az előre nem látható események következményeinek enyhítése és az általános felkészültség fokozása (Attar 2011).

A szemléltetés érdekében bemutatjuk az ipari ágazatban már hatékonyan működő kockázatelemző programok alapvető működési elveit, ebből akár inspirációt és technikai megoldásokat nyerhetünk. Ilyen program például az Industrial Risk Consulting (IRC) és a SafetyCulture. Ezeknek a kockázatelemző szoftvereknek a célkitűzése a potenciális kockázatok azonosítása, értékelése és kezelése, hogy minimalizálják a vállalkozások működésére gyakorolt hatásokat. Az első lépés azon veszélyek azonosítása, amelyek káros hatással lehetnek a vállalkozásra (például gépek meghibásodása, veszélyes vegyi anyagoknak való kitettség, tűzveszélyek vagy ergonómiai problémák). Ezt követi a kockázatelemzés folyamata, amely során a rizikófaktorok valószínűségét és súlyosságát értékelik, hogy megértsék az infrastruktúra sebezhető pontjait, és célzott intézkedéseket hozzanak ezek enyhítése és megszüntetése érdekében (Safety Educations 2024). A kockázatkezelés részeként preventív karbantartási programokat alkalmaznak, amelyek magukban foglalják a gépek és berendezések rendszeres ellenőrzését, karbantartását és javítását, hogy megelőzzék a problémák kialakulását (HSI [é. n.]). Végül a kockázatkommunikáció keretében a veszélyekkel kapcsolatos információkat közlik a kezelőkkel. Következtetésképpen elmondhatjuk, hogy a civil szektorban használt kockázatelemző programok holisztikus és proaktív megközelítést alkalmaznak a kockázatok kezelésére (Safety Culture Content Team 2025).

A bűnüldözés és a kockázatelemzés kapcsolata

A bűnüldözés területén a kockázatelemzés kritikus szerepet tölthet be a közbiztonság fenntartásában. A kockázatelemzés révén a rendészeti szervek képesek prognosztizálni és mérsékelni a lehetséges fenyegetéseket, amelyek a társadalom jólétét veszélyeztetik

(Scism 2017). Ez magában foglalja a bűncselekmények megelőzését, a rendőri műveletek biztonságának fokozását, valamint a közösség bizalmának fenntartását. Ezenkívül ez a megközelítés lehetővé teszi a hatóságok számára, hogy hatékonyabban reagáljanak az előre nem látható eseményekre is (Fritsvold 2018).

Az automatizált kockázatelemző szoftverek fejlesztése szignifikánsan fokozhatja a folyamat hatékonyságát és pontosságát. A magas színvonalú szoftverrendszerek, különösen a mesterséges intelligencián (MI) alapulók, képesek nagy mennyiségű adat feldolgozására, a potenciális kockázatok előrejelzésére és kockázatcsökkentési stratégiák kidolgozására (Risk Wizard Team 2024). A prediktív rendészet területén például már alkalmaznak algoritmikus rendszereket a meglévő bűnügyi adatok elemzésére és a jövőbeli bűnözői tevékenységek előrejelzésére. Ezek az előrejelzések magukban foglalják a lehetséges bűncselekmények jellegét, valószínű helyüket, valamint a potenciálisabb áldozatokat és elkövetőket (Browning–Arrigo 2021). A kockázatelemzés ezen technológiai előrehaladása jelentős előrelépést jelent a bűnüldözésben. Fontos azonban, hogy ezeket az eszközöket (szoftvereket) kritikus szemlélettel vizsgáljuk, figyelembe véve mind az előnyöket, mind a korlátokat. Mint minden analitikai megközelítés esetében, az MI-alapú kockázatelemzés hatékonysága az inputadatok minőségétől, az algoritmusok komplexitásától és az eredmények képzett szakemberek általi interpretációjától függ.

Számos jelentős program mutatja be ezt a technológiát jelenleg is. A PredPol a bűnügyi adatok algoritmikus elemzését használja a potenciális bűncselekmények előrejelzésére, mind időben, mind térben, lehetővé téve a célzottabb rendőri jelenlétet. Hasonlóképpen a HunchLab, amely különféle adatforrásokat integrál, beleértve a bűnügyi adatokat, a meteorológiai adatokat és a közösségi események információit, hogy optimalizálja a rendőrségi erőforrások allokációját az előrejelzett bűnözési valószínűség alapján. Hangtani alapú technológiákat is kifejlesztettek a gyors reagálás érdekében: a ShotSpotter akusztikai szenzorokat alkalmaz, hogy bemérje és lokalizálja a lövések hangját, majd mesterséges intelligencia segítségével meghatározzák ezek pontos helyét. A Palantir platform különleges megközelítést képvisel a bűnüldözés *big data* elemzéséhez, ugyanis az elsődleges funkciója a minták és trendek azonosítása különböző adatpontok összekapcsolásával (Kisfonai 2023).

Ha átevezünk a körülöttünk lévő fizikai világból az online térbe, más szoftverek lesznek említésre méltók a virtuális világ sajátosságaiból adódóan. Például a SocialNet elnevezésű szoftver az online tevékenységek, közösségi média és *dark web* fenyegetések monitorozására szolgál. A program különböző forrásokból származó adatokat összesít, hogy azonosítsa a potenciális bűncselekményeket és fenyegetéseket (Kwet 2021; ShadowDragon [é. n.]). Az online tranzakciók során a csalások prevenciójára irányuló törekvések is profitáltak a mesterséges intelligencia fejlesztéseiből. A LexisNexis ThreatMetrix elnevezésű szoftvere valós idejű kockázatelemzést biztosít a digitális identitásellenőrzés és a viselkedési adatok integrálásával. A rendszer mesterséges intelligenciát alkalmaz a csalási mintázatok és korrelációk elemzésére, megkönnyítve a precíz kockázatértékelést és javítva az ügyfelek védelmét a csalárd tevékenységekkel szemben (LexisNexis 2022).

Fontos, hogy megismerjük a nemzetközi kooperációs erőfeszítéseket, amelyek tovább bővítették a mesterséges intelligencia hatókörét a bűnmegelőzésben, ezen belül

pedig a kockázatelemzésben. Kiemelkednek az Europol AP Check-the-Web és AP Twins projektjei. Az előbbi a nyílt internetes források nyomon követésére összpontosít az iszlamista terrorizmus indikátorai után, míg az utóbbi a gyermekek szexuális kizsákmányolásának és bántalmazásának minden formája elleni harcra irányul (Simon 2018). Az áldozatazonosítási munkacsoport *(victim identification task force)* a mesterséges intelligencia egy további alkalmazását jelenti a bűnüldözésben. Ez a kezdeményezés különféle elemzési technikákat alkalmaz az ismeretlen áldozatok azonosítására, beleértve a digitális nyomok, képek, videók és egyéb releváns adatforrások vizsgálatát (Mezei 2019).

A mesterséges intelligencia által támogatott bűnüldözés és bűnmegelőzés terén elért fejlemények rámutatnak a büntető igazságszolgáltatásban a technológiai megoldások állandó fejlődésére.

Kockázatelemzés a digitális térben (szoftverfejlesztési ötlet)

A korábban bemutatott rendészeti programokat célszerű megvizsgálni. Választ kaphatunk, hogyan lehet olyan szoftvert kifejleszteni, amely kockázatelemzést végez a digitális térben, és amely szintén az analizálás módszerein és mesterséges intelligencián alapulna. A SWOT-analízis (Day–Holznienkemper 2024) segítségével komplex képet kaphatunk a fejlesztendő szoftver erősségeiről, gyengeségeiről, lehetőségeiről és veszélyeiről, ami segíthet a stratégiai döntéshozatal során és a fejlesztési folyamat optimalizálásában (1. táblázat).

A rendszer fő erőssége abban rejlik, hogy proaktív megközelítést biztosít a felhasználóknak online tevékenységeik kezeléséhez, ezáltal csökkentve a lehetséges kockázatokat. A mesterséges intelligencia használatával a program alkalmazkodik a környezetéhez, képes tanulni, változni, és valós idejű, automatizált elemzést nyújt a felhasználói magatartásról. Ez a funkció lehetővé teszi a potenciális veszélyek gyors azonosítását és az azonnali felhasználói figyelmeztetéseket, elősegítve az azonnali reagálást az áldozattá válás kockázatának minimalizálása érdekében.

Számos kihívás megfontolást igényel. Ezek közül a legfontosabb a szigorú adatvédelmi és etikai előírások betartása a felhasználói adatok kezelésének során. Ez alapvető a felhasználói bizalom megőrzéséhez és a transzparencia biztosításához. Ezenkívül az MI-modell fejlesztése technikai kihívásokkal jár, beleértve a nagy mennyiségű adatok feldolgozását, a modell pontosságának és megbízhatóságának garantálását, valamint az új fenyegetésekhez való alkalmazkodóképesség fenntartását. A rendszerfejlesztés és -karbantartás összetettsége jelentős szakértelmet és erőforrásokat követel meg, ami megnövekedett költségekhez és hibalehetőségekhez vezethet.

1. táblázat: A program SWOT-elemzése

SWOT-elemzés		
Belső tényezők	**Erősségek**	**Gyengeségek**
	Innovatív megközelítés az online biztonság terén MI-alapú automatizálás Valós idejű kockázatelemzés	Adatvédelmi és etikai kérdések Reprezentativitás biztosítása Technikai kihívások az MI-modell fejlesztésében Technikai és műszaki komplexitás
Külső tényezők	**Lehetőségek**	**Veszélyek**
	Növekvő igény a kiberbiztonsági megoldásokra Együttműködések kutatóintézetekkel és vállalatokkal Oktatási programok integrálása Felhasználói tudatosság növelése	Jogi szabályozások változása Felhasználói bizalom hiánya Technológiai fejlődés gyors üteme Versenytársak megjelenése/megerősödése Adatvédelmi incidensek

Forrás: a szerzők szerkesztése

A program számos fejlesztési és expanziós lehetőséget kínál. Tekintettel az online fenyegetések fokozódó prevalenciájára, egyre nagyobb piaci kereslet jelentkezik a hatékony kiberbiztonsági megoldások iránt. A kutatóintézetekkel és az egyéb partnerekkel való kollaboráció megkönnyítheti a program további tökéletesítését, hozzáférést nyújtva a legújabb kutatási eredményekhez és technológiai fejlesztésekhez. Ezenkívül az oktatási tantervekbe történő integrálás növelheti a felhasználók tudatosságát az online biztonsággal kapcsolatban, potenciálisan bővítve a program hatókörét és hatását.

Mindazonáltal számos lehetséges veszélyt hordoz magában. A kiberbiztonsági és adatvédelmi jogszabályok dinamikus jellege szükségessé teszi a rendszer és az adatkezelési gyakorlatok állandó frissítését a szabályozási megfelelés biztosítása érdekében. A felhasználói bizalom továbbra is kulcsfontosságú: a rendszer biztonságába vagy adatkezelési gyakorlatába vetett bizalom bármilyen erózió jelentősen akadályozhatja az elfogadást és ezáltal a felhasználást. A technológiai fejlődés gyors üteme folyamatos adaptációt igényel a feltörekvő technológiákhoz és fenyegetésekhez, ami állandó rendszerfrissítéseket és fejlesztéseket tesz szükségessé. Ezenkívül a kiberbiztonsági piac versenykörnyezetének dinamikája nyomást helyezhet a szoftverre, hogy megőrizze pozícióját és konstans bővítse kínálatát. Végezetül az adatvédelmi incidensek kockázata jelentős fenyegetés, súlyosan ronthatja a felhasználók bizalmát és a szoftver reputációját, ami hangsúlyozza a szilárd adatvédelmi intézkedések kritikus jelentőségét.

Egy olyan konkrét szoftver fejlesztése célravezető lenne, amely az online térben történő áldozattá válás kockázatát méri és elemzi. A kockázatelemzés alapját egy kategorizálási rendszer képezné, amely a felhasználók tevékenységét értékeli abból a szempontból, hogy az milyen mértékben növeli az áldozattá válás valószínűségét. Ez az értékelési

keretrendszer lehetőséget biztosítana arra, hogy az egyének tudatosabbá váljanak saját kockázati szintjükkel kapcsolatban.

A folyamat automatizálása mesterséges intelligenciával is megvalósítható. Egy ilyen rendszer működtetésére két alapvető megközelítést gondoltam el: az egyik egy előre meghatározott feltételeken alapuló adatbázis alkalmazása, amely egy rögzített szabályrendszeren keresztül elemzi a felhasználói tevékenységet, míg a másik egy felhasználók által generált adatokból dolgozó modell létrehozása, amely folyamatosan tanul és adaptálódik a valós online környezethez. Mindkét megközelítés esetén fontos etikai és jogi kérdés a személyes adatok gyűjtésének jogalapja, valamint az adatkezelés módja és átláthatósága.

Amennyiben a rendszer önkéntes alapon működne, az egyik kulcsfontosságú kihívás az adatbázis reprezentativitásának biztosítása. Amennyiben a rendszer kizárólag az önkéntesen részt vevő felhasználók adataira támaszkodna, előfordulhat, hogy a kockázati kategóriák torzulnának, és nem tükröznék teljes mértékben az egész online populáció viselkedésmintáit. Cserébe viszont egy reprezentatív adathalmaz alkalmazása lehetőséget biztosítana arra, hogy a rendszer objektívebb módon határozza meg a különböző kockázati tényezőket, és hogy konkrét cselekményekre figyelmeztesse a felhasználókat, ezáltal növelve az információbiztonsági tudatosságukat.

Az áldozattá válás kockázatának mérésére egy pontozásos rendszer is alkalmazható lenne. Ebben a modellben a különböző online tevékenységek és viselkedési mintázatok eltérő súlyozású kockázati értékeket kapnának. Például egy nem biztonságos (http:// előtaggal rendelkező) weboldalra történő kattintás +1 pontot eredményezhetne, míg egy mesterséges intelligencia által generált *deepfake* tartalom valósként való elfogadása és megosztása +3 pontot jelenthetne. Amennyiben a felhasználó által elért pontszám meghaladna egy meghatározott küszöbértéket, a rendszer figyelmeztető jelzést küldhetne, amelyben releváns információk és megelőzési javaslatok szerepelnének.

A reprezentativitás kérdése (és fontossága) a szoftverrel kapcsolatban

A (kutatási) módszertan területén a reprezentativitás kérdése a legfontosabb. Az eredmények pontossága és érvényessége attól függ, hogy a szoftver képes-e pontosan tükrözni a teljes online populáció viselkedési mintáit. Ez nemcsak a kockázatelemzés pontosságát növeli, hanem a felhasználók bizalmát is erősíti, mivel felismerik, hogy a rendszer átfogó és reprezentatív adatokra épül. Ezenkívül a reprezentativitás megvalósítása enyhítheti a lehetséges torzításokat, és relevánssá és előnyössé teheti a rendszert a különböző demográfiai csoportok számára. Az adatbázis folyamatos frissítése és bővítése lehetővé teszi a gyors alkalmazkodást a felmerülő fenyegetésekhez és viselkedésekhez. A kutatás sikere alapvetően a reprezentativitástól függ, hiszen ez az egyetlen eszköz annak biztosítására, hogy az eredmények hűen tükrözzék a teljes lakosság online magatartási mintáit és ezek kockázatait.

– A véletlenszerű mintavételi technikák fontos szerepet játszanak a reprezentativitás elérésében. Azáltal, hogy minden felhasználó egyenlő valószínűséggel kerül a mintába, ezek a módszerek mérséklik az elfogultságot és javítják a reprezentativitást. Ez a megközelítés kulcsfontosságú, mivel lehetővé teszi, hogy a minta

valósághűen reprezentálja a teljes népességet, nem pedig egy szűk, potenciálisan torzított részhalmazt. A véletlenszerű mintavétel során az egyes felhasználók egyenlő kiválasztási esélye növeli az eredmények érvényességét és megbízhatóságát. A gyakorlati alkalmazások közé tartozhat a véletlenszám-generátorok vagy a szisztematikus mintavételi technikák használata.
- Az optimális mintanagyság meghatározása szintén kiemelendő. A reprezentatív eredményekhez szükséges résztvevők számát a kutatási célok és a populáció nagysága alapján kell kiszámítani. Az alulméretezett minta megbízhatatlan eredményeket hozhat, amelyek nem képesek tükrözni a teljes populáció viselkedési mintáit. Ezzel szemben a túlméretezett minta felesleges erőforrásokat igényelhet, ami a hatékonyság csökkenéséhez vezethet. Az optimális mintanagyság megtalálása tehát elengedhetetlen a kutatás eredményességéhez.
- A stratifikált (rétegzett) mintavétel alkalmazása tovább növeli a reprezentativitást. Ez a módszer magában foglalja a populáció különböző szegmensekre osztását, például életkor, nem és földrajzi elhelyezkedés, valamint az egyes rétegekből randomizált minta kiválasztását. Ez a megközelítés biztosítja az összes jelentős demográfiai csoport képviseletét, és megelőzi az elfogultságot bármely adott csoport irányába. Ez különösen előnyös lehet, hiszen a demográfiai jellemzők hatással vannak a vizsgált tevékenységekre.
- Az adatgyűjtési módszerek diverzifikálását is prioritásként kell kezelni annak érdekében, hogy különböző preferenciákkal és viselkedésmintákkal rendelkező felhasználókat is elérhessen a szoftver. A különféle módszerek alkalmazása biztosítja, hogy minden demográfiai csoport megfelelően reprezentált legyen a mintában.

Összefoglalva, a reprezentativitás alapvető fontosságú a kutatási módszertanban, mivel növeli az eredmények megbízhatóságát és érvényességét. A véletlenszerű mintavételi technikák alkalmazása, a megfelelő mintaméretek kiválasztása, a rétegzett mintavétel és az adatgyűjtési módszerek sokszínűsítése együttesen hozzájárul ahhoz, hogy a minta megfelelően tükrözze a teljes online populáció magatartási mintáit. Ezek a módszertanok nemcsak a kockázatelemzés pedantériáját javítják, hanem a felhasználói bizalmat is növelik azáltal, hogy bizonyítják, a rendszer kiterjedt és reprezentatív adatokra épül.

Adatvédelmi kérdések

A fent elkészített SWOT-analízis rávilágít arra, hogy az adatvédelem a digitális kockázatelemző szoftver egyik legkritikusabb gyengesége és potenciális veszélyforrása. Ezért elengedhetetlen, hogy ezt a kérdéskört vizsgáljuk, különös tekintettel a jogszabályi előírásokra, a technikai és szervezési kihívásokra, valamint azokra a speciális problémákra, amelyek a digitális térben, különösen harmadik országokkal való adatkapcsolatok esetén merülnek fel. Ezzel a fókuszváltással megteremthetjük a kapcsolatot a szoftverfejlesztési ötletünk gyakorlati megvalósíthatósága és az adatvédelmi követelmények között, amelyek nélkül a rendszer nem működhet hatékonyan és jogszerűen.

Az internetes csalások és az adatvédelem kapcsolata

Az internetes csalások során az elkövetők gyakran személyes adatokat használnak fel az áldozatok megtévesztésére vagy további bűncselekmények elkövetésére. Az adathalászat *(phishing),* az adatszivárgás és a hamis weboldalak üzemeltetése mind azt a célt szolgálják, hogy a felhasználóktól érzékeny információkat szerezzenek meg. Az ilyen incidensek rávilágítanak arra, hogy az adatvédelem nem csupán jogi kötelezettség, hanem a digitális biztonság alapvető eleme.

Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) szigorú szabályokat határoz meg a személyes adatok kezelésére vonatkozóan (Európai Parlament és Tanács [2016]: Általános Adatvédelmi Rendelet [GDPR]). A GDPR egyik legfontosabb elve az adatok biztonságos kezelése és az incidensek átlátható kezelése, ami kötelezi az adatkezelőket a felhasználók jogainak védelmére.

Az adatvédelmi előírások szerepe a megelőzésben

A GDPR előírásai szerint az adatkezelők kötelesek megfelelő technikai és szervezési intézkedéseket tenni az adatbiztonság garantálása érdekében. Ilyen intézkedések például az adatok titkosítása, a kétfaktoros azonosítás bevezetése, a rendszeres biztonsági frissítések alkalmazása, vagy a biztonságtudatossági képzések szervezése.

Az adatvédelmi incidensek esetén a GDPR értelmében 72 órán belül értesíteni kell a felügyeleti hatóságot, és szükség esetén az érintetteket is (Voigt – von dem Bussche 2017). Így az érintettek gyorsan reagálhatnak a potenciális károk minimalizálása érdekében, mint jelszóváltoztatás vagy egyéb, fent felsorolt biztonsági intézkedések.

Adatvédelmi kihívások harmadik országok esetében

Az Európai Unión belül is jelenthet kihívást a csaló weboldalak eltávolítása, ám erre vonatkozóan még mindig több lehetőség áll a hatóságok rendelkezésére (például elektronikus adat hozzáférhetetlenné tétele). Különös figyelmet érdemel, amikor a felhasználók adatai olyan weboldalakhoz kerülnek, amelyek harmadik országban, például az Európai Unión kívül működnek. A GDPR értelmében a személyes adatok EU-n kívüli továbbítása csak akkor megengedett, ha az adott ország megfelelő szintű adatvédelmet biztosít, vagy ha más jogi eszközök – például szerződéses kikötések, kötelező erejű vállalati szabályok vagy az érintett hozzájárulása – megfelelő védelmet nyújtanak (GDPR 44–50. cikkek).

Az ilyen adatátvitel azonban komoly kockázatokat hordoz, például:

- hiányos jogi védelem: sok harmadik ország nem rendelkezik az EU-szabályozással egyenértékű adatvédelmi törvényekkel. Ez az adatok jogosulatlan felhasználásához, megfigyeléséhez vagy akár értékesítéséhez vezethet;
- jogorvoslat hiánya: az érintetteknek nehezebb érvényesíteni jogaikat vagy panaszt tenni, ha adataik külföldre kerülnek;

– nem átlátható adatfeldolgozás: gyakran nem derül ki, milyen célból és hogyan kezelik az adatokat a harmadik országokban.

Különösen problémás, ha az internetes csalók olyan, harmadik országban üzemeltetett hamis weboldalakat használnak, amelyek adatokat gyűjtenek, majd jogi kényszer nélkül használják azokat fel újabb bűncselekményekhez (Kuner 2013).

Ezért a felhasználók számára kiemelten fontos, hogy csak megbízható, ellenőrzött weboldalakon adjanak meg személyes adatokat, és mindig ellenőrizzék az adatvédelmi tájékoztatót, különösen, ha az oldal üzemeltetője nem az EU területén található.

Megoldásként lehet gondolni a különböző weboldalak monitorozására, amennyiben a rendőrség harmadik országbeli weboldalakat blokkol, úgy igen, de az alábbi korlátozásokkal és feltételekkel:

A nyilvánosan elérhető weboldalakat – még ha azok harmadik országban (például Oroszország, USA, Kína stb.) üzemelnek is – a magyar hatóság passzívan monitorozhatja, azaz:

– információt gyűjthet róluk (például automatikus keresővel vagy manuálisan);
– elemzéseket készíthet, ha az adatok publikusak;
– ezt megteheti bűnüldözési célból, ha az eljárás nem jár tiltott beavatkozással (például nem sérti más ország szuverenitását, vagy nem alkalmaz hekkertámadást).

Nem megengedhető egy rendszerbe történő behatolás vagy a weboldal infrastruktúrájába való aktív beavatkozás a rendvédelmi szervek részéről (például szerverfeltörés, exploitálás), amennyiben az jogsértő, és/vagy a nemzetközi jogot sértheti meg. Továbbá szigorúan tilos a személyes adatok gyűjtése, ha azok nem nyilvánosak, és nem az EU-ból származnak, valamint ha az adatkezelés érint EU-s állampolgárokat, de az adatokat harmadik országban tárolják, akkor az átadásra vonatkozó szabályokat is figyelembe kell venni (lásd Schrems II. ítélet – EU–USA adattovábbítás).

Jövőbeli kilátások – a harmadik országokkal kapcsolatos adatvédelmi trendek

A globális adatáramlás növekedésével a harmadik országokkal kapcsolatos adatvédelmi kihívások tovább fognak erősödni. Várható fejlemények:

– Nemzetközi adatvédelmi megállapodások. Az EU és egyes harmadik országok (például Japán, Dél-Korea) között már létrejöttek megfelelőségi határozatok. A jövőben egyre több ilyen megállapodás várható, bár ezek politikai feszültségek miatt is ingatagok lehetnek (például az USA-val kötött Privacy Shield érvénytelenítése után, Schrems II. ügy, 2020).
– Nagyobb adatkezelési transzparencia. Az EU jogalkotási célja, hogy az adatkezelőknek részletesebb tájékoztatást kelljen adniuk az adatátvitelről és annak kockázatairól.

– Fokozott felhasználói tudatosság. Egyre több kampány ösztönzi majd a felhasználókat arra, hogy figyeljenek a weboldalak származási országára és adatvédelmi gyakorlatára.
– Technológiai megoldások a földrajzi korlátozásra. A jövőben elterjedhetnek olyan technológiák, amelyek automatikusan figyelmeztetnek, ha egy weboldal nem biztonságos, vagy harmadik országba továbbít adatokat.

Összességében a nemzetközi adatáramlások biztonságosabbá tétele kulcsfontosságú lesz az internetes csalások megelőzésében.

A rendőrség akadályai és adatvédelmi aggályai a weboldalak monitorozása során

A rendőrségi szervek fontos szerepet játszanak az internetes csalások elleni küzdelemben, beleértve a gyanús weboldalak azonosítását és figyelését. Azonban az ilyen tevékenység során több jogi, technikai és etikai akadállyal is szembesülnek.

Az egyik aggály a jogi vagy jogszabályi korlátok, hiányosságok kérdése. A személyes adatokhoz való hozzáférés, a titkos adatgyűjtés, illetve a digitális kommunikáció megfigyelése szigorú jogi szabályokhoz kötött. A rendőrségnek minden esetben tiszteletben kell tartania az Alaptörvény és az Általános Adatvédelmi Rendelet (GDPR) által biztosított alapvető jogokat, különösen a magánélet védelmét és az információs önrendelkezést.

A GDPR előírja az adatminimalizálás elvét, amely szerint csak a szükséges mértékben és céllal lehet adatokat gyűjteni. A weboldalak tömeges, általános monitorozása sértheti ezt az alapelvet, különösen, ha nem egyedi gyanú alapján történik az adatkezelés.

Az átláthatóság és jogorvoslat lehetősége során a felhasználóknak alapvető joguk van arra, hogy tudják, ha adataikat gyűjtik vagy figyelik.

Kihívást jelentenek a technikai nehézségek, hiszen a weboldalak elérhetőségének gyors változása, az anonimitást biztosító technológiák (például a Tor hálózat), a hamis tanúsítványok használata és a titkosított adatforgalom komoly próbatételt jelent a megbízhatóság értékelésekor.

Etikai kérdések is felmerülnek, hiszen az általános „webfigyelés” során fennáll annak a veszélye, hogy más felhasználók adatai is a hatóságok látókörébe kerülnek, ami felvetheti a tömeges megfigyelés kritikáját és a polgári jogok sérelmének kockázatát.

Nem utolsósorban a nemzetközi joghatósági problémák is jelentkezhetnek, mivel sok hamis vagy csaló weboldal külföldi szervereken található, ami jelentősen megnehezíti a bizonyítékgyűjtést, a weboldalak leállítását, illetve a felelősök felelősségre vonását.

Bár a rendőrségi webmonitorozás elengedhetetlen az internetes csalások megelőzésében, ennek során szigorúan be kell tartani az adatvédelmi, jogi és etikai követelményeket. A megfelelő egyensúly megteremtése az eredményes bűnmegelőzés és a polgári szabadságjogok tiszteletben tartása között kulcsfontosságú.

A rendőrség lehetőségei az internetes csalások elleni fellépésben

Az internetes csalások megelőzése és felderítése érdekében a rendőrség többféle módszerrel és jogi eszközzel élhet, ugyanakkor minden esetben figyelembe kell vennie az adatvédelmi szabályokat és az arányosság elvét.

- *Nyílt forrású adatelemzés (OSINT).* A rendőrség nyilvánosan elérhető adatforrások (például weboldalak, közösségi média) elemzésével anélkül is gyűjthet információt, hogy személyes adatokhoz való közvetlen hozzáférést igényelne. Ez jogszerű és adatvédelmi szempontból kevésbé problémás.
- *Célzott adatgyűjtés bírói engedéllyel.* Amennyiben gyanú merül fel bűncselekmény elkövetésére, a rendőrség bírói engedély alapján jogosult lehet adatforgalom megfigyelésére, illetve adatok lefoglalására vagy rendszerek átvizsgálására (például elektronikus bizonyítékok rögzítése).
- *Együttműködés szolgáltatókkal.* Az internetes szolgáltatók, tárhelyszolgáltatók és domainregisztrátorok bevonásával a rendőrség kérheti weboldalak felfüggesztését, tartalom eltávolítását vagy forgalmi adatok kiadását, megfelelő jogi alap és eljárás megléte esetén.
- *Nemzetközi együttműködés.* Mivel az internetes csalások gyakran országhatárokon átnyúlók, a rendőrség nemzetközi hálózatokon (például Europol, Interpol) keresztül együttműködhet más államok hatóságaival információcsere és közös nyomozások céljából.
- *Technológiai eszközök alkalmazása.* A mesterséges intelligencia, gépi tanulás és hálózatelemző szoftverek használatával a rendőrség képes lehet automatizáltan felismerni a gyanús tevékenységeket, például csaló weboldalak mintázatait, de ezeknél is figyelni kell az adatkezelési jogszerűségre.

A rendőrség rendelkezik több jogszerű és arányos eszközzel az internetes csalásokkal szembeni fellépéshez, ugyanakkor az adatvédelmi szabályok betartása és az alapjogok tiszteletben tartása minden esetben elsődleges szempont marad. A jogszerű, célhoz kötött és átlátható adatkezelés biztosítja, hogy a rendőrségi fellépés nemcsak hatékony, hanem jogállami keretek között is marad.

Az adatvédelemmel kapcsolatos konklúzió

A jövőbeli kihívások között szerepel ugyanakkor a technológiai fejlődéssel párhuzamosan növekvő adatgyűjtés és megfigyelés kérdése is, ami új adatvédelmi dilemmákat vet fel (ENISA 2022).

Az internetes csalások elleni hatékony fellépés elengedhetetlen része az erős adatvédelmi gyakorlatok kialakítása. A jogi szabályozás, a technológiai fejlesztések és a felhasználók tudatosságának növelése együttesen képesek csökkenteni a kockázatokat. A jövőben elengedhetetlen, hogy a szervezetek és az egyének egyaránt proaktív módon közelítsenek az adatvédelem kérdéséhez, és folyamatosan alkalmazkodjanak az új fenyegetésekhez.

A bűnüldözési célú adatkezelésre azonban külön DPIA- (Data Protection Impact Assessment) követelmény vonatkozik, amit el lehet kerülni, ha nem történik személyes adatok kezelése (például kizárólag IP-nélküli, nem azonosítható metaadatokat használnak), illetve ha kizárólag statikus webtartalmat dolgoznak fel AI vagy emberi beavatkozás nélkül, és nincs lehetőség az érintettek azonosítására.

Az internetes csalások megelőzésének jövője az adatvédelmi technológiák és a jogszabályi környezet folyamatos fejlődésétől függ.

Várható, hogy:

- a mesterséges intelligencia (AI) még nagyobb szerepet kap az anomáliák észlelésében és a csalási minták automatikus felismerésében (Brenner 2023);
- a Zero Trust elv alkalmazása – amely minden hozzáférést folyamatosan ellenőriz – általánossá válik a vállalati és állami rendszerekben (Kindervag 2010);
- új, nemzetközi együttműködési mechanizmusok jönnek létre, amelyek célja a határokon átnyúló internetes csalások gyorsabb felderítése és szankcionálása;
- az adatvédelmi szabályozások, mint a GDPR, más régiókban is szigorodnak, például az Egyesült Államokban vagy Ázsiában;
- nagyobb hangsúlyt kap a fogyasztók adatvédelmi tudatosságának növelése és a *privacy by design* elv érvényesítése már a digitális termékek és szolgáltatások tervezési szakaszában.

Mivel a veszélyes vagy csaló weboldalak gyakran személyes adatokkal dolgoznak, és a megfigyelés célja is a személyek azonosítása lehet, így a DPIA szinte mindig szükséges.

Az internetbiztonság másik legfontosabb tényezője a felhasználók tudatossága. A tájékozott internethasználók képesek lehetnek felismerni a gyanús tevékenységeket, például a hamis e-maileket vagy a megtévesztő weboldalakat (Nemzeti Kibervédelmi Intézet 2023), de a kevésbé tudatos a felhasználók védelme érdekében szükséges lenne oktatási programok kidolgozása (akár gyermekkortól kezdve), kötelező biztonsági figyelmeztetések alkalmazása az internetes weboldalak esetében.

A tudatos internethasználat csökkentheti a csalások sikerességének esélyét, valamint erősítheti a digitális társadalom ellenálló képességét (Csiszár 2019).

Összegzés

A digitális térben zajló szervezett bűnözés és a kiberbűnözés elleni fellépés komplex, interdiszciplináris megközelítést igényel, amelyben a technológiai innovációk, a jogi szabályozás, a bűnüldözési gyakorlatok és a társadalmi tudatosság erősítése egyaránt kulcsszerepet játszanak. A szervezett bűnözés folyamatosan adaptálódik a társadalmi, gazdasági és technológiai változásokhoz, így a bűnözői csoportok a digitális környezetben is képesek új, decentralizált vagy éppen centralizált struktúrákat létrehozni, amelyek kihívást jelentenek a hatóságok számára a felderítésben és a prevencióban.

A kiberfenyegetések elleni védekezés hatékonysága nagymértékben függ a fejlett kockázatelemzési protokollok és mesterségesintelligencia-alapú rendszerek integrálásától, amelyek képesek valós idejű adatelemzésre és prediktív fenyegetés-előrejelzések küldésére.

Ugyanakkor a technológiai megoldások önmagukban nem szufficiensek: a jogi és etikai keretrendszerek, különösen az adatvédelem (például GDPR) szigorú betartása elengedhetetlen a felhasználói bizalom és a rendszer legitimációja szempontjából.

A reprezentatív adatgyűjtés, a sztochasztikus és rétegzett mintavételi technikák, valamint a felhasználói magatartás folyamatos monitorozása biztosítja, hogy a kockázatelemző rendszerek objektív és érvényes eredményeket szolgáltassanak, amelyek a teljes online populációra vonatkozóan is exportálhatókká válnak így. Az adatvédelmi kihívások, különösen a harmadik országokba történő adattovábbítás, továbbá a bűnüldöző szervek webmonitorozásának jogi és etikai korlátai, újabb dilemmákat generálnak, amelyek megoldása a nemzetközi együttműködés, a szabályozási harmonizáció és a technológiai fejlesztések összehangolt alkalmazásával érhető el.

Összességében a digitális bűnözés elleni hatékony fellépés kizárólag holisztikus módon, technológiai, jogi, szervezeti és a társadalmi tényezők integrált kezelésével valósítható meg, ahol a proaktív prevenció, a felhasználók tudatosságának növelése és a folyamatos adaptáció egyaránt nélkülözhetetlenek.

Felhasznált irodalom

Attar, Hooman (2011): The Scientific Approaches to Risk and Risk Management: A Critical Review. *Trends in Applied Sciences Research,* 6(4), 386–393. Online: https://doi.org/10.3923/tasr.2011.386.393

Barabás A. Tünde – Koplányi Gergely (2023): Viktimizáció az online térben. Egy nemzetközi kutatás eredményei hazai szemszögből. *Belügyi Szemle,* 71(10), 1697–1713. Online: https://doi.org/10.38146/BSZ.2023.10.1

Birch, Emily S. (2010): *Deindividuation in the Online Social Networking Context: What Situations Might Encourage Deindividuation on Facebook?* Albany Campus, Massey University, New Zealand. Online: https://mro.massey.ac.nz/bitstreams/b3c8914b-4962-45a8-833b-7d0ba7009d38/download

Browning, Matthew – Arrigo, Bruce (2021): Stop and Risk: Policing, Data, and the Digital Age of Discrimination. *American Journal of Criminal Justice,* 46(2), 298–316. Online: https://doi.org/10.1007/s12103-020-09557-x

Concha-Salgado, Andrés et al. (2022): Moral Disengagement as a Self-Regulatory Cognitive Process of Transgressions: Psychometric Evidence of the Bandura Scale in Chilean Adolescents. *International Journal of Environmental Research and Public Health,* 19(19), 12249. Online: https://doi.org/10.3390/ijerph191912249

Csiba István – Bodor Endre (1983): A szervezett jellegű bűnözés megnyilvánulásai a fővárosban. *Belügyi Szemle,* 21(9), 3–9.

Csiszár Csilla Margit (2019): Adatvédelem a digitális térben avagy mennyire vagyunk biztonságban. In Veresné Somosi Mariann – Lipták Katalin (szerk.): *„Mérleg és Kihívások" XI. Nemzetközi tudományos Konferencia.* Miskolc, Miskolci Egyetem Gazdaságtudományi Kar, 62–68.

Dános Valér (1988): A szervezett bűnözés és egyes elemeinek megjelenése a hazai bűnözésben. *Jogász Szövetségi Értekezések,* 11(1).

Dános Valér (1999): *Kriminológiai ismeretek.* Bűnözés bűnözéskontroll. Budapest: Rejtjel.

Kerezsi Klára (2001): *Bűnözés és társadalmi kontroll.* Budapest: Napvilág.

Kisfonai Bernadett (2023): A bűnügyek jövőbeli megelőzése, avagy a prediktív rendészet új arca. *Rendőrségi Tanulmányok,* 6(3), 58–73. Online: https://doi.org/10.53304/rt.2023.3.02

Kuner, Christopher (2013): *Transborder Data Flows and Data Privacy Law.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

McGuire, Michael (2012): *Organised Crime in the Digital Age.* London: John Grieve Centre for Policing and Security.

Megginson, Leon C. (1963): Lessons from Europe for American Business. *The Southwestern Social Science Quarterly,* 44(1), 3–13. Online: http://www.jstor.org/stable/42866937

Mezei Kitti (2019): *A kiberbűnözés egyes büntetőjogi szabályozási kérdései.* PhD-disszertáció. Pécsi Tudományegyetem. Online: https://pea.lib.pte.hu/handle/pea/23209

Patkós Csaba – Tóth Antal (2012): A bűnözés néhány térbeli jellemzője a rendszerváltás utáni Magyarországon. *Területi Statisztika,* 52(3), 250–263. Online: https://real.mtak.hu/id/eprint/194400

Simon Béla (2018): A kiberbűnözés aktuális trendjei. *Magyar Rendészet,* 18(1), 161–168. Online: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1390

Szabó A. (2008): Transznacionális bűnszervezetek a Kárpát-medencében. *Rendvédelem-tudomány,* 1(1), 63–77.

Voigt, Paul – von dem Bussche, Axel (2017): *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Springer. Online: https://doi.org/10.1007/978-3-319-57959-7

Vókó György (2004): A szervezett bűnözés elleni fellépés jogi lehetőségei és korlátai. *MTA Law Working Papers,* 2004/2.

Internetes források

BSR [é. n.]: *Bűnügyi Statisztikai Rendszer.* Online: https://bsr.bm.hu/Document

Day, Bratt – Holznienkemper, Lauren (2024): What Is a SWOT Analysis? *Forbes,* 2025. augusztus 28. Online: https://www.forbes.com/advisor/business/what-is-swot-analysis/

ENISA (2022): *Threat Landscape 2022.* European Union Agency for Cybersecurity. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Federal Bureau of Investigation (2023): *Internet Crime Report 2023.* Online: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

Fritsvold, Erik (2018): *Why Risk Management in Law Enforcement is More Essential Than Ever.* University of San Diego. Online: https://onlinedegrees.sandiego.edu/risk-management-in-law-enforcement/

HSI [é. n.]: *Risk Management in Industrial Environments: 7 Strategies for Prevention and Mitigation – HSI.* Online: https://hsi.com/blog/7-industrial-risk-management-strategies

Kindervag, John (2010): *Build Security Into Your Network's DNA: The Zero Trust Network Architecture.* Forrester Research. Online: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

Kwet, Michael (2021): ShadowDragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move. *Criminal Legal News,* 4(1), 1. Online: https://www.criminallegalnews.org/news/2021/nov/15/shadowdragon-inside-social-media-surveillance-software-can-watch-your-every-move/

LexisNexis (2022): *ThreatMetrix.* Online: https://risk.lexisnexis.co.uk/products/threatmetrix

Az MNB kezdeményezése a kiberbiztonságért (2022). Kiberpajzs.hu. Online: https://kiberpajzs.hu/a-kezdemenyezesrol

Mastercard (2025): *A kiberbűnözés kora 2025*. Online: https://kiberpajzs.hu/letoltes/a-kiberbuno-ze-s-kora-2025-o-sszefoglalo-kiberpajzs-0220fin-mnb.pdf

Nemzeti Kibervédelmi Intézet (2023): *Állítsuk meg a telefonhívásos csalásokat!* 2023. július. Online: https://nki.gov.hu/it-biztonsag/kiadvanyok/sans-ouch/allitsuk-meg-a-telefonhivasos-csalasokat-sans-ouch-2023-julius/

Risk Wizard Team (2024): *The Power of AI Risk Analysis: How It Could Benefit You*. Online: https://www.riskwizard.com/post/the-power-of-ai-risk-analysis-how-it-could-benefit-you

SafetyCulture Content Team (2025): Risk Analysis: A Comprehensive Guide. *SafetyCulture,* 2025. szeptember 17. Online: https://safetyculture.com/topics/risk-analysis/

Safety Educations (2024): *Hazard Identification and Risk Assessment HIRA: A Comprehensive Guide. Safety Education*. Online: https://safetyeducations.com/hazard-identification-and-risk-assessment/

Scism, Rex M. (2017): Risk Management for Law Enforcement. *Police Magazine,* 2017. augusztus 7. Online: https://www.policemag.com/patrol/article/15346469/risk-management-for-law-enforcement

ShadowDragon [é. n.]: *Social Net: Social Media Investigation Tool*. Online: https://shadowdragon.io/socialnet/

Jogi forrás

Európai Parlament és Tanács (2016): Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet, GDPR). Online: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=HU