DOI: 10.38146/BSZ.2019.2.3

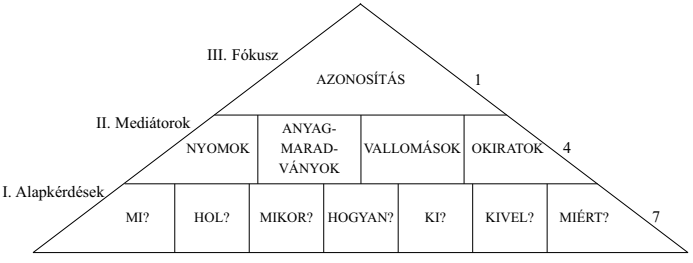
FENYVESI CSABA – ORBÁN JÓZSEF

Az elektronikus adat mint a 7-5-1-es kriminalisztikai piramismodell építőköve

Jelen folyóirat olvasói emlékezhetnek a 2012 októberében, majd 2014 szeptemberében megjelent kriminalisztikai piramisábráinkra[1], amelyben a hét alapkérdést (mi?, hol?, mikor?, hogyan? ki-kivel?, miért?) a középső, mediátoroknak nevezett részen a nyomok, az anyagmaradványok, a vallomások, majd a bővített, 7-4-1-es modellben az okiratok követték, majd ezek fölött ült a tevékenység fókusza, az azonosítás *(1. számú ábra)*.

1. számú ábra

A kriminalisztika piramismodellje



A 7-5-1-es piramismodell

Legújabb kutatásunk és a 2017. évi XC. törvény, az új, IV. büntetőeljárási törvény szabályozása alapján azonban úgy véljük, a modell további revízióra, pontosításra szorul. Mégpedig éppen a már citált második tanulmányunkban is kiemelt digitális adatok miatt. Ott ezt a szót használtuk, és ösztönöztük kriminalisztikai kutatásainkkal, monográfiánkkal[2], hogy a törvényhozó is vegye

1 Fenyvesi Csaba: A kriminalisztika piramismodellje és alapelvei. Belügyi Szemle, 2012/10., 14–26. o., illetve Fenyvesi Csaba: A kriminalisztika piramismodelljének második változata. Belügyi Szemle, 2014/9., 32–43. o.

2 Lásd erről Fenyvesi Csaba: A kriminalisztika tendenciái. Dialóg Campus Kiadó, Budapest–Pécs, 2014, 2017

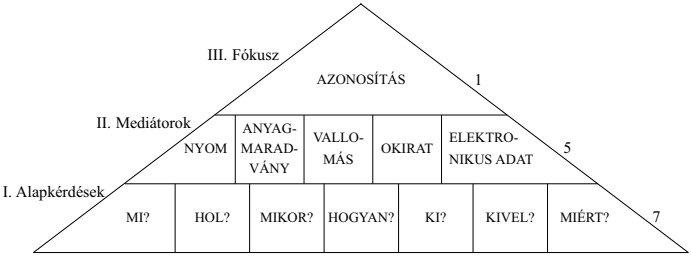
figyelembe. Ami nagyon gyorsan be is következett, miután a hivatkozott számú büntetőeljárási kódex 165. szakasza behelyezte a „bizonyítási eszközök” közé, megjelölte név szerint az elektronikus adatot.[3]

Így a kriminalisztikai piramismodellünk (remélhetőleg most hosszú időre érvényesen) a 7-5-1-es felépítésnek felel meg. Vagyis az alapkérdések *(Sieben Golden Fragen, 7 Main Questions, 7 W Questions)* öt közvetítő, segítő (mediátor) útján kaphatnak azonosítási választ, ami változatlanul a piramis egyeduralkodó fókusza. (Egyetértve *Angyal Miklós*sal, hogy az azonosítás helyébe akár a „megismerés”-t is behelyezhetjük, hiszen a kérdések megválaszolásával megismerjük a múltbéli releváns, Be. szerint megkövetelt „valósághű” tényeket.)[4]

Tehát legújabb modellezésünk szerint a kriminalisztika mint alkalmazott tudomány fejlesztésében, a diszciplína gyakorlati alkalmazásában és a kriminalisztika mint tantárgy oktatásában is szemléletesen felhasználható ábra ekként mutat *(2. számú ábra).*

2. számú ábra

A kriminalisztikai azonosítás 7-5-1-es piramis modellje



Az elektronikus adat (és bizonyíték) értelmezése

A kérdés az, hogy az általunk már korábbi tanulmányainkban, értekezéseinkben[5] részletezett digitális adat mennyiben tér el, vagy hasonlít a törvényi

3 165. § A bizonyítás eszközei: a) tanúvallomás, b) a terhelt vallomása, c) a szakvélemény, d) a pártfogó felügyelői vélemény, e) a tárgyi bizonyítási eszköz, ideértve az iratot és az okiratot is, és f) az elektronikus adat.

4 Angyal Miklós – Balassa Bence – Bezsenyi Tamás – Petrétei Dávid: Kognitív kriminalisztika. Kézirat. Nemzeti Közszolgálati Egyetem, Budapest, 2018

5 Lásd még erről a témáról Fenyvesi Csaba: A felismerésre bemutatás és a digitális adatok jelentősége egy személyremsértő bűncselekmény tükrében. Belügyi Szemle, 2016/9., 119–129. o.; Fenyvesi Csaba: A digitális adatok jelentősége a kriminalisztikában. Jura, 2016/2., 50–59. o.; Orbán József: Bayes-

megfogalmazásban szereplő elektronikus adathoz képest. Azt a kérdéssort is feltehetjük: mennyiben része az egyik a másiknak, mi az egymáshoz való viszonyuk, mi a tartalma, lényegi ismérve az elektronikus adatnak?

Annál is inkább aktuális a kérdéscsokor, mivel az elmúlt években az elektronikus információkkal kapcsolatosan digitális jelzőről lehetett hallani, olvasni egyes tanulmányokban, szakmai körökben. Azután megérkezett a 2017. XC. tv., azaz a IV. Be. és a 205. § (1) bekezdésének meghatározása szerint az *„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja”.* Helyesnek tartjuk a törvényalkotó szóhasználatát, amikor elektronikus és nem digitális adat megfogalmazással él. Megítélésünk szerint a törvényhelyen szereplő információs rendszer szűkítő értelmű.

Megfogalmazásunkban az *elektronikus adat* egy elektronikus rendszerben előállított, feldolgozott, továbbított vagy visszanyert információt tartalmazó elem. Ebbe beletartozónak tekintjük azt is, amikor az előbbi lánc valamelyik eleme fény, hang vagy rádiófrekvencia segítségével jön létre. Az elektronikus adat magában foglalja az analóg és a digitális formában megjelenő információt egyaránt. Tiszta analóg jelnek tekinthető például a régi bakelitlemezekről megszólaló hang, tiszta digitális információ a forgalomirányító közlekedési lámpa zöld vagy a haladást kizáró piros jelzése. A digitális adaton leginkább a bináris számokat érthetjük, azaz a kettes számrendszerbeli egynulla ábrázolást, amely mostanáig többé-kevésbé megállta a helyét. A forgalomirányító háromszínű közlekedési lámpa legalább három, de inkább négy állapotot jelez. Ezt azért tartottuk fontosnak megjegyezni, mert az elektronikai miniatürizálás hamarosan eléri a fizikai határokat, s akkor az információsűrűség növelésének egyik lehetséges útja a sokállapotú jel lehet, amely visszakanyarodást jelenthet az analóg elektronikus információhordozás felé.

A Be. 204. § (1) bekezdése alapján sommásan megfogalmazható, hogy az *elektronikus bizonyíték* elektronikus adaton (azon belül információ) alapuló tárgyi bizonyíték, amely a bűncselekményhez kötődő releváns tartalommal bír. Így például a bűncselekmény elkövetésének, vagy azzal összefüggésben az elkövető nyomait hordozza, az elkövetés útján jött létre, netán eszközül használták, illetve amelyre (amelyért) a bűncselekményt elkövették.

hálók a bűnügyekben. PhD-értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2018; Domokos Andrea – Orbán József: Az identifikáció múltja és jövője. Miskolci Jogi Szemle, 2017/2., 5–18. o.

Az elektronikus adatok egy része fizikai tulajdonságánál fogva illékony[6], illetve az érintett rendszer feszültségmentesítése után visszaállíthatatlanul megsemmisül.[7] Más elektronikus adatok mechanikus erővel (is) megsemmisíthetők, ám hozzátesszük, hogy csak elektronikusan változtathatók meg.[8]

Nézetünk szerint az elektronikus bizonyíték mint kategória magában foglalja az elektronikus analóg és az elektronikus digitális bizonyítékot is. Az elektronikus bizonyítékokkal kapcsolatos felderítési bizonyítási feladatok több hatóság független vagy együttes munkáját is igényelhetik.[9] A kisugárzott rádiófrekvenciás jelekkel kapcsolatos kivizsgálásokat általában a hírközlési tevékenységeket ellenőrző hatóságok[10] intézik. A kisugárzott információ analóg rádiófrekvenciás hullámokba ágyazott digitálisjel-csomag.[11] A jelcsomagokból visszaállított üzenet a tényleges tartalom.

A kommunikáció az informatikai eszközök esetében is *Shannon*[12] meghatározására épül. Tartalma szerint ez azt jelenti, hogy

– a forrás előállítja az üzenetet (vagy üzenetek sorát), amelyet továbbítani szeretne a vevőhöz. Az üzenet lehet hang, szöveg, kép stb.;
– a forrás oldalán az üzenetet olyan jelekké kell alakítani, hogy a kommunikációs csatorna továbbítani tudja (kódolás);
– a csatornában a közlemény legtöbbször sérül, leginkább azzal, hogy az információhoz adódik hozzá (például sercegő rádióadás, nehezen érthető mobiltelefon, vibráló képernyő). Az üzenet a kommunikációs csatornán keresztül jut el a vevőhöz;
– a vevő oldalán vissza kell alakítani a jeleket (dekódolás);

6 Az elektromágneses térben észlelhető bizonyítékok alaphelyzetben illékonynak tekinthetők, hacsak jogszabály joghatállyal bíró rögzítésüket nem írja elő.

7 Ilyennek tekinthető a számítógép operatív memóriájában tárolt adatok csoportja. Mindazonáltal az alvó üzemmódba kapcsolt gépek esetén ezek az adatok menthetők, így a hibernálás előtti információk megtekinthetők.

8 Az elektronikusinformáció-tárolókon található bizalmas adatok megsemmisítésekor az adatok kezeléséért felelős elrendeli a tárolóeszköz fizikai megsemmisítését is. Különös tekintettel arra, hogy egyes adattörlési módszerek csak az információ láthatóságát változtatják meg, de a törlés fajtájától függően eredeti állapotuk visszaállítható. Ebből következik, hogy a fizikailag ép, de töröltnek tartott adathordozó mindig ott rejtheti a szükséges elektronikus bizonyítékot.

9 Tanulmányunkban nem érintjük a nemzetbiztonsági és a katonai alkalmazásokat.

10 Magyarországon a Nemzeti Média- és Hírközlési Hatóság.

11 A digitális hírközlés elterjedése miatt az analóg sugárzás egyre kevésbé jellemző. Örökölt kivételnek tekinthető a légi jármű vezetője és a légi irányítási központok közötti analóg hangalapú kommunikáció.

12 Claude E. Shannon – Warren, Weaver: The Mathematical Theory of Communication. University of Illinois Press, Urbana–Chicago, 1998, p. 34.

– az így visszaállított információ érkezik meg a rendeltetési helyre. A csatorna által továbbított információ a közlemény, vagy más megfogalmazással, a tartalom.

A kommunikációs csatornában háromféleképpen is lehet bűncselekményt elkövetni:

1. a rádiófrekvenciás jelek nem engedélyezett kisugárzásával;
2. más engedélyezett és jogkövető sugárzásának megzavarásával;
3. az engedélyezett sugárzás során közölt törvénysértő tartalommal. Utóbbi kategóriába tartozik a rádió- vagy tévéadáson keresztül sugárzott gyűlöletbeszéd[13], továbbá az internetes oldalakon közzétett vagy megszerzett, továbbá bármilyen elektronikus formában tárolt vagy továbbadott gyermekpornográfia-tartalmú felvétel.

Az engedély nélküli rádiófrekvenciás sugárzás okozhatja mások gazdasági[14] vagy fizikai sérelmét[15] is.

Az előbbiek alapján érzékelhető, hogy az elektronikus bizonyíték lényegesen nagyobb területet foglal magában, mint a digitális bizonyíték vagy a számítógépes bűnözéssel kapcsolatban megszerezhető adatok.

Az elektronikus adatok osztályozása és forrásai

Az osztályozás nem csak az elméleti kriminalista számára bír jelentőséggel. Az klasszifikáció segíthet az adatok helyes kezelésében, a bennük rejlő információ kinyerésében és az odaillő értelmezésében. Ahogy *Tremmel Flórián* is megfogalmazta már: *„fontos elvi vagy gyakorlati szempontokra vezethető vissza, ezért érdemes velük foglalkoznunk”*[16]. Tremmel felosztását megtart-

13 Alvaro Ortigosa – Ioannis Inglezakis: D4.1b: FAQ on Responding to online hate speech Monitoring and Detecting Online Hate Speech. 2017. http://mandola-project.eu/m/filer_ public/3e/32/3e32fcaa-e420-4868-b3e2-070e2a7983cb/d41b_faq_final.pdf

14 Itt említhető a mobiltelefonálást és a GPS-alapú helymeghatározást ellehetetlenítő eszközök használata.

15 Egyelőre költsége és mérete miatt csak katonai területen ismert a fájdalmat, vagy akár személyi sérülést is okozó rádiófrekvenciás fegyverek kísérleti alkalmazása, ám az elektronika rohamos fejlődése miatt elképzelhető, hogy tehetősebb bűnözői körök is hamarosan megszerzik az eszközöket. Az ilyen fegyverekkel elkövetett bűncselekményeket a hagyományos eszközökkel nehéz lenne bizonyítani. Mindamellett már ma is előállítható házilagosan olyan eszköz, amely egy pacemakeres ember külsérelmi nyomok nélküli halálát okozhatja.

16 Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus Kiadó, Budapest–Pécs, 2006, 82. o.

va[17], ám az elektronikus bizonyítékok specialitásait figyelembe véve további osztályozási szempontokat vezetünk be. Megítélésünk szerint az osztályozás a gyakorlati felhasználás szempontjából jelentős lehet.[18]
A csoportosítás többféle (I–IX.) szempontrendszer szerint is elkészíthető. Így:

I. A *„klasszikus" megközelítés* szerint az analóg, és digitális felosztás tekinthető alapnak.

II. A *használhatóság módja* szerinti felosztásnál három csoport lehetséges:
a) azonnal használható (audio-, video-, dokumentumjellegű),
b) feldolgozás után használható,
c) a kevert összetevőjű bizonyíték.
Az első, vagyis az *a)* csoport külön magyarázatot nem igényel. A feldolgozást igénylő bizonyítékok a megszerzett állapotukban nem értelmezhetők, önmagukban bizonyító erejük nincs. Ennek az egyik legkönnyebben belátható formája a visszafejtést igénylő kódolt információ lehet. Lefordítása és értelmezése speciális tudással és eszközökkel bíró szakértő közreműködését igényli. Kevert információ lehet a mobiltelefonnal küldött hang- vagy videóinformáció. Azért tekinthetjük kevertnek, mert a hang és kép mellett szükségszerűen továbbítandók a hívással kapcsolatos, úgynevezett metaadatok is.

III. Az *elkövetés módja (a modus operandi)* szerinti felosztási szempontnál a rádiófrekvenciás fegyverrel, számítógéppel vagy kommunikációs eszközzel, továbbá ezek felhasználásával támogatott bűncselekmények bizonyítékait említhetjük.[19]

IV. A bűncselekmény *elkövetési helye vagy a bizonyíték fellelhetősége* alapján lehetnek fizikai vagy kibertérben találhatók. A kibertérben egyre népszerűbbek a felhőalapú szolgáltatások. Vitathatatlan előnye egyben a sérülékenységi pontja is. A jogos felhasználó bárhonnan hozzá tud férni a tarta-

17 Tremmel a szakirodalomra hivatkozva az eredeti és származékos bizonyítékok; személyi és tárgyi jellegű bizonyítékok; a terhelő és mentő bizonyítékok; és végül közvetlen és közvetett bizonyítékok osztályait különbözteti meg. Tremmel Flórián: Uo.

18 Ez különösen igaz az operatív intézkedéseknél, vagy a számítógépes nyomozást segítő programok megalkotásánál.

19 Megjegyezzük, hogy katonai alkalmazásban idesorolják az irányított energiájú mikrohullámú fegyvereket, amelyek az emberi szövetek felmelegítésével, az érzékszervek vagy az idegrendszer bénításával kényszerítik a sértettet arra, hogy valamit tegyen vagy ne tegyen. A fegyver lőszer és lövedék használata nélkül fejti ki hatását. A technika fejlődésével feltehetően már a közeljövőben elérhetők lesznek ölésre használható mikrohullámú fegyverek is.

lomhoz, miközben a sértettől távol az elkövető is képes cselekménye végrehajtására.

A valós vagy fizikai térben elkövetett bűncselekmények nyomai keletkezhetnek vagy rögzülhetnek elektromos jeleken keresztül is, ezért idetartozik az elektronikusnyom-rögzítés is (például digitális fénykép, digitális helyszínrajz).[20]

V. A bizonyítékok *forrása alapján* vezetékes, vezeték nélküli, valamint elektronikus információhordozón elérhető forrásosztályokat hozhatunk létre.

VI. A *tartósság alapján* megkülönböztethető illékony vagy tartós elektronikus adat.

Magyarázatként hozzátesszük, hogy a büntetőeljárás folyamatában a bizonyítékok keletkezése, megszerzése, megőrzése és bemutatása fajtánként eltérő utat jár be. Különösen igaz ez az elektronikus bizonyítékok életciklusára. Bizonyos esetekben a keletkezéskori megszerzés az egyetlen lehetőség. A tárolás sok esetben a bizonyíték minőségének romlását okozza. Példaként idesorolható az elkövetők közötti rádiókommunikáció, a számítógép memóriájában vagy a felhőben tárolt adatok csoportja. Utóbbi forenzikus megőrzésének problematikájával számos tanulmány[21] és monográfia[22] foglalkozik. A mobiltelefon használatának adatait a szolgáltató eszközei bizonyos ideig megőrzik, ezért ezek a tárolási idő végéig megszerezhetők.

---

20 Az Európai Bizottság Forlab *(Forensic Laboratory for in-situ evidence Analysis in a post blastscenario)* munkacsoportjának beszámolójában összegzi egy robbantási helyszín nyomrögzítési problematikáját és megoldási útjait. A lézeres 3D rögzítés lehetővé teszi a nyomok és az anyagmaradványok létének és helyének rekonstrukcióját. A nem GPS használatán alapuló rendszer tíz centiméter helymeghatározási pontosságot tesz lehetővé kül- és beltérben egyaránt. Az alkalmazott technológiák között említik a LIF *(Laser Induced Fluorescence)* lézeres pásztázó letapogató rögzítést, amely a műanyag- és polimertörmelékek észlelését végzi. Továbbá a LIBS *(Laser Induced Breakdown Spectroscopy),* amely a lézersugár segítségével pikogrammnyi anyagmennyiséget plazma állapotúvá hevít, s megállapítja összetevőit, valamint a vegyiparban használt Raman elemzőrendszert, amely lehetővé teszi a robbanóanyag maradványait tartalmazó töredékek elkülönítését a vizsgálat szempontjából jelentéktelen törmeléktől. Az ajánlott eszközök sorában említik még az NLJD *(Non-Linear Junction Detector)* berendezést, amely a helyszínen létező elektronikai eszközöket mutatja ki, függetlenül azok üzemelő vagy kikapcsolt állapotától. Lényeges elem, hogy a bizonyítékok azonnali továbbítása a nyomozást koordináló központba lehetővé teszi a helyszín távoli rekonstrukcióját, a valódi forrónyomon futó követést, a tettes azonosítását és utolérhetőségét. A rendszer további előnye, hogy képes a helyszín bűncselekmény előtti állapotának rekonstruálására is.
Forrás: https://cordis.europa.eu/result/rcn/191750_fr.html

21 Prasad Purnaye – Varshapriya Jyotinagar: Cloud forensics: Volatile data preservation. International Journal of Computer Science Engineering, vol. 4, no. 2, 2015

22 Rocky Termanini: The Cognitive Early Warning Predictive System Using the Smart Vaccine. The New Digital Immunity Paradigm for Smart Cities and Critical Infrastructure. CRC Press Taylor & Francis Group, Boca Raton, 2016

VII. A *kommunikációs osztályok szerint* is megkülönböztethetjük vezetékes vagy mobiltelefonnal, továbbá más rádióadóval[23] elkövetett, illetve támogatott cselekmények nyomait.

VIII. A forrásokat *tartalmi osztályokba* is sorolhatjuk. Lehetnek:

a) adatok;

b) metaadatok;

c) közvetlen; és

d) értelmezendő tartalmak.

Az *adatok* alosztályába a közvetlen tényeket sorolhatjuk.

A *metaadatok* az elektronikus adatba mélyebben beágyazott, a felhasználó számára általában rejtett adatok, úgymint az adat keletkezési körülményei, a létrehozóra utaló információ, és olyan további tény, amely a struktúra megalkotója szerint figyelemre tarthat számot. Itt említhetjük a digitális fotókat, amelyek tartalmazzák a készítés időpontját, a gép gyártóját és típusát, a felbontást, a színmélységet, expozíciós időt és az újabb eszközöknél – ha engedélyezték a készüléken GPS-t – a készítés pontos földrajzi koordinátáját. A szöveges üzenetek továbbításakor – tartalma mellett – a továbbítás és azok elolvasásának időpontja is kinyerhető a rendszerből. Mobilhívásnál a beszélgetésben részt vevő felek[24] telefonszáma és a beszélgetés hossza a telefonokról is megszerezhető. Az olyan információk, mint a beszélgetők földrajzi koordinátái, mozgásuk vektora, vagy még további bizalmas, rejtett adat már csak a szolgáltatók adattárából szerezhető meg. A vektoriális adatokból a közlekedési eszközre is következtetni lehet.

A *közvetlen tartalmak* alosztályán a szöveges, a hangos, a képi és a videóállományokból érzékeléssel megtudható bizonyítékokat értjük.

Az *értelmezendő tartalmak* alosztálya a *de facto* kódolt vagy titkosított információt, továbbá egy meghatározott korban és közösség körében jelentéssel bíró tényeket foglalja magában.[25]

IX. *Megjelenésük szerint* az elektronikus adatokat (bizonyítékokat) a következők szerint csoportosíthatjuk:

1. elektronikus hangbizonyítékok:

a) analóg formájú hangfelvétel;

b) digitalizált, vagy digitálisan rögzített hanganyag.

23 A három eszközcsoport közül az utóbbi szorul magyarázatra. Idesorolhatjuk a törvényesen birtokolt adóvevők alkalmazását bűncselekmény során. Jogsértő a sugárzás, ha az engedélyes az engedélyben vagy más korlátozásban meghatározott kereteket túllépve sugároz, vagy törvénysértő tartalmat közvetít adása során.

24 Konferenciabeszélgetés esetén kettőnél többen is részt vehetnek a társalgásban.

25 Utóbbira példa lehet a szlengkommunikáció korosztályonkénti változása, továbbá a gyűlöletbeszéd.

2. képi bizonyítékok:
   a) állóképes információ (arc, írisz, retina stb.);
   b) mozgóképes fix irányítottságú forrás[26];
   c) infrakamera (gyengén megvilágított környezet észlelésére);
   d) manuális követőrendszerrel megszerzett képi bizonyíték;
   e) mesterséges intelligenciával vezérelt mozgóképes képi követőrendszerek.
3. képalkotó rendszerek, amelyeken keresztül bizonyítékok szerezhetők:
   a) orvosi képalkotó rendszerek (dRTG, CT, MRI, fMRI stb.)[27];
   b) bűnügyi célú személyi testátvilágító rendszerek (THz frekvenciájú eszközök);
   c) infrakamera testhőtérkép készítésére[28];
   d) csökkentett energiájú csomagátvilágító röntgenkészülékek[29];
   e) föld alatti képalkotó rendszerek (például talajradar);
   f) földfelszíni képalkotó rendszerek (gépjármű-átvilágító rendszer);
   g) légköri képalkotó rendszerek (nem ellenőrzött légtérben mozgó eszközök bűnügyi célú felderítése és követése)[30].
4. elektronikusan észlelt szaginformáció[31];
5. rádiófrekvenciás bizonyíték:
   a) rádiófrekvenciás passzív felderítési információ;
   b) rádiófrekvenciás szemiaktív[32] bizonyíték (RFID[33]);
   c) rádiófrekvenciás aktív bizonyíték.

26 A bizonyítékgyűjtés tárgya a megfigyelt terület.

27 A fogászati röntgenek bizonyító ereje régóta ismert. A korszerű eszközök nemcsak az azonosítást teszik lehetővé, hanem az időbélyegző alapján a kérdéses személy alibijét is igazolhatják vagy cáfolhatják.

28 A testhőtérkép következtetési lehetőséget adhat a ruházat alatt elrejtett nagyobb tárgyakra, izgalmi állapot miatt megemelkedett testhőmérsékletre.

29 Az ipari röntgenek nagy energiájú változata anyagvizsgálati mérésekre szolgál. A csomagok átvizsgálása kisebb energiájú röntgensugárzással megoldott. A képalkotó rendszer a spektrális tulajdonságok alapján mesterségesen kiszínezi a csomag belsejében található tárgyakat.

30 A nem ellenőrzött légtér légiforgalmi irányítási fogalom. Ebben a légtérrészben a légiforgalom irányításáért felelős szervezet csak tájékoztatást ad, a légtér felderítése nem vagy csak korlátozottan lehetséges.

31 Már léteznek olyan beléptetőrendszerek, amikor a vizsgált személy kis méretű zsilipkamrán halad át, amelynek elszívott levegőjét érzékelőkkel elemzik, s vélelmezik a kábítószer- és robbanóanyag-mentességet.

32 A szemiaktív eszköz csak rádiófrekvenciás környezetben használható, a bizonyíték nyugalmi állapotában azonosításra nem. Megfelelő rádiófrekvenciás környezetben energiát von el. A nyert energiából rádiófrekvenciás sugárzással a rá jellemző adatokat kisugározza. Egyes esetekben, például az ellenőrzött állatfajoknál a kötelezően beültetendő eszköz hiánya megalapozza a bűncselekmény gyanúját (hamisítás, csempészés, lopás stb.).

33 RFID *(Radio Frequency IDentification)* olyan alkatrészbe, áruba vagy élőlénybe beépített eszköz, amely a dolog vagy élőlény saját tulajdonságát vagy tulajdonosi viszonyokat hordozó információkat

6. körülhatárolható informatikai környezetben létező bizonyíték[34]:
   a) informatikai adathordozókban és alkatrészekben (CD, DVD, USB kulcs, merevlemez stb.);
   b) intelligens mobilkommunikációs és számítástechnikai eszközökben (okostelefon, tablet, e-könyv, notebook, laptop stb.);
   c) szigetüzemű informatikai rendszerekben[35];
   d) wifit is tartalmazó kishálózatokban;
   e) közepes méretű tűzfallal védett informatikai rendszerekben;
   f) nagy kiterjedésű tűzfallal és VPN-nel[36] védett informatikai rendszerekben.
7. kibertérben létező bizonyítékok:
   a) nyílt interneten található adatok (Facebook, LinkedIn, Twitter, Videa stb.);
   b) illegális hálózatokon tárolt és továbbított adatok[37].
8. informatikai eszközökkel rekonstruált bizonyítékok;
9. a tevékenységet követő és rekonstruáló rendszerek bizonyítékai;
10. elektronikus nyomozások során feltárt, máshova nem sorolható bizonyítékok.

Összegzés

Meggyőződésünk, hogy az úgynevezett „második generációs" bizonyítékok körébe tartozó (büntetőjogilag releváns) elektronikus adatok (közöttük a digitálisak) titkos vagy nyílt kriminalisztikai módszerekkel történő hatékony

tartalmaz. Ilyennek tekinthetjük az áruvédelmi eszközöket vagy az állatazonosításhoz használt beültetett chipeket is.

34 A körülhatárolható informatikai környezetben a bizonyítékok megszerzése egyszerűbb. Megsemmisítésük esetén a tettes vagy tettesek személyi köre meghatározott. Mindamellett a külső behatolások bűncselekmény jellege – kivéve a hálózat biztonságosságának ellenőrzésére szolgáló jogszerű, úgynevezett *white hat* behatolásokat – rossz szándék *(black hat)* vélelmezését alapozza meg.

35 A szigetüzemű informatikai rendszerek jellemzője, hogy a vezetékes vagy vezeték nélküli eszközök a rendszeren kívüli más eszközzel nincsenek kapcsolatban. A rendszerben fellelt kriminális adat a hálózat használóival közvetlen vagy közvetett kapcsolatban van. A jogellenes informatikai behatolás fizikai jelenlétet igényel.

36 VPN: *Virtual Private Network,* vagyis virtuális magánhálózat.

37 Az ilyen hálózatokat üzemeltető személyek vagy szervezetek kiszolgálják a kábítószer-értékesítéssel és illegális fegyverkereskedelemmel foglalkozó bűnszervezeteket, továbbá létesítői és fenntartói a gyermekpornográfiára és a szórakoztatásra szánt szadista vagy megrendelt ölési cselekményeket bemutató oldalaknak.

felderítése, megőrzése, felhasználása nyomatékosan segítheti a bűnüldözőket, a „digitkommandókat", a kriminalisztikai piramis alapjában szereplő fő kérdések minél precízebb megválaszolását, a személy-, tárgy-, cselekményazonosításokat, az élesedő múltba nézést, a torzításmentes tükörtartást, végső soron a valósághű tényfeltárást.