

Az elektronikus adatok térhódítása Kamerás megfigyelés a személyes adatok védelmének hálójában

Absztrakt

A kamerás megfigyelőrendszerek kulcsfontosságú szerepet játszanak a bűncselekmények bizonyításában: akár képpel és hanggal, több látószögből rögzítik az eseményeket, segítik a történetek rekonstruálását, a tanúk beszámolóinak ellenőrzését, a bűnügy felderítését és a tettesek azonosítását. Az adatkezelésre vonatkozó kérdések folyamatosan felszínre kerülnek, mert a lefoglalt és a lefoglalással nem érintett elektronikus (és más) adatok kezelése, nyilvántartása, rendszerezése, tárolása és megsemmisítése, illetve a személyes adatok védelme önmagában is komoly kihívások elé állítja a jogalkalmazást. A digitalizáció begyűrűzése és az információtechnológiai eszközök fejlődése kétségtelenül megkönnyíti az életünket, de számos bizonytalanságot, ellentmondást és nem utolsósorban visszaéléseket hozott a felszínre.

Kulcsszavak: *információtechnológia, személyes adatok, kamerás megfigyelőrendszer, büntetőeljárás*

Abstract

The rise of electronic data. Camera surveillance in the net of personal data protection

Camera surveillance systems play a key role in proving crimes: they record events from multiple angles, whether with images or sound, they help reconstruct what happened, check witness accounts, investigate criminal cases, and identify criminals. Data management issues are constantly being brought to the surface, because the management, registration, systematization, storage and destruction of seized and non-seized electronic (and other) data, as well as the protection of personal data, in themselves pose serious challenges to law enforcement. The impact of digitization and the development of information technology tools undoubtedly make our lives easier, but it has brought many uncertainties, contradictions and, not least, abuses to the surface.

Keywords: *information technology, personal data, camera surveillance system, criminal procedure*

* Dr. Garai Renáta PhD, LL.M, tudományos munkatárs, OKRI. ORCID: 0009-0009-7211-5919.

A témakör jelentősége

A személyes adatok védelme és az online térben elkövetett bűncselekmények egyre szorosabb összefüggést mutatnak az elektronikus adatok kezelésével és azok eljárásjogi sorsával. Az internet felhasználásával történő bűnözésnek számos formája létezik (adathalászat, személyazonosság-lopás, online csalás, vírusok terjesztése stb.), mely esetekben az elkövetők az elektronikus adatokat és felületeket használják fel mások személyes vagy pénzügyi adatainak megszerzésére, valamint zaklatására, zsarolására. Nem kétséges, hogy a világszerte és folyamatosan előállított, óriás méretűvé duzzadt elektronikusadat-mennyiség (Big Data) az informatikai fejlődés újabb mérföldkövét jelentik, de ezzel egyidejűleg az adatvédelem területén is új kihívásokat hoztak létre, egyúttal további fejlődési lehetőségeket hordoznak magukban. (ORBÁN, é. n.) Az online és az offline világ viszonya egyre inkább összefonódik, és bár az emberek még próbálnak egyensúlyt teremteni a kettő között, úgy tűnik, az online győzedelmeskedni akar vetélytársa felett.

Az Országos Kriminológiai Intézetben *A lefoglalt elektronikus adatok kezelése és a személyes adatok védelme, a lefoglalt adatról készített másolat eljárásjogi megítélése és sorsa a büntetőeljárásban* címmel lefolytatott kutatásunk (GARAI – KISS, 2023) megannyi kérdést vetett fel: szakkérdés-e az adat azonosítása és kinyerése; miként zajlik a mobiltelefon, tablet, laptop szilárdtest-memória lefoglalása és adatmentése; milyen mértékben szükséges ügyészi és bírói szakértelem a másolatok felhasználása és megítélése során; miért elengedhetetlen a magas szintű informatikai tudás a jogalkalmazók körében, és még megannyi problematika akadt fenn a jogalkalmazás hálóján. Kiemelt hangsúlyt fektettünk az egyes jogok összeütközésére, így a terhelt iratmegismerési joga és a sértett emberi méltósághoz fűződő jogának viszonyára, különös tekintettel a nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények okán történt adatkezelésekre (fényképek, videófelvételek) és a visszaélészerű joggyakorlásra is. A kamerás megfigyelésekkel összefüggő anomáliákat azért helyeztük fókuszba, mert a jogszabályi háttér tükrében tévhitet kell eloszlatni a társasházakban felszerelt, vagy éppen a vendéglátóipari egységekben, szálláshelyeken, köznevelési intézményekben működtetett kamerák tekintetében, továbbá a konferenciákon és egyéb rendezvényeken történő kép- és hangfelvételt illetően.

Az információtechnológia fejlődése és a kiberbiztonság fontossága

Kijelenthetjük, hogy az internet nélkülözhetetlen eszközzé nőtte ki magát az információmegosztásban és a kommunikációban egyaránt (MUHI, 2017: 42), a tartalomfogyasztási szokások megváltozásával a számítógépek, mobiltelefonok és egyéb információtechnológiai eszközök az élet minden területén létfontosságúvá váltak (e-ügyintézés, oktatás, igazságszolgáltatási rendszerek stb.). A digitalizáció üteme megköveteli az informatikai tudásszint mértékének növelését, ezáltal összességében változtatta meg a hatóságok és bűnüldöző szervek korábbi hozzáállását, és tulajdonképpen az egész munkájukra hatást gyakorol. Figyelemmel arra, hogy a bűnelkövetők is felismerték az infokommunikációs technológiák előnyeit és az abban rejlő lehetőségeket (BŐCZNÉ, 2020), egy új típusú bűnözés jelent meg azáltal, hogy az elkövetések nagymértékben áthelyeződtek a virtuális térbe. (NAGY, 2016: 17) A világháló adottságainak kihasználásával elkövetett incidensek óriási károkat okozhatnak, az egyre inkább elburjánzó online csalások megrendítik a bizalmat, és mivel az online tér vonzereje töretlen, annak következményei olykor beláthatatlan méreteket öltenek. Az internetes levelezésre használt e-mailben szövegek mellett egyéb mellékletek is küldhetők, de a nemzetközi határokat átlépő és globális tényezővé vált közösségi média felületein történő kapcsolatfelvétel is megvalósulhat a másik fél akarata ellenére. A Facebook, Instagram, TikTok, YouTube, SnapChat vagy a Twitter kulcsfontosságú szerepet tölt be, fejlődésük akár a technikát, akár a felhasználók számát tekintve rohamosan halad előre. (PAPP, 2021: 7)

És most tegyük a szívünkre a kezünket: hogyan érezzük magunkat, ha ott-hon hagyjuk a mobiltelefonunkat? Ez bizonyára elő sem fordulhat, mert a „más világban” nemcsak ismeretterjesztő, szórakoztató vagy kikapcsolódást biztosító időtöltésre lehetünk, hanem pörögnek az események, zúdulnak az információk és a hírek, nem lehetnénk naprakészek, esetleg még lemaradnánk valamiről, vagy nem érnének el minket. Az ún. FOMO-jelenség (*fear of missing out*), vagyis a „kimaradás félelme” már nemcsak az Alfa- és Z-generációnál figyelhető meg, hanem a náluk idősebbeknél is (Y, Baby-boom). Ez egy létező, pszichológiailag kimutatható jelenség, melynek alapja az a félelem, hogy ha nem nézik állandóan a telefonjukat, akkor pótolhatatlan dolgokról maradnak le, a többiek beszélni fognak róla, ők pedig nem tudnak hozzászólni sem. Ezek lehetnek bagatell, érdektelen „történetek”, a lényeg az állandó online jelenlétben ölt testet. Egyetemi körökben a fiatalok arról számolnak be, hogy ez már olyan szinten vált szokássá és épült be a napi rutinjukba, úgy pörgetik végig – óránként többször – ugyanazokat a közösségimédia-platformokat, hogy észre sem veszik, mennyi időt töltenek valójában a telefonjuk képernyőjétől elvárásolva.

Megdöbentő látvány, ahogy mindenki szakadatlanul nyomkodja, fel sem nézve, átszellemülve, teljes mértékben beszippantva (járdán, gyalogátkelőhelyen, lépcsőn, gépjárművet vezetve). De észleljük az offline helyzetek veszélyeit, miközben az online térben lesben áll? Vajon merre viszi az emberiséget ez az irány, mi lesz velünk évtizedek vagy évszázadok múltán? Jövőbe látó képességünk hiányában erről csupán feltételezéseink lehetnek, de hogy elgondolkodtató életképek rajzolódnak ki, abban talán egyetérthetünk.

Végül, de nem utolsósorban meg kell említeni a mesterséges intelligenciát, ami jelentős innovációként léptette át az emberiséget a felfoghatatlan és bejósolhatatlan változások küszöbén. Ennek kapcsán talán nem a szabályozás nehézségei vagy a dogmatikai keretek szétfeszítése táplálják aggodalmainkat, hanem a gép és az ember viszonyának gyökeres átalakulásához kapcsolódó vélt vagy valós hatás okozta félelem generálja azt. (G. KARÁCSONY, 2020a: 145) A bűnmegelőzés egyik legfontosabb célja a bűnözés mennyiségi visszaszorítása, de a modern informatika szolgáltatásait mára egyetlen alkalmazási terület – így a különböző szervek, szervezetek és hatóságok, illetve az igazságszolgáltatás szereplői – sem nélkülözheti. (HORVAYNÉ – MUNK, 2011: 218)

Személyes adat, adatkezelés, elektronikus adatok és bizonyítékok

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679/EU rendelet, vagyis az *általános adatvédelmi rendelet* (a továbbiakban: GDPR) a természetes személyeket védi adataiknak a magánszektor és a közszféra nagy része által történő kezelése során. Az uniós adatvédelmi csomag másik fő eleme a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó, 2016/680/EU számú, ún. *bűnügyi irányelv*, amely a tagállami jogharmonizációk által biztosítja többek között, hogy az áldozatok, a tanúk és a bűncselekményekkel gyanúsítottak személyes adatai megfelelő védelemben részesüljenek, és megkönnyíti a határokon átnyúló együttműködést a bűnözés és a terrorizmus elleni küzdelemben. A modern technológia a személyes adatok minden eddiginél nagyobb mértékű kezelését teszi lehetővé olyan tevékenységek végzése érdekében is, mint a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy a büntetőjogi szankciók végrehajtása, ezért elő kell segíteni az illetékes hatóságok közötti információáramlást – többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése érdekében. A személyes adatok bűnüldözési célú kezelésére az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt (a továbbiakban: Infotv.)

kell alkalmazni, melynek rendelkezései nagyrészt egybeesnek a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) vonatkozó előírásaival, de vannak olyan területek, ahol az alapvető érvényesülések oltalmára további jogszabályalkotás indokoltsága fogalmazódik meg. (MÁNDI, 2023)

A büntetőeljárásban felmerülő *személyes adat* az azonosított vagy azonosítható természetes személyre (érintettre) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.¹ *Adatkezelésnek* minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, a közlés-továbbítás terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, az összehangolás vagy összekapcsolás, a korlátozás, a törlés, valamint a megsemmisítés.²

A Be. 165. §-a sorolja fel a bizonyítás eszközeit, amelyek a tanúvallomás, a terhelt vallomása, a szakvélemény, a pártfogó felügyelői vélemény, a tárgyi bizonyítási eszköz (ideértve az iratot és az okiratot is) és az elektronikus adat. A múltban történt események feltérképezése a nyomozás során történő digitális vagy egyéb bizonyítékok összegyűjtésében és a tanúvallomások értékelésében realizálódik: az információk felhasználásával igyekszünk a személyeket és az eseményeket időben és térben elhelyezni annak érdekében, hogy a bűncselekmények okait, módszereit a lehető legpontosabban, legprecízebben feltárjuk. (SIMON – GYARAKI, 2020: 126) A Be. és a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) is az „elektronikus” kifejezést használja, de a hazai és a nemzetközi szakirodalomban használatos „digitális” kifejezés éppúgy érvényes. A *digitális adat* lényegében kódolási eljárással jön létre, és alkalmas az elektronikus dokumentum előállítására és a dokumentum tartalmának azonosítására. *Digitalizálás* alatt azt a folyamatot értjük, melynek

¹ 2016/680 EU irányelv az Európai Parlament és a Tanács (EU) irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a továbbiakban: 2016/680 irányelv), 3. cikk, 1. pont

² 2016/680 irányelv, 3. cikk, 2. pont

során a korábban más (analóg) hordozón rögzített tartalmakat valamilyen eszköz segítségével a számítógép által értelmezhető formában kódoljuk, illetve rögzítjük a gép által olvasható adattároló eszközre. Ilyen digitális bizonyíték lehet a közösségi oldalak és különböző applikációk (Messenger, Viber, Skype, e-mail stb.) tartalma is, amelyek sokszor több információt hordoznak a hatóság számára, mint az elektronikus bizonyítékok; a tartalmakhoz történő hozzáférés nagyobb segítséget nyújthat, mint a kizárólag elektronikus úton keletkezett evidenciák. (SIMON – GYARAKI, 2020: 127)

Személyes jellegű adataink és féltve őrzött bizalmas információink számtalan módon kinyerhetők a digitális kommunikáció során, miként egy bekapcsolva hagyott számítógépbe vagy „nyitva hagyott” e-mail-fiókba történő betekintés is jogosulatlan kifürkészés. Mindezek célja és motívuma a tartalom megismerésén és az üzleti titoksértésen túl önös érdekeket szolgálhat (NAGY, 2020: 42–43), ezért nem lehet elégszer hangsúlyozni a fokozott óvatosság és körültekintés szükségességét. A Be.-ben 149-szer szerepel az elektronikus adat kifejezés, ekként a 205. § (1) és (2) bekezdése definíciót és értelmező rendelkezést is tartalmaz. E szerint *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. Ahol a törvény tárgyi bizonyítási eszközt említ, azon eltérő rendelkezés hiányában az elektronikus adatot is érteni kell.

Dilemmák és ellentmondások a kamerás megfigyelésekkel összefüggésben

A GDPR a személyes adatokat a kezelésük során használt technológiától függetlenül védi, vagyis a jogszabály „technológiasemleges”, és nem számít az sem, hogy az adatokat milyen módon tárolják. Személyes adatunk a név, lakcím, vagyoni helyzet, végezettség, okmányazonosító számok, egészségügyi adatok, képmás, hang, testalkat, és minden olyan információ, ami által beazonosíthatóak vagyunk, ami valamit elárulhat rólunk. Jártunkban-keltünkben már nem is tudjuk, hol figyelnek meg minket, a milliók által használt *Waze* navigációs alkalmazás valós idejű közúti figyelmeztetésekkel és naprakész térképekkel nyújt segítséget, ha pedig nekünk nincs is, másoknál foroghatnak a minket (és autónkat, rendszámunkat, hollétünket) rögzítő kamerák. Megfigyelés alatt lehetünk az utcákon, tereken, miként a vonaton, metróban, nyaralás közben, vagy bárhol, ahová elindulunk, és talán nem is gondolunk bele ebbe.

Számos büntetőeljárásban kerül sor a kamerarendszer adatainak lefoglalására, illetve azok tartalmának mint bizonyítékoknak a felhasználására. A *Nemzeti Adatvédelmi és Információszabadság Hatóság* (a továbbiakban: NAIH) ügyeinek jelentős részét teszik ki az ezzel kapcsolatos panaszok és kérdések, de a „szokásos” ügyeken túl az elmúlt években a hatóság az eddigiekhez képest eltérő szempontokat ítélt meg, illetve új értelmezési kérdésekben is határozott.³

Az igazságszolgáltatás által bizonyítékként felhasznált tartalmak

Az ügyészség és a rendőrség által megosztott – természetesen utóbb kiterjedve, elhomályosítva közzétett – kamerafelvételek kapcsán általában kétféle kommunikáció használatos: az egyik esetben azt láthatjuk a hivatalos honlapokon, hogy a „*térfigyelő kamera felvétele*”, máskor pedig, hogy a „*biztonsági kamera felvétele*”. Ez utóbbiakra minden esetben az adott kereskedelmi egység által üzemeltetett és a bűnüldöző hatóságok részére átadott (lefoglalt) külső biztonsági kamerák felvételei szolgálnak. A televízióban és az interneten egyaránt látható, hogy a hivatalos szervek számos alkalommal tesznek közzé olyan felvételt, amelyek segítségével nem a közterületi kamerának (mert az nincs), hanem éppen a mások által felszerelt külső kamerafelvételeknek köszönhetően történt a bűncselekmény rekonstruálása, majd az elkövetők beazonosítása.

Amint arra már több felsőbb bírósági döntés rámutatott, nem minősül jogsértésnek, ha a felvételt kizárólag ilyen célból használják fel, vagyis átadják azt a hatóságok részére. A személyhez fűződő jogok megsértése megvalósulhat hangfelvétel készítésével is, de például ha a szomszéd saját lakásában rögzíti a személyével kapcsolatos, falon keresztül áthallatszó kijelentéseket, ez a magatartás nem jelent más jogvéde érdekkörébe történő illetéktelen behatolást, jogsértést.

Az igazság érvényesülése közérdek, vagyis nem lehet az egyébként jogsértés nélkül készült hangfelvétel felhasználását visszaélésnek tekinteni, ha ez a készítőjével szemben elkövetett jogsértéssel kapcsolatos bizonyítás érdekében történik. (BH 1985.57.)

A más nyilatkozatát tartalmazó hangfelvétel akkor is felhasználható, ha személyhez fűződő jogok megsértésével keletkezett vagy jutott nyilvánosságra. (BH 2001.110.)

A rejtett kamerával készített videofelvétel a büntetőeljárásban bizonyítási eszközként, illetve bizonyítékként felhasználható. (EBH 2000.296.)

³ NAIH beszámoló a 2022. évi tevékenységről. <https://naih.hu/ev-es-beszamolok?download=648;naih-beszamolok-a-2022-evi-tevekenysegről>

Nem minősül visszaélésnek a képmás vagy hangfelvétel készítése vagy felhasználása, amennyiben arra közvetlenül fenyegető vagy már bekövetkezett jogsértés bizonyítása érdekében közérdekből vagy jogos magánérdekből kerül sor, feltéve, hogy a készítés vagy felhasználás a bizonyítani kívánt jogsértéshez képest nem okoz aránytalan sérelmet. (BDT 2011.2442.)

A fenti néhány iránymutató döntésből is következik, hogy amennyiben a kép-, illetve hangfelvételek felhasználása a tényállás tisztázása és az igazság kiderítése érdekében történik, a bűncselekmény sértettje nem kerülhet hátrányosabb helyzetbe, mint a bűncselekmény elkövetője. Ehelyütt nem releváns, de éppen a tanúk nélkül zajló családon belüli erőszakos bűncselekmények bizonyításánál kerül előtérbe a közvetett bizonyítékok szerepe, hiszen a terheltek tagadásával szemben éppen ezek a felvételek lehetnek bizonyító erejűek.

Menetrögzítő kamerák használata és a felvételek bizonyítékként történő felhasználása

A fedélzeti kamerák működtetése adatvédelmi szempontból igen összetett, mert azon kívül, hogy szórakoztatási célt szolgálnak (pl. vloggerek és bloggerek, úti beszámolók, bakifelvételek) vagyónvédelmi és bizonyítékrögzítő funkcióval rendelkeznek; természetes személyekről, azok cselekményeiről, és egyáltalán a közterületen zajló eseményekről is felvételeket készítenek. (VARGA, 2020) Akár autós, akár motoros vagy fejtűző sisakra szerelt kerékpáros készülékről van szó, a kamera használója adatkezelőnek minősül, a GDPR előírásainak történő megfelelés pedig kizárólag az ő felelőssége. Az adatkezelés akkor jogszerű, ha az az adatkezelő jogos érdekének érvényesítéséhez szükséges,⁴ ilyen tipikusan a közúti baleset körülményeinek bizonyítékául szolgáló felvétel. Ezen jogalap előfeltétele az ún. érdekmérlegelési teszt, és az átláthatóság elve mellett figyelemmel kell lenni arra is, hogy a bizonyítékgyűjtés céljából történő felvétel csak korlátozott ideig őrizhető meg, továbbá garantálni kell a személyes adatok védelmét a jogosulatlan hozzáférésekkel szemben. (BALOGH, 2023) Mindezek csupán az adatvédelem felszínét képezik, és mivel az állampolgárok többsége nincs tisztában a GDPR valamennyi részletszabályával, folyamatosan napirenden lévő kérdés, hogy felhasználhatóak-e a kétségtelenül kaotikus szabályozásnak teljes mértékben nem megfelelő, esetlegesen jogsértő módon készített felvételek?

Jelenleg sincsen olyan jogszabály, amely kifejezetten megengedné vagy tiltaná – elsődlegesen a gépjármű műszerfalára, a szélvédő mögé elhelyezett – a közúton (közterületen) történtek megfigyelésére és rögzítésére alkalmas kamerák

⁴ GDPR 6. cikk (1) bekezdés f) pont

elhelyezését. Az Infotv. rendelkezéseiből kiindulva adatkezelésnek minősül a fénykép-, hang vagy képfelvétel készítése,⁵ ezen törvény előírásait viszont nem kell alkalmazni természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire,⁶ bár ezt a kivételszabályt szűken kell értelmezni. Az Infotv. 2. § (4) bekezdése akkor jelenthet kivételt az Infotv. rendelkezései alól, ha az adatkezelés annak teljes időszakában a „saját személyes cél” fordulat alá tartozik. Ilyen például, hogy a kamera üzemeltetője csak magánszemély lehet, tehát nem mentesít az Infotv. hatálya alól, ha például a gazdasági társaság vagy más szervezet a tulajdonában álló, ám a munkavállaló által használt ún. „céges” autóba szerel fel kamerát. Fontos kiemelni, hogy a törvény alóli kibúvás csak a felvételek készítésére és tárolására vonatkozik, a rögzített felvételeken végzett további adatkezelési műveletekre (így különösen a nyilvánosságra hozatalra) már nem. Mindent összevetve megállapítható, hogy abban az esetben, amikor a kivételt képező kritériumok nem állnak fenn, a felvétel készítője adatkezelőként felel, annak minden kötelezettségével és ódiomával egyetemben.

Fő szabály szerint személyiségi jogot sértő bizonyítási eszköz a polgári perben nem használható fel, ugyanakkor a bíróság a körülmények mérlegelésével bármikor dönthet úgy, hogy a jogsértő bizonyítási eszközt mégis figyelembe veszi (pl. jogsérelem sajátossága és mértéke, tényállás felderítésére gyakorolt hatás).⁷ A NAIH állásfoglalása⁸ szerint a felvételek készítésének, tárolásának vagy nyilvánosságra hozatalának jogszerűségét el kell határolni annak bizonyítékként történő felhasználásától, egyúttal leszögezve: a személyes adatok védelméhez fűződő jog megsértésével készített (pl. rejtett kamerás) felvételek bizonyítékként történő felhasználása elsődlegesen nem adatvédelmi jogi kérdés. A bírói gyakorlat mind a polgári, mind pedig a büntetőeljárásokban számos esetben elfogadja bizonyítékként a személyiségi jogok megsértésével készített felvételeket, hiszen a Kúria már egy korábbi döntésében elvi élel mondta ki, hogy

bírósági vagy szabálysértési eljárásban közömbös az, hogy a felvétel készítése a személyiségi jogok megsértésével történt. A bíróság vagy más hatóság előtt folyó eljárásban az igazság érvényesülésének biztosítása közérdek és a bizonyítás ezt a célt szolgálja. (EBH 2000.296).

⁵ Infotv. 3. § 10. pont

⁶ Infotv. 2. § (4) bekezdés

⁷ A polgári perrendtartásról szóló 2016. évi CXXX. törvény (Pp.) 269. § (1) és (4) bekezdés; a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) 2:43. §

⁸ NAIH állásfoglalás a magánszemélyek által a saját gépjárműveikbe szerelt kamerák használatának jogszerűségéről. https://naih.hu/files/allasfoglalas_kamera_sajat_gepjarmuben.pdf

Vendéglátóipari egységnél üzemeltetett külső kamera

Az egyik üzlethelyiségre felszerelt kamerarendszer a közterületet és egy közeli társasház lakóinak mozgását is megfigyelés alatt tartotta. Az adatkezelő cég egy kávézót üzemeltetett úgy, hogy az üzlet előtti járdarészen teraszt hozott létre, ahová a vendégek és a személyzet testi épségének védelme, illetve a vagyontárgyak megóvása érdekében kamerákat szereltetett fel.

A hatóság álláspontja szerint a cég jogalap nélkül kezelte a személyes adatokat azzal, hogy az asztalokat megfigyelve a vendégekről folyamatosan képet és hangot rögzített, ami nem felel meg az arányosság követelményének. Az éjszaka és a rendes munkaidőn kívül üzemelő megfigyelőrendszer általában megfelel a vagyont fenyegető veszélyek elkerüléséhez, ezért ha az adatkezelés egyéb körülményei alapján igazolható a szükségesség és jogszerűség, arányos korlátozást valósíthat meg, de a hangrögzítés ezen időszakban sem tekinthető jogszerűnek. Mindezek miatt a hatóság kötelezte a vállalkozást, hogy megfelelő jogalap és tájékoztatás mellett üzemeltesse a kamerákat vagy szüntesse meg az adatkezelést.⁹

Társasházak, lépcsőházak kamerás megfigyelése

Kamerarendszer jogszerű célból akkor alkalmazható, ha az adott cél más módszerrel nem érhető el, a technikai eszköz alkalmazása elengedhetetlenül szükséges mértékű, és nem jár az információs önrendelkezési jog aránytalan korlátozásával. További követelmény, hogy a közös tulajdonban álló területek megfigyelését szolgáló kamerarendszer létesítéséről és üzemeltetéséről az összes tulajdoni hányad szerinti (és nem a lakógyűlésen megjelent) tulajdonosok legalább kétharmados többségének igenlő szavazatával dönthet a közgyűlés. Lényeges kritérium, hogy a szervezeti-működési szabályzatnak tartalmaznia kell a szükséges adatkezelési szabályokat, és a kamerák nem irányulhatnak a külön tulajdonban álló lakás vagy nem lakás céljára szolgáló helyiség bejáratára vagy más nyílászárójára, akkor sem, ha az a közös tulajdonban álló épületen, épületrészen vagy területen van elhelyezve.

Nem lehet elégszer hangsúlyozni, hogy a kamerákkal megfigyelt területre belépni, ott tartózkodni szándékozó személyeket tájékoztatni kell a személyes adatok védelmére vonatkozó előírások alapján szükséges információkról, így különösen az alkalmazás tényéről, az érintetteket megillető jogokról, az üzemel-

⁹ NAIH-88/2022. számú határozat

tető személyéről és elérhetőségeiről. Az ettől eltérő adatkezelés (jogsértés) egy konkrét esetben 200 000 forint összegű adatvédelmi bírságot eredményezett.¹⁰

Munkatársak és páciensek megfigyelése az orvosi rendelőben

Egy fogorvosi rendelő tulajdonosa a telephelyén és két fióktelepén is kamerával figyelte a munkavállalókat és a pácienseket, akikről nem csak várakozás közben, de a kezelés alatt is hozzájárulásuk nélkül készített felvételeket. Egy laborral és bőrgyógyászati rendelővel közös váróteremben, illetve a kezelőhelyiségben két-két kamera üzemelt; a falon lévő látószöge az egész kezelőre irányult, a másik pedig az asszisztensi pult fölött, a monitorra irányítva helyezkedett el. Az adatkezelő jogalapként a jogos érdekét, céljaként pedig a testi épség, személyi szabadság, üzleti titok és a vagyon védelmét, illetve a veszélyes anyagok őrzését jelölte meg.

A helyszíni vizsgálat során meggyőződtek arról, hogy a fogászati ellátásra érkezett pácienseken kívül a vérvételre és bőrgyógyászati rendelésre várakozó betegek is a kamerák látószögébe esnek. Az orvosi vizsgálattal érintett páciensekről készített felvételek már önmagukban is szolgáltathatnak szenzitív adatokat az egészségügyi állapotról, hiszen további információkat sugallhatnak a személyekről azáltal, hogy milyen típusú rendelésre várakoznak.

Fontos hangsúlyozni, hogy a hatóság nem észlelt a váróteremben olyan értékes tárgyat (italautomatát, külső recepciós pultot, számítógépet, festményt, bútort stb.), amely tárgyak megfigyelése megfelelné a vagyonvédelmi célnak, és ebből az indokból a kamerák a védendő vagyontárgyakra irányulnának.

A hatóság korábbi állásfoglalásai során is rögzítette, hogy a kamera nem mutathatja/rögzítheti azonosítható módon a páciens kezelés közben, kivéve annak kifejezett írásos hozzájárulása esetén (például tudományos, oktatási célból). A páciensek a belépésüktől kezdve a kezelés végéig felismerhetőek és beazonosíthatóak voltak, és legfeljebb akkor/addig nem látszódtak, amikor a kezelőorvos éppen kitakarta őket.

Egyebek mellett kitért a hatóság arra, hogy az egész napos megfigyelés az érintetti kör – a páciensek és a munkavállalók – közül leginkább a munkavállalók alapvető jogait érinti aránytalan és indokolatlan módon (folyamatos kontroll). A készpénz őrzése valóban indokolhatja a kamerás megfigyelést, de ebben az esetben a vagyonvédelem jogszerű célként kizárólag akkor lenne elfogadható,

¹⁰ NAIH-3463/2023. számú határozat

ha a kamera látószöge valóban csak a pénz átadására, illetve annak őrzési helyére irányulna. A hatóság az ügyben 500 000 forint adatvédelmi bírságot szabott ki.¹¹

Szálláshely területén működő kamerarendszer

Súlyos jogsértés történt egy balatoni szálláshelyen, ahol két egymástól elkülöníthető – egy csak élőképet közvetítő fix analóg kamerából álló, illetve egy képet és hangot egyaránt tároló IP-kamerából álló – kamerarendszer üzemelt. Az analóg rendszer kamerái a parkolót, illetve a kaputól a bejáratig terjedő sávot figyelték meg, míg az IP-kamerák a recepciót, az étkezőt, a belső udvart, valamint az épület teraszán elhelyezett jakuzzit. A jakuzzira irányuló kamerát olyan módon állították be, hogy az alkalmas volt a szomszédos ingatlanon tartózkodó személyek megfigyelésére is.

Az adatkezelő jogalapként szintén a jogos érdekét, céljaként pedig a személyes vagyónvédelmet jelölte meg. A hatóság az analóg kamerarendszer útján megvalósuló adatkezelést jogszerűnek találta, mivel a kamerák látószögébe kizárólag az ingatlan olyan részei estek bele, ahol a szállóvendégek csak áthaladnak, illetve ahol ténylegesen alkalmasak vagyónvédelmi célok betöltésére (az utcafrontról is látható kamerák visszatartó erővel bírnak az illetéktelen behatolással, illetve egyéb vagyon elleni bűncselekmények elkövetésével szemben). A hatóság ugyanakkor megállapította, hogy az IP-kamerából álló rendszer útján történő hangrögzítés jogellenes, mivel az adatkezelés az elérni kívánt céllal nem arányos, és annak szükségességét az adatkezelő az eljárásban sem igazolta. A hangrögzítés (még) nem feltétlenül tekinthető általánosan bevett vagyónvédelmi gyakorlatnak, így az érintettek tájékoztatás hiányában nem is számíthatnak arra, hogy képmásuk mellett a hangjukat, beszélgetéseiket is rögzíti a kamera. A hatóság az étkezőben lévő kamera elhelyezését sem tartotta az elérni kívánt céllal arányosnak, mert a vendégek elvárásaival ellentétes az, ha őket pihenés, kikapcsolódás, étkezés közben figyelik meg. A jakuzzit és a belső udvart figyelő kamera tekintetében ugyanezt hangsúlyozta a hatóság, mivel az érintettek nem voltak tisztában azzal, hogy őket ott kamerával megfigyelik, róluk felvétel készül intim szituációk közben. A recepció sávjában lévő kamera útján megvalósuló adatkezelés szükségességét a hatóság elfogadta, mert ott tényleges történik készpénzforgalom, illetve a pénzkazetta is a kamera látószögébe eső szekrényben került elhelyezésre.

¹¹ NAIH-903/2022. számú határozat

A hatóság mindent összevetve feltárta, hogy az adatkezelő nem nyújtott átlátható, könnyen hozzáférhető tájékoztatást az érintetteknek, illetve a közölt információk tévesek, félrevezetőek voltak. Mindezek alapján elrendelte az étkezőben elhelyezett, illetve a belső udvarra és a jakuzzira irányuló kamerák leszerelését, eltiltotta az adatkezelőt a további jogsértéstől, valamint 3 000 000 forint adatvédelmi bírság megfizetésére kötelezte.¹²

Szépségszalokban működő kép- és hangfelvevő rendszerek

Több bejelentés érkezett annak kifogásolásával, hogy egy arc- és testkezeléseket, valamint orvosesztétikai beavatkozásokat végző szépségszalokban minden helyiségben (irodában, kezelőben, folyosón, recepción) kamerák üzemelnek, melyeken keresztül mind a munkavállalókat, mind a vendégeket lehallgatják. A bejelentések szerint a hangfelvétel készítésének a munkatársak ellenőrzésén túli célja, hogy információkat szerezzenek a vendégekről, és ezek alapján még több kezelést és arcápoló terméket adjanak el nekik.

A tényállás tisztázását követően a hatóság megállapította, hogy a cég többek között a hangrögzítésre nézve jogsértő megfigyeléseket folytatott, emellett a kamerafelvételek felhasználása, a hozzáférés módja és belső szabályozása sem volt megfelelő. Feltárták többek között, hogy a társaság adatkezelési folyamatai átláthatatlanok, az adatbázisában szereplő több ezer bejegyzés vonatkozásában nem tudták igazolni az adatkezelés jogalapját, illetve jogszerűtlenül kezeltek különleges egészségügyi adatokat. A jogsértések miatt igen magas összegű, 30 000 000 forint adatvédelmi bírság kiszabására került sor, a hatóság egyes helyiségekben megtiltotta a kamerás adatkezelést, illetőleg elrendelte a videófelvételek, az egészségügyi adatok, valamint az ügyfélajánlás során keletkezett adatok törlését.¹³

Konferenciákon és egyéb rendezvényeken történő kép- és hangfelvétel

A Ptk. 2:42. § (3) bekezdése szerint nem sért személyiségi jogot az a magatartás, amelyhez az érintett hozzájárult. A Ptk. 2:48. § (1)–(2) bekezdése szerint képmás vagy hangfelvétel elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges, de erre nincsen szükség tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén. A hozzájárulás megadható szóban, írásban és ráutaló magatartással is, de mivel a szóbeli bizonyítása nehézkes

¹² NAIH-5114/2022. számú határozat

¹³ NAIH-2732/2023. számú határozat

vagy utóbb szinte lehetetlen, célszerű ragaszkodni az írásbeli és ráutaló magatartással történő hozzájáruláshoz. Az írásbeli hozzájárulás lehetősége számos program esetén a résztvevők nagy számára tekintettel teljesen kizárt, ezért a szervezők többnyire a ráutaló magatartással történő hozzájárulást részesítik előnyben a jogszerűsége törekvésben. Mindez természetesen csak akkor lenne tökéletes, ha az előzetes regisztráció folyamatába iktatott tájékoztatás és az ehhez kapcsolt checkboxban (jelölőnégyzetben) elhelyezett „pipa” vagy a hozzájárulás megadásának bármilyen más online formája lehetővé tenné a nyilatkozó kellő azonosítását. Azért csak „lenne”, mivel egyes rendezvényeken a regisztrálók általában több személyt/szervezetet regisztrálnak egyszerre, ekként nem vélelmezhetjük, hogy a természetes személyek (munkavállalók, meghívottak) nevében jogosultak nyilatkozni a képmás-felhasználásról. Ezek az adatkezelésre vonatkozó tájékoztató „szövegek” akkor megfelelőek, ha nemcsak a regisztrációt végző konkrét személyhez, hanem valamennyi résztvevőhöz eljutnak, ami viszont azért lehet problémás, mert általában csak a regisztrációnál megjelölt e-mail címre jutnak el, pedig lehet, hogy ez alatt jóval több természetes személy kap belépési lehetőséget. A másik megoldás egy, a beléptetési pont előtt elhelyezett, jól látható (pl. fényképező ikonnal jelölt) figyelmeztető szöveg (esetleg roll-up), amely – szemben az előbbi megoldással – valóban eljut minden belépőhöz. Fontos továbbá, hogy számos esetben nemcsak képfelvétel-készítéshez, hanem „kommunikációs” célú felhasználáshoz is hozzájárulást szeretnének kapni, ekként javasolt ezen célok bővebb kifejtése.

Példa:

„Felhívjuk szíves figyelmét, hogy a rendezvényen kép- és videófelvétel készül. A rendezvényre történő belépéssel hozzájárul ahhoz, hogy a közönség részeként Önről felvételek készüljenek, és ezeket a Szervező saját kommunikációs célból felhasználja, így például sajtóközleményben, kiadványban, honlapon vagy más hasonló marketinganyagaiban feltüntesse. A felvételekkel kapcsolatos adatkezelésről a [...] alatt részletesen tájékozódhat.”

Ahogy fentebb olvasható, tömegfelvétel készítéséhez és felhasználásához nem kell hozzájárulás, a bírói gyakorlat azonban nem egységes azzal kapcsolatban, hogy mi minősül „tömeg”-nek. Egy akár ötven embert ábrázoló felvétel sem feltétlenül tömegfelvétel, ha az olyan módon ábrázolja emberek sokaságát, hogy például egy bizonyos személyt előtérbe állít, kiemel. Ennek ellenére erre a szabályra vita esetén érdemben lehet hivatkozni, de ettől függetlenül nem teszi szükségtelessé a fenti tájékoztató, figyelmeztető szöveget. Ha teljesen precíz akarunk lenni, akkor valamennyi rendezvényszervezőnek egy tárhelyre felhelyezett és a tájékoztatóban megjelölt linken lévő bővebb tájékoztatást is készí-

teni kell, mivel a GDPR alapján a képmás személyes adat, így az adatkezeléssel kapcsolatban meg kell felelni a rendeletnek is. Ez a tájékoztató tartalmazza többek között a képek tárolásának módját, a hozzáférő alanyok körét, a tárolás és felhasználás idejét és az érintettek jogait.

Összegzés, konklúziók

Mindannyian elismerhetjük a technológia mélyreható és korántsem veszélytelen voltát, hiszen már nem is vagyunk tudatában annak, hogy napjaink jó részét – az offline világot háttérbe szorítva – virtuális környezetben töltjük. (SORBÁN, 2016: 81) Éppen ezért tartjuk rendkívül fontosnak a fiatalok online tudatosságra nevelését, mert visszajelzéseik alapján az online képernyő előtt eltöltött idejük ijesztő mértéket ért el (napi 4-6-8 óra). Minden korosztály jelen van a virtuális térben úgy, hogy a bűnelkövetők világszerte használnak digitális eszközöket bűncselekményeik végrehajtására. A kiberbűnözés tipikusan határokon átívelő jellege óriási leterheltséget és nehézséget okoz (DOMOKOS, 2020), illetve egyre kiterjedtebb, komplikáltabb és fennakadásokat jelentő globális problémákkal szembesíti a jogalkalmazást (POLT, 2018: 20). Az is nyilvánvaló, hogy a jogfejlődés következő lépéseit minden bizonnyal a technológiai fejlődés fogja vezérelni (G. KARÁCSONY, 2020b), ezért a tudományos következtetéseket is folyamatosan új tartalommal kell megtölteni (POLT, 2022: 2393), mert a digitalizáció hatása nagymértékben változtatta meg az igazságszolgáltatás működését és szokásait (VÁMOSI, 2022: 90–91). A számítógépes bűncselekmények esetszámának növekedési üteme az ilyen deliktumokra történő koncentrációt jelzi, a kiberkörnyezetben megvalósított bűncselekmények bizonyítása pedig döntő részben digitális adatokon nyugszik, amelyeknél a gyors hozzájutás, az adatok hiteles rögzítése és kezelése determináló jelentőségű. (BELOVICS, 2018: 28, 36) A bűnözés elleni harcot egyfajta ellenszélben folytatott, véget nem érő küzdelemhez hasonlíthatjuk, melynek során az adatok könnyen megsemmisülhetnek, eltűnhetnek, ráadásul másodpercek alatt megváltoztathatók, mozgathatók, reprodukálhatók vagy törölhetőek. Szabó Imre véleménye szerint ezért a siker kulcsa a hatékonyságban és a nyomozás titkosságában rejlik. (SZABÓ, 2011: 13) Éppen az információtechnológiai eszközök vonatkozásában történt a legtöbb módosítás a régi Be. szövegéhez képest, de ezzel egyidejűleg megválaszolendő kérdések tömkelege jelentkezett: Mit tekinthetünk számítógép útján való előterjesztésnek? Az egyéb elektronikus eszközök (pl. mobiltelefon) számítógépnek minősülnek? Elvárható az eljárás résztvevőjétől, hogy használjon számítógépet és rendelkezzen az elektronikus ügyintézéshez szükséges valamennyi berendezéssel? (HERKE, 2019: 104–105) Milyen mértékű és mélységű informatikai tudásra

van szüksége a rendőrnek, ügyésznek és a bírónak a vele szemben támasztott követelményeknek való megfeleléshez? Hogyan tudja ellátni a munkáját, ha nem képes maradéktalanul elsajátítani az informatikusok számára is sokszor fejtörést okozó ismereteket?

Az elektronikus adatok és bizonyítékok térhódításával a kamerás megfigyelés szabályai ugyancsak homlokterbe kerülnek, mert az adatvédelem hálójában olykor tényleg nehéz kibogozni az adott szituációra vonatkozó rendelkezéseket. A térfigyelő és biztonsági kamerák gyakorlati haszna vitathatatlan, emellett a felelősség megállapításában is segítenek a „digitális szemek”. Az ilyen felvételek keletkezésének jogszerűségét és az adatkezelő tevékenységét azonban meg kell különböztetni a bizonyítékként történő felhasználásuktól: a jogsértő módon történő adatkezelés nem vitásan adatvédelmi bírságot vonhat maga után, de ez nem jelenti azt, hogy az igazság napvilágra kerülése, az elkövető azonosítása és a bűncselekmény bizonyítása érdekében ezeket a felvételeket ne használhatnánk fel az egyes eljárások keretében. Ebben a tekintetben Európa számos országában változások következtek be, és egyre inkább úgy tűnik, hogy a személyes adatok védelménél bizonyos esetekben erősebbé válik a bűnüldözési érdek. (MÁTYÁS, 2017: 91)

A téma kapcsán legfőbb konklúzióink az lehet, hogy:

- folytonos éberséggel, a tendenciákra történő odafigyeléssel, önkontroll beiktatásával és óvatossággal járjunk el az online térben (és erre hívjuk fel az idősebb korosztály figyelmét is);
- személyes adataink védelme érdekében mindenkor legyünk figyelmesek és körültekintőek, a nem kívánt hatások érdekében tájékozódjunk az adatvédelemmel összefüggésben;
- bővítsük folyamatosan az informatikai tudásunkat (az igazságszolgáltatás szerveinek érdemes erre képzéseket és oktatásokat szerveznie);
- a kamerarendszerek működtetése során is törekedjünk a jogszabályi rendelkezések maradéktalan betartására;
- átlagemberként, illetve az igazságszolgáltatás szereplőjeként pedig ne engedjük el ezeket a kincsként funkcionáló bizonyítékokat, vagyis a gyakran mással nem pótolható kamerás felvételeket.

Felhasznált irodalom

- BALOGH B. (2023): A menetrögzítő kamerák alkalmazásának adatvédelmi aspektusai. *Jogi Fórum*, október 30. <https://www.jogiforum.hu/cikk/2023/10/30/a-menetrogzito-kamerak-alkalmazasanak-adatvedelmi-aspektusai/>
- BELOVICS E. (2018): A kiberbűnözés elleni harc szerepe és jelentősége napjainkban. Együtműködések és megoldások. In: BARABÁS A. T. (szerk.): *Globális Biztonságpolitikai kérdések az interneten, különös tekintettel Kína és Magyarország kapcsolatára*. Budapest: Országos Kriminológiai Intézet, 28–37.
- BÓCZNÉ NEPARÁCZKI A. (2020): A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja*, 1. szám, 71–85.
- DOMOKOS A. (2020): A magyar büntető eljárás és a digitalizáció. Miskolci Jogi Szemle, 15. évf., 1. szám, 67–76. https://www.mjsz.uni-miskolc.hu/files/10813/11_domokosandrea_tordelt.pdf
- G. KARÁCSONY G. (2020a): *Okoseszközök – okos jog? A mesterséges intelligencia szabályozási kérdései*. Budapest: Dialóg Campus. https://tudasportal.unike.hu/xmlui/bitstream/handle/20.500.12944/16020/Web_PDF_Okoseszkozok_okos_jog_web.pdf?sequence=1&isAllowed=y
- G. KARÁCSONY G. (2020b): Inkább bízunk a robotokban? A mesterséges intelligencia döntéseieért való emberi felelősség kritikája. *Jog–Állam–Politika*, 12. évf., 31. különszám, 31–42. https://jap.sze.hu/images/lapsz%C3%A1mok/2020/K%C3%BC1%C3%B6nsz%C3%A1m/JAP_2020_KOLONSZAM_g-karacsony-gergely.pdf
- GARAI R. – KISS A. (2023): *A lefoglalt elektronikus adatok kezelése és a személyes adatok védelme, a lefoglalt adatról készített másolat eljárásjogi megítélése és sorsa a büntetőeljárásban*. Kutatási jelentés (II/B/19/2023), kézirat. Budapest: OKRI.
- HERKE Cs. (2019): A digitalizáció szerepe a büntetőeljárásban. In: MEZEI K. (szerk.): *A bűnügyi tudományok és az informatika*. Pécs: PTE ÁJK–MTA TK Jogtudományi Intézet, 104–124. https://jog.tk.hu/uploads/files/06_buntetojog_informatika_HERKECS.pdf
- HORVAYNÉ FEHÉR J. – MUNK S. (2011): A rendőrségi informatikai hálózat fogalma, rendeltetése. *Hadmérnök*, 6. évf., 2. szám, 217–226. https://www.matarka.hu/kliikk.php?cikkmutat=2328449&mutat=http://hadmernok.hu/2011_2_horvayne_munk.pdf
- MÁNDI V. (2023): A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata. *Büntetőjogi Szemle*, 1. szám, 54–63. https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202301_54-63o_MandiVeronika.pdf
- MÁTYÁS Sz. (2017): A térfigyelő kamerák alkalmazásának jogszabályi háttere. *Pécsi Határőr Tudományos Közlemények*, 19. szám, 85–91. <https://pecshor.hu/periodika/XIX/matyas.pdf>

- MUHI B. B. (2017): E-Marketing és a közösségi média. Lehetőségek, trendek. In: KISS F. (szerk.): *Tudomány és erő. Vajdasági magyar tudóstalálkozó 2016. Konferenciakötet*. Újvidék: Vajdasági Magyar Akadémiai Tanács, 42–47.
https://vmat.rs/wordpress/wp-content/uploads/2017/02/VMT_2016-Tudomany_es_ero-Kotet-Teljes-dolgozatok.pdf
- NAGY Z. (2016): Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarországnak! *Magyar Jog*, 63. évf., 1. szám, 17–24.
- NAGY Z.: (2020): A kiberbűncselekmények fogalma és csoportosítása. In: KISS T. (szerk.): *Kibervédelem a bűnügyi tudományokban*. Budapest: Dialóg Campus, 33–44.
https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf
- ORBÁN A. (é. n.): Big Data. NKE Közzolgálati Online Lexikon.
<https://lexikon.uni-nke.hu/szocikk/big-data/>
- PAPP J. T. (2021): *A közösségi média platformok szabályozása a demokratikus nyitvánosság védelmében*. Budapest: Wolters Kluwer.
- POLT P. (2018): Jogalkalmazói kihívások a kibertérben. Együttműködések és megoldások. In: BARABÁS A. T. (szerk.): *Globális Biztonságpolitikai kérdések az interneten, különös tekintettel Kína és Magyarország kapcsolatára*. Budapest: Országos Kriminológiai Intézet, 20–27.
- POLT P. (2022): Digitális fejlődés és büntetőjog – akkor és most. *Belügyi Szemle*, 70. évf., 11. szám, 2389–2393. <https://doi.org/10.38146/BSZ.2022.11.47>
- SIMON B. – GYARAKI R. (2020): Kiberbűncselekmények felderítése és nyomozása. In: KISS T. (szerk.): *Kibervédelem a bűnügyi tudományokban*. Budapest: Dialóg Campus, 121–150.
https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf
- SORBÁN K. (2016): A digitális bizonyíték a büntetőeljárásban. *Belügyi Szemle*, 64. évf., 11. szám, 81–96. <https://doi.org/10.38146/BSZ.2016.11.5>
- SZABÓ I. (2011): A számítástechnikai adat mint elektronikus bizonyíték. *Kriminológiai Tanulmányok*, 48. szám, 13–28.
https://www.okri.hu/images/stories/KT/kt48_2001_sec.pdf
- VÁMOSI V. C. (2022): Digitalizáció és büntetőjog, különös tekintettel a pénzmosás bűncselekményre. *Miskolci Jogtudó*, 3. szám, 84–93.
https://jogtudo.uni-miskolc.hu/files/20473/MJ2022_ksz8_V%C3%A1mosiV_final.pdf
- VARGA B. (2020): A Nagy Testvér mindent lát, avagy autós kamerák törvényes használata. *Autó pult*, március 10.
<https://autopult.hu/magazin/a-nagy-testver-mindent-lat-avagy-az-autos-kamerak-torvenyes-hasznalata.html>