https://doi.org/10.66102/BSZ.2025.4.8

Szalai Kitti Katalin

# „Okosbörtönök" és „okosbűnözés" – A digitalizáció biztonsági árnyoldalai

## *'Smart prisons' and 'smart crime' – The dark side of digitalization*



A tanulmány a büntetés-végrehajtási szervezet digitalizációjának kevésbé látható oldalát vizsgálja: azt, hogy az „okosbörtönök" miként válhatnak egyszerre a biztonság eszközévé és új kockázatok forrásává.

A digitális transzformáció – elektronikus felügyelet, digitális egészségügyi rendszerek, mesterséges intelligencián alapuló megoldások – hatékonyabb kontrollt ígér, ugyanakkor olyan támadási felületeket hoz létre, amelyek megkérdőjelezik a hagyományos felügyeleti logikát. A tanulmány hazai és nemzetközi példákon keresztül mutatja be a kibervédelmi kockázatokat, a tiltott kapcsolattartás új formáit, a szabadulás után visszaesők és családi kapcsolatok szerepét, valamint a kódolt üzenetváltások jelentette fenyegetéseket.

A tanulmány arra a következtetésre jut, hogy a büntetés-végrehajtás jövője nem technológiai verseny, hanem tudatos egyensúlykeresés a biztonság és a kockázatok között.

**Kulcsszavak:** okosbörtönök, digitális felügyelet, kiberbiztonsági kockázatok, tiltott kapcsolattartás, intézményi sebezhetőség

*This study examines the less visible side of the digitalization of the prison system: how 'smart prisons' can become both a tool for security and a source of new risks.*

*Digital transformation – electronic surveillance, digital health systems, artificial intelligence-based solutions – promises more effective control, but at the same time creates attack surfaces that challenge traditional surveillance logic. The study uses domestic and international examples to illustrate cyber security risks, new forms of prohibited communication, the role of recidivism and family relationships after release, and the threats posed by encrypted messaging.*

*The study concludes that the future of the prison service is not a technological race, but a conscious search for balance between security and risk.*

***Keywords:*** *smart prisons, digital surveillance, cybersecurity risks, prohibited communication, institutional vulnerability*

## Bevezetés

A büntetés-végrehajtási szervezetben (a továbbiakban: bv. szervezet) zajló modernizáció első pillantásra a hatékonyság és a biztonság ígéretét hordozza. Az „okosbörtönök" megjelenése, a digitális egészségügyi nyilvántartások és az algoritmusokkal támogatott kockázatelemzés mind azt mutatják, hogy a műszaki megoldások hatékonyabb működést, költségcsökkentést és magasabb szintű biztonságot ígérnek.

Ugyanakkor minden fejlődés magában hordozza a biztonsági kockázatok növekedését. A digitalizált rendszerek sebezhetősége, az adatbiztonsági problémák, valamint a szabaduló fogvatartottak digitális eszközhasználata komoly biztonsági kérdéseket vet fel. Ezen eszközök újításai így egyszerre jelenthetnek lehetőséget a reintegrációra és a felügyelet megerősítésére, ugyanakkor új formákat adhatnak az „okosbűnözésnek" is. Ez a kettősség – a modernizáció előnyei és a potenciális árnyoldalai – alapjaiban határozza meg a büntetés-végrehajtás jövőjét. Bár Magyarországon a bv. intézetekben a mesterséges intelligencia jelenleg még csupán tesztelési fázisban van jelen, már ebben a korlátozott formájában is ráirányítja a figyelmet az informatikai modernizáció árnyoldalaira és az új típusú biztonsági kockázatokra.

A tanulmány célja, hogy bemutassa e kettősséget: miként alakítja át a digitális transzformáció a magyar bv. szervezetet, és milyen biztonsági árnyoldalakkal kell szembenézni a 21. századi börtönök korában.

## A magyar bv. szervezet technológiai állapota

Az elmúlt években a magyar büntetés-végrehajtásban is megkezdődött az informatikai fejlesztések fokozatos térnyerése. Ennek egyik leglátványosabb példája a csengeri „okosbörtön", amely Közép-Európa legmodernebb börtönei közé tartozik, és fejlett videóanalitikai, helymeghatározó és elektronikus felügyeleti rendszereket alkalmaz.

Az egészségügyi ellátás területén a FEDRA rendszer és a telemedicina bevezetése jelent előrelépést, amely lehetővé teszi az adatok digitális kezelését, valamint egyes szakellátások távoli biztosítását. Ez hozzájárul a humánerőforrás-hiány mérsékléséhez és az ellátás minőségének javításához.

### *Védelmi intézkedések és jogszabályi garanciák a büntetés-végrehajtás digitalizációjában*

A büntetés-végrehajtás digitalizációs folyamata nem védelmi mechanizmusok nélkül valósul meg. A digitális rendszerek bevezetését szigorú jogszabályi keretek, adatvédelmi

előírások és informatikai biztonsági protokollok kísérik, amelyek célja a személyes adatok védelme és a rendszerek integritásának biztosítása. A hazai szabályozás összhangban áll az európai adatvédelmi elvekkel, különös tekintettel az érzékeny egészségügyi és büntetés-végrehajtási adatok kezelésére.

A büntetés-végrehajtási szervezet technikai szinten is törekszik a digitális kockázatok mérséklésére. Ide tartoznak a hozzáférés-szabályozási rendszerek, a többszintű azonosítás, a hálózati védelmi megoldások, valamint a rendszeres informatikai auditok és biztonsági frissítések. A kommunikációs csatornák felügyelete és az adatforgalom monitorozása szintén a visszaélések megelőzését szolgálja.



E védelmi intézkedések célja nem csupán a külső kibertámadások kivédése, hanem a bv. szervezeten belül lehetséges visszaélések megakadályozása is. A digitalizáció tehát nem önmagában növeli a kockázatokat, hanem megfelelő szabályozás és felügyelet mellett a biztonság megerősítésének eszköze is lehet.

Mindazonáltal a technológiai fejlődés gyors üteme folyamatos alkalmazkodást igényel a bv. szervezet részéről. A kockázatok és a védelmi megoldások közötti egyensúly fenntartása hosszú távon kulcsfontosságú ahhoz, hogy a digitális innováció valóban a biztonságot és a reintegrációt szolgálja.

***A digitális rendszerek előnyei a büntetés-végrehajtásban***

A büntetés-végrehajtási intézetek korszerű megoldásai számos területen hozhatnak kézzelfogható előnyöket. A modern informatikai rendszerek bevezetése lehetővé teszi a nyilvántartások pontosabb vezetését és az adminisztráció gyorsabb lebonyolítását, ezáltal csökkentve a hibalehetőségeket és az erőforrásigényt. Az automatizált folyamatok hosszú távon költségcsökkentést eredményeznek, miközben hatékonyabbá teszik az intézetek működését.

A biztonság területén a videóanalitikai rendszerek, az elektronikus nyomkövető eszközök és a helymeghatározó rendszerek új szintet képviselnek a felügyeletben. Ezek révén a fogvatartottak mozgása pontosabban nyomon követhető, a rendkívüli események pedig gyorsabban észlelhetők.

Az egészségügyi ellátásban a telemedicina és a digitális adatkezelés elősegíti a minőségi betegellátást, és mérsékli a humánerőforrás-hiányból adódó problémákat.

A digitalizáció a reintegráció szempontjából is előnyökkel járhat: az e-learning és más online képzési lehetőségek hozzájárulhatnak a fogvatartottak munkaerőpiaci esélyeinek javításához a szabadulás után.

Összességében a digitalizáció olyan eszköz, amely – megfelelő alkalmazás esetén – a hatékonyság, a költségtakarékosság, a biztonság és a reintegráció területén egyaránt képes erősíteni a büntetés-végrehajtás rendszerét.

## Kibervédelmi sebezhetőségek

A bv. szervezet digitális rendszerei – mint a kamerahálózatok, beléptetőrendszerek vagy az egészségügyi adatbázisok – új célpontot jelentenek a kibertámadások számára. Egy sikeres támadás adatlopáshoz, vagy a biztonsági rendszerek megbénításához is vezethet.

Mindez rávilágít arra, hogy az online rendszerek elterjedésével párhuzamosan elengedhetetlen a hálózati biztonság és az adatvédelem megerősítése, különben a modernizáció könnyen saját gyengeségévé válhat.

Ezt nemzetközi példák is bizonyítják:

- 2024 novemberében megszűnt a nyomkövetés és a vészhívó működése a brit fogvatartotti szállító járműveken. Egy telematikai szolgáltató, a Microlise elleni kibertámadás miatt a Serco (nemzetközi informatikai szolgáltató vállalat) által működtetett furgonok GPS és riasztórendszerei leálltak. Az eset egyedi és nem bizonyított, hogy a támadók ezt kihasználták volna.
- Angliában és Walesben bv. intézetek alaprajzai szivárogtak ki. Részletes börtön alaprajzok kerültek fel a dark webre, komoly biztonsági kockázatot jelentve az intézetek védelme szempontjából.
- Egy másik esetnél több mint 320 GB érzékeny adat szivárgott ki az amerikai Szövetségi Börtönigazgatóságtól. Hackerek hatalmas mennyiségű fogvatartotti és személyi állományi adatot hoztak nyilvánosságra.

Hazai példák:

- A BVOP toborzóoldala elleni adathalász-támadás: A Büntetés-végrehajtás Országos Parancsnoksága honlapját (gyereahuvosre.hu) adathalász támadás érte, onnan egy hamisított adathalász oldalra irányították át a látogatókat. A rendszert helyreállították, és feljelentést tettek az ügyben.[1]

1 HVG.hu (2021)

## Tiltott kapcsolattartás és a szabadulás után visszaesők szerepe

A digitális kommunikációs csatornák térnyerésével a büntetés-végrehajtás egyik legérzékenyebb kockázati területévé vált a tiltott kapcsolattartás a külvilág és a bv. intézeten belül tartózkodó fogvatartottak között. Különösen magas kockázatot jelentenek azok a szabadult fogvatartottak, akik korábbi bűnözői hálózataikat megőrizve újabb bűncselekmények elkövetésében vesznek részt, és digitális eszközök segítségével tartják fenn kapcsolataikat a bent maradt társaikkal. A tiltott mobiltelefonok és titkosított üzenetküldők mellett ma már a digitális innovációk is új lehetőségeket teremtenek az illegális kommunikáció számára. Különös kockázatot jelentenek a dokumentumgeneráló programok, vagyis olyan digitális alkalmazások, amelyek előre beállított sablonok és mesterséges intelligencia segítségével képesek hivatalosnak tűnő leveleket, nyilatkozatokat és iratokat automatikusan előállítani és személyre szabni. E technológiák révén hitelesnek látszó, ám valójában hamis ügyvédi, egyházi vagy egyéb dokumentumok készíthetők, amelyekkel kijátszhatók az ellenőrzési mechanizmusok. A levelezés így különösen kockázatossá válhat, mivel a külvilágban lévő bűntársak digitális eszközök segítségével képesek hivatalosnak vagy családi kapcsolattartásnak tűnő üzeneteket generálni. Ezek a valósághű tartalmak mesterséges intelligenciával előállított szövegeket, stilizált levélformátumokat és hitelesnek tűnő megszólításokat tartalmazhatnak, amelyek papíralapú vagy elektronikus úton jutnak el a fogvatartotthoz. A digitális eszközök lehetővé teszik az üzenetek gyors szerkesztését, sokszorosítását és személyre szabását, ami jelentősen megnehezíti azok valódiságának felismerését a felügyelet számára.

Az AI-alapú rendszerek deepfake technológiával képesek a fogvatartott családtagjainak vagy közeli hozzátartozóinak hangját lemásolni, amelyet bűntársak alkalmazhatnak telefonos vagy digitális kapcsolattartás során a felügyelet megtévesztése és bűnszervezeti tevékenységek koordinálása céljából. Emellett chatbot-szerű megoldások lehetővé teszik, hogy egy bűntárs a külvilágból folyamatosan a fogvatartottal kommunikáljon, miközben hozzátartozónak adja ki magát, ezzel fenntartva az illegális információáramlást és koordinálva a bűnözői tevékenységet és „hiteles" üzenetváltásokban tartson fenn kapcsolatot a fogvatartottal. A családtagok a digitális kommunikációs platformokon keresztül különösen hatékony fedőcsatornát biztosíthatnak az üzenetek továbbítására. Míg a papíralapú levelezés és a hagyományos telefonhívások esetében az információcsere lassabb és korlátozottabb volt, addig az online hívások és digitális kapcsolattartás folyamatos, gyors és nehezebben nyomon követhető kommunikációt tesz lehetővé. Ezek a csatornák első pillantásra ártalmatlannak tűnnek, ugyanakkor alkalmasak kódolt tartalmak rendszeres közvetítésére, ami jelentősen megnehezíti a felügyelet munkáját.

A kódnyelv alkalmazása mindig is jelen volt a bűnözői kommunikációban, azonban a digitális kommunikáció térnyerésével új dimenzióba lépett. Míg a hagyományos

levelezés és telefonbeszélgetések esetében a kódolt üzenetek terjedelme és gyakorisága korlátozott volt, a modern digitális csatornák lehetővé teszik a folyamatos, gyors és nagy mennyiségű információcserét. Az üzenetek könnyen módosíthatók, törölhetők és továbbíthatók, ami megnehezíti azok nyomon követését és értelmezését. Emellett a digitális platformok vizuális elemei – emojik, rövidítések, képek vagy előre egyeztetett kifejezések – tovább bővítik a kódolás lehetőségeit, így a kommunikáció a felügyelet számára egyre kevésbé válik átláthatóvá. Előre megbeszélt kifejezések, szimbólumok, látszólag jelentéktelen utalások rejthetnek bűnszervezeti utasításokat, amelyeket a felügyelet nehezen tud értelmezni. Ha ez a kódnyelv elterjed a fogvatartottak között, intézményeken belül is bűnszervezeti hálózatok alakulhatnak ki, amelyeket a digitális műszaki rendszer tart össze és tesz még nehezebben feltérképezhetővé.

## *Miért reális ez a kockázat?*

Az eszközpark elsősorban a civil környezetben hozzáférhető. A deepfake hangklónozás, a szöveggenerálás és a chatbot-alapú kommunikáció ma már bárki számára könnyen használható, speciális informatikai tudás nélkül. Bár a fogvatartottak digitális eszközhasználata korlátozott, a kockázatot éppen az jelenti, hogy a szabadult fogvatartottak, bűntársak vagy családtagok ezeket a technológiákat a külvilágban alkalmazva képesek megtévesztő tartalmakat előállítani, amelyek a kapcsolattartási csatornákon keresztül jutnak el az intézményen belülre. Így a digitális visszaélések nem közvetlen eszközhasználaton, hanem közvetített kommunikáción keresztül jelennek meg a büntetés-végrehajtás rendszerében. Dokumentált esetek vannak AI-generált hamis dokumentumokról, családtagok hangját utánzó telefonos csalásokról és pénzügyi tranzakciók manipulálásáról. A bv. intézeten belüli kommunikáció sajátos sérülékenysége, hogy a felügyelet a fogvatartottak kapcsolattartásának ellenőrzése során kiemelten támaszkodik az úgynevezett „védett" kommunikációs csatornákra, mint a családtagokkal folytatott levelezés és telefonhívások, valamint az ügyvédekkel és egyházi személyekkel történő kapcsolattartás. Ezek a csatornák jogszabályi és adatvédelmi garanciák miatt részben vagy teljes egészében mentesülnek a tartalmi ellenőrzés alól, mivel céljuk a magánélet védelme és a jogi képviselet biztosítása. A felügyeleti rendszer elsősorban formai kontrollt tud alkalmazni – azonosításra, időkeretekre és jogosultságokra koncentrál –, miközben a kommunikáció tényleges tartalma nem vizsgálható. Éppen ez a védettség teszi e csatornákat különösen sérülékennyé a visszaélésekkel szemben. Így, ha ezeket digitális eszközökkel meghamisítják, a rendszer szinte védtelen. A visszaesők motivációja és hálózatai abban ragadhatók meg leginkább, hogy a szabadult fogvatartottak sokszor megtartják kapcsolataikat a bent maradt társaikkal, amelyeket digitális eszközök révén nemcsak fenntartani, hanem tudatosan erősíteni is képesek a bűnszervezeti működés érdekében.

## Az egészségügyi rendszerek sérülékenysége

A büntetés-végrehajtási intézetekben a digitális fejlődés iránya az egészségügyi ellátásban is megjelent: Magyarországon a FEDRA rendszer és a telemedicina lehetővé teszi a fogvatartottak egészségügyi adatainak elektronikus kezelését, valamint a távoli szakellátás biztosítását. Bár ezek a fejlesztések javítják az ellátás minőségét és hatékonyságát, egyben új biztonsági kockázatokat is teremtenek.

Az egészségügyi rendszerekben tárolt adatok rendkívül érzékenyek: személyes, és egészségügyi információk, amelyek kezelése különös körültekintést igényel.

További kockázatot jelent, hogy a telemedicina során alkalmazott eszközök és kommunikációs csatornák – ha nem megfelelően védettek – külső behatolók számára is hozzáférhetővé tehetik a konzultációkat vagy a diagnosztikai eredményeket.

Az egészségügyi digitális átalakulás tehát kétélű fegyver: miközben elősegíti a korszerű ellátást, olyan sérülékeny elemeket is bevezet a büntetés-végrehajtás rendszerébe, amelyek célzott támadás esetén az egyik leggyengébb láncszemmé válhatnak.

A külföldi tapasztalatok azt bizonyítják, hogy a bv. szervezetek világszerte ki vannak téve a kiberfenyegetéseknek:

- Írországban 2021. május 4-én az ír egészségügyi szolgálatot (HSE) ransomware támadás érte: rendszereit a Conti nevű zsarolóvírus bénította meg. Az ország kórházai és rendelői hetekre működésképtelenné váltak, több mint 520 beteg személyes és egészségügyi adatai kerültek nyilvánosságra.[2]

Hazai példák:

- Magyar orvosi rendelők és egészségügyi szolgáltatók is célponttá váltak a kibertámadások során. Az ilyen incidensek következtében megbénulhatnak az időpontfoglaló és betegnyilvántartó rendszerek, ellehetetlenülhet a laboreredményekhez és gyógyszerfelírásokhoz való hozzáférés, valamint megszakadhat az ellátás digitális koordinációja. Egy rendszerleállás során az orvosok kénytelenek papíralapú működésre visszatérni, ami késedelmekhez, adatvesztéshez és a betegbiztonság csökkenéséhez vezethet. Súlyosabb esetekben az életmentő beavatkozásokhoz szükséges információk elérhetetlenné válása akár közvetlen életveszélyt is jelenthet.[3]

2 BBC (2021)
3 Pénzcentrum (2025)

- Az egészségügyi adatfájlok értéke felértékelődött. A dark weben egyetlen egészségügyi adatfájl értéke ma már akár kétmillió forintra is rúghat, ami tovább erősíti, hogy a bv. szervezet egészségügyi rendszereinek védelme nemcsak etikai, hanem nemzetbiztonsági érdek is.[4]
- 2025 augusztusában országszerte elérhetetlenné vált az EESZT, ami miatt a patikák nem tudták kiadni a korábban felírt gyógyszereket, és az orvosok sem fértek hozzá a betegek adataihoz. A leállás nem szoftveres hiba, hanem hardver-meghibásodás következménye volt, amit a NISZ szakemberei próbáltak elhárítani. Így átmenetileg megrendült a hazai egészségügyi rendszer működése, és a gyógyszerkiváltás is csak papír alapú megoldásokkal volt ideiglenesen biztosítható.[5]

### *Miért releváns ez a büntetés-végrehajtás számára?*

Magyarországon is dokumentáltak már zsarolóvírusos támadásokat egészségügyi intézményekkel szemben, a COVID-19-időszakban ugrásszerűen nőtt az ilyen incidensek száma, amelyek közvetlenül veszélyeztették a betegellátás folyamatosságát. Emellett egyre több támadás éri a rendelőket, ahol bármilyen működészavar akár az életveszélyesség határát súrolhatja.

Mivel a magyar büntetés-végrehajtás egészségügyi rendszerei (például FEDRA) is közvetlenül kapcsolódnak az országos EESZT-hez, az ott bekövetkező incidensek érinthetik a fogvatartottak ellátását. Ez rámutat arra, hogy a bv. szervezet egészségügyi digitalizációja nem izolált, hanem országos sebezhetőségekhez kötődik.

## A felügyelet paradoxona

Az IT-innovációk egyik fő ígérete a bv. szervezetben a szorosabb és pontosabb felügyelet: a kamerarendszerek, az elektronikus nyomkövetők, a telefonhívások rögzítése vagy a digitális levelezés mind azt a célt szolgálják, hogy a fogvatartottak ellenőrzése hatékonyabb legyen. Paradox módon azonban éppen ezek a megfigyelési formák is teremthetnek új visszaélési lehetőségeket.

### *Lehetséges visszaélések*

Az alábbi példák egyaránt bemutatják a hagyományos és a digitális környezetben megjelenő visszaélések formáit, szemléltetve, hogy a technológiai fejlődés miként erősíti fel a korábban is létező kockázatokat.

4 Telex.hu (2025)
5 Portfolio.hu (2025)

### *Kódolt kommunikáció*

A digitálisan rögzített kommunikáció önmagában nem garantálja az ellenőrizhetőséget, mivel a kódolt kifejezések alkalmazása az üzenetek jelentését a felügyeleti rendszerek számára értelmezhetetlenné teheti.

A nemzetközi esetek rávilágítanak arra, hogy a börtönök digitális infrastruktúrája globálisan is sebezhető:

- Olaszországban a tévéműsorok élő szövegsávjában küldött SMS-eket a maffia „titkos üzenetként" használta a fogvatartásban lévő vezetőiknek.[6]
- Közép-Amerikában (Honduras) a fogvatartottak kézzel írt „titkos ábécék" segítségével továbbítottak kódolt utasításokat külső bűntársaik felé, amelyeket csak a beavatottak tudtak visszafejteni. Ez az analóg példa jól szemlélteti a kódolt kommunikáció régóta fennálló gyakorlatát, amely a digitális csatornák segítségével jelentősen felgyorsult és hatékonyabbá vált, hiszen az üzenetek ma már gyorsan terjeszthetők, sokszorosíthatók és nehezebben nyomon követhetők.[7]
- Szicília esetében Bernardo Provenzano maffiavezér úgynevezett pizzinók, vagyis apró papírdarabokra írt kódolt üzenetek segítségével tartotta fenn a kapcsolatot a bűnszervezet tagjaival. Ez az analóg kommunikációs forma bemutatja, hogy a rejtett információátadás már a digitális korszak előtt is központi szerepet játszott a szervezett bűnözésben. A digitális technológiák megjelenésével azonban ezek a kódolt üzenetküldési módszerek gyorsabbá, szélesebb körben terjeszthetővé és nehezebben ellenőrizhetővé váltak, ami növelheti a büntetés-végrehajtás kockázati tényezőit.[8]

### *A felügyelet információs túlterheltsége*

Bár a szabályozás a kommunikációs csatornák esetében valós idejű ellenőrzést, illetve a levelezésnél a kézbesítést megelőző kontrollt ír elő, az adatok és kommunikációs tartalmak nagy mennyisége gyakran korlátozza a mélyreható elemzést. Ennek következtében számos esetben csak utólagos értékelésre nyílik lehetőség, ami csökkentheti a megelőző beavatkozás hatékonyságát. Ez lehetőséget ad a fogvatartottaknak rövid idejű, de súlyos visszaélésekre. Bár a szabályozás a kommunikációs csatornák esetében valós idejű ellenőrzést, illetve a levelezésnél a kézbesítést megelőző kontrollt ír elő, ám előfordulhat, hogy a hívások, üzenetek, levelek és digitális kommunikációs tartalmak nagy mennyisége korlátozza a részletes tartalmi elemzés lehetőségét.

6 The Telegraph (2010)
7 Vice.com (2014)
8 Wikipedia (2006)

Ez időbeli késedelmet eredményezhet olyan visszaélések esetében, mint tiltott tárgyak becsempészésének megszervezése, kábítószer-kereskedelem koordinálása vagy bűncselekmények előkészítése a külvilágban. A rövid idő alatt lebonyolított, kódolt üzenetváltások így lehetőséget adhatnak különböző jogsértésekre még azelőtt, hogy azok felismerésre kerülnének.

Az elektronikus nyomkövető rendszerek túlterheltsége és a riasztások pontatlan kezelése biztonsági kockázatot jelenthet. Egy Los Angeles megyei esetben a rendszer olyan nagy mennyiségben generált – gyakran téves vagy jelentéktelen – riasztásokat, hogy a felügyelők nem tudták időben kiszűrni a valódi veszélyhelyzeteket. Ennek következtében több felügyelet alatt álló személy hosszabb időre eltűnt a hatóságok látóköréből, miközben a rendszer formálisan működőképes maradt.[9]

***Családtagok és hozzátartozók szerepe***

A digitális kommunikáció révén a családtagok – akár tudatosan, akár bűntárs által felhasználva – közvetítőkké válhatnak.

Például egy atlantai börtönben egy elkobzott levél első látásra egy családtagnak íródott, valójában azonban kódolt üzenet rejtőzött benne: a fogvatartott így adott parancsot egy bűntárs likvidálására. A titkosítás úgy működött, hogy minden ötödik szó egyetlen utasítást alkotott, amit csak kriptoelemzéssel lehetett megfejteni. A kódolt üzenetek hagyományos, papíralapú levelezés útján jutottak el a fogvatartottakhoz, ahol a szöveg látszólag hétköznapi mondatokból állt. A titkosítás lényege az volt, hogy minden ötödik szó külön utasítást alkotott, amelynek rejtett jelentését csak a hatóságok utólagos kriptoanalitikai vizsgálata tárta fel. Ez erőteljesen mutatja, hogy a felügyelők által ártalmatlannak tartott levelek is lehetnek rejtett biztonsági fenyegetést hordozók.[10]

***Összegzés***

A felügyelet paradoxona abban rejlik, hogy minél több digitális ellenőrzést vezet be a bv. szervezet, annál kifinomultabb módszerekkel próbálják kijátszani azt a fogvatartottak. Így az automatizált megoldás egyszerre növeli a biztonságot és hozza létre az új típusú fenyegetéseket.

9 Los Angeles Times (2014)
10 yahoo!finance (2018)

## Zárógondolatok

A büntetés-végrehajtásban a digitális infrastruktúra-fejlesztés egyszerre kínál korszerű megoldásokat és hordoz magában biztonsági kockázatokat. Az okosbörtönök, az elektronikus nyomkövető eszközök, a digitális egészségügyi rendszerek és a mesterséges intelligencián alapuló elemzések a hatékonyság és a biztonság új szintjét ígérik.

Ugyanakkor a „felügyelet paradoxona" rámutat: minél fejlettebb a kontroll, annál leleményesebb módszerekkel próbálják kijátszani azt a fogvatartottak és esetleges bűntársaik.

Hazai és nemzetközi példák egyaránt bizonyítják, hogy a digitalizált rendszerek sebezhetősége valós: kibertámadások bénították meg különböző intézményi rendszerek működését, hagyományos papíralapú levelezésben kódolt üzenetek jutottak át a felügyeleten. Mindez világosan mutatja, hogy a korszerű műszaki megoldások nemcsak a rend fenntartásának, hanem a visszaéléseknek is új eszköztárat teremthetnek. A jövő bv. szervezetének legnagyobb feladata tehát az egyensúly megtalálása: a digitális fejlesztések akkor válhatnak valóban a biztonság és a reintegráció eszközévé, ha az előnyök mellett a kockázatokat is figyelembe vesszük.

Mert végső soron az „okosbörtönök" jövője nem a technológián múlik, hanem azon, mennyire tudunk éberek maradni a kockázataikkal szemben.

# Felhasznált irodalom


BBC (2021): Cyber attack ‚most significant on Irish state'. Online: https://www.bbc.com/news/world-europe-57111615 (Letöltés ideje: 2025. augusztus 21.)

BBC News (2024): Prison layouts reportedly leaked on dark web. Online: https://www.bbc.com/news/articles/ce8y5jm4lyzo (Letöltés ideje: 2025. augusztus 21.)

HVG.hu (2021): Támadás érte a büntetés-végrehajtás toborzó oldalát, adathalász oldalt csináltak belőle. Online: https://hvg.hu/tudomany/20210517_bvop_buntetes_vegrehajtas_adathalasz_oldal_kibertamadas (Letöltés ideje: 2025. augusztus 21.)

Los Angeles Times (2014): Probation officials concede failures in GPS tracking of felons. Online: https://www.latimes.com/local/la-me-electronic-monitors-20140226-story.html (Letöltés ideje: 2025. augusztus 18.)

MSN News (2024): Cyber attack disables prison vans panic alarms. Online: https://www.msn.com/en-us/news/world/cyber-attack-disables-prison-vans-panic-alarms/ar-AA1tD6hS (Letöltés ideje: 2025. augusztus 18.)

Pénzcentrum (2025): Orvosi rendelőkben portyáznak a kiberbűnözők: nyomtalanul fosztják ki a magyar betegeket. Online: https://www.penzcentrum.hu/egeszseg/20250806/orvosi-rendelokben-portyaznak-a-kiberbunozok-nyomtalanul-fosztjak-ki-a-magyar-betegeket-1183089 (Letöltés ideje: 2025. augusztus 18.)

Portfolio.hu (2025): EESZT-leállás: megszólalt az államtitkár az egészségügyet sújtó rendszerkrízisről. Online: https://www.portfolio.hu/gazdasag/20250809/eeszt-leallas-megszolalt-az-allamtitkar-az-egeszsegugyet-sujto-rendszerkrizisrol-779161 (Letöltés ideje: 2025. augusztus 21.)

SC World (2025): Federal Bureau of Prisons purportedly compromised. Online: https://www.scworld.com/brief/federal-bureau-of-prisons-purportedly-compromised (Letöltés ideje: 2025. augusztus 19.)

Telex.hu (2025): Kétmillió forintot is érhet egy ember egyetlen egészségügyi adatfájlja a sötét weben. Online: https://telex.hu/techtud/2025/07/04/egeszsegugyi-adatok-kiberbiztonsag-hekkerek-hunren-sztaki (Letöltés ideje: 2025. augusztus 19.)

The Telegraph (2010): Mafia using football show to send messages to jailed bosses. Online: https://www.telegraph.co.uk/news/worldnews/europe/italy/7958800/Mafia-using-football-show-to-send-messages-to-jailed-bosses.html (Letöltés ideje: 2025. augusztus 19.)

Vice.com (2014): The Secret Codes That Cartel Bosses Use to Send Handwritten Orders from Prison. Online: https://www.vice.com/en/article/the-secret-codes-that-cartels-use-to-send-orders-from-prison/ (Letöltés ideje: 2025. augusztus 21.)

Wikipedia (2006): Pizzino. Online: https://en.wikipedia.org/wiki/Pizzino (Letöltés ideje: 2025. augusztus 19.)

yahoo!finance (2018): An Atlanta jail intercepted a letter from an inmate who was using a secret code to orchestrate a murder. Online: https://finance.yahoo.com/news/atlanta-jail-intercepted-letter-inmate-151500503.html (Letöltés ideje: 2025. augusztus 19.)