



# A megfigyelés paradigmája

## A kínai modell és globális hatásai

### The Paradigm of Surveillance: The Chinese Model and Its Global Impacts

**Tujner Viktória**

doktorandusz  
Nemzeti Közszolgálati Egyetem,  
Hadtudományi Doktori Iskola  
tujner.viktoria.barbara@stud.uni-nke.hu



**Tóth Levente**

Dr. PhD, szakmai igazgató, adjunktus  
TVT Vagyongvédelmi Zrt.  
Nemzeti Közszolgálati Egyetem,  
Rendészettudományi Kar  
toth.levente@uni-nke.hu



## Absztrakt

**Cél:** A cikk célja, hogy feltárja a megfigyelő társadalom koncepcióját, elsősorban Kína példáján keresztül, valamint elemezze annak globális hatásait a társadalmi kontroll és a technológiai fejlődés szempontjából.

**Módszertan:** A szerzők különböző kutatási tanulmányokból és szabványokból merített észrevételekkel tárgyalják a hatékony videómegfigyeléshez kapcsolódó technológiai feltételeket és emberi tényezőket.

**Megállapítások:** A kutatás megállapítja, hogy Kína megfigyelési rendszere nemcsak a belső politikai kontrollt erősíti, hanem globális trendeket is befolyásol a technológia exportjának és ezen keresztül a digitális autoritarizmus terjedésének köszönhetően.

**Érték:** A cikk hozzájárul a megfigyelési politikák megértéséhez, és rávilágít a globális hatásokra, amelyeket a technológiai fejlődés és a politikai döntések generálnak. Fontos alapot nyújt a jövőbeni kutatásokhoz és a politikai diskurzushoz.

**Kulcsszavak:** megfigyelés, digitális autoritarizmus, társadalmi kontroll, videó-megfigyelő rendszerek

A szerzők a kéziratot magyar nyelven nyújtották be. Benyújtás: 2024. 11. 07. Átdolgozás: 2024. 11. 19.  
Elfogadás: 2025. 01. 06.

## Abstract

**Aim:** The article aims to explore the concept of the surveillance society primarily through the example of China, as well as to analyze its global impacts in terms of social control and technological development.

**Methodology:** The authors discuss the technological conditions and human factors related to effective video surveillance, drawing insights from various research studies and standards.

**Findings:** The research finds that China's surveillance system not only strengthens internal political control but also influences global trends due to technology exports and the spread of digital authoritarianism.

**Value:** The article contributes to the understanding of surveillance policies and highlights the global impacts generated by technological advancements and political decisions. It provides an important foundation for future research and political discourse.

**Keywords:** Surveillance, Digital authoritarianism, Social control, Video surveillance systems

## Bevezetés

A modernkori társadalmak biztonságérzete jelentősen megváltozott a térfigyelő és infravörös hőkamerák, és legújabbban az objektum- és arcfelismerő algoritmusokat alkalmazó kamerarendszerek elterjedésével. Az előző évszázadban a hidegháború időszakában, különösen a szocialista tömb országokban, leginkább hangalapú, vagy besúgókon keresztül megvalósuló megfigyeléstől tartottak azok az állampolgárok, akik a rendszer számára vélt vagy valós fenyegetést jelentettek. Az 1990-es évektől a szórakoztatóipar termékeiben, például filmekben (Truman Show), illetve reality tv-műsorokban (Big Brother) is találkozhattunk éjjel-nappal „forgó” kamerákkal, vagyis folyamatos megfigyeléssel. A 21. században elmondhatjuk, hogy a megfigyelés gyakorlata velünk maradt, technológiai szempontból jóval magasabb szinten megvalósítva. Nemcsak a titkosszolgálatok módszereiről, vagy az emberek fantáziáját megmozgató, kíváncsiságot ébresztő „orwelli” koncepcióról beszélhetünk, hanem az állami akaratervényesítés és a rendfenntartás egyik legfontosabb eszközéről.

Folyamatosan használt okoseszközeinknek köszönhetően sokkal nehezebbé válik elrejtőzni a kíváncsi „szemek” elől. A weboldalak által használt sütik képesek nyomon követni online tevékenységünket, a telefonunk által vett GPS-jelek pedig fizikai hollétünkről is lenyomatot képeznek. Mivel ez a fajta megfigyelés nem

teljesen evidens vagy szembeötlő minden felhasználó számára, így legtöbbszörben nem kelt kellemetlen érzést. Az utcákat, közösségi tereket pásztázó kamerák azonban sokkal nyilvánvalóbban követik minden lépésünket a fizikai valóságban.

Amikor a megfigyelésre alkalmas technológiák biztonságérzetünkre gyakorolt hatásáról beszélünk általában két, egymással ellentétes vélemény jelenik meg, ez a kettőség pedig alapjaiban határozza meg a megfigyelésről szóló diskurzust: az egyik tábornak megnyugvást, biztonságérzetet ad, ha tudják, valahonnan figyelik, hiszen így azt is láthatják, ha segítségre van szükségük, vagy valami baj történik. A másik oldal feszeng a megfigyelés gondolatától, mivel a privátszféra megsértésének érzik, mintha valaki folyamatos kontrollt gyakorolna felettük (Lyon, 2001).

A legtöbb demokratikus berendezkedésű országban eddig – látszólag – helyt adtak ez utóbbi aggodalomnak. Mindeközben számos autoriter állam – pontosan az előbb említett biztonságérzetre hivatkozva – a rend fenntartását mindenek elé helyezve olyan megfigyelő rendszereket üzemeltetnek, melyek nemcsak céltalanul véletlenszerűen gyűjtik a hang- és videóanyagokat, hanem a kamerák arcfelismerő képességének köszönhetően pontosan tudják követni az adott személyeket, akár név szerint beazonosítva (Qiang, 2019).

Az alábbi cikk fő célja, hogy részletesen bemutassa az említett megfigyelő társadalom koncepcióját, különös figyelmet fordítva Kína példájára. Az ország politikai kontextusában a felügyeleti rendszerek nem csupán technológiai újítások, hanem jelentős stratégiai ágazatot képviselnek, amely alapvetően befolyásolja a társadalmi és gazdasági struktúrákat. A cikk első részében a megfigyelő társadalom fogalmának mélyebb megértésére törekszünk, feltárva a Kínában alkalmazott különféle felügyeleti technikákat és rendszereket, valamint azok politikai és társadalmi hatásait. A cikk második felében a megfigyelő technológiák exportjára összpontosítunk, kiemelve, hogy ez a jelenség hogyan terjedt el más régiókban, és milyen következményekkel jár a globális szinten. Ezen kívül a technikai megvalósíthatóság kérdéseit is érintjük, elemezve, hogy a különböző országok miként alkalmazzák a megfigyelési technológiákat, és milyen etikai, jogi vagy technikai kihívásokkal néznek szembe. Az írás célja, hogy átfogó képet nyújtson a megfigyelő társadalomról, annak fejlődéséről és a jövőbeli trendekről, figyelembe véve a globális politikai és társadalmi változásokat.

## **Állandó felügyelet – A megfigyelő társadalom koncepciója**

Wood és munkatársai definíciója szerint a megfigyelő társadalom egy olyan típusú társadalom, amelyet megfigyelésalapú technikákkal szabályoznak (Wood

et al., 2006). Ilyen technikák lehetnek a közösségi terekben elhelyezett kamerarendszerek, biometrikus azonosítók társítása a személyazonosságot igazoló okmányokhoz, chipekkel ellátott útlevelek, de gondolhatunk akár a digitális lábnyomunkra is. Az internetes előzményeink, vásárlási szokásaink, telefonhívásaink mind lekérhetőek, lehallgathatók az illetékes állami titkosszolgálatok által. Akkor beszélhetünk továbbá megfigyelésről, amennyiben a részletes, személyes információk gyűjtése tervszerű, rutinszerű (folyamatos), rendszerszintű és célzott módon valósul meg, befolyásolás, irányítás vagy akár védelem céljából (URL1).

Összefoglalva tehát egy olyan társadalomról van szó, ahol az állampolgárokról bizonyos technológiákon keresztül közvetlen vagy közvetett módon folyamatosan képes a hatalom számára értékes információkat szerezni, illetve azokat valamilyen módon feldolgozni. Napjainkban a megfelelő eszközökkel erre minden fejlett ország (demokratikus és autoriter berendezkedésű egyaránt) képes lehet, így egy teljesen általános jelenségről beszélhetünk.

Ahogy a bevezetőben is említésre került, a megfigyelő társadalom nem a 21. század találmánya, az azonban kétségtelen, hogy a modernkori technológia sokkal könnyebben kivitelezhetővé, gyorsabbá és hétköznapibbá tette a megfigyelést. E tekintetben Kína abban különbözik az összes többi államtól, hogy sikerült valóban rendszerszintűvé tennie a különböző megfigyelési módszereket, amelyek alapjaiban határozzák meg a társadalom működését (Liang et al., 2018). Ezek a technikák teszik lehetővé a Kínában bevezetett, nyugati államok által élesen bírált „társadalmi kreditrendszer” működését.

## **Piros pont, fekete pont – A megfigyelésalapú kreditrendszer**

Ez a pontozáson alapuló rendszer az állampolgárok megbízhatóságát hivatott meghatározni, mely alapvetően – a megfigyelés gyakorlatához hasonlóan – szintén nem egy precedens nélküli koncepció, hiszen nyugati államok is folytatnak hasonló gyakorlatot. Az egyelőre országszinten sem egységesen működő kínai kreditszámitás, valamint az amerikai típusú hitelképességi pontszámok közötti különbség, hogy az előbbi nem csak pénzügyi korlátokat szabhat az állampolgároknak. A „büntetettek” számára korlátozhatják a tömegközlekedésben való részvételt, a vonatjegyek, repülőjegyek vásárlását, a magasabb besorolású szállodákban való tartózkodást, valamint kizárhatják őket oktatási intézményekből, nem vállalhatnak bizonyos munkákat, esetenként pedig nyilvános megaláztatás is vár rájuk (Creemers, 2018; URL2).

A hivatalosan 2014-ben indult projekt teljes kidolgozásának és a kreditrendszer egységesítésének határideje 2020-ban járt le (Liu, 2019). Ugyanebben az

időszakban, 2015-től 2020-ig zajlott az úgynevezett Sharp Eyes, vagyis „éles szemek” program,<sup>1</sup> melynek eredményeképpen 2017-re a világ legkiterjedtebb videómegfigyelési hálózata épült ki Kínában (Qiang, 2019). Nehéz megítélni, hogy 2024-ben hol tart az említett rendszerek tökéletesítésének és összehangolásának folyamata. Amit azonban egyértelműen láthatunk, hogy ezen projektek szoros összefüggésben állnak egymással: az egyre fejlettebb megfigyelésre alkalmas technológiák, például az „okosvárosokban” működő kamerarendszerek tökéletes alapot biztosítanak az állampolgárok viselkedésének folyamatos ellenőrzéséhez.

## **Totális kontroll vagy őrző szemek? – A megfigyelő társadalom előnyei és hátrányai**

Ahhoz, hogy a társadalmi kreditrendszer működőképes legyen, az államnak folyamatosan pontos, részletes információkat kell gyűjtenie a lakosokról. A nyilvános tereket figyelő kamerákban működő kifinomult tárgy- és arcfelismerő technológiának köszönhetően már a szabálysértés elkövetésének pillanatában rögzítésre kerülhet a tettes személyazonossága. Egy jól működő, automatizált rendszerben tehát azonnali „igazságszolgáltatás” történhet, az elkövető kredit-számának csökkentésével. Mivel a megfigyelés tudata önmagában elrettentő erővel bír és a kamerák jelenléte szerepet játszhat bizonyos bűncselekmények megelőzésében, ezért ezek a technológiák valóban elősegíthetik a rend fenntartását (Piza et al., 2019). A széles körű, folyamatos megfigyelés azonban ismét a korábban már említett dilemmához vezet bennünket, melyre csak és kizárólag a saját, szubjektív megítélésünk alapján adhatunk választ: mit jelent számunkra ez a technológia, biztonságot és békét, vagy a magánélet teljes porba tiprását?

Ahhoz, hogy felmérjük milyen előnyökkel, illetve hátrányokkal jár egy megfigyelő társadalom kiépítése, két külön nézőpontot kell megvizsgálnunk. Egyrészt az államét, vagyis Kína esetében a Kommunista Pártét (KKP), illetve a lakosságét. Az egyértelműen autoriter módszerekkel operáló KKP számára a megfigyelő technológiák lehetővé teszik, hogy ebben az elrettentésre alapuló rendszerben fegyelem és rend legyen, mely egybecseng a Community of Shared Future for Mankind (Közös Jövő Közössége, CSFM) (Hui, 2019), illetve a Global Security Initiative (Globális Biztonsági Kezdeményezés) (URL3) koncepciókban megfogalmazott célokkal. Kína az említett kezdeményezésekben

---

1 A Sharp Eyes projektet a 2005-ben indult Skynet program előzte meg, melynek célja szintén a videó-megfigyelő technológiák fejlesztése volt.

foglaltak szerint vezető szerepet vállal egy új, békésebb és biztonságosabb világrend megteremtésében. A megfigyelő társadalom létrehozásával Peking bizonyíthatja alkalmasságát erre a szerepre a teljes nemzetközi közösség, valamint a szimpatizáns országok előtt.

A lakosság szempontjából, amennyiben hajlandóak alkalmazkodni a rendszerhez (vagy rákényszerítik annak elfogadásra), szintén előnyként említhetjük, hogy a megfigyelés elrettentő ereje csökkentheti a bűnözést, növelheti a biztonságérzetet. Ha ismerik a szabályokat és betartják azokat, előnyökhöz juthatnak és kiszámíthatóbb életet élhetnek. Kína esetében bizonyos csoportok egészen biztosan kiszolgáltatott helyzetbe kerülhetnek, és inkább a rendszer célkeresztjében érezhetik magukat. Ilyen csoport például a muszlim vallású ujjur kisebbség (URL4). A jutalmak és büntetések rendszeréről a KKP dönt, így a társadalmi kreditpontszámok megítélése is egyértelműen a vezetők belátása szerint alakulhat. Előfordulhat, hogy a rendszer más ellenségei, kisebbségek vagy kritikusok tettei súlyosabb elbírálás alá kerülnek, a kiterjedt megfigyelő rendszerek pedig nem engedik, hogy ezek a csoportok észrevétlenek maradjanak.

Az előnyöket és hátrányokat vizsgálva jelenleg azt láthatjuk, hogy a mérleg nyelve inkább az állam felé dől. Ezen aránytalanság mértéke nagyban függ attól, milyen magasszintű megfigyelési technológiákat képesek országszinten alkalmazni, illetve mennyire hatékonyan dolgozzák fel az óriási mennyiségű beérkező adatot.

## Megfigyelés a gyakorlatban

Az 1980-as évek végén a Siemens Plessey<sup>2</sup> korszerű, amerikai Pelco kamerával ellátott Scoot megfigyelő rendszert exportált Kínába. A Tienanmen téren elhelyezett kamerák azonban nem csupán megfigyelési célokat szolgáltak. Az 1989-es diáktüntetést követően a tömegről készült felvételeket többször is sugározták a kínai televízióban, jutalmat kínálva olyan információért, aminek eredményeként szinte az összes rendbontót azonosították (Klauser, 2017).

Az 1990-es évek vége óta a Kínai Kommunista Párt hangsúlyozza a hazai társadalmi stabilitás fenntartásának kritikus fontosságát, és jelentős adminisztratív és pénzügyi forrásokat fordít erre a célra. A videómegfigyelő kamerák kiterjedt hálózata a pártállam azon törekvésének egyik legszembevetőbb megnyilvánulása, hogy figyelemmel kísérje polgárait. A kormány olyan cégekkel működik

---

2 A Plessey Company plc egy brit elektronikai, védelmi és távközlési vállalat volt, melyet 1989-ben a GEC és Siemens által létrehozott konzorcium vásárolt fel.

együtt, amelyek arcfelismerő és mesterséges intelligencia technológiákat kínálnak, lehetővé téve, hogy az összegyűjtött adatokból fontos információkat, például arcokat, életkorokat, rendszám táblákat és egyéb releváns adatokat nyerjenek ki (Cai, 2019; Tóth, 2024). Ennek következtében a kínai magánbiztonsági termékeket gyártó cégek globális szinten egyre erősödnek (például Hikvision, Dahua). A fejlődésüket tekintve fontos mérföldkő a 2010-ben elfogadott biztonsági szolgáltatásokról szóló törvény, amely a vagyonvédelmi cégek típusait határozza meg, és mindkét fő típus alapításánál alapfeltétel az 51%-os állami tulajdon (URL5).

A mai Kínát „államkapitalistaként” jellemezhetjük, ami azt jelenti, hogy bár a gazdaság nagy része nyitott a piaci verseny előtt, az állam megtartja a stratégiai területeken működő vállalatok tulajdonjogát, és politikai ellenőrzést gyakorol a stratégiailag fontos vezető nagyvállalatok felett. A piacgazdaságra való áttérés következtében bekövetkezett tömeges migráció és privatizáció gyengítette a korábbi gyakorlatokat (mint például a „hukou” rendszer<sup>3</sup>), amelyek lehetővé tették az állam számára az emberek nyilvántartását és nyomon követését. A megfigyelés megerősítése és kiterjesztése érdekében a Közbiztonsági Minisztérium új technológiák felé fordult, és 2003-ban ténylegesen<sup>4</sup> elindította a Nemzeti Közbiztonsági Informatizálási Projektet, közismert nevén *Arany-pajzs Projektet*. A projekt célja egy országos, fejlett digitális megfigyelő rendszer létrehozása, amely lehetővé teszi az egyének azonosítását és tartózkodási helyük meghatározását, továbbá egy gombnyomással azonnali hozzáférést biztosít az állam számára a személyes dokumentumokhoz. A program hangsúlyos része a kiberszuverenitás fenntartása és a nemzetbiztonság biztosítása a külföldi weboldalakhoz való hozzáférés megakadályozásán, és az információáramlás ellenőrzésén keresztül.

Az első szakasz (2003–2005) három fő területre összpontosít:

- elektronikus lakossági adatbázis létrehozása, amely tartalmazza a személyi fényképeket, a személyi igazolványszámokat, a lakcímekeket és a család összetételét;
- offline személyazonosság-követés megvalósítása, nyomkövető berendezések telepítése szállodákban, internetkávézókban, vasútállomásokon, repülőtereken stb.;
- hálózat ellenőrzése, beleértve a fontos webhelyek, fórumok és közösségi oldalak figyelése, a társadalomra veszélyes tényezők időben történő jelzése,

---

3 A kínai „hukou” kifejezés magyarul „háztartási regisztrációt” jelent. A hukou rendszerben az egyéneket vidéki vagy városi lakosokként sorolják be származási helyük és családjuk regisztrált hukou státusza alapján. Ennek a besorolásnak messzemenő következményei vannak az egyének alapvető társadalmi juttatásokhoz és lehetőségekhez való hozzáférésére.

4 Eredetileg a projekttervet a Kínai Közbiztonsági Minisztérium 1998-ban ismertette.

valamint egyes, nemkívánatos webhelyek megtámadása vagy a közvélemény irányítása.

Miközben az internet és a vele járó információs technológia fontos a kínai gazdaság számára, pusztán létezése aláássa az ország politikai stabilitását. Kína folyamatosan arra törekszik, hogy egyensúlyt teremtsen e két cél között, és a kormány eltökélt szándéka, hogy ellenőrizze az online tartalmakat és polgárait abban a tekintetben, hogy milyen típusú információkhoz férnek hozzá.

2005 végén megkezdődött az *Aranypajzs Projekt* második szakaszának megvalósítása, amely a közúti térfigyelő kamerák telepítésére és a meglévő térfigyelő rendszerek integrálására összpontosított. Ennek a törekvésnek a mentén számos térfigyelő rendszer fejlesztését támogató program indult, mint például a *3111* kísérleti projekt, a *Safe Cities* projekt, a *Skynet* projekt és a 2015-ben induló *Sharp Eye*<sup>5</sup> projekt. A 3111-es kísérleti projekt keretében, 22 várost választottak ki, ahol térfigyelőkamera-rendszereket telepítettek a közterületeken. E városokat 2012-re már 660 megye és körzet követte, így a rendszer folyamatosan bővült, és egyre szélesebb körű megfigyelést tett lehetővé (Su et al., 2021). 2017-ben a kínai CCTV televíziós csatorna arról számolt be, hogy befejeződött a *Skynet* projekt, amely a húszmillió kameraszámával a világ legnagyobb videómegfigyelő rendszerét hozta létre (URL6). A nagyméretű háttértárakat is tartalmazó rendszer valós idejű megfigyelést biztosít a városi közbiztonság fenntartásának érdekében. A rendszer kiépítését elősegíti, hogy a kortárs társadalom szoros kapcsolatban áll a digitális technológiákkal, és ez megkönnyíti a személyes és viselkedési adatok gyűjtését és elemzését. Bár a felhasználók gyakran tisztában vannak ezen eszközök használatával járó kockázatokkal, sokszor nem értik meg az applikációk által kért engedélyek megadásának, valamint a személyes adataik lehetséges felhasználásának veszélyeit (Fornasier & Borges, 2023).

A 13. ötéves tervben<sup>6</sup> szereplő *Sharp Eye* program szintén sikeres befejezéséről számolt be a CPS China Security Network 2021 márciusában. Eredetileg a tervben Kína közterületeinek kamerák általi 100%-os lefedettsége volt a cél, erről azonban nem történt hivatalos említés. A beszámolóban ráadásul megemlítik, hogy úgy tűnik a programnak nincs vége, és a térfigyelő kamerák telepítése tovább folytatódik (URL7).

---

5 A Sharp Eye (éles szemek), kínai nevén Xueliang Project, utalás egy idézetre Mao Ce-tung egykori kommunista vezetőtől, aki egykor azt írta, hogy „az embereknek éles szemek vannak”, amikor olyan szomszédokat figyelnek meg, akik nem felelnek meg a kommunista értékeknek és eszméknek.

6 2016–2020 közötti időszak.



## A közösség ereje – A kínai lakosság bevonása

A Xueliang Project egy társadalmi összefogáson alapuló közterületet felügyelő és ellenőrző rendszer, mely ugyan rendelkezik városi, megyeszintű városi, illetve tartományi megfigyelő központtal, azonban a hatékonyság növelése érdekében a kameraképek felügyeletébe a lakosságot is bevonták. Ennek megvalósítására a meglévő kábeltévé hálózatra integrálják a közterületi térfigyelő kamerák képeit. Az otthoni megfigyelés kétirányú, egy esetleges inkriminált esemény észlelésekor a lakosoknak a tévé távirányítója segítségével lehetősége van jelzést küldeni a felügyeleti központba. A közterületi kameraképek nemcsak helyhez kötöttek, otthonról felügyelhetők, hanem az erre a célra kifejlesztett mobil applikáción keresztül is (Peterson, 2020). A különböző videómegfigyelő rendszerek finanszírozásának nagy része a központi költségvetésből származik, de a regionális önkormányzatok és városok is hozzájárulnak a fejlesztésekhez. Időnként a megyék megfigyelési kiadásai messze meghaladják az egyéb önkormányzati szolgáltatásokat (URL8).

A *ChinaFile* több mint 76 000 darab kormányzati közbeszerzési értesítő elemzéséből kiderült, hogy a térfigyelő rendszerek kiadásai a városok költségvetésének jelentős részét teszik ki. Például Zhoukou városának szerződéseit átvizsgálva, 2018-ban közel ugyanannyit költöttek a videómegfigyelő rendszerre, mint az oktatásra, és ez a volumen két és félszerese volt a környezetvédelmi programokra szánt összegnek. A lakosság rendszer iránti elköteleződését mutatja, hogy a fejlesztésekre és működésre szánt költségek egy része közadományból biztosított. Shandong tartományban, Linyi város lakói 13 millió jüant<sup>7</sup> gyűjtöttek össze a videókamerák teljes lefedettségének támogatására (URL9). Egy ilyen rendszer kiépítése során már nem támaszkodhatunk kizárólag a megfigyelő központokban dolgozó operátorok és az otthoni tévét figyelő lakosság percepcióis képességeire.

A különböző, normálistól eltérő események és viselkedésformák észlelésére, valamint a gépjárművek és a lakosság monitorozására intelligens képanalizáló szoftvereket is alkalmaznak. A rendszer mesterséges intelligenciával ellátott kamerái figyelik a gépjárművek mozgását és a gyalogosok viselkedését, nemét, ruházatát és magasságát. Végso soron az állam célja egy gigantikus online adatbázis integrálása egy mindent átfogó megfigyelő hálózattal, amely magába foglalja a beszéd- és arcfelismerést, a zártláncú televíziós rendszerből kinyerhető adatokat, a smart kártya és hitelkártya nyilvántartásokat, a gépjárművek GPS-alapú mozgásinformációit és az interneten végzett tevékenység

---

7 Hozzávetőlegesen 740 millió forint.

monitorozási adatait (URL10). Kína 14. ötéves terve, amely 2021–2025 között valósul meg, továbbra is kiemelt figyelmet fordít arra, hogy a helyi önkormányzatok még több biztonsági projektet indítsanak, hogy „*megerősítse a közbiztonság megelőzési és ellenőrzési rendszerének kiépítését*” (URL11). Több hatalom és társadalmi kontroll jut a helyi önkormányzatoknak, még több adat generálódik a társadalomról, és a lakosság is megfigyelheti egymást.

Ez a lakossági attitűd a kínai társadalom etikai nevelését leginkább uraló konfuciánus ideológia mentén alakult ki. A konfuciánus ideológia hangsúlyozza a kollektív értékek és a társadalmi harmónia fontosságát az egyéni jogokkal szemben. Ez a kulturális perspektíva a megfigyelési gyakorlatok nagyobb elfogadásához vezethet a kínai társadalomban, mivel ezeket gyakran indokolják a közrend és biztonság fenntartásának eszközeiként. A konfucianizmus hagyományosan támogatja a tekintély és a hierarchikus struktúrák tiszteletben tartását. Ez a kulturális háttér hozzájárulhat az állam által vezetett felügyeleti kezdeményezések társadalmi elfogadásához, mivel ezeket a hatóságok törvényes intézkedéseként tekintik a társadalmi harmónia és biztonság biztosítása érdekében.

## **Globális ambíciók – A megfigyelő technológiák exportja**

Ez az ideológia azonban nem csak Kína belpolitikájában jelenik meg. A konfuciánus eszmék, a béke, rend és biztonság megteremtésének célja a Global Security Initiative,<sup>8</sup> illetve a Community of Shared Future,<sup>9</sup> kezdeményezések részét képezik. Annak érdekében, hogy Peking elérje célját és ambícióinak megfelelően békés nemzetközi környezetet biztosítson fejlődéséhez, Hszi Csin-ping kínai elnök 2013-ban elindította a *Belt and Road Initiative* (Egy övezet, egy út kezdeményezés, BRI) nevezetű globális külpolitikai kezdeményezést. A projekt fókuszában főként nehéz infrastruktúra-fejlesztési beruházások álltak (URL12). Kína több mint 120 milliárd dollárnyi hitelt nyújtott szerte a világon, nem csak fejlődő, de fejlett európai országok számára is (URL13).

A BRI szerves részét képezi a kínai technológia, és ezzel együtt a digitális autoriter módszerek exportálása (URL14). A kezdeményezés részeként Kína exportálja a szimpatizáns országok számára saját megfigyelő technológiáit, többek

---

8 A Globális Biztonsági Kezdeményezés a Kínai Kommunista Párt főtitkára, Hszi Csin-ping kezdeményezése. Célja, hogy olyan diplomáciai és biztonsági architektúrát építsen ki, amely felveszi a versenyt az Egyesült Államok által vezetett multilaterális szerződések, szövetségek és intézmények rendszerével.

9 A közös jövő globális közössége. Az emberiség közös jövőjével rendelkező közösség építése Hszi Csin-ping diplomáciáról szóló gondolatának alaplétele. Ez Kína megoldása arra a kérdésre, hogy milyen világot építsen és hogyan építsen.

között az okosváros projektek kiterjesztésével. A továbbiakban bemutatásra kerülnek az említett autoriter módszerek, valamint azok globális terjesztésének folyamata.

## **A digitális autoritarizmus mint termék**

Az autoriter módszerek alkalmazása a digitális térben is megengedi a KKP számára, hogy totális kontrollt gyakorolhasson a kínai lakosság felett, és folyamatosan ellenőrizze viselkedésüket. Az *Aranypajzs Projekt* egyik fontos pillérét jelentő kínai internetmodell egy zárt, szigorúan szabályozott rendszer, melyben az adatok egy ellenőrzött csatornán az állam felé futnak. Az úgynevezett „internetszuverenitás modelljét” más autoriter berendezkedésű államok is alkalmazzák, gyakran nyíltan vállalva, hogy Kína példáját követik (Gravett, 2020). A gyakorlatban ez az internetes tartalmak cenzúráját, az online szólásszabadság korlátozását jelenti. Ez a modell teszi lehetővé a KKP számára, hogy ne csak a fizikai térben, az offline valóságban, de az interneten is nyomom kövesse az állampolgárok tevékenységét, felkutassa a rendszer ellenségeit (Hillman, 2021).

Elsősorban ezek azok a módszerek, melyek vonzóvá teszik más hasonló berendezkedésű, gyakran harmadik világbéli országok számára a Kínával való együttműködést, a kínai technológiák megvásárlását (URL 14). A BRI-ben részt vevő országok számára ezek a „termékek” mind elérhetők: Peking biztosítja az eszközöket egy alternatív internetkormányzási modell megvalósításához bárhol a világon, ahol igény mutatkozik arra. Tanzánia kiváló példa erre az együttműködésre, ahol számos, kínai hitelből finanszírozott beruházás valósult meg, köztük az ország teljes telekommunikációs hálózatának fejlesztése (URL 15). Ezt követően 2015-ben érvénybe lépett az úgynevezett Cybercrimes Act, egy olyan szabályozás, mely nyíltan a kínai példát követi, miszerint az online térben fel kell venni a harcot a „*valótlan, illetve dekadens tartalmak*” terjedése ellen (Gravett, 2020). A tiltott, korlátozandó tartalmak alatt legtöbb esetben az aktuális hatalom érdekeivel szembemenő információkat kell értenünk.

## **Határon túli okosváros projektek**

Szintén kínai beruházásoknak köszönhetően egyre elterjedtebbé válnak az úgynevezett „okosváros” projektek, melyek elengedhetetlen részét képezik a közösségi tereket figyelő kamerarendszerek. Fontos megemlíteni, hogy 2019-es adatok szerint az említett beruházások jelentős része közepes vagy alacsony

jövedelmű, autoriter berendezkedésű, fejlődő országokban valósul meg (URL16). Nem szabad figyelmen kívül hagyni, hogy a kiválasztott országok többségében a liberális demokrácia fenntartásához szükséges politikai kultúra alapjai a poszt-koloniális korszak nagy részében (a legtöbb afrikai állam esetében nagyjából hat évtizedig) gyengék voltak.

A tekintélyelvű és félautoritárius uralkodók, többnyire külföldi nyomás hatására, a demokráciát imitáló intézkedéseket vezettek be. Ilyen látványos tevékenység a rendszeres (bár manipulált) választások és a hatalmi ágak de jure (és nem de facto) szétválasztása. Ebben a politikai környezetben a megfigyelés és ennek egyik technikai lába a videórendszerek sokszor a hatalmon lévők pozíciójának megtartását segítik. Sok országban a *Safe City* programba csomagolt, kedvezményes hitelekkel támogatott térfigyelő rendszerek mesterséges intelligencia által támogatott digitális megoldásokat tartalmaznak. Céljuk az olyan alapvető feladatok optimalizálása, mint a közlekedésirányítás, vagy a rendfenntartás (URL17).

A *Safe City* koncepció számos összekapcsolt nyomkövető eszközt, videokamerát, szoftvert és felhőalapú tárolórendszert használ a köz- és magánplatformok koherensebb módon történő összefogására az olyan közcélok előmozdítása érdekében, mint a rendfenntartás, a forgalomirányítás és az adminisztratív szolgáltatások egyszerűsítése. A rendszerek e hálózatahoz való hozzáférés látszólag növeli a rendőrök és a helyi hatóságok láthatóságát, akik így valós időben proaktívan nyomon követhetik a bűncselekményeket, és reagálhatnak azokra. Kínai vállalatok globális szinten több mint 60 országban, 350 különböző okosváros projekt megvalósításában vesznek részt (URL18). Ezek a beruházások összhangban vannak a CSFM koncepcióban meghatározott célokkal és értékekkel: egy alternatív, békésebb és igazságosabb világ megteremtésére való törekvéssel, ahol rend és fegyelem uralkodik.

Ahhoz tehát, hogy egy okosváros hatékonyan működjön, szükség van egy kiterjedt kamerarendszerre, mely folyamatosan adatokat gyűjt és dolgoz fel. A Pakisztánban található Lahorban – a Huawei támogatásának köszönhetően – már több mint 8000 darab IP-kamera<sup>10</sup> üzemel, Zimbabwében pedig a szintén kínai CloudWalk vállalat telepített hasonló rendszereket (URL18). Ezek a kamerák arc- és rendszámfelismerő funkciókkal is rendelkeznek, melyek segíthetik a rendfenntartó szervek munkáját a bűnözés visszaszorítása érdekében. Egyelőre nem létezik hasonló nyugati projekt, mely reális alternatívát jelenthetne a kínai okosvárosokkal szemben (URL17).

---

10 Az új típusú IP-kamerák internetes kapcsolaton keresztül (internetprotokolttal használva) továbbítják a beérkező adatokat, szemben a hagyományos, analóg jeleket használó CCTV kamerákkal.

A kezdeményezésben részt vevő országok jellemzői alapján valóban tekinthetünk ezekre a projektekre úgy, mint Kína által exportált (autoriter) állami akaratérvényesítési eszközökre, vagy akár magának a kínai megfigyelő rendszernek más régiókra történő kiterjesztésére.

## A kínai megfigyelő rendszer mint követendő példa

Mielőtt megvizsgálánk hogyan követik Kína példáját, és milyen digitális autoriter módszereket alkalmaznak a támogatott országok, fontos megjegyeznünk, hogy nem bizonyítható egyértelműen az összefüggés a kínai támogatás és az elnyomó rezsimek gyakorlata között. Mivel olyan államokról beszélünk, melyeket alapvetően hasonló elvek alapján működnek, mint a KKP, ezért nem mutatható ki ok-okozati összefüggés a kínai eszközök megvásárlása és az autoriter törekvések között. Azt azonban biztosan kijelenthetjük, hogy az olyan együttműködések, mint az okosváros projektek, elősegítik az említett rezsimek hatalmának fenntartását. A kínai megfigyelő rendszert így okkal tekinthetik követendő példának.

Tanzánián kívül számos példát hozhatunk fel olyan fejlődő országokra, melyek valamilyen módon digitális eszközök felhasználásával próbálják korlátozni az állampolgárok tevékenységét. 2019-ben a kampalai rendőrség 126 millió dollár értékben vásárolt zárt láncú televíziós kamera rendszert a kínai Huawei távközlési óriástól, a város növekvő bűnözésének visszaszorítására. Az ellenzék és a civil társadalom vezetői azt állítják, hogy az arcfelismerő technológián alapuló térfigyelő kamerákat ehelyett a kormánykritikusok nyomon követésére és megcélzására használják (URL19). Az országban a – nyíltan Kína-párti – miniszterelnök 2021-es újráválasztásakor több mint négy napra állította le az internetszolgáltatást országában abból a célból, hogy akadályozza a választási csalásról, valamint a fegyveres erők túlkapasairól (ellenzékiek meggyilkolásáról) szóló hírek terjedését a közösségimédia-felületeken (URL20; URL21).

Hasonló módszereket alkalmaznak egyes ázsiai államokban is, például Indiában. 2023-ban Punjab térségében 27 millió ember maradt offline négy teljes napon át, míg a rendőrség szeparatista felkelőket üldözött (URL22). Az említett példákon túl közterületi videómegfigyelő rendszer épült többek között Algéria, Angola, Botswana, Dél-Afrikai Köztársaság, Elefántcsontpart, Egyiptom, Ghána, Madagaszkár, Malawi, Mauritius, Mozambik, Namíbia, Nigéria, Ruanda, Tanzánia, Zambia, Zimbabwe – többnyire – fővárosaiban (URL23).

Ezek az államok tehát nem riadnak vissza olyan digitális autoriter módszerek alkalmazásától, melyek az információáramlás terjedését célozzák általában

olyan szituációkban, amikor ellenzéki, a vezetőkkel szemben kritikus kisebbség véleményét kívánják elhallgattatni. A Kínától beszerzett megfigyelő technológiák, valamint a társadalmi kreditrendszer megvalósítása nagyban segítené ezeket az elnyomó államokat, hogy felkutassák a rendszer kihívóit, így elejét vehetnék a lázadásoknak. Az okosváros projektek, tehát a folyamatos megfigyelés hivatalosan a közjót szolgálná, segítene fenntartani a rendet, megelőzni az erőszakos bűncselekményeket. Az autoriter berendezkedésű államokban pedig minden bizonnyal kijelenthetjük, hogy valójában csak még egy eszközt jelentene a jelenlegi rendszer fenntartására, a lakosság megfélemlítésére.

Az Afrikai Unió Kiberbiztonsági és Személyes Adatvédelmi Egyezménye 2014-ben jött létre, hogy keretet biztosítson a kiberbiztonság számára Afrikában. Ennek részeként a tagállamokat arra kéri, hogy alakítsanak ki nemzeti kiberbiztonsági politikákat, valamint jogi, szabályozási és intézményi kereteket a kiberbiztonság irányításához. Ha az érintett országok nem fordítanak kellő figyelmet az informatikai rendszereik biztonságára, az jelentős piaci versenyhátrányt okozhat a vállalatok, ezzel a teljes gazdaság számára (Takács & Tóth, 2024). Az egyezmény hatálybalépéséhez szükséges 15 ország ratifikálásához kilenc év kellett. Ez az elhúzódó szabályozás is az oka annak, hogy sok afrikai ország sebezhetővé vált a megfigyelési technológiák visszaéléseivel szemben.

## **Több mint üzlet – Mit nyer Kína az együttműködésekben?**

Kína visszautasítja azokat a vádakat, miszerint exportálja megfigyelési gyakorlatait. A 2018-as Pekingi Csúcs során a Kína–Afrika Együttműködési Fórum (FOCAC) keretében Xi elnök kifejezetten rámutatott az afrikai politikában alkalmazott „öt nem” megközelítésre, azaz nincs beavatkozás az egyes országok fejlődési útjaiba, nincs beavatkozás a belső ügyeikbe, nincs Kína akaratanak ráerőltetése, nincs politikai feltételekhez kötött segítségnyújtás, és nincs önző politikai nyereség keresése a befektetési és finanszírozási együttműködés során (URL24). Felmerülhet a kérdés, hogy akkor Kína mit nyer valójában a vizsgált beruházásokból, miért előnyös, ha saját megfigyelő technológiáját politikailag instabil, szegény fejlődő országokba exportálja.

Az egyik lehetséges válasz az üzlet, tehát anyagi haszonszerzés. A Huawei álláspontja szerint a vállalat csak értékesít, nem tud felelősséget vállalni az eladott kamerarendszerek felhasználási módja miatt (Hillman, 2021), vagyis semmilyen formában nincs beleszólása mire használják azokat. Azonban azt is látnunk kell, hogy a támogatott országokban ezek a projektek leggyakrabban Kínától kapott hitelekkel kerülnek finanszírozásra, így nincs azonnali profit,

a megtérülésre akár évtizedeket kell várni. Az okosváros projektek továbbá alkalmasak a mesterséges intelligencia-alapú arcfelismerési funkció tökéletesítésére: az Afrikában telepített kamerák idővel képesek lesznek megkülönböztetni a sötét bőrtónusú arcokat is, így ezt a terméket egyre több régióban adhatják majd el (URL23; URL18).

A kamerarendszerek kiépítésére más államokban úgy is gondolhatunk, mint Kína rendszerének kiterjesztésére abból a célból, hogy saját állampolgárait tartsa felügyelet alatt külföldön (URL25). Természetesen ez a hálózat más jellegű adatok gyűjtésére is alkalmazható: a korábban említett Huawei által megvalósított pakisztáni okosváros projekt során azzal vádolták a kínai vállalatot, hogy egy helyi rendvédelmi szervek munkáját segítő szoftver tesztelése közben a pakisztáni kormány számára érzékeny, nemzetbiztonsági kérdéseket is érintő adatokat gyűjtöttek be (URL26). Korábban szintén a Huawei-ről derült ki, hogy az Afrikai Unió központi épületébe telepített kamerarendszer felvételeit rendszeresen továbbították egy sanghaji szerverre (URL27). Arra a kérdésre, hogy Kína az összegyűjtött adatokat milyen módon használja fel, szintén nem lehet egyértelmű választ adni.

Láthatjuk, hogy a megfigyelő technológiák, illetve a begyűjtött nagy mennyiségű érzékeny adat igen sokféle, egyelőre nem bizonyított – vagy csak sejtethető – módon használható fel mind a fogadó országok, mind Kína által. Az egyik lehetséges magyarázat szerint mind a két fél jelentős hasznot húzhat az okosváros projektekből. A kínai technológiát megvásárló államok – akarva vagy akaratlanul – elfogadják a lehetséges negatív következményeket, a kínai kémkedés kockázatát annak érdekében, hogy saját állampolgáraikat folyamatos megfigyelés alatt tarthassák. Amennyiben a kínai termékek és módszerek széles körben elterjednek, akkor elmondhatjuk, hogy Peking egy lépéssel közelebb járhat a CSFM-ben meghatározott vízió eléréséhez, növelve befolyását új régiókban, és bebizonyítva, hogy a megfigyelő technológiák, vagy maga a megfigyelő társadalom koncepciója valóban egy értékesíthető termék, egy „brand”, melyre komoly kereslet mutatkozik.

## Összefoglalás

A cikk középpontjában a megfigyelő társadalom koncepciója áll, különös figyelmet szentelve a kínai gyakorlatnak. Az első rész a megfigyelő társadalom fogalmának mélyebb megértésére törekszik, feltárva a Kínában rendszerszinten alkalmazott különféle felügyeleti technikákat és rendszereket, valamint azok politikai és társadalmi hatásait.

Külön figyelmet kap a társadalmi kreditrendszer, amely az állampolgárok megbízhatóságát méri, és komoly következményekkel járhat a magánélet és a szabadság szempontjából. Látható, hogy a vizsgált rendszer elsősorban az állam érdekeit és céljait szolgálja, így csak másodlagosan tekinthetjük a közbiztonság és rendfenntartás hatékony eszközekének. Megvizsgálva Kína jövőbe mutató vízióit és terveit, egyértelművé vált, hogy a felügyeleti rendszerek nem csupán technológiai újítások. A folyamatos megfigyelés jelenléte mélyen áthatja a kínai társadalmi struktúrát, továbbá egyfajta elfogadottság, sőt egyetértés mutatkozik abban a kérdésben, hogy van-e létjogosultsága a bemutatott rendszernek.

A második rész a megfigyelési technológiák globális exportjára összpontosít, kiemelve azok gyors terjedését más régiókban, bemutatva, milyen következményekkel jár ez a folyamat a globális szintéren. Míg a demokratikus országokban figyelmet fordítanak a magánszféra védelmére, addig az autoriter államok a rendfenntartás érdekében kiterjedt megfigyelő rendszereket működtetnek, egyre gyakrabban a Kína által exportált technológiákat alkalmazva, kombinálva azt más digitális autoriter módszerekkel. Ilyen lehet például az online tartalmak szűrése, vagy az internetszolgáltatás korlátozása. Számos afrikai, illetve ázsiai ország példáján keresztül egyértelműen kiderült, hogy erős igény mutatkozik a megfigyelésre alkalmas technológiák vásárlására.

A jövőbeli trendek figyelembevételével a cikk átfogó képet nyújt a megfigyelő társadalom fejlődéséről, kihívásairól és etikai kérdéseiről. A megfigyelés által létrehozott kontroll és az állami akarat érvényesítése a lakosság életének minden aspektusát érintheti, különösen az autoriter rendszerekben, ahol a technológiai fejlesztések a társadalmi rend fenntartásának eszközeivé válnak. Elmondható, hogy amennyiben ez a trend folytatódik – márpedig Pekingnek érdekében áll, hogy exportálja saját gyakorlatát –, úgy a jövőben nagy valószínűséggel egyre több kínai mintára kiépülő megfigyelő társadalom felvirágzásának lehetünk tanúi.

## Felhasznált irodalom

---

- Cai, Y. (2019). Information as a source of pressure: Local government and information management in China. *Interdisciplinary Political Studies*, 5(2), 477–509. <https://doi.org/10.1285/i20398573v5n2p477>
- Creemers, R. (2018). *China's social credit system: An evolving practice of control*. SSRN. <https://doi.org/10.2139/ssrn.3175792>
- Fornasier, M. O., & Borges, G. S. (2023). The Chinese 'sharp eyes' system in the era of hyper-vigilance: Between state use and risks to privacy. *Revista Brasileira de Políticas Públicas*, 13(1), 1–28. <https://doi.org/10.5102/rbpp.v13i1.7997>



- Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20(1), 125–146. <https://doi.org/10.17159/1996-2096/2020/v20n1a5>
- Hillman, J. E. (2021). *The digital Silk Road: China's quest to wire the world and win the future*. Profile Books.
- Hui, Z. (2019). A community of shared future for mankind–The contemporary development of the social foundations theory of international law. *Social Sciences in China*, 40(1), 186–202. <https://doi.org/10.1080/02529203.2019.1556489>
- Klausner, F. R. (2017). *Surveillance and space*. SAGE Publications Ltd.
- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415–453. <https://doi.org/10.1002/poi3.183>
- Liu, C. (2019). *Multiple social credit systems in China*. OSF Preprints. <https://doi.org/10.31235/osf.io/v9frs>
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.
- Peterson, D. (2020). *Designing alternatives to China's repressive surveillance state*. Center for Security and Emerging Technology. <https://doi.org/10.51593/20200016>
- Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>
- Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*, 30(1), 53–67. <https://doi.org/10.1353/jod.2019.0004>
- Su, Z., Xu, X., & Cao, X. (2021). What explains popular support for government monitoring in China? *Journal of Information Technology & Politics*, 19(4), 377–392. <https://doi.org/10.1080/19331681.2021.1997868>
- Takács S., & Tóth A. (2024). Folyamatmenedzsmen a fizikai biztonság területén. *Magyar Rendészet*, 24(2), 105–120. <https://doi.org/10.32577/mr.2024.2.6>
- Tóth L. (2024). Hazai közterületi videomegfigyelő rendszerek állapota és fejlesztési lehetőségei. *Belügyi Szemle*, 72(2), 243–265. <https://doi.org/10.38146/BSZ.2024.2.4>
- Wood, D. M., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006). *A report on the surveillance society*. Surveillance Studies Network.

## A cikkben szereplő online hivatkozások

---

URL1: *A report on the surveillance society*. <https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf>

URL2: *China just announced a new social credit law. Here's what it means*. <https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/>

- URL3: *Dissecting China's Global Security Initiative (GSI) and Global Development Initiative (GDI)*. <https://www.cescube.com/vp-dissecting-china-s-global-security-initiative-gsi-and-global-development-initiative-gdi>
- URL4: *How China Uses High-Tech Surveillance to Subdue Minorities*. <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>
- URL5: *A magánbiztonság kialakulása, fejlődése, trendjei és jogi szabályozása Kelet-Ázsiában*. <http://www.irisro.org/tarstud2021junius/41RottlerVioletta.pdf>
- URL6: *中国天网监控被忧或侵害个人隐私, 美国之音 (A kínai Skynet megfigyelés aggasztó vagy sérti a személyes adatokat)*. <https://www.voachinese.com/a/news-china-builds-largest-camera-minitoring-system-20170926/4044624.html>
- URL7: 年 · “雪亮工程”仍在继续? (2021-ben folytatódik a „Xueliang projekt”?) <http://m.cps.com.cn/index.php?m=Index&a=show&id=939474>
- URL8: *Budgeting for Surveillance*. <https://www.chinafile.com/budgeting-surveillance>
- URL9: *Sharper Eyes: Shandong to Xinjiang (Part 3)*. <https://chinadigitaltimes.net/2019/09/sharper-eyes-shandong-to-xinjiang-part-3/>
- URL10: *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*. <https://ora.ox.ac.uk/objects/uuid:084840ac-b192-407b-ab6c-f8f810310369>
- URL11: (受权发布) 中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议\_新华网 (*A Kínai Kommunista Párt Központi Bizottságának javaslat a nemzeti gazdasági és társadalmi fejlődés 14. öt éves tervének és a 2035-ös hosszú távú célkitűzéseknél a megfogalmazásáról*). [https://web.archive.org/web/20201104114039/http://www.xinhuanet.com/politics/zywj/2020-11/03/c\\_1126693293.htm](https://web.archive.org/web/20201104114039/http://www.xinhuanet.com/politics/zywj/2020-11/03/c_1126693293.htm)
- URL12: *China's Massive Belt and Road Initiative*. <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>
- URL13: *Belt and Road Tracker*. <https://www.cfr.org/article/belt-and-road-tracker>
- URL14: *China's Digital Silk Road: strategic technological competition and exporting political illiberalism*. [https://pacforum.org/wp-content/uploads/2019/08/issuesinsights\\_Vol19-WP8FINAL.pdf](https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf)
- URL15: *China-powered ICT Infrastructure: Lessons from Tanzania and Cambodia*. <https://www.jstor.org/stable/resrep38689>
- URL16: *Watching Huawei's "Safe Cities"*. [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030\\_HillmanMcCalpin\\_HuaweiSafeCity\\_layout\\_v4.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf)
- URL17: *Global Networks 2030 Developing Economies and Emerging Technologies*. <https://www.csis.org/analysis/global-networks-2030-developing-economies-and-emerging-technologies>
- URL18: *China's Digital Expansion in. Digital Development Working Paper Series* [https://humedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/dd\\_wp95.pdf](https://humedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/dd_wp95.pdf)
- URL19: *Uganda's cash-strapped cops spend \$126 million on CCTV from Huawei*. <https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50RF/>

- URL20: *Uganda elections 2021: Bobi Wine takes on Yoweri Museveni.* <https://www.bbc.com/news/world-africa-55649467>
- URL21: *India cuts internet to 27 million as Punjab police hunt Sikh separatist.* <https://www.cnn.com/2023/03/20/india/india-separatist-manhunt-internet-shutdown-intl-hnk/index.html>
- URL22: *100 hours in the dark: How an election internet blackout hit poor Ugandans.* <https://www.reuters.com/article/world/100-hours-in-the-dark-how-an-election-internet-blackout-hit-poor-ugandans-idUSKBN29P1V7/>
- URL23: *The Rise of Chinese Surveillance Technology in Africa (part 1 of 6).* <https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/>
- URL24: *Full text of Chinese President Xi Jinping's speech at opening ceremony of 2018 FOCAC Beijing Summit* [http://www.xinhuanet.com/english/2018-09/03/c\\_129946189.htm](http://www.xinhuanet.com/english/2018-09/03/c_129946189.htm)
- URL25: *China's overseas police stations: An imminent security threat?* Brookings. <https://www.brookings.edu/articles/chinas-overseas-police-stations-an-imminent-security-threat/>
- URL26: *Huawei accused of stealing trade secrets, spying in Pakistan.* <https://www.reuters.com/legal/transactional/huawei-accused-stealing-trade-secrets-spying-pakistan-2021-08-12/>
- URL27: *A Addis-Abeba, le siège de l'Union africaine espionné par Pékin.* [https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois\\_5247521\\_3212.html](https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html)

## A cikk APA szabály szerinti hivatkozása

---

Tujner V. & Tóth L. (2025). A megfigyelés paradigmája – A kínai modell és globális hatásai. *Belügyi Szemle*, 73(5), 1017–1035. <https://doi.org/10.38146/BSZ-AJIA.2025.v73.i5.pp1017-1035>

## Nyilatkozatok

---

### Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

### Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

### Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

### Nyílt hozzáférésről szóló tájékoztatás

Jelen cikk a Creative Commons Attribution 4.0 International License (CC BY NC-ND 2.0) (<https://creativecommons.org/licenses/by-nc-nd/2.0/>) feltételei szerint publikált Open Access közlemény, melynek szellemében a cikk bármilyen médiumban szabadon felhasználható, megosztható és újraközölhető, feltéve, hogy az eredeti szerző és a közlés helye, illetve a CC License linkje feltüntetésre kerülnek.

### Levelező szerző

A cikk levelező szerzője Tóth Levente, aki a [toth.levente@uni-nke.hu](mailto:toth.levente@uni-nke.hu) e-mail címen érhető el.