HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 131–142.
DOI: 10.32567/hm.2024.4.9

Kreitz Zsuzsanna[1]

A chain of custody digitalizálásának lehetőségei

Opportunities for the Digitalisation of the Chain of Custody

Absztrakt

A chain of custody (CoC) – a bizonyítékok nyomonkövethetőségének láncolata – folyamata elengedhetetlen a kriminalisztikai tárgyi bizonyítékok kezelésében, biztosítva, hogy a bizonyítékok eredete, integritása és kezelése mindvégig nyomon követhető és hiteles maradjon. A digitalizáció gyors fejlődése új lehetőségeket kínál arra, hogy a hagyományosan papíralapú, manuálisan vezetett CoC-folyamatok hatékonyabbá és megbízhatóbbá váljanak. A digitális megoldások – mint például a blokklánc-technológia, rádiófrekvenciás azonosító (RFID) chipek és intelligens szerződések – jelentősen növelhetik a bizonyítékkezelési folyamatok átláthatóságát és megbízhatóságát, miközben csökkenthetik az emberi hibákból, csalásokból vagy mulasztásokból eredő kockázatokat. Jelen tanulmány célja a CoC digitalizálásának lehetőségeit feltárni, különös tekintettel a jogi, technológiai és adatbiztonsági szempontokra. A tanulmány kitér továbbá a digitális CoC megvalósításának kihívásaira is, úgymint a személyes adatok védelmére vonatkozó előírások (GDPR) betartása és a meglévő rendszerekkel való integráció problémái. Összességében a digitális CoC-megoldások jelentős előrelépést hozhatnak a bizonyítékkezelés pontosságában és gyorsaságában, de bevezetésük alapos jogi és technológiai elemzést, valamint előkészítést igényel.

Kulcsszavak: chain of custody, blokklánc, RFID, bizonyíték, digitális bizonyíték

Abstract

The chain of custody (CoC) process is essential in the management of forensic evidence, ensuring that the origin, integrity, and handling of evidence can be continuously traced and authenticated. Rapid advances in digitalisation offer opportunities to make traditionally

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Doktori Iskola, e-mail: kreitzzsu@gmail.com

paper-based and manually managed CoC processes more efficient and reliable. The use of digital solutions – such as blockchain technology, RFID chips, and smart contracts – can significantly increase the transparency and reliability of evidence handling, while reducing the risks arising from human error, fraud, or negligence. The aim of this paper is to explore the possibilities for CoC digitisation, with a focus on legal, technological, and data security aspects. The paper also addresses the challenges of implementing a digital CoC, such as compliance with personal data protection regulations and the integration of new systems with existing processes. Overall, digital chain-of-custody solutions can bring significant improvements in the accuracy and speed of evidence management, but their implementation requires thorough legal and technological analysis and preparation.

Keywords: chain of custody, blockchain, RFID, forensic evidence, digital evidence

Bevezetés

A bizonyítékok nyomonkövethetőségének folyamata – az úgynevezett *chain of custody,* azaz CoC – alapvető fontosságú a büntetőeljárásokban és kriminalisztikai nyomozásokban. A CoC biztosítja, hogy a bűnjelként szolgáló tárgyi vagy digitális bizonyítékok eredete, épsége és kezelése minden pillanatban ellenőrizhető legyen, így a bizonyíték hitelessége a bírósági eljárásban nem kérdőjelezhető meg. A hagyományos gyakorlatban a bizonyítékkezelés jellemzően papíralapú nyilvántartásokkal és manuális átadás-átvételi jegyzőkönyvekkel történik. Ez a megközelítés nemcsak idő- és munkaigényes, de növeli az emberi mulasztásból vagy adminisztrációs hibából fakadó láncszakadás kockázatát is.

Napjainkban a rendvédelmi szerveknek, ügyészségeknek és bíróságoknak még nem sikerült olyan egységes, minőségbiztosított és szabványosított CoC-rendszert kialakítaniuk, amely biztosítja a bizonyítékok sérthetetlenségét, ugyanakkor nem ró aránytalan adminisztratív terhet a szakemberekre. A klasszikus bűnjelkezelési eljárások során rendszerint csak utólagos ellenőrzésre van lehetőség, és gyakran nem látható át teljes egészében, hogy a bizonyíték a lefoglalástól a bírósági felhasználásig milyen utat járt be. A digitalizáció és a korszerű informatikai megoldások térnyerése azonban lehetőséget ad arra, hogy ezen a területen is paradigmaváltás következzen be. A blokklánc alapú elosztott főkönyvi rendszerek, az RFID-alapú azonosítás és nyomon követés, az okoseszközök hálózatba kapcsolása (Internet of Things, IoT), valamint az ezekhez társítható intelligens szerződések mind új utakat nyitnak a CoC folyamatainak megerősítésére. E technológiák alkalmazásával a bizonyítékok útja valós időben, manipulálhatatlan módon rögzíthető, és akár automatizált riasztások, értesítések is kiadhatók szabálytalanság esetén (például jogosulatlan hozzáférési kísérlet).

A CoC követelményei a különböző jogrendszerekben eltérő módon jelentek meg. Az angolszász *(common law)* jogrendszerekben a bizonyítékok elfogadhatóságának alapfeltétele a folytonos és dokumentált láncolat, ennek hiánya a bizonyíték kizárásához vezethet az ítélkezés során. Ezzel szemben a kontinentális *(civil law)* jogrendekben – így Magyarországon is – a bizonyítékok kezelését és nyilvántartását részben központi jogszabályok határozzák meg, és a bíróság, illetve hatóság maga is részt vesz a bizonyítékok beszerzésében. Magyarországon a *chain of custody* kifejezés nem

honosodott meg a jogi terminológiában, de a büntetőeljárási törvény és kapcsolódó rendeletek tartalmaznak a bizonyítékok kezelésére vonatkozó előírásokat. Ugyanakkor jelenleg hiányzik egy integrált, digitális eszközökre támaszkodó CoC-rendszer, amely a nemzetközi legjobb gyakorlatokat átültetné a hazai gyakorlatba. Ezek a különbségek történeti okokból is adódnak, és mélyen beágyazódtak a két jogrendszer bűnügyi eljárásaiba.[2]

Kutatási célkitűzések és hipotézisek

A tanulmány elsődleges célja, hogy elemezze, miként javíthatják a modern digitális technológiák (különösen a blokklánc, RFID és kapcsolódó eszközök) a bizonyítékok nyomon követésének folyamatát, és hogyan illeszthetők ezek a megoldások a magyar jogi keretrendszerbe a nemzetközi szabványokkal összhangban. E célt szem előtt tartva az alábbi hipotéziseket fogalmaztuk meg:

- **H1:** A digitális technológiák alkalmazása a chain of custody folyamatában jelentősen növeli a bizonyítékok kezelésének integritását és átláthatóságát a hagyományos módszerekhez képest.
- **H2:** Az RFID-alapú azonosítás és nyomon követés bevezetése csökkenti a bizonyítékkezelés során előforduló hibákat és késedelmeket, és javítja a folyamat hatékonyságát.
- **H3:** A magyar jogszabályi környezet megfelelően alakítható oly módon, hogy lehetővé tegye a CoC-folyamatok digitalizációját – beleértve a blokklánc és más új technológiák alkalmazását –, bár bizonyos területeken (például adatvédelem, eljárásjogi szabályok) szükség lehet a jogszabályok módosítására vagy kiegészítésére.

Az alábbiakban e hipotézisek vizsgálatára egy nemzetközi és hazai szabályozási összehasonlítást, valamint a technológiai lehetőségek értékelését mutatjuk be, majd javaslatot teszünk empirikus vizsgálati módszerekre a felvetett megoldások tesztelésére.

Módszertan

A kutatás elsősorban kvalitatív módszertanon alapul, irodalmi és jogszabályi elemzésre épít. Áttekintettük a vonatkozó nemzetközi szabványokat, ajánlásokat és szakirodalmi forrásokat a chain of custody témájában, valamint elemeztük a magyar jogi környezet idekapcsolódó elemeit. Ennek keretében összehasonlító elemzést végeztünk a hazai szabályozás és a nemzetközi standardok között, azonosítva az esetleges hiányosságokat és fejlesztési lehetőségeket. Ezenfelül áttekintettük a blokklánc, RFID, IoT és más releváns technológiák alkalmazásáról szóló nemzetközi kutatásokat (beleértve gyakorlati esettanulmányokat és prototípus-alkalmazásokat), hogy feltárjuk, milyen konkrét megoldásokkal és eredményekkel járhat a CoC-folyamat digitalizálása.

[2] Azarenok 2022.

Mivel empirikus adatgyűjtésre a kutatás keretében nem került sor, a tanulmány javaslatokat fogalmaz meg a jövőbeni gyakorlati tesztelésre. A *H1* és *H2* hipotézisek vizsgálatára például egy kísérleti pilotprojekt szolgálhatna: egy bűnjelraktárban vagy kriminalisztikai laborban prototípus jelleggel bevezethető egy blokklánc alapú, RFID-címkékkel támogatott bizonyítéknyilvántartó rendszer. Az új rendszer mellett párhuzamosan futtatott hagyományos eljárásokkal összehasonlítva mérhető lenne a feldolgozási idő (például a bizonyíték átvételének és kiadásának ideje), a dokumentáció teljessége és az esetleges hibák száma. Például elemezhető, hogy egy adott bizonyíték útját hány ponton és milyen részletességgel sikerül rögzíteni a digitális rendszerben, szemben a papíralapú nyilvántartással, valamint hogy egy illetéktelen beavatkozási kísérletet azonnal jelzett-e a rendszer. A kísérlet eredményeit statisztikai módszerekkel lehetne kiértékelni (például hibaarányok összehasonlítása, átlagos ügyintézési idők különbségeinek tesztelése).

A *H3* hipotézis (jogi keretek illeszthetősége) vizsgálatához jog-összehasonlító módszertant alkalmaztunk. Ennek során egyrészt megvizsgáltuk a hazai jogszabályokat [különösen a büntetőeljárásról szóló törvény és a 11/2003. (V. 8.) IM–BM–PM együttes rendelet előírásait], másrészt összevetettük azokat olyan nemzetközi ajánlásokkal, mint az ISO/IEC szabványok és a SWGDE, ASTM, ENFSI által közzétett iránymutatások. A jogi illeszkedés empirikus tesztelése a gyakorlatban történhet például szakértői interjúk vagy fókuszcsoportos megbeszélések formájában, amelyek során bírák, ügyészek, nyomozók és igazságügyi szakértők értékelik a javasolt digitális CoC-rendszer alkalmazhatóságát és elfogadhatóságát a jelenlegi jogi környezetben.

A vizsgálat során nyert eredményeket tematikusan rendeztük: először a nemzetközi és hazai szabályozási keretek elemzését mutatjuk be, majd ismertetjük a lehetséges digitális megoldásokat és azok előnyeit/kihívásait. Ezt követően a kapott eredményeket megvitatjuk, külön kitérve a hipotézisekre és a gyakorlati megvalósítás feltételeire.

Eredmények

Nemzetközi szabványok és legjobb gyakorlatok a CoC terén

A bizonyítékok kezelésére és a CoC fenntartására számos nemzetközi szabvány és iránymutatás létezik. A legjelentősebb szervezetek és dokumentumok az alábbiak:

- ISO/IEC-szabványok: Globális szabványok írják elő a kriminalisztikai laboratóriumok működésének és a bizonyítékkezelésnek a követelményeit. Idetartozik például az ISO/IEC 17025:2017, amely a vizsgáló laborok kompetenciájának általános követelményeit rögzíti, valamint az ISO/IEC 27037:2012 és 27042:2015 szabványok, amelyek a digitális bizonyítékok gyűjtésének, elemzésének és értelmezésének módszertanára adnak útmutatást. Ezek a szabványok globálisan elfogadott keretet biztosítanak a bizonyítékkezeléshez, elősegítve az eljárások egységességét és megbízhatóságát.
- SWGDE-irányelvek: A Scientific Working Group on Digital Evidence egy nemzetközi szakértői csoport, amely nem kötelező erejű, de széles körben hivatkozott ajánlásokat fogalmaz meg a digitális és multimédiás bizonyítékok

kezelésére. Irányelvei lefedik a bizonyítékgyűjtés, dokumentáció, tárolás, feldolgozás és szállítás legjobb gyakorlatait, kiemelve például a veszteségmentes adatformátumok (RAW, TIFF stb.) használatát és a részletes jegyzőkönyvezést. Bár ezek nem formális szabványok, globális referenciapontként szolgálnak a digitális bizonyítékok kezelése során, és hozzájárulnak a bevált gyakorlatok terjedéséhez.

- ASTM-szabványok: Az ASTM International az anyagvizsgálatok és egyes kriminalisztikai elemzések szabványosítására szakosodott szervezet. Szabványai részletes protokollokat nyújtanak a fizikai bizonyítékok (például eszköznyomok, fegyverek, dokumentumok, biometrikus minták) vizsgálatára és a laboratóriumi CoC fenntartására. Az ASTM hangsúlyozza a bizonyítékok gyűjtésének és kezelésének pontos dokumentálását és a laboratóriumi folyamatok validálását.
- ENFSI-ajánlások: A European Network of Forensic Science Institutes (ENFSI) európai kriminalisztikai intézetek hálózataként működik, és célja a szakértői módszerek harmonizációja. Best practice útmutatóik kiegészítik az ISO, SWGDE, ASTM által lefektetett kereteket, európai kontextusra szabva azokat. Az ENFSI például kiadta a *Digitális technológia igazságügyi vizsgálatának legjobb gyakorlata* kézikönyvet (2015), amely a digitális bizonyítékok vizsgálatának és láncolatának európai szemléletű standardjait foglalja össze.
- Interpol-kézikönyvek: Nemzetközi rendészeti szervezetek is készítettek útmutatókat a bizonyítékok kezeléséhez. Az Interpol 2014-ben kiadott egy környezeti bűncselekményekre fókuszáló igazságügyi nyomozati kézikönyvet, amely hangsúlyozza a helyszíni mintavétel és a bizonyíték-nyilvántartás szakszerű végrehajtását, biztosítva a bizonyítékok nyomonkövethetőségét és integritását a nemzetközi együttműködésekben is.

E nemzetközi standardok és ajánlások közös célja, hogy növeljék a bizonyítékkezelés megbízhatóságát és elősegítsék a különböző országok gyakorlatainak közelítését. Összességében az ISO, SWGDE, ASTM és ENFSI szervezetek eltérő fókuszuk ellenére egymást kiegészítve járulnak hozzá a CoC-folyamatok fejlesztéséhez. Míg az ISO globális érvényű keretet ad az interoperabilitás érdekében, addig a SWGDE specifikusan a digitális bizonyítékokra koncentrál, az ASTM a fizikai bizonyítékok laboratóriumi kezelésére kínál standardokat, az ENFSI pedig regionális (európai) szinten harmonizálja a gyakorlatot. A nemzetközi előírások mindegyike a bizonyítékok integritásának megőrzését, a folyamatok dokumentáltságát és szükség szerint a modern technológiák bevonását szorgalmazza.

Hazai jogszabályi keret

A magyar jogrendszer a chain of custody fogalmát külön nem nevesíti, de több előírás szolgálja a bizonyítékok hitelességének megőrzését. A büntetőeljárásról szóló 2017. évi XC. törvény (Be.) 204. §-a határozza meg a *tárgyi bizonyítási eszköz* (fizikai bizonyíték) fogalmát, míg a 205. § az *elektronikus adat* (digitális bizonyíték) definícióját. A lefoglalt tárgyak kezelésének részleteit a 11/2003. (V. 8.) IM–BM–PM együttes rendelet rögzíti,

amely szabályozza a lefoglalt dolgok nyilvántartását, őrzését, előzetes értékesítését, megsemmisítését, valamint az elkobzás végrehajtását. E rendelet alapján a hatóságoknak minden bizonyítékot egyedi azonosítóval kell ellátniuk és nyilvántartási rendszerben szerepeltetniük.

A gyakorlatban a bizonyítékok útját a különböző eljárási szakaszokban (lefoglalás, szállítás, szakértői vizsgálat, bíróság) papíralapú jegyzőkönyvek és átadás-átvételi dokumentumok kísérik. Egy központosított, elektronikus CoC-nyilvántartás azonban jelenleg nem létezik, így az információk széttagolódhatnak a rendőrség, ügyészség, bíróság és szakértői intézetek saját nyilvántartásai között. Ez a fragmentáltság azt eredményezheti, hogy a bizonyítékok teljes életciklusának nyomon követése nehézkes, és utólagos ellenőrzéskor hiányosságok merülhetnek fel (például nem dokumentált mozgatás vagy késedelem). Digitális bizonyítékok esetén a hatályos jog csak annyit mond ki, hogy azokat hasonló módon kell kezelni, mint a tárgyi bizonyítékokat; speciális technológiai megoldások (például hash-értékkel való lezárás vagy elektronikus naplózás) alkalmazását nem írja elő a jogszabály.

1. táblázat: A chain of custody folyamat néhány kulcselemének összehasonlítása a nemzetközi ajánlások és a magyar gyakorlat között

Szempont	Nemzetközi ajánlások / standardok	Magyar gyakorlat
Nyilvántartás módja	Részletes, folyamatos dokumentáció minden átadásról digitális naplóban (pl. blokklánc alapú vagy elektronikus rendszer).	Papíralapú jegyzőkönyvek, különálló (esetleg elektronikusan iktatott) dokumentumok szakaszonként; nincs egységes, központi elektronikus nyilvántartás.
Integritás ellenőrzése	Kriptográfiai módszerekkel (hash-algoritmusok) biztosított bizonyítékintegritás; minden módosítás kizárása vagy naplózása.	Fizikai plombák, pecsétek a csomagoláson; hash használata csak digitális adatoknál eseti jelleggel, nem egységes követelményként.
Technológia használata	RFID-címkék és szenzorok a valós idejű helymeghatározásra, környezeti adatok rögzítésére; automatizált riasztások eltérés esetén.	Hagyományos vonalkód vagy leltári szám; manuális ellenőrzés, fizikai tárolás felügyelete emberi erővel. Elektronikus érzékelők használata nem jellemző.
Szabványok és protokollok	Nemzetközi szabványok (ISO 17025, ISO 27037 stb.) és ajánlások (SWGDE, ASTM, ENFSI) által kidolgozott protokollok a teljes CoC-folyamatra.	A Be. és a 11/2003-as rendelet alapvető kereteket ad; részletes protokollok intézményenként eltérők, nem egységesek. Nemzetközi szabványok átvétele korlátozott.
Adatvédelem és hozzáférés	Szigorú hozzáférés-kezelés, naplózás és auditálás (pl. szerepkör alapú hozzáférés a digitális rendszerben).	Hozzáférés jogszabályban korlátozott (pl. csak az eljáró hatóságok férhetnek hozzá), de a nyilvántartások ellenőrzése jellemzően utólagos és manuális.

Forrás: a szerző szerkesztése

Fontos kiemelni, hogy az adatkezelésre vonatkozó általános előírások – különösen az Európai Unió általános adatvédelmi rendelete (GDPR) – a bizonyítékok digitalizált nyilvántartása esetén is érvényesek. Ez azt jelenti, hogy a személyes adatokat tartalmazó bűnügyi nyilvántartásoknak szigorú hozzáférés-kezeléssel és auditálhatósággal kell rendelkezniük, hogy megfeleljenek az adatvédelmi követelményeknek.

Emellett a hazai kriminalisztikai laboratóriumok esetenként alkalmazzák az ISO/IEC 17025:2017 szabvány előírásait a saját minőségirányításukban, amely magában foglalja a minták és bizonyítékok kezelésének nyomonkövethetőségét. Ez azonban szakintézményi gyakorlat, nem pedig minden hatóságra kiterjedő kötelező szabály. Összességében a jelenlegi hazai keretrendszer biztosít néhány alapvető garanciát (például nyilvántartási kötelezettség), de nem terjed ki a modern digitális eszközökkel támogatott, valós idejű és automatizált nyomon követésre.

Technológiai megoldások a CoC digitalizálására

Blokklánc és kriptográfia a bizonyítéklláncban

A blokklánc- *(blockchain)* technológia alapja egy decentralizált, elosztott főkönyvi rendszer, amelyben az egymást követő tranzakciók blokkok formájában, kriptográfiailag összefűzve tárolódnak. Ennek köszönhetően minden egyes művelet (például egy bizonyíték átadása a helyszínről a laborba, vagy a vizsgálati eredmény továbbítása a bírósághoz) egy új blokként rögzül, amely visszakereshető és utólag nem módosítható. A blokklánc rendkívül ellenálló a manipulációval szemben: egy blokk utólagos megváltoztatása csak úgy lehetséges, ha az utána következő összes blokkot is megváltoztatják, ami a konszenzusos hálózat miatt gyakorlatilag kivitelezhetetlen.

A kriptográfiai hash-algoritmusok kulcsszerepet játszanak a digitális bizonyítékok integritásának védelmében. Minden digitális fájlhoz, vagy akár egy elektronikus nyilvántartó bejegyzéshez generálható egy egyedi „lenyomat" (például SHA-256 hash), amely bizonyítja, hogy a tartalom nem változott. A korábban széles körben használt MD5 és SHA-1 algoritmusokról időközben kiderült, hogy bizonyos ütköztetési támadásokkal kijátszhatók, ezért ma már korszerűbb hash-eket alkalmaznak. A blokklánc-technológia ötvözése a hash-alapú integritásvédelemmel olyan többrétegű biztonsági megoldást eredményez, amely a szakirodalom szerint hatékonyan biztosítja a digitális bizonyítékkezelés sérthetetlenségét. Az intelligens szerződések *(smart contracts)* tovább növelhetik a hatékonyságot, mivel ezek olyan, blokkláncra telepített programok, amelyek automatikusan végrehajtják a meghatározott üzleti logikát.[3] Például beállítható, hogy egy bizonyíték átadására csak akkor kerüljön sor, ha a rendszerben az ahhoz szükséges összes jogosultságot és engedélyt rögzítették – enélkül a tranzakció nem teljesül. Így az okosszerződések biztosíthatják, hogy a CoC-protokollokat minden esetben betartsák, emberi beavatkozás nélkül is.

Számos nemzetközi kutatás foglalkozott már a blokklánc alapú CoC-rendszerek fejlesztésével. Ahmad és társai (2020) egy privát Ethereum-hálózaton megvalósított bizonyítéklánc-modellt javasoltak, amely valós idejű, hamisításbiztos naplózást tett lehetővé.[4] Santamaría és kollégái (2023) egy működő prototípust építettek, amelyben okosszerződésekkel kezelték a digitális bizonyítékok láncolatát, és sikeresen demonstrálták a rendszer gyakorlati alkalmazhatóságát. Hasonlóképpen Miller

[3] Santamaría et al. 2023.
[4] Ahmad et al. 2020.

és Singh (2024) kutatása egy innovatív modellt mutatott be a digitális bizonyítékok integritásának ellenőrzésére és megőrzésére, amely tovább erősíti a CoC-folyamat megbízhatóságát a kibervédelmi vizsgálatokban.[5] Ezek az eredmények azt sugallják, hogy a blokklánc-technológia megfelelő alkalmazása esetén jelentős mértékben fokozható a bizonyítékkezelés átláthatósága és biztonsága. Ugyanakkor érdemes megjegyezni, hogy a blokkláncrendszerek bevezetése alapos tervezést igényel, különös tekintettel az interoperabilitásra és a skálázhatóságra, amire a tanulmány későbbi részében még visszatérünk.

RFID- és IoT-alapú nyomon követés

A rádiófrekvenciás azonosítás (RFID) olyan technológia, amely lehetővé teszi tárgyak érintés nélküli azonosítását és nyomon követését rádióhullámok segítségével. Egy teljes RFID-rendszer tipikusan három fő elemből áll: RFID-címkékből (mikrochippel ellátott azonosítók, aktív vagy passzív kivitelben), olvasóberendezésekből és a háttérben működő adatkezelő szoftverből. A bizonyítékokra erősített RFID-címkék egyedi azonosítót és szükség esetén további adatokat (például ügyszám, gyűjtés helye/ideje) hordoznak. Az olvasók a bűnjelraktárakban, laborokban vagy akár szállító járművekben folyamatosan figyelhetik a bizonyítékok jelenlétét, helyét, és a rendszer automatikusan rögzíti, amikor egy bizonyíték elhagy egy adott zónát vagy belép annak területére.

Az IoT- (dolgok internete) eszközök integrálása tovább bővíti a lehetőségeket. Például a bizonyítékokat tároló helyiségekben vagy konténerekben elhelyezett szenzorok valós időben mérhetik a környezeti paramétereket, mint a hőmérséklet és a páratartalom, hogy biztosítsák az optimális tárolási feltételeket. Smith és munkatársai (2019) rámutattak, hogy egyes érzékeny nyomok (például lábnyomok gipszöntései) esetében az RFID-címkékkel ellátott minták folyamatos felügyelete – beleértve a környezeti feltételek monitorozását is – nagyban hozzájárul a bizonyítékok épségének megőrzéséhez. Az RFID-alapú rendszerek képesek valós idejű riasztások kiadására is: például ha egy bizonyíték engedély nélküli mozgatása történik, vagy a tárolási körülmények kritikus szintre romlanak, a rendszer azonnal jelez (akár automatikus értesítést küld a felelős személyeknek).

Az RFID- és IoT-technológiák alkalmazásával a fizikai bizonyítékok kezelése lényegesen hatékonyabbá válhat. A leltározás és keresés ideje lerövidül, mivel nem kell manuálisan azonosítani minden egyes tárgyat, hanem az olvasók automatikusan beolvassák a jelenlétüket. A rendszer naplózza a pontos időpontokat, amikor egy bizonyíték megérkezik vagy távozik egy adott helyről, ezáltal precíz, percre kész láncolati naplót hozva létre.

Természetesen e technológiák bevezetése nem mentes a kihívásoktól. Az RFID-rendszer kezdeti kiépítése költséges lehet, különösen nagy mennyiségű bizonyíték és több telephely esetén. A rádiójelek zavara vagy árnyékolása okozhat adatkihagyást (például fémtárolók vagy vastag falak gyengíthetik a jelet). Továbbá biztosítani kell hogy az RFID-/IoT-rendszer összekapcsolódjon a meglévő rendőrségi és bírósági informatikai

[5] Miller–Singh 2024.

rendszerekkel, hogy az adatok áramlása zökkenőmentes legyen. E nehézségek ellenére számos példa igazolja az RFID sikeres alkalmazását a bűnjelkezelésben: több ország igazságügyi laboratóriumaiban már kísérleti jelleggel vezettek be RFID-alapú nyomkövetést, és arról számoltak be, hogy a nyilvántartások pontossága és az ellenőrzések gyorsasága javult.[6]

Mindezek alapján kijelenthető, hogy az RFID- és az IoT-technológiák a fizikai és digitális bizonyítékok kezelésének modernizálásában kulcsszerepet játszhatnak, kiegészítve a blokklánc által kínált adatintegritási garanciákat.

Konklúzió

A fenti eredmények fényében megállapítható, hogy a kitűzött hipotézisek helytállók. A H1 (a digitális technológiák növelik a CoC integritását és átláthatóságát) hipotézisünket alátámasztják mind a szakirodalmi források, mind a nemzetközi kísérletek tapasztalatai. A blokklánc alapú nyilvántartások és a hash-algoritmusok kombinációja ténylegesen képes szavatolni, hogy a bizonyítékokkal kapcsolatos adatokat ne lehessen észrevétlenül megváltoztatni vagy eltüntetni. Az RFID bevezetése pedig demonstrálható módon csökkenti az adminisztratív hiányosságokat: a rendszer automatikus jelzései révén időben kiderül, ha egy láncszem kimaradna vagy szabálytalanság történne. Mindez azt eredményezi, hogy a bizonyítékok útja sokkal átláthatóbbá válik, ezáltal nő a bűnüldözési folyamatokba vetett bizalom is. H2 (az RFID csökkenti a hibákat és gyorsítja a folyamatot) szintén igazolást nyer, hiszen a vizsgálatok rámutattak, hogy a fizikai azonosítás és leltározás digitalizálása nemcsak tehermentesíti a humán erőforrásokat, de pontosabb nyilvántartást is eredményez. Rövidebbé válik a bizonyítékok keresésének ideje, és kevesebb esély van arra, hogy egy tételeltévesztés miatt egy bizonyíték „elvész" a rendszerben.

A H3 (a jogi keret igazítható a digitális CoC igényeihez) hipotézis kapcsán a nemzetközi és hazai szabályozás összehasonlítása alapján megállapítható, hogy bár a magyar joganyagban jelenleg nincsenek expliciten rögzítve a digitális CoC eszközei, a meglévő keret nem zárja ki azok alkalmazását sem. Sőt, bizonyos területeken már most is megfigyelhető a közelítés a nemzetközi standardokhoz – például a szakértői intézetek ISO 17025 szerinti akkreditációja vagy az elektronikus ügykezelési rendszerek terjedése. Mindazonáltal a sikeres implementációhoz szükség lesz a jogi környezet finomhangolására. Célszerű lehet külön szabályozni a digitális CoC-nyilvántartások hitelességét (például minősített elektronikus aláírás vagy pecsét használata a digitális naplók lezárásához), továbbá egyértelműsíteni kell hogy a blokklánc alapú naplózás során keletkező adatok a bíróság előtt bizonyító erővel rendelkeznek. Emellett az adatvédelmi megfelelésnek is eleget kell tenni: biztosítani kell hogy a rendszerben tárolt személyes adatokat csak a szükséges mértékben és ideig kezeljék, és azokhoz csak az arra jogosultak férjenek hozzá auditálható módon. Ezek a jogi-szabályozási finomítások hozzájárulnak ahhoz, hogy a digitális CoC-megoldások bevezetése zökkenőmentes és sikeres legyen.

[6] Kumar–Singh 2021.

A technológiai újítások bevezetése kapcsán további fontos szempont a szervezeti és kulturális tényezők szerepe. Egy ilyen átfogó változás – a papíralapú adminisztrációról a digitális rendszerre való áttérés – nem pusztán technológiai upgrade, hanem szemléletváltás is egyben. Elengedhetetlen, hogy a rendszer végfelhasználói (nyomozók, raktárosok, szakértők, ügyészek stb.) megfelelő képzésben részesüljenek az új eszközök használatát illetően, és megértsék azok előnyeit. A folyamatos oktatás és a változáskezelés kulcsfontosságú a bizalom kiépítéséhez az új rendszer iránt. Ha a személyzet látja, hogy a digitális CoC nem többletterhet jelent, hanem éppen ellenkezőleg, megkönnyíti a munkáját (kevesebb papírmunka, gyorsabb visszakeresés, egyértelmű felelősségi lánc), akkor a kezdeti ellenállás leküzdhető.

További gyakorlati kihívások is megfontolandók. A rendszer kiépítésének költségei jelentősek lehetnek – ideértve a technikai infrastruktúra (szerverek, hálózat, RFID-olvasók stb.) telepítését, valamint a szoftverfejlesztést és -integrációt. Ugyanakkor hosszú távon ezek a beruházások megtérülhetnek a hatékonyságnövekedés és a hibák miatti pótlólagos eljárások elkerülése révén. A blokkláncrendszerek skálázhatósága és energiaköltsége szintén szempont; valószínűleg egy privát vagy konzorciumi blokklánchálózat alkalmazása célszerű a bűnüldözési szervek között, hogy kontrollált környezetben működjön a megoldás. Az interoperabilitás biztosítása érdekében nyílt szabványokat kell követni, hogy a későbbiekben más rendszerek (például európai szintű bűnügyi nyilvántartások) is tudjanak csatlakozni vagy adatot cserélni a CoC-rendszerrel.

Összességében elmondható, hogy a digitalizált chain of custody bevezetése reális és szakmailag megalapozott törekvés. A nemzetközi trendek egyértelműek. Számos ország és szervezet kísérletezik ilyen rendszerekkel, és a globális szabványok adaptálása elengedhetetlen ahhoz, hogy a magyar igazságszolgáltatás lépést tartson a nemzetközi elvárásokkal. A tanulmány eredményei rámutatnak, hogy a technológiai feltételek adottak, a jogi feltételek megteremthetők, és a gyakorlati tapasztalatok alapján megfelelő tervezéssel és képzéssel a kihívások leküzdhetők. A CoC digitalizációja nem csupán technológiai innováció, hanem az igazságszolgáltatás hatékonyságának, átláthatóságának és hitelességének növelését szolgáló átfogó fejlesztés, amely hosszú távon hozzájárulhat a kriminalisztikai bizonyítékkezelés és ezáltal a bűnüldözés és a bírósági munka magasabb színvonalához.

Következtetések

A vizsgálat rávilágított, hogy a chain of custody folyamat digitalizálása időszerű és indokolt lépés a bizonyítékkezelés terén. A tanulmány keretében áttekintettük a CoC jelentőségét és hagyományos gyakorlatát, összehasonlítottuk a magyar szabályozást a nemzetközi standardokkal, valamint felmértük a legmodernebb technológiai eszközök – így különösen a blokklánc, az RFID és az IoT – alkalmazásának lehetőségeit. Megállapítottuk, hogy a digitális megoldások integrálása jelentős előnyökkel jár: növelhető a bizonyítékok nyomon követésének pontossága, csökkenthetők az emberi mulasztásokból fakadó kockázatok, és gyorsíthatók az eljárások. Ugyanakkor hangsúlyoztuk, hogy a sikeres bevezetés feltétele a megfelelő jogi és szervezeti keretek kialakítása – ideértve az adatvédelmi szempontok figyelembevételét és a felhasználók képzését is.

Összefoglalva, a CoC digitalizációja olyan innováció, amely egyszerre javítja a bűnüldözés hatékonyságát és erősíti a büntetőeljárások tisztességét. A nemzetközi példák és a jelenlegi technológiai trendek azt mutatják, hogy Magyarország is képes lehet a digitális bizonyítéklánc alkalmazására, bevezetésére, amennyiben az ehhez szükséges jogszabályi módosításokat és infrastrukturális fejlesztéseket végrehajtja. A változás eredményeként a bizonyítékok kezelése a 21. századi elvárásoknak megfelelően válhat átláthatóvá és hitelessé, ami végső soron hozzájárul az igazságszolgáltatásba vetett közbizalom erősítéséhez. Jövőbeli kutatások és pilotprojektek segíthetnek azonosítani a gyakorlati megvalósítás további részleteit, azonban az eddigi eredmények alapján egyértelmű, hogy a digitális CoC-rendszerek bevezetése a büntető igazságszolgáltatás terén komoly hozzáadott értéket képvisel.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Ahmad, Liza – Khanji, Salam – Iqbal, Farkhund – Kamoun, Faouzi (2020): *Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management.* Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020), 1–8. Online: https://doi.org/10.1145/3407023.3409199

Alruwaili, Fahad F. (2021): CustodyBlock: A Distributed CoC Evidence Framework. *Information,* 12(2). Online: https://doi.org/10.3390/info12020088

Azarenok, N. (2022): Conditionality of Anglo-Saxon and Romance-Germanic Types of Criminal Procedure. *Vestnik Tomskogo Gosudarstvennogo Universiteta – Pravo,* 478, 219–228. Online: https://doi.org/10.17223/15617793/478/25

ENFSI (2015): *Best Practice Manual for the Forensic Examination of Digital Technology.* European Network of Forensic Science Institutes.

Garcia, L. – Taylor, R. (2020): Advanced Storage Solutions for Evidence Management. *International Journal of Criminal Justice,* 29(3), 150–165.

Interpol (2014): *Pollution Crime Forensic Investigation Manual.* Interpol Environmental Crime Programme.

Interpol (2014): *Pollution Crime Forensic Investigation Manual.* Interpol Environmental Crime Programme.

ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories.

ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence.

Kumar, S. – Singh, P. (2021): RFID in Forensic Science: Applications and Challenges. *Indian Journal of Forensic Sciences,* 12(2), 55–70.

Miller, Adir – Singh, Avinash (2024): *CoC and Evidence Integrity Verification Using Blockchain Technology.* Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024), Johannesburg, South Africa, 2024. Online: https://doi.org/10.34190/iccws.19.1.2025

Santamaría, Pablo – Tobarra, Llanos – Pastor-Vargas, Rafael – Robles-Gómez, Antonio (2023): Smart Contracts for Managing the Chain-of-Custody of Digital Evidence: A Practical Case Study. *Smart Cities,* 6(2), 709–727. Online: https://doi.org/10.3390/smartcities6020034

Smith, J. et al. (2019): RFID and Digital Evidence Management: A Modern Approach. *Forensic Science Today,* 10(4), 200–220.

SWGDE (2017a): *SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage.* Scientific Working Group on Digital Evidence.

SWGDE (2017b): *SWGDE Best Practices for Data Acquisition from Digital Video Recorders.* Scientific Working Group on Digital Evidence.

SWGDE (2021): *SWGDE Best Practices for Computer Forensic Acquisitions.* Scientific Working Group on Digital Evidence.

Schmitt, Veronica – Jordaan, Jason (2013): Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in These Algorithms. *International Journal of Computer Applications,* 68(23), 38–46. Online: https://doi.org/10.5120/11723-7433

Jogi források

2017. évi XC. törvény a büntetőeljárásról

11/2003. (V. 8.) IM–BM–PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról

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 (GDPR)