

A TUDOMÁNY, AZ OKTATÁS ÉS A KÖZGYŰJTEMÉNYI KISZOLGÁLÁS ÚJ INFORMATIKAI SZINERGIÁI

**NETWORKSHOP 2026
35. Országos Informatikai Konferencia**

**2026. március 31–április 2.
Debreceni Egyetem, Debrecen**

Szerkesztette: Tick József, Kokas Károly, Holl András

**HUNGARNET Egyesület
Budapest, 2026**



HUN-REN
Magyar Kutatási Hálózat

NETWORKSHOP

Szerkesztette: Tick József, Kokas Károly, Holl András

Tipográfia és tördelés: Vas Viktória

Korrektúra: Danyi Melinda

Angol nyelvi lektor: Lukács Katalin

Networkshop 2026 konferencia előadásainak közleményei

Debreceni Egyetem, Debrecen

2026. március 31–április 2.

ISBN 978-615-6792-29-7

DOI: <https://doi.org/10.31915/NWS.2026>

Kiadja a HUNGARNET Egyesület
az MTA Könyvtár és Információs Központ közreműködésével

Budapest

2026

Borítókép: [freepik.com](https://www.freepik.com)

JOGI ÉS TECHNOLÓGIAI KIHÍVÁSOK AZ ELEKTRONIKUS MEGFIGYELÉSBEN A KÖZNEVELÉSI INTÉZMÉNYEKBEN

LEGAL AND TECHNOLOGICAL CHALLENGES OF ELECTRONIC SURVEILLANCE IN PUBLIC EDUCATION INSTITUTIONS

Dr. Albert Ágota LL. M
Karinthy Frigyes Gimnázium
dralbertagota@gdprszakszeruen.hu

Absztrakt

Az elektronikus megfigyelőrendszerek alkalmazása a köznevelési intézményekben az elmúlt években jelentősen megnövekedett, ideértve a kamerás megfigyelés, a biometrikus azonosítás és az automatizált beléptető rendszerek használatát is. De vajon a biztonsági, vagyoni védelmi vagy éppen adminisztratív célok mennyiben igazolják ezt az „innovációt”? Az új technológiák új problémákat teremtenek különösen azért, mivel az érintettek jelentős része gyermek, illetve kiszolgáltatott helyzetben lévő munkavállaló.

Jelen tanulmány áttekinti az elektronikus megfigyelés legfontosabb jogi és technológiai kihívásait a köznevelési intézményekben, különös tekintettel a GDPR alapelveire, a szükségesség és arányosság követelményére, valamint a biometrikus adatkezelések kockázataira. A tanulmány célja annak bemutatása, hogy a technológiai lehetőségek önmagukban nem elegendőek a jogszerűség igazolására, és az oktatási intézmények számára komplex adatvédelmi, adatbiztonsági és szervezeti megfelelési kötelezettségek keletkeznek.

Kulcsszavak: GDPR, elektronikus megfigyelés, CCTV, biometrikus adat, köznevelés, adatvédelem

Abstract

The use of electronic surveillance systems in public education institutions has significantly increased in recent years, including the use of CCTV systems, biometric identification technologies, and automated access control solutions. However, to what extent do security, asset protection, or administrative objectives justify this form of “innovation”? New technologies create new challenges, particularly because a significant proportion of the affected individuals are children or employees in vulnerable positions.

This study reviews the most important legal and technological challenges of electronic surveillance in public education institutions, with special focus on the principles of the GDPR, the requirements of necessity and proportionality, and the risks associated with biometric data processing. The aim of the study is to demonstrate that technological possibilities alone are not sufficient to justify lawfulness, and that educational institutions face complex obligations regarding data protection, information security, and organizational compliance.

Keywords: GDPR, electronic surveillance, CCTV, biometric data, education, data protection

1. Bevezetés

A digitális technológiák fejlődése az oktatási intézmények életére is kihat, és a köznevelési intézményekben is egyre gyakoribbá váltak a kamerás megfigyelőrendszerek, az elektronikus beléptető rendszerek és bizonyos esetekben a biometrikus azonosítási megoldások alkalmazása. Ezen rendszerek bevezetésének célja jellemzően a vagyonsvédelem, a személyi biztonság növelése, az illetéktelen belépések megakadályozása, illetve az intézményi incidensek kezelése.

A köznevelési intézmények azonban sajátos környezetet jelentenek nemcsak alapjogi, hanem adatvédelmi szempontból is. Az érintettek jelentős része gyermek, akik a hatályos adatvédelmi szabályozása alapján fokozott védelemre jogosultak. A gyermekek sok esetben nem képesek teljes mértékben felmérni az adatkezelések hosszú távú következményeit, illetve a jogaik érvényesítése terén is hátrányos helyzetben vannak, ezért az intézményekre fokozott felelősség hárul. A köznevelési intézmények ráadásul olyan intézmények, ahol a jelenlét és a részvétel sok esetben nem önkéntes jellegű, ezért az érintettek mozgástere korlátozott – és ez nemcsak a gyermekekre, illetve azok szüleire jellemző, hanem az intézményekben dolgozó munkavállalókra (pedagógusokra, valamint a pedagógusok munkáját segítő személyekre) is igaz, azaz az ő kiszolgáltatott helyzetükre is figyelemmel kell lenni az új technológiák bevezetésekor.

Az elektronikus megfigyelés technológiai fejlődése az utóbbi években új dimenziókat nyitott. A hagyományos CCTV-rendszereket egyre gyakrabban egészítik ki intelligens elemző funkciók, mozgásérzékelő algoritmusok, rendszámfelismerés, arcfelismerés vagy automatizált viselkedéselemzés. Ezek a rendszerek már nem pusztán rögzítenek, hanem képesek személyek azonosítására, események kategorizálására és automatikus döntések támogatására is úgy, hogy általánosan elérhetővé váltak a széles közönség (azaz jelen esetben az oktatási intézmények) számára is.

A technológiai fejlődés ugyanakkor gyakran gyorsabb, mint az intézmények adatvédelmi és szervezeti felkészültsége. Éppen ezért egy kamerarendszer telepítése első látásra „csak”

technikai projektnek tűnhet, valójában azonban komplex jogi, adatbiztonsági és szervezeti kérdéseket vet fel. Már a rendszer tervezési szakaszában felmerülhetnek olyan problémák, mint például a kamerák látóterének jogszerű kialakítása, a szomszédos ingatlanok érintettsége, a közös adatkezelés kérdése, az adatfeldolgozók megfelelő kiválasztása, illetve az érintetti jogok érvényesítésének módjai.

2. Az elektronikus megfigyelés adatvédelmi keretei

Az elektronikus megfigyelőrendszerek működtetése során elsődlegesen az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) alkalmazandó. Emellett relevánsak a tagállami adatvédelmi szabályok, a köznevelési szektorális jogszabályok, az adatvédelmi hatóság és az Európai Adatvédelmi Testület iránymutatásai, valamint a hazai és uniós hatósági és bírósági jogalkalmazás is.

A GDPR alapján a kamerafelvételek és biometrikus azonosítók személyes adatnak minősülnek, amennyiben azokon/azokkal egy természetes személy azonosítható vagy azonosítottá válik. Az arcfelismerésre vagy ujjlenyomatra épülő rendszerek esetében ráadásul a személyes adatok különleges kategóriájába tartozó adatok kezeléséről beszélünk, amelyre szigorúbb szabályok alkalmazandók. Éppen ezért, amennyiben kamerarendszert kívánunk telepíteni az intézményünkben, számos körülményt nem hagyhatunk figyelmen kívül. Jelen tanulmány célja ezen körülmények elemzése, a terjedelmi korlátok miatt nem a teljesség igényével.

2.1. A jogszerűség és átláthatóság követelménye

A GDPR egyik alapelve a jogszerűség, tisztességes eljárás és átláthatóság elve. Ez a gyakorlatban azt jelenti, hogy adatkezelőként jogszerűen kell eljárunk, valamint pontosan meg kell határoznunk a tervezett adatkezelésünk célját, jogalapját és körülményeit, azaz a megfigyelésünk nem történhet általános, korlátlan („parttalan”, „figyeljünk meg mindent és mindenkit”) vagy meghatározatlan (homályos, „majd utólag kitaláljuk”) célból. Amennyiben csak „biztonság” vagy „saját biztonság” céljából van szükségünk videokamerás megfigyelésre, az nem lesz kellően konkrét megfogalmazás és nem fogja alátámasztani a megfigyelésünk jogszerűségét.

A gyakorlatban ez mit jelent? Azt, hogy előre meg kell határoznunk – többek között, de nem kizárólag –, hogy milyen területeket akarunk megfigyelni, milyen célból történik majd a megfigyelés, kik férhetnek hozzá a felvételekhez, mennyi ideig őrizzük meg a felvételeket (adatokat), és milyen esetekben és hogyan használjuk fel a felvételeket.

Az átláthatóság követelménye alapján az érintetteket megfelelő módon tájékoztatnunk kell. Ez a tájékoztatás azonban nem merülhet ki egy, a bejárat közelében lehelyezett figyelmeztető piktogramban. Adatkezelőként részletes adatkezelési tájékoztatót¹ kell biztosítanunk, amelyből az érintettek (pedagógusok, gyermekek, egyéb, az intézmény területén dolgozó-tartózkodó személyek) és a szülők is pontosan megismerhetik az adatkezelésünk körülményeit, ideértve az adatkezelés céljait, az adatkezelő kilétét és az érintett jogainak meglétére és gyakorlására vonatkozó részletes tudnivalókat, valamint az adatkezelés legnagyobb hatásaival kapcsolatos információkat.

2.2. Célhoz kötöttség és funkcióbővülés

A GDPR célhoz kötöttség elvének megfelelően személyes adat csak meghatározott, egyértelmű és jogszerű célból kezelhető. Ez különösen fontos az oktatási intézményekben, ahol a biztonsági célból gyűjtött adatokat könnyen más célokra is fel lehetne használni. Gyakorlati problémát jelenthet például, ha a vagyonvédelmi célból telepített kamerákat munkavállalók vagy a diákok ellenőrzésre használjuk, a tanórákat megfigyeljük, illetve ez a megfigyelés a pedagógusok értékelésének eszközzé válik, valamint a beléptetési adatokat jelenléti vagy teljesítményelemzési célokra használjuk.

A modern rendszerek esetében különösen jelentős kockázat az úgynevezett „function creep”, vagyis a funkcióbővülés jelensége. Egy eredetileg egyszerű kamerarendszert – különösebb nehézségek nélkül – később arcfelismerő vagy viselkedéselemző funkciókkal egészíthetjük ki, amely már teljesen más adatvédelmi kockázati szintet jelent. Az, hogy egy CCTV rendszer képes bizonyos funkciókra, még nem jelenti azt, hogy az a funkció jogszerű.

2.3. Szükségesség és arányosság

A GDPR egyik legfontosabb adatvédelmi követelménye a szükségesség és arányosság elve. Az érdekek mérlegelése során nem elegendő arra hivatkoznunk, hogy a megfigyelési rendszerünk növeli a biztonságot, azt is bizonyítanunk kell, hogy a választott megoldás valóban szükséges, és nem létezik kevésbé korlátozó, a megfigyelték privát szférájába kevésbé behatoló alternatíva.

Az intézményünk főbejáratának kamerás megfigyelését indokolhatjuk például vagyonvédelmi vagy biztonsági célokkal, ugyanakkor az osztálytermek folyamatos megfigyelése, a diákok biometrikus azonosítása vagy az automatizált viselkedéselemzés már súlyos alapjogi kérdéseket vet fel, különös tekintettel például a tanítás szabadságára, valamint a biometrikus adatok kezelésének korlátaira.

¹ lásd EDPB 3/2019. számú iránymutatása a személyes adatok videoeszközökkel történő kezeléséről, az első szintű tájékoztatásnak (figyelmeztető tábla) információ-tartalma (114. pont), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_hu.pdf

A szükségességi-arányossági vizsgálat során figyelembe kell vennünk az adatkezelésünk célját, az érintettek körét, a kezelt adatok érzékenységét, az adatkezelésünk időtartamát, a megfigyelésünk intenzitását, valamint az esetleges alternatív megoldásokat. A szükségesség esetében az adattakarékosság elve is mindig irányadó, azaz a gyűjtött személyes adatoknak az adatkezelésünk céljai szempontjából megfelelőnek és relevánsak kell lenniük, és a szükségesre kell korlátozódniuk.

Adatkezelőként kötelesek vagyunk felmérni, hogy hol és mikor szükséges feltétlenül a videokamerás megfigyelés – például más megfigyelést tehet szükségessé a tanítási időn belüli és kívüli időszak, valamint az oktatási intézményben is tilos megfigyelni olyan területeket, amely a munkavállalók pihenésére, kötetlen beszélgetésére szolgál (például a tanári szoba). Hasonlóan azt is át kell gondolnunk, melyek a megfigyelésünk szükséges határai, és a megfigyelésünk szempontjából nem releváns területeket ki kell takarnunk (például mosdókba, öltözőkbe nem láthatunk be). Előfordulhat, hogy a kamerák látószögébe beleesik a szomszédos ingatlan területe, ekkor vagy kitakaráshoz (maszkoláshoz, kikockázáshoz) folyamodhatunk, vagy a megfigyelt terület használójával megállapodásban rögzíthetjük a megfigyelés körülményeit (például hozzájárulás, közös adatkezelésre vonatkozó megállapodás).

3. Biometrikus rendszerek és technológiai kockázatok

A biometrikus azonosítási technológiák alkalmazása az egyik legérzékenyebb terület az elektronikus megfigyelésen belül, mivel az arcfelismerés, az ujjlenyomat-azonosítás vagy más biometrikus megoldások olyan különleges személyes adatokat kezelnek, amelyek az érintettek egyedi azonosítására alkalmasak. A GDPR 9. cikkének (1) bekezdése tiltja a biometrikus adatok kezelését, illetve a (2) bekezdése fogalmazza meg ezen tiltás alóli kivételeket. Ezen kívül tagállami jogalkotás is szűkítheti az adatkezelők mozgásterét.

Az európai adatvédelmi gyakorlat több olyan esetet is ismer, ahol oktatási intézmények biometrikus rendszereinek alkalmazását kifogásolták. Egy katalán iskola például arcfelismeréses rendszert vezetett be a diákok jelenlétének ellenőrzésére. Az adatvédelmi hatóság álláspontja szerint ez a rendszer aránytalan volt, mivel a cél hagyományos módszerekkel is elérhető lett volna. Emellett az intézmény nem biztosított megfelelő tájékoztatást a szülők számára, és nem rendelkezett megfelelő adatfeldolgozási megállapodással sem. Hasonló vitákat váltott ki egy francia iskola arcfelismeréses beléptetőrendszere is, ahol az azonosítás egyes esetekben (például ikrek esetében) ujjlenyomat-kezeléssel egészült ki.

Az ilyen, biometrikus azonosítást alkalmazó rendszerek kapcsán felmerül a kérdés, hogy az oktatási intézményekben valóban szükséges-e ennyire intenzív megfigyelési technológiák alkalmazása, és a nemzetközi esetek közös tanulsága az, hogy az ilyen intézményekben a biometrikus adatok kezelése általában nem szükséges és nem arányos, azaz nem elfogadható.

Miért? A biometrikus adatok egyik legnagyobb sajátossága azon kívül, hogy egy adott személyt konkrétan beazonosítanak az, hogy azok nem módosíthatók. Egy jelszó vagy belépőkártya cserélhető, azonban az arckép vagy az ujjlenyomat nem, ezért például egy esetleges adatvédelmi incidens következményei hosszú távon fennmaradhatnak. Éppen ezért, amennyiben biometrikus adatokat kezelő rendszert szeretnénk alkalmazni, tisztában kell lennünk annak jelentős kockázataival, így például a jogellenes adatkezelés lehetőségével, a nem megfelelően alkalmazott jogalappal, a hozzájárulás érvénytelenségével, az elégtelen tájékoztatás kockázataival, az adatbiztonsági hiányosságok, a túlzott adatgyűjtés és az algoritmikus hibák és torzítások magas kockázatával.

Különösen problémás a hozzájárulás kérdése. Az adatkezelők szeretnek hozzájárulásra hivatkozni, azonban az oktatási környezetben nehezen biztosítható a hozzájárulás egyik alapkövetelménye, az önkéntesség, mivel a diákok és szülők sok esetben kiszolgáltatott helyzetben vannak. Hasonló probléma merül fel a pedagógusok és egyéb munkavállalók esetében is, ahol a munkaviszonyból (köznevelési foglalkoztatotti jogviszonyból) eredő alá-fölérendeltség megkérdőjelezheti a hozzájárulás valódi önkéntességét.

Az új generációs megfigyelőrendszerek gyakran mesterséges intelligenciára épülnek, és képesek lehetnek arcok automatikus felismerésére, mozgások elemzésére, viselkedési minták azonosítására, illetve rendellenes események automatikus jelzésére. Ezek a technológiák ugyanakkor számos és igen jelentős hibalehetőségeket hordoznak, például az algoritmusok téves azonosításokat eredményezhetnek, különösen rossz fényviszonyok, tömeges környezet vagy nem megfelelő tanítóadatok esetén. A hibás felismerések diszkriminatív következményekkel is járhatnak, bizalmatlanságot szülve és mérgezve az intézményünk légkörét.

A mesterséges intelligencia alkalmazása további kérdéseket vet fel az automatizált döntéshozatal és az emberi felülvizsgálat, mint követelmény tekintetében is. Különösen aggályos lehet, ha az oktatási intézményekben automatizált rendszerek alapján történik személyek gyanúsításának minősítése vagy bizonyos magatartások előszűrése, éppen ezért nemcsak a GDPR rendelkezéseit kell szem előtt tartanunk, hanem a mesterséges intelligencia alkalmazásáról szóló rendeletet² is.

A kockázatok csökkentése érdekében a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatot kell lefolytatnunk, mely során adott esetben ki kell kérnünk az érintettek képviselőinek véleményét, valamint az adatvédelmi tisztviselő szakmai tanácsát.

2 AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2024. június 13-i (EU) 2024/1689 RENDELETE a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet)

4. Adatbiztonsági és szervezeti kihívások

Az elektronikus megfigyelőrendszerek működtetése nemcsak adatvédelmi, hanem komoly adatbiztonsági kihívásokat is jelent. A kamerafelvételek és biometrikus adatok érzékeny információknak minősülnek, ezért megfelelő technikai és szervezeti intézkedéseket kell alkalmaznunk.

Az egyik legfontosabb kérdés, hogy ki férhet hozzá a felvételekhez és milyen feltételek mellett. A hozzáféréseket szigorúan korlátoznunk és minden hozzáférést dokumentálnunk kell. Szabályozniuk szükséges például a jogosultsági szinteket, a hozzáférés naplózását, a felvételek exportálását, a törlési folyamatokat, valamint az incidenskezelési eljárásokat.

A megőrzési idő meghatározása szintén kulcsfontosságú kérdés. A felvételek nem őrizhetők meg korlátlan ideig, és előre meg kell határoznunk a szükséges és arányos megőrzési időt.

A gyakorlatban a kamerarendszereket és beléptető rendszereket sok esetben külső szolgáltatók telepítik vagy üzemeltetik. Ez adatfeldolgozói jogviszonyt hozhat létre, amely a GDPR 28. cikkének megfelelő írásbeli szerződéses szabályozást igényel részünkről. További problémákat vethet fel a felhőalapú adattárolás alkalmazása, mely esetben is tisztában kell lennünk az adattárolás helyével, harmadik országba történő adattovábbítással, a szolgáltató biztonsági intézkedéseivel, valamint az incidenskezelési folyamatokkal.

Amennyiben oktatási intézményként nem rendelkezünk megfelelő informatikai és adatvédelmi erőforrásokkal ezen rendszerek teljes körű ellenőrzésére, az további kockázatokat eredményezhet.

5. Következtetések

Az elektronikus megfigyelőrendszerek alkalmazása a köznevelési intézményekben összetett jogi, technológiai és etikai kérdéseket vet fel. A gyermekek fokozott adatvédelmi védelme miatt az oktatási intézményeknek különösen körültekintően kell eljárniuk a megfigyelési rendszerek tervezése és működtetése során.

A technológiai fejlődés önmagában nem elegendő az adatkezelések jogszerűségének igazolására, a szükségesség és arányosság követelményének vizsgálata minden adatkezelés esetében elengedhetetlen. Különösen igaz ez a biometrikus rendszerekre és a mesterséges intelligencián alapuló megfigyelési technológiákra.

A jogszerű működéshez az intézményeknek megfelelő adatvédelmi dokumentációval, adatbiztonsági intézkedésekkel, adatkezelési tájékoztatókkal, hatásvizsgálatokkal és szerződéses garanciákkal kell rendelkezniük. Emellett fontos szerepe van az adatvédelmi tisztviselőknek és az intézményi tudatosság növelésének is.

A jövő egyik legfontosabb kihívása annak biztosítása lesz, hogy az oktatási intézmények a biztonsági és szervezeti célok megvalósítása mellett képesek legyenek megőrizni az érintettek alapvető jogait, különösen a gyermekek, a szülők és a munkavállalók (köznevelési foglalkoztatottak és egyéb munkavállalók) magánszférájának védelmét.