

Zsivity Tímea<sup>✦</sup>

## A modern információs technológiák hatása a társadalmi nyilvánosságra Szerbiában

DOI 10.17047/HADTUD.2026.36.1.57

Az információs technológiák robbanásszerű fejlődése és az internet megjelenése lehetővé tette az információk gyors, tér- és időbeli korlátokat meghaladó áramlását, ezzel alapvetően átalakítva a társadalmi nyilvánosság szerkezetét és működését. A tanulmány az új információs technológiák szerbiai társadalmi nyilvánosságra gyakorolt hatásait vizsgálja, kiemelve a biztonság- és védelempolitikai kihívásokat. Rámutat a digitális fenyegetések (kibertámadás, propaganda, álhírek, dezinformáció) közvéleményre és döntéshozatalra gyakorolt hatására. Hangsúlyozza az EU-s jogharmonizáció és a biztonsági kockázatok kezelését szolgáló jogi és intézményi megoldások kidolgozásának fontosságát.

**KULCSSZAVAK:** információs technológia, digitális platformok, kiberbiztonság, társadalmi nyilvánosság, Szerbia

### *The Impact of Modern Information Technologies on Public Life in Serbia*

*The explosive development of information technologies and the emergence of the Internet have enabled the rapid flow of information across space and time, fundamentally changing the structure and functioning of the social public sphere. This paper examines the impact of new information technologies on the social public sphere in Serbia, with a focus on security and defence challenges. It highlights the impact of digital threats (cyber-attacks, propaganda, fake news, disinformation) on public opinion and decision-making. It stresses the importance of EU harmonisation and the development of legal and institutional solutions to address security risks.*

**KEYWORDS:** information technology, digital platforms, cybersecurity, public opinion, Serbia

✦ Nemzeti Közszolgálati Egyetem, Európa Stratégia Kutatóintézet Nyugat-Balkán kutatója és a Hadtudományi Doktori Iskola doktorandusza. –  
Ludovika National University of Public Service, Europe Strategy Research Institute, researcher, PhD Student.  
email: zshivity.timea@gmail.com <https://orcid.org/0009-0008-7961-772X>

## Bevezetés

A modern információs technológiák megjelenése és az internet elterjedése alapjában alakította át a társadalmi nyilvánosságot. Az interneten elérhető digitális platformok és kommunikációs csatornák egyrészt megkönnyítették a felhasználók közötti kapcsolattartást, a gyors információcserét, másrészt jelentős befolyással vannak a közéleti diskurzus alakulására. Az online tér egyre nagyobb szerepet játszik a politikai véleményformálásban, miközben az így erősödő társadalmi polarizáció és digitális megosztottság új geo-, és biztonságpolitikai kihívásokat idéznek elő.

A tanulmány célja az új információs technológiák és a társadalmi nyilvánosság kapcsolatának átfogó vizsgálata, külön figyelmet fordítva a szerb jogszabályi háttér uniós elvárásokkal való összehangolására, a társadalmi polarizáció és az online platformokhoz való hozzáférés problémájának, valamint a digitális tér biztonsági és védelmi kihívásainak elemzésére.

Módszertanilag – a téma összetettsége miatt – az interdiszciplinaritás elvét követem. A tanulmány írásakor figyelembe vettem a releváns jogi, gazdasági, politikai, szociológiai, biztonságpolitikai, statisztikai és demográfiai szempontokat.

A tanulmány négy fejezetből áll. Az első áttekintést nyújt, hogyan befolyásolja a modern információs technológia a digitális tér fejlődését. A második fejezet a szerb jogszabályi keret és az uniós szabályozás harmonizációjának szükségességét elemzi. A harmadik a digitális tér társadalmi nyilvánosságra és közvéleményre gyakorolt hatását elemzi. Vizsgálja az internetes infrastruktúra és az online média használatának helyi sajátosságait. Bemutatja, hogy a társadalmi-gazdasági különbségek miként befolyásolják az online térben való közéleti részvételt, az információhoz való hozzáférést. A negyedik fejezet az új információs technológiák és a digitális tér biztonsági és védelempolitikai kihívásait vizsgálja. A kibertámadások jelentette veszélyek kapcsán bemutatja, hogy ezek a kockázati tényezők miként befolyásolják Szerbia biztonság- és védelempolitikai döntéshozatalát. A tanulmány elemzi továbbá a propaganda, az álhírek, a dezinformációk és a deepfake okozta fenyegetések társadalmi kohézióra, közéleti diskurzusra és politikai döntéshozatalra gyakorolt hatásait.<sup>1</sup>

---

1 Megjegyzés: a propaganda, az álhírek, a dezinformáció és a deepfake fogalmát gyakran tévesen, egymás szinonimájaként használják, összeszova a jelentésüket. A tanulmányban a *propaganda* kifejezés alatt az információk narratívászerű, egyoldalú és manipulatív célú terjesztését értem, amely a befogadók érzelmeire hatva igyekszik befolyásolni véleményüket és viselkedésüket. *Álhírnek* azt a szándékosan hamis vagy félrevezető információt tekintem, amelyet valós hírnek álcáznak, és a hitelesség látszatát keltve terjesztenek. A *dezinformáció* szintén szándékosan hamis és megtévesztő információ, amelyet azért hoznak létre és terjesztenek, hogy kárt okozzanak, politikai célokat érjenek el, olyan cselekvésre vagy döntésre ösztönözze a befogadó felet, amelyet a közlő szeretne elérni, valamint aláássák a bizalmat vagy megzavarják a közvéleményt.

A *deepfake* mesterséges intelligencia segítségével előállított, manipulált videó- vagy hanganyag, amely rendkívül valóság-hűen képes egy személy arcát vagy hangját egy másikéra cserélni, illetve olyan szavakat adni a szájába, amiket soha nem mondott. Lásd bővebben: Török Bernát – Zódi Zsolt (2022): *Az internetes platformok kora*, Budapest, Ludovika Kiadó.

## *A modern információs technológiák hatása a digitális tér alakulására Szerbiában*

Az információ mindig meghatározó szerepet játszott a társadalmi és gazdasági fejlődésben, előnyt biztosítva azoknak, akik rendelkeztek vele. A 20. század technológiai áttörése még nyilvánvalóbbá tette az információ jelentőségét, és az információs forradalom révén az információs technológiák a mindennapok és a fejlődés kulcsfontosságú elemévé váltak, lehetővé téve az adatok gyors és hatékony kezelését.

A modern információs technológiák magukba foglalják az információk kezelését támogató eszközöket, rendszereket és módszereket, beleértve a hardvereket (például számítógépek, szerverek) és a szoftvereket (alkalmazások, programok) egyaránt. A tanulmány ezen fejezetében a korszerű információs technológiák azon elemeit vizsgálom, amelyek döntő hatással vannak a digitális tér alakulására Szerbiában. Kiemelten elemzem a hálózati infrastruktúrát és kommunikációs technológiákat, mint az internet, amely alapvető kommunikációs csatornaként szolgál a digitális térben, valamint a szélessávú hálózatokat (5G, 4G, optikai kábelek), amelyek biztosítják az adatok gyors cseréjét és a valós idejű kommunikációt. A Wi-Fi és mobilhálózatok szerepe alapvető az eszközök közötti zökkenőmentes interakciók lebonyolításában, amelyek nélkülözhetetlenek a digitális tér működéséhez és fejlődéséhez. Így a digitális tér magában foglalja az online világot, az internetes interakciókat, a digitális platformokat, valamint az információk digitalizált formában történő tárolását, felhasználását és megosztását.

Szerbia az elmúlt évtizedekben jelentős mértékű technológiai fejlődésen ment keresztül, és ezzel párhuzamosan az internethasználat széleskörű elterjedése figyelhető meg. A számítógép megjelenésének és fejlődésének történetét Szerbiában a Jugoszláv Szocialista Szövetségi Köztársaság kontextusában kell vizsgálni. A számítógép-fejlesztés története Jugoszláviában az 1950-es évek közepén kezdődött, amikor a Vinča Nukleáris Intézetben mérnökök dolgoztak az első jugoszláv számítógépek kifejlesztésén. Az első számítógép, a CER-10 1960-ban készült el.<sup>2</sup> A szigorú importszabályok, amelyek akkor érvényben voltak, jelentősen befolyásolták a számítógépek fejlődését az országban.<sup>3</sup> Az 1980-as évek végén megjelentek az első IBM-kompatibilis számítógépek. A 1990-es években a délszláv háborúk miatt stagnálás következett be az új számítógépek fejlesztésében. Ebben az időszakban a kutatók fokozott figyelmet kezdtek fordítani az internethez való csatlakozás lehetőségeire. Az 1990-es évek elejére az internet hálózata fokozatosan terjedni kezdett, és Belgrádban létrejött az Akadémiai Hálózat, amely a legfejlettebb számítógépes infrastruktúrát képviselte Szerbiában, összekapcsolva több jelentős egyetemet, így az Elektrotechnikai Kart, a Természettudományi Kart, a Szervezéstudományi Kart, valamint a Technológiai és Metallurgiai Kart.<sup>4</sup> Ezt követően 1996. november 1-jén a Sezam Pro vállalat teljes körű internet-hozzáférést biztosított, ezzel Szerbia hivatalosan is csatlakozott a globális internetes hálózathoz, elindítva az internet korszakát az országban.<sup>5</sup>

2 Navidiku, 2024.

3 Navidiku, 2024.

4 Milić, 2023.

5 Milić, 2023.

Az 1999-es NATO-bombázás jelentős mértékben hozzájárult a technológiai fejlődés újabb stagnálásához. A légitámadások következtében súlyos károk keletkeztek, többek között harminc számítástechnikai központ, melyek áthelyezésére nem volt lehetőség, megsemmisült a támadások során.<sup>6</sup> Ennek ellenére a 2000-es éveket már a távközlési infrastruktúra fejlesztése és az internet sebességének növekedése jellemezte.

A Szerb Köztársaság Statisztikai Hivatalának legfrissebb, 2025-ös felmérési adatai szerint a háztartások 90,1%-a rendelkezik internet hozzáféréssel.<sup>7</sup> 2015-ben ez a szám 63,8% volt.<sup>8</sup>

A megkérdezettek 71,8%-a használt számítógépet az elmúlt három hónapban,<sup>9</sup> valamint 89,8%-a naponta többször csatlakozik a világhálóra.<sup>10</sup> A háztartások 95,8%-a rendelkezik mobiltelefonnal, 95,5%-a TV készülékkel. A felmérésben résztvevők több mint 84%-a rendelkezik közösségimédia-fiókkal. A megkérdezettek 95,5%-a az internetet leginkább online telefon- és videohívásra használja, 84,7%-a a közösségimédia-platformok szolgáltatásait veszi igénybe, míg 83,8%-a online újságokat és folyóiratokat olvas.<sup>11</sup>

A BIRN (Balkan Investigative Reporting Network, Balkáni Oknyomozó Újságírói Hálózat) adatai szerint 2023-ban Szerbiában a mobil- és internetszolgáltatások többségét az ország három szolgáltatója: az MTS, a Yettel és az A1 biztosította.<sup>12</sup> A három szolgáltató lefedi a kártyás és az előfizetéses mobilpiacot. A mobilszolgáltatók piaci részesedése: Telekom Srbija 43,3%, Yettel 31,3%, A1 24,57%.<sup>13</sup> Az MTS részvénytársaságként alakult, amelyben a Szerb Köztársaság birtokolja a részvények többségét, 58%-át. A Telekom Srbija részvényeinek 58%-át a Szerb Köztársaság birtokolja, 20%-át a Telekom Srbija a.d. Beograd, míg 22%-át a szerb állampolgárok tulajdonolják.<sup>14</sup> A vállalat kiterjesztette tevékenységét Bosznia-Hercegovinára, Montenegróra és Észak-Macedóniára, és tovább bővül a kábel- és multimédiás szolgáltatások területén, helyi kábeltársaságok felvásárlásával és TV-kábelcsatornák létrehozásával.

A Yettel viszonylag új szereplő a piacon, 2022 márciusában vette át a norvég Telenor korábbi tevékenységeit. Az anyavállalata a cseh PPF befektetési alap, amely a Yettel márkanévét használja mobilszolgáltatói számára Bulgáriában, Magyarországon és Szerbiában.

Az A1 Serbia a nemzetközi Telekom Austria Csoport tagja. 2007 óta van jelen a szerb piacon.

Szerbia Elektronikus Hírközlési és Postai Szolgáltatásokat Szabályozó Ügynökségének (RATEL) 2023 második negyedévére vonatkozó jelentése szerint a Telekom

6 Milić, 2023.

7 Republički zavod za statistiku 2025, 12.

8 Republički zavod za statistiku 2025, 12.

9 Republički zavod za statistiku 2025, 15.

10 Republički zavod za statistiku 2025, 22.

11 Republički zavod za statistiku 2025, 23.

12 Media Ownership Monitor Serbia 2023.

13 Media Ownership Monitor Serbia 2023.

14 Media Ownership Monitor Serbia 2023.

Srbija rendelkezik a legtöbb felhasználóval. A dokumentum szerint a Telekom Srbija piaci részesedése 42,85%.<sup>15</sup> A második legnagyobb távközlési szolgáltató, a Yettel 31,92%-kal. A vizsgált időszakban az előfizetéssel (postpaid) rendelkezők száma 5,2 millió, míg a kártyás (prepaid) felhasználók száma 3,189 millió volt.<sup>16</sup>

Az elmúlt években a távközlési szolgáltatók (az állami tulajdonú Telekom Srbija és a magánkézben lévő SBB) – kábeltelevízió állomások létesítésével és meglévők megvásárlásával – a médiapiac aktív szereplőjévé váltak. A Telekom Srbija és az SBB nem csak piaci versenyre törekszik, hanem médiabefolyásuk révén a politikai folyamatok alakítására is. Ezt tükrözi szerkesztéspolitikájuk is: a Telekom Srbija érdekelt-ségébe tartozó csatornák jellemzően a kormányzati álláspontokkal összhangban számolnak be az eseményekről, míg az SBB tulajdonában lévő United Media Group médiumai kritikusabb hangvételűek. Ez a különbség hozzájárul a médiatér polarizálódásához, és befolyásolja a közvélemény formálódását, valamint a politikai diskurzust. Az Európai Bizottság 2025-ös jelentése szerint aggodalomra ad okot a médiára nehezedő politikai befolyásolás lehetősége. Ezt egy kiszivárgott telefonbeszélgetés is alátámasztani látszik, amelyben a Telekom Srbija és egy magán médiacsoport vezetői a hatóságokkal szemben kritikusnak tartott szerkesztőségekben tervezett személyi változásokról egyeztettek.<sup>17</sup>

A nyomtatott és online sajtópiacra két cégcsoport, a Ringier és a MONDO dominál, amelyek bulvár jellegű tartalmaikkal és népszerű weboldalaikkal uralják a piacot.<sup>18</sup> Ez a két cég birtokolja a leglátogatottabb webhelyeket is, mint például a blic.rs, a kurir.rs és az espresso.rs. A Dnevni list Danas, a „Nova S” újság és az N1 és Nova S kábelcsatornák mellett a United Media Group része lett.

Az elektronikus médiában a Telekom Srbija és az SBB közvetlen befolyással bír a televíziós csatornák szerkesztői politikájára, illetve a tartalomgyártásra. A Telekom Srbija együttműködik a kormánypárti B92, Prva TV és Pink csatornákkal, míg az SBB tulajdonában lévő United Media Group által üzemeltetett N1 és Nova S csatornák kritikusabb irányvonalat képviselnek.<sup>19</sup>

Az Európai Bizottság 2024. évi országjelentésében megállapította, hogy a 2023 októberében elfogadott közérdekű tájékoztatásról és médiáról szóló törvény számos jogszabályi újítást vezetett be.<sup>20</sup> Ezek közül kiemelkedik az Elektronikus Médiaszabályozó Testület (REM) függetlenségének és átláthatóságának erősítése, valamint a média pluralizmusát fenyegető veszélyek kezelésére vonatkozó felhatalmazásának bővítése. Ugyanakkor a médiatörvény kapcsán további módosításokra van szükség, hogy az teljes mértékben megfeleljen az uniós normáknak. Az új szabályozás, amely lehetővé teszi állami vállalatok számára a médiatulajdonlást, nem nyújt elegendő védelmet a médiapluralizmus és a szerkesztői függetlenség megőrzésére.<sup>21</sup>

15 Media Ownership Monitor Serbia 2023.

16 Media Ownership Monitor Serbia 2023.

17 European Commission 2025, 43.

18 Media Ownership Monitor Serbia 2023.

19 Media Ownership Monitor Serbia 2023.

20 European Commission 2024,70.

21 European Commission 2024,70.

Bár az új rendelkezések a REM függetlenségének és hatékonyságának erősítését célozták, a szabályozó szerv továbbra sem használta ki teljes mértékben jogköreit, függetlenségét illetően aggályok merültek fel. 2023 novemberében kinevezték a REM új igazgatóját, de a Tanács új tagjainak megválasztására vonatkozó eljárást 2024. november 4-ig még nem indították el, megsértve ezzel a törvényi előírásokat.<sup>22</sup>

A Bizottság 2025-ös országjelentésében felszólította Szerbiát, hogy maradéktalanul hajtsa végre a már elfogadott médiatörvényeket, biztosítsa a szabályozó hatóságok (REM és RATEL) pénzügyi és működési függetlenségét, valamint hangolja össze a vonatkozó jogszabályokat az európai médiaszabadságról szóló rendelettel.<sup>23</sup> Tekintettel arra, hogy a REM Tanácsának új tagjait 2025 őszéig sem sikerült megválasztani, a szerb vezetés ígéretet tett a helyzet rendezésére.<sup>24</sup>

A Bizottság megállapította, hogy Szerbia mérsékelten felkészült a digitális átalakulás területén.<sup>25</sup> Megállapításra került, hogy városi területeken a digitális kapcsolódási infrastruktúra jól kiépített, ugyanakkor a vidéki régiókban továbbra is fejletlen, mivel a kereskedelmi szolgáltatók számára ezek a területek kevésbé vonzóak gazdasági szempontból. Ezt alátámasztják a szerb Köztársasági Statisztikai Hivatal által végzett legfrissebb felmérés adatai is. Belgrád és környékén a háztartások 95,5%-a rendelkezik internetkapcsolattal, Šumadija és Nyugat-Szerbiában 88,3%, Vajdaság területén 88,8%, Dél- és Kelet-Szerbiában ez a szám 86,7%.<sup>26</sup>

A digitális szolgáltatások terén Szerbia továbbfejlesztette a kormányzati információs portált és új e-kormányzati szolgáltatásokat vezetett be, de még nem igazodott a digitális szolgáltatások és piacokról szóló törvényekhez.

Az adatkezelés kapcsán Szerbia még nem harmonizálta teljes mértékben szabályozását az EU nyílt adatokra vonatkozó irányelvvel.

Szerbia elindította az 5G frekvenciaárverést, miután elfogadta az 5G frekvenciaárverés keretében az egyes üzemeltetők frekvenciahasználati engedélyeinek kiadására vonatkozó minimumfeltételekről szóló végrehajtási jogszabályokat. Az ország átültette az EU 5G kiberbiztonsági eszköztárát, amelynek előírásait teljes körűen végre kell hajtania. Ez magában foglalja a beszállítók kockázati profiljának értékelését, valamint a magas kockázatúnak minősített beszállítókkal szemben megfelelő korlátozások és/vagy kizárások bevezetését. A regionális együttműködést illetően Szerbia még nem írta alá a digitális átalakulást szolgáló 5G-ütemtervről szóló egyetértési megállapodást.

A versenyjogi szempontból releváns biztosítékok tekintetében nem történt érdemi előrelépés. Ezzel párhuzamosan a kábelszolgáltatói piac további koncentrációja figyelhető meg, amely a médiaszolgáltatók tartalomszolgáltatási piaci részesedésében is változásokat eredményezett.<sup>27</sup>

---

22 European Commission 2024, 70.

23 European Commission 2025, 13.

24 Tanjug, Euronews Srbija 2025.

25 European Commission 2025, 13.

26 Republički zavod za statistiku 2025, 15.

27 European Commission 2025, 81.

A Bizottság jelentése és a Media Ownership Monitor Serbia adatbázisában szereplő adatok rámutatnak a szerb digitális tér és média működésének hiányosságaira, fejlesztést igénylő területeire, valamint a jogszabályi háttér uniós normákkal való harmonizációjának szükségességére.

### *A szerb jogszabályi háttér és az uniós elvárások*

A Bizottság 2025. évi országjelentése szerint Szerbia közepesen felkészült a digitális átalakulás és a médiaszabályozás területén. A dokumentum szerint korlátozott előrelépés történt az elektronikus hírközlésről szóló törvény elfogadása, az e-kormányzat, e-közigazgatás kapcsán, valamint az EU digitális egységes piacának célkitűzéseire való igazodás területén.

A Bizottság 2025-ös évre vonatkozó ajánlásai csak részben kerültek végrehajtásra, ezért felhívta Szerbia figyelmét, hogy 2026-ban:

- Hangolja össze az elektronikus hírközléssel, a digitális bizalommal, a kibertbiztonsággal kapcsolatos jogszabályokat az uniós szabályozással, ideértve a gigabites infrastruktúráról szóló törvényt, az eIDAS 2.0-t, a NIS2 irányelvet<sup>28</sup> és a mesterséges intelligenciáról szóló törvényt.<sup>29</sup>
- Biztosítsa a REM és a RATEL teljes pénzügyi és működési függetlenségét.<sup>30</sup>
- A már elfogadott médiatörvényeket teljes körűen végre kell hajtani, ideértve a Közszolgálati Médiaszolgáltatók és a REM Tanács pénzügyi és működési függetlenségének biztosítását is. Ezen túlmenően a médiatörvényeket tovább kell módosítani annak érdekében, hogy azok összhangban álljanak az Európai Médiaszabadságról szóló Rendelettel, mindezt átlátható és inkluzív jogalkotási folyamat keretében.<sup>31</sup>

Szerbia folyamatosan fejleszti a jogi, stratégiai és intézményi kereteket a tömegtájékoztatás, a közérdekű adatokhoz való hozzáférés és az információbiztonság területén.

Már a 2006. évi szerb alkotmány 50. cikke kimondja, hogy a törvényben előírt nyozott módon bárki szabadon, jóváhagyás nélkül alapíthat sajtót és más tömegtájékoztató eszközöket. A Szerb Köztársaságban nincs cenzúra.<sup>32</sup> Az 51. cikk pedig így szól: „Mindenkit megillet a közérdekű kérdésekről való hiteles, átfogó és kellő időben történő tájékoztatásra való jog, és a tömegtájékoztató eszközök e jogot kötelesek tiszteletben tartani. Mindenkit megillet a közmegbízattal felruházott állami szervek és szervezetek birtokában levő adatokhoz való hozzáférés joga, a törvénnyel összhangban.”<sup>33</sup>

A gyakorlatban azonban az Európai Bizottság 2025-ös jelentése a véleménynyilvánítás szabadsága terén való visszalépést állapított meg. Az újságírók és a sajtóorgánumok helyzete jelentősen romlott, egyes magas rangú köztisztviselők nyilatkozatai

28 Lásd bővebben: <https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive>

29 European Commission 2025, 13.

30 European Commission 2025, 13.

31 European Commission 2025, 13.

32 Ustav Republike Srbije 2006.

33 Ustav Republike Srbije 2006.

pedig korlátozó hatással vannak a véleménynyilvánítás szabadságára. A közéleti részvétel megakadályozását célzó stratégiai perek (SLAPP-ok) egyre gyakrabban gátolták az oknyomozó média munkáját.<sup>34</sup>

Fontos kiemelni, hogy a szerb médiapiac kicsi és telített. A Szerbiai Gazdasági Nyilvántartási Ügynökség (APR) adatai alapján jelenleg több mint 2500 médiaszolgáltató van bejegyezve az országban.<sup>35</sup> Ez a szám azonban nem feltétlenül a médiapluralizmusról, a tényalapú információ közlés lehetőségének széles palettájáról, a szerbiai polgárok tájékozottságának valós állapotáról szól. Az online médiumok és közösségi-platformok megjelenése kedvezett a szubjektív, érzelmi alapú véleménynyilvánítás térnyerésének. Mindez súlyos társadalmi-gazdasági, politikai és biztonsági kockázatokkal járhat. Az érzelmekre építő tartalmak kedveznek a propaganda, az álhírek és dezinformációk terjesztésének. Ez destabilizálhatja a közvéleményt, polarizálhatja a társadalmat, és alááshatja az állami intézményekbe vetett bizalmat. A polarizált és szubjektív információkkal elárasztott társadalmak kiszolgáltatottabbak a külső szereplők politikai nyomásgyakorlásával szemben. Az érzelmekre ható tartalmak megkönnyítik az adathalász támadásokat, így a felhasználók könnyebben válhatnak kibertámadások célpontjává.

Az elmúlt években Szerbia erőfeszítéseket tett a magánszektorral és a civil társadalommal együttműködve az információbiztonság területét szabályozó jogi és stratégiai keretek meghatározására. Szerbiában az információbiztonság területét a 2016-os információbiztonsági törvény szabályozza, amely meghatározza minden jogi személy és állami szerv jogait, kötelességeit és felelősségeit, amelyek IKT-rendszereket működtetnek és használnak.<sup>36</sup> A törvény részletesen taglalja az IKT-rendszereket érintő kihívásokat, kockázatokat és fenyegetésekkel szembeni védelmi intézkedéseket. Emellett meghatározza a rendszerek védelméért felelős szervezetet, a szereplők közötti koordináció formáit és az előírt intézkedések végrehajtásának módját. Három évvel az elfogadása után a törvényt módosították és kiegészítették, hogy javítsák annak alkalmazását, és orvosolják a gyakorlatban felmerült problémákat.

Szerbia kiberbiztonsági szabályozási rendszere fejlettnek tekinthető, melyet az alacsonyabb szintű jogszabályok, valamint a személyes adatok védelmére, kritikus infrastruktúrára és elektronikus kommunikációra vonatkozó törvények egészítenek ki. A csúcstechnológiai bűnözés<sup>37</sup> elleni küzdelem területét a csúcstechnológiai bűnözés

34 European Commission 2025, 7.

35 Simić 2024.

36 Zakon o informacionoj bezbednosti, 2016.

37 Megjegyzés: a csúcstechnológias bűncselekmény fogalmát a „a csúcstechnológiai bűnözés elleni küzdelemben résztvevő állami szervek szervezeti és illetékességi hatásköréről szóló törvény” 2. cikke a következőképp határozza meg: „A törvény értelmében a csúcstechnológias bűncselekmény olyan bűncselekmények elkövetése, amelyek során számítógépek, számítógépes rendszerek, számítógépes hálózatok, számítógépes adatok, valamint ezek anyagi vagy elektronikus formában lévő termékei bűncselekmények elkövetésének tárgyaként vagy eszközöként jelennek meg.

Elektronikus formátumú termékek alatt különösen a számítógépes programokat és az elektronikus formában felhasználható szerzői műveket kell érteni.

A számítógép, számítógépes adat, számítógépes program, számítógépes vírus, számítógépes rendszer és számítógépes hálózat kifejezéseket e törvény a Büntető Törvénykönyv rendelkezései szerint értelmezi.

Lásd: [https://www.paragraf.rs/propisi/zakon\\_o\\_organizaciji\\_i\\_nadleznosti\\_drzavnih\\_organazacija\\_na\\_borbu\\_protiv\\_visokotehnoloskog\\_kriminala.html](https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organazacija_na_borbu_protiv_visokotehnoloskog_kriminala.html)

elleni küzdelemben résztvevő állami szervek szervezeti és illetékességi hatásköréről szóló törvény,<sup>38</sup> az Európa Tanács számítástechnikai bűnözésről szóló egyezménye (budapesti egyezmény), valamint a kapcsolódó büntetőjogi és eljárásjogi rendelkezések szabályozzák. Noha a jogi keret szilárd alapot nyújt, a végrehajtás hatékonysága nem tart lépést a kibertérben megjelenő dinamikus fenyegetésekkel, miközben az új technológiák további, jelenleg még szabályozatlan kihívásokat eredményeznek.

Az információbiztonság stratégiai keretét illetően 2020 végéig két stratégia volt érvényben: az Információbiztonság fejlesztési stratégia (2017–2020) és a Szerb Köztársaság információs társadalmának fejlesztési stratégiája (2010–2020).<sup>39</sup> Mivel mindkét dokumentum érvényessége lejárt, ezért elfogadásra került a Szerb Köztársaság információs társadalmának és információbiztonságának fejlesztési stratégiája (2021–2026).<sup>40</sup> Emellett Szerbia kormánya elfogadta a Mesterséges intelligencia fejlesztési stratégiáját (2020–2025),<sup>41</sup> amely az állam azon törekvését tükrözi, hogy fejlett technológiákat integráljon a működésébe. A két stratégiát egybevetve megállapítható, hogy az állam a digitális társadalom fejlesztését helyezi előtérbe az információbiztonsággal szemben. A szerb kormány prioritásként kezeli a digitális társadalom építését, amelynek célja növelni az állami intézmények és helyi önkormányzatok működésének hatékonyságát, ezzel eleget téve a polgárok és az üzleti szektor által megfogalmazott igényeknek.

A szerb információbiztonsági szektor intézményi keretét a Kereskedelmi, Távközlési és Idegenforgalmi Minisztérium (MTTT), a RATEL, a nemzeti CERT és az Információbiztonsági Feladatot Koordináló Testület alkotja.<sup>42</sup>

Az MTTT javasolja Szerbiában az e területre vonatkozó törvényeket és stratégiákat és felel az információbiztonsággal kapcsolatos tevékenységek végrehajtásáért. A minisztérium beszámolókat nyújt be a parlamentnek, amelyeket bizottsági üléseken és nyilvános meghallgatásokon mutat be.

A RATEL független állami ügynökség, amelynek keretében működik a Nemzeti CERT.<sup>43</sup>

Az Információbiztonságról szóló törvény 15. cikke értelmében a Nemzeti CERT feladata az IKT rendszerek biztonsági kockázataival kapcsolatos információk gyűjtése és megosztása, valamint az IKT rendszerek működtetőinek tájékoztatása, támogatása és tanácsadás nyújtása.<sup>44</sup>

38 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala 2005.

39 Bjeloš, Pavlović 2022, 6.

40 Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine

41 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine

42 Bjeloš, Pavlović 2022, 7.

43 Megjegyzés: A Nemzeti CERT a Szerb Köztársaság területén működő IKT-rendszerek biztonsági kockázatainak megelőzésére szakosodott nemzeti központot képviseli. A Nemzeti CERT országos szinten koordinálja az IKT-rendszerek biztonsági kockázatainak megelőzését és védelmét. A Nemzeti CERT munkájáért az Elektronikus Hírközlési és Postai Szolgáltatások Szabályozó Testülete (RATEL) felelős. Lásd bővebben: <https://www.cert.rs/rs/cesto-postavljana-pitanja.html>

44 Zakon o informacionoj bezbednosti, 2016.

A Nemzeti CERT mellett más szervezetek is rendelkeznek saját CERT-tel, mint például a Belügyminisztérium (MUP), a Biztonsági-Információs Ügynökség (BIA) és a Szerb Hadsereg.<sup>45</sup> Az állami szervek információs és kommunikációs rendszereinek biztonsági központját (az állami szervek CERT-jét) az Információs-Technológiai és Elektronikus Közigazgatási Iroda keretében hozták létre, az Információbiztonságról szóló törvénnyel összhangban. Az állami szervek CERT-je az állami intézmények egységes információs és kommunikációs hálózatában végzi az incidensek elleni védekezéssel kapcsolatos tevékenységeket, kivéve a független üzemeltetőket.

Az állami központokon kívül gazdasági társaságok és civil egyesületek 14 különálló CERT-et hoztak létre.<sup>46</sup> A SHARE Alapítvány az egyetlen civil szereplő, amely saját CERT-tel rendelkezik. A SHARE Alapítvány CERT-jét a digitális jogok és szabadságok megsértésének nyomon követésére hozták létre. Elsősorban újságírók, aktivisták és civil szervezetek használják, akik jogi és technikai támogatást igényelnek. A legaktívabb nem állami szereplő a Szerbiai Bankok Szövetsége, amely saját CERT-et alapított azzal a céllal, hogy pénzügyi CERT-ként működjön.<sup>47</sup>

Az állami szervek és a magánszféra közötti együttműködés kulcsfontosságú a kibertámadások és a kibertérben elkövetett bűncselekmények visszaszorításában. Ezt a feladatot az MTTT keretében az Információbiztonsági Feladatot Koordináló Testülete végzi.<sup>48</sup> A Testület tagjai között megtalálhatók az információbiztonságot felelős állami intézmények, az akadémiai szféra, civil szervezetek és a magánszektor képviselői. A testület évente kétszer ülésezik. Az ülések következtetései és ajánlásai nem nyilvánosak. Szakértők úgy vélik, hogy a Testület döntéshozókra gyakorolt hatása korlátozott, mivel elsősorban tanácsadói funkciót tölt be, továbbá hiányzik a kormányzati politikai akarat annak érdekében, hogy szélesebb jogkörrel ruházzák fel.

Összegezve a fent leírtakat megállapítható, hogy bár a jogi keret meglehetősen szilárd, az intézményi válasz az online térben történő incidensek kezelésére és kibertámadások elleni küzdelemben lassú ütemben halad. A büntető igazságszolgáltatási rendszer nem képes lépést tartani a technológiai fejlődéssel. Emellett a kiberbiztonság megfelelő szintű oktatásának és ismeretének hiánya az állami szereplők, különösen a bírák, ügyvédek és rendvédelmi dolgozók körében, a „magas technológiai” bűncselekmények számos esetében eredményezi a felderítetlenséget.

A fent leírtakból megállapítható, hogy a szerb jogszabályi háttér szilárd, azonban az intézményi fellépés a korszerű információs technológiák okozta kihívásokkal szemben hatékonysági problémákkal küzd. A büntetőjogi szabályozás nem tart lépést a technológiai fejlődéssel, ezért az új típusú csúcstechnológiák által elkövetett bűncselekmények kívül esnek a büntetőjogi kereteken.

---

45 Bjeloš, Pavlović 2022, 8.

46 Bjeloš, Pavlović 2022, 8.

47 Bjeloš, Pavlović 2022, 8.

48 Bjeloš, Pavlović 2022, 8.

## *A digitális tér hatása a társadalmi nyilvánosságra*

Szerbia digitális tere – az új információs technológiák fokozódó használatával, az internetes infrastruktúra fejlődésével, az online média és a platformszolgáltatók térnyerésével – folyamatosan alakítja a társadalmi nyilvánosságot. Az internet, különösen a közösségimédia-platformok lehetőséget biztosítanak az egyének és csoportok számára, hogy véleményüket kifejezzék, és kapuőrök nélkül<sup>49</sup> legyenek aktív részesei a társadalmi vitáknak. A digitális tér egyszerre nyújt lehetőséget a demokratikus részvételre és az információhoz való szélesebb körű hozzáférésre, ugyanakkor fokozza a társadalmi és gazdasági egyenlőtlenségeket, különösen azok körében, akik nem férnek hozzá az online világhoz. Az eszközök elérhetőségének és a digitális készségek fejlesztésének hiányosságai akadályozzák az inkluzív társadalmi nyilvánosság megvalósulását, míg a digitális térben zajló aktivitások jelentősen alakítják a közvéleményt és a politikai részvétel dinamikáját. Az internet megjelenése és széleskörű elterjedése optimizmust váltott ki a demokratikus nyilvánosság fejlődésével kapcsolatban, ám hamar nyilvánvalóvá váltak a negatív hatásai, mint a társadalmi manipuláció, álhírek, gyűlöletbeszéd terjedése. Jürgen Habermas szerint az internet egyszerre szélesítette ki és tette töredezetté a kommunikációs kontextust, ezzel gyengítve a hagyományos média hatalmát.<sup>50</sup> Habermas kritikával illeti az internetet, mint egalitárius médiumot, amely lehetőséget teremtett az anonim és decentralizált információ-hozzáférésre anélkül, hogy ezek bármilyen módon szabályozottak lennének.<sup>51</sup> Ezáltal az értelmiségiek mint a közvélemény fókuszának irányításáért felelős szereplők jelentősége csökken. Valójában arra hívja fel a figyelmet, hogy hiányzik a racionális diskurzus, illetve azok az alapelvek, amelyek a kommunikációt a közös megértés irányába terelnék. Az online aktivizmus révén a digitális tér a társadalmi és politikai mozgósítás eszközévé válhat, különösen a fiatalok körében. Ugyanakkor azt sem szabad figyelmen kívül hagyni, hogy a digitális térben keletkezett feszültségek átszivároghatnak a valós térbe, s ez veszélyt jelenthet az egyénekre és különböző társadalmi csoportokra. Manuel Castells ezzel szemben arra hívja fel a figyelmet, hogy a legjelentősebb hatalom a hálózatok létrehozásának a képessége, amely magába foglalja a hálózat programozását és a kommunikációs áramlatok irányítását a hálózatok között. Ezek az aktorok képesek előnyben részesíteni bizonyos ötleteket, valamint az általuk meghatározott mederbe terelni a kommunikációt.<sup>52</sup> Ezek olyan társadalmi szereplőkből álló csoportok, amelyek sajátos társadalmi helyzetükből adódóan hatalommal rendelkeznek, amit a kommunikációs hálózat biztosít számukra. Castells szerint ez az összekapcsolt társadalomban a hatalom legmagasabb formája. Természetesen az ilyen típusú hatalommal szemben az ellenállók is megjelennek, akik a hálózat újraprogramozásával, az áramlatok átirányításával és a kommunikáció akadályozásával próbálják meg felvenni a harcot.

49 Török, 2021.

50 Habermas, 2006.

51 Habermas, 2006.

52 Castells, 2012, 9.

A Szerb Köztársasági Statisztikai Hivatal 2025. évi, az információs és kommunikációs technológiák használatáról szóló felméréseinek adatai alátámasztják a fentiekben ismertetett elméleti megállapításokat, miközben átfogó képet nyújt az IKT-technológiák elterjedtségéről és alkalmazásáról az egyének, háztartások és vállalkozások mindennapi életében. E technológiák használata, a gazdasági növekedésre és a fejlődésre gyakorolt pozitív hatások mellett bizonyos negatív következményeket is eredményezett és ezek a digitális megosztottság különféle alább bemutatásra kerülő formáiban mutatkoznak meg.

Az előző fejezetekben említettem, hogy Szerbiában 2025-ben a háztartások 90,1%-a rendelkezik internethozzáféréssel és 71,7%-a számítógéppel, azonban ezek az arányok jelentős területi eltéréseket mutatnak. Belgrádban a háztartások 81,7%-a rendelkezik számítógéppel, míg Dél- és Kelet-Szerbiában ez az arány csak 67,0%.<sup>53</sup> A városi és vidéki háztartások közötti eltérés (73,8% szemben 67,5%-kal) jól tükrözi a társadalmi részvétel földrajzi különbségeit, amely hatással van az egyének online közösségi aktivitására.<sup>54</sup>

A felmérés adataiból megállapítható, hogy a digitális infrastruktúra elérésének területi és jövedelmi különbségei tovább mélyítik a társadalmi megosztottságot. A szerb Köztársasági Statisztikai Hivatal adatai szerint a magasabb jövedelemmel rendelkező háztartások nagyobb valószínűséggel rendelkeznek digitális eszközökkel: a 70 000–90 000 dinár közötti jövedelemkategóriában a háztartások 65,3%-a rendelkezik számítógéppel, szemben a max. 70 000 dináros kategória 50,6%-ával.<sup>55</sup>

A háztartások 91,1%-a rendelkezik vezetékesszélessávú internettel, ami alapot biztosít az online közigazgatási szolgáltatások bővítéséhez. Fontos kiemelni, hogy a Covid-19 járvány<sup>56</sup> alatt tapasztalt gyors digitalizáció rávilágított arra, hogy a technológiai előrelépések ellenére a sérülékeny csoportok digitális integrációja továbbra is kihívást jelent.

A felmérésből kiderül, hogy a digitális készségek terén is komoly eltérések tapasztalhatók. A felsőfokú végzettséggel rendelkezők 90,8%-a használ számítógépet, míg az alacsonyabb végzettségűek körében ez az arány mindössze 45,4%.<sup>57</sup> Ez a demográfiai eltérés polarizálja a digitális nyilvánosságot, hiszen az alacsonyabb végzettségű és az idősebb generációk kevésbé tudnak bekapcsolódni az online diskurzusba.

Az internethasználat nemek szerinti megoszlása tekintetében megállapítható, hogy az elmúlt három hónapban a férfiak 91,4%-a, míg a nők 88,7%-a internetezett. A válaszadók zöme online üzenetküldés (WhatsApp, Viber, Skype, Messenger) 92,1%, internetes telefon- és videohívás 95,5%, valamint online újságok és folyóiratok olvasása céljából 83,8% csatlakozott a hálózatra.<sup>58</sup> Ezek az adatok rávilágítanak az internet társadalmi kapcsolatokban játszott szerepére, ugyanakkor azt is jelzik, hogy az eszközhasználat célja leginkább személyes és kommunikációs jellegű.

53 Republički zavod za statistiku 2025, 10.

54 Republički zavod za statistiku 2025, 11.

55 Republički zavod za statistiku 2025, 27.

56 Megjegyzés: a szerb Köztársasági Statisztikai Hivatal 2025-ös felmérése alapján 2020-ban a háztartások 81,0%-a rendelkezett internethozzáféréssel, 2025-ben már 90,1%-a.

57 Republički zavod za statistiku 2025, 16.

58 Republički zavod za statistiku 2025, 23.

Általánosságban elmondható, hogy a médiatartalmak széles körben hozzáférhetőek Szerbiában, ami kedvező környezetet teremt az információk szabad áramlásához. A Freedom House 2023. június és 2024. május közötti időszakban végzett vizsgálata szerint a szerb kormány nem korlátozta az internet-hozzáférést.<sup>59</sup> Az internetszolgáltatók (ISP-k) infrastruktúrája nem központosított, annak ellenére, hogy az állam többségi részesedéssel rendelkezik a Telekom Szerbiában. Az ország internetes adatcseréjét koordináló Szerbiai Open eXchange (SOX) egy magánvállalkozás, amely decentralizált hálózati struktúrát működtet.

Ez a decentralizált, széleskörű internetes hozzáférés kedvező feltételeket teremt a digitális aktivizmushoz, ugyanakkor a közösségimédia-platformok és online terek elérhetősége önmagában nem garantálja a politikai és társadalmi kérdésekben való aktív állampolgári részvételt. Ezt támasztják alá a szerb Köztársasági Statisztikai Hivatal 2025-ös felméréseinek eredményei is. A kutatás rámutatott, hogy a közösségi platformokon politikai vagy társadalmi kérdésekről véleményt nyilvánítók aránya alacsony: a 16–24 évesek 4,0%-a osztott meg ilyen témájú bejegyzést, míg a 35–44 év közöttiek körében ez az arány 8,5%, a 65–74 korosztály pedig mindössze 2,3%.<sup>60</sup> Összességében a férfiak 6,5%-a és a nők 5,1%-a osztott meg politikai vagy társadalmi kérdésekkel kapcsolatos véleményt online.

Az aktív részvételt igénylő online konzultációkban – például petíciók aláírásában vagy szavazásokon – még ennél is alacsonyabb részvételi arányt tapasztaltak. A 16–24 évesek mindössze 1,7%-a, a 25–34 év közöttiek 5,2%-a, a 65–74 évesek körében pedig csupán 0,2% vett részt ilyen aktivitásokban.<sup>61</sup> Némek szerint vizsgálva a részvételt, a férfiak 1,9%-a, míg a nők 3,0%-a nyilvánult meg ilyen módon.

Ezzel szemben a Freedom House jelentése szerint a közösségi média fontos szerepet játszik társadalmi megmozdulások szervezésében, de az online megnyilvánulások nem minden esetben maradnak következmények nélkül. Egyes felhasználók ellen eljárásokat indítottak vagy őrizetbe vették őket az online térben kifejtett véleményük miatt, amit sok esetben rágalmazás és becsületsértés vádjával indított perek követtek.<sup>62</sup>

A jelentés példaként említi a belgrádi fellebbviteli bíróság egyik bírójának ügyét, aki két keresetet is benyújtott a Crime and Corruption Reporting Network (KRIK) nonprofit oknyomozó újságíró szervezet ellen.<sup>63</sup> A keresetek alapját a bírákról készített adatbázis képezte, amelyet a szervezet hozott nyilvánosságra. Dušanka Đorđević bírónő profilja a KRIK adatbázisában tartalmazza igazságszolgáltatási pályafutásának részleteit, az általa vezetett főbb ügyeket, valamint a férjével közösen birtokolt ingatlanokra vonatkozó információkat.<sup>64</sup> A bírónő állítása szerint ezek nyilvánosságra hozatala sértette az ő és férje magánélethez való jogát. Követelésében 10 hónapos börtönbüntetést, pénzbírságot, valamint a riporterek két évre szóló újságírói tevékenységtől való

59 Freedom House 2024.

60 Republički zavod za statistiku 2025, 32.

61 Republički zavod za statistiku 2025, 32.

62 Freedom House 2024.

63 International Press Institute 2024.

64 KRIK Prosudi ko sudi, 2024.

eltiltását kérte.<sup>65</sup> A KRIK jelentése szerint az elmúlt három évben összesen 13 pert indítottak a szervezet ellen, ami jól szemlélteti az online újságírói tevékenységre nehezedő nyomás mértékét.

Mindez arra világít rá, hogy a digitális tér ugyan számos lehetőséget kínál a társadalmi és politikai aktivizmus számára, azonban az online tevékenységek jelentős kockázatokkal is járhatnak, különösen azok számára, akik kritikusan lépnek fel a hatalmi szereplőkkel szemben. Ez egyúttal azt is jelzi, hogy a technológiai infrastruktúra és hozzáférés megléte önmagában nem elégséges a társadalmi részvétel növeléséhez. Ahhoz, hogy a digitális tér valóban a demokratikus diskurzus katalizátorává váljon, szükség van a felhasználók tudatosságának növelésére, a digitális készségek fejlesztésére, valamint a véleménynyilvánítás szabadságának védelmére irányuló intézkedésekre.

### *Biztonság- és védelempolitikai kihívások*

A modern információs technológiák robbanásszerű fejlődésével, az információs hálózatok terjedésével az állami és nem állami szereplők felismerték a kibertér stratégiai jelentőségét. A kibertér fogalmának meghatározása a folyamatosan fejlődő és változó technológiák, eszközök, platformok, különféle internetes alkalmazások miatt nehézségekbe ütközik. Daniel Kuehl úgy fogalmaz: „a kibertér egy globális tartomány az információs környezetben, amelynek jellegzetes és egyedi karakterét az elektronika és az elektromágneses spektrum felhasználása határozza meg az információk létrehozására, tárolására, módosítására, cseréjére és kiaknázására az információs-kommunikációs technológiákat használó, egymástól függő és összekapcsolt hálózatokon keresztül.”<sup>66</sup> Az Észak-atlanti Szerződés Szervezete (NATO) is hasonló módon határozza meg a kibertér fogalmát:<sup>67</sup> „globális tartomány, amely minden összekapcsolt kommunikációs, információs technológiai és egyéb elektronikus rendszert, hálózatokat és adatokat tartalmaz, beleértve azokat is, amelyek elkülönültek vagy függetlenek, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak.”<sup>68</sup> A két definíció közötti hasonlóság arra utal, hogy a kibertér fogalmának meghatározásában kulcsfontosságú az információs-technológiai rendszerek és hálózatok globális összekapcsoltsága, valamint az ezekben rejlő lehetőségek és kihívások felismerése mind állami, mind nem állami szereplők részéről.

Szerbia esetében a digitális infrastruktúra fejlődése, az online információmegosztás széleskörű elterjedése, valamint a közösségi média dominanciája új biztonsági és védelmi kihívásokat teremtett. A kiberbiztonság kulcsfontosságú szerepet játszik az állam nemzetbiztonsági stratégiájában, különösen a kritikus infrastruktúrák és az információs rendszerek védelme tekintetében. Ezért fontos a kibertér fenyegetések elleni védelmi rendszerek kiépítése, valamint a kibertér biztonságának megerősítése.

65 International Press Institute 2024.

66 Kuehl 2009, 27.

67 Megjegyzés: a NATO 2016-ban önálló hadszínterré nyilvánította a kibertérrel.

68 NATO glossary of terms and definitions 2019, 37.

Az Európai Bizottság 2025. évi jelentése szerint Szerbia a digitális bizalmat és a kiberbiztonságot illetően rendelkezik a megfelelő jogi kerettel és intézményi felépítéssel, azonban a kiberbiztonságra vonatkozó uniós vívmányokkal, többek között a NIS 2 irányelvvel való további jogszabályok összehangolására van szükség. Szerbiának emellett igazodnia kell az új európai digitális identitás és bizalmi szolgáltatások keretrendszeréhez is, hogy hatékonyan reagálhasson a digitális térben rejlő veszélyekre. A jelentésből kiderül, hogy a hibrid fenyegetések, valamint a külföldi információs manipuláció és beavatkozás (FIMI), beleértve a dezinformációt is, továbbra is aggodalomra adnak okot, amelyeket sürgősen kezelni kell.<sup>69</sup> Szerbia 2023-ban, 2024-ben és 2025-ben sem igazodott az EU nyilatkozataihoz és korlátozó intézkedéseihöz a kibertámadásokra adott reakciók terén.

A kibertér globális jellege nemcsak lehetőségeket teremt, hanem új típusú geopolitikai kihívásokat is előidéz. A nagyhatalmak (USA, Oroszország és Kína) jelentős szereplői ennek a térnek, és tevékenységeik számos biztonsági fenyegetést jelentenek az államok és nemzetközi szervezetek számára. Az orosz dezinformációs kampányok és a kínai technológiai dominanciaépítés, például a kritikus infrastruktúrákban alkalmazott technológiák terén, új dimenziót adnak a kibertér biztonsági kérdéseinek. Ezért a nemzetállamok, köztük Szerbia, nemcsak belső stratégiájuk megerősítésére, hanem nemzetközi együttműködésre is rákényszerülnek.

A Nyugat-Balkán országaiban is egyre inkább terjed a kiberbűnözés. A hivatalos statisztikák szerint Szerbiában jelentős növekedés figyelhető meg a kibertámadások és a kiberbűnözés terén. 2020-ban mintegy 26 millió kibertámadás érte az IKT rendszereit, amelyek többsége ezen rendszerekbe való behatolási kísérlet és engedély nélküli adatgyűjtés volt.<sup>70</sup> 2022-től kezdődően több internetes csalás és személyazonosság-lopás is történt, például a Raiffeisen Bank és a Szerb Posta felhasználói adataival kapcsolatban.<sup>71</sup> Emellett állami nyilvántartásokat értek hekkertámadások, valamint elektronikus bombariadó bejelentések is előfordultak, amelyek ideiglenesen megbénították az érintett köz- és magánintézmények működését.

Az Európai Parlament a nyugat-balkáni szervezett bűnözés elleni küzdelem területén folytatott együttműködésről szóló állásfoglalásában felszólította a régió államait, hogy bővítsék kapacitásukat a kiberbűnözés elleni küzdelem tekintetében és növeljék a kiberbűnözéssel kapcsolatos büntetőeljárások számát.<sup>72</sup> Kiemelte, hogy az európai partnerekkel együttműködve fel kell lépni a manipulatív félretájékoztatással szemben. A hibrid fenyegetések, a dezinformációk terjesztése, valamint a kibertámadások – különösen a kritikus infrastruktúrák ellen – továbbra is politikai és biztonsági kihívást jelentenek a térség országai számára. Az orosz–ukrán háború kitörését követően megfigyelhetővé vált, hogy Moszkva milyen módon tudja saját javára felhasználni a Nyugat-Balkán etnikai konfliktusait. Oroszország befolyása folyamatosan nő a kulcsfontosságú nyugat-balkáni államokban. Ezzel is azt a képet mutatja magáról, hogy továbbra is olyan hatalom, amelyet számításba kell venni, az uniós szankciók és

69 European Commission 2025, 105.

70 Bjeloš, Pavlović 2022, 9.

71 Bjeloš, Pavlović 2022, 4.

72 European Parliament 2021.

diplomáciai elszigeteltsége ellenére. Az Európai Bizottság 2023. 2024. és 2025. évi jelentésében is felszólította a szerbiai vezetést, hogy sürgősen intézkedjen a külföldi információmanipuláció és az EU-ellenes narratívák terjesztésének megakadályozása kapcsán.<sup>73</sup> Erre azért volt szükség, mert az EU által szankcionált orosz, államilag támogatott csatorna sugároz rádió- és multimédiás műsorokat Szerbiában, köztük a Russia Today (RT) is. Az Európai Bizottság értékelése szerint a csatorna a Wagner félkatonai csoport katonai toborzását is népszerűsítette, ami a szerbiai jogszabályok szerint tilos, de az ügyészség mégsem vizsgálta ki az ügyet. Ezek a médiatartalmak nagyban befolyásolják nemcsak a szerbiai, hanem az egész régió közvéleményét is. Ezt az állítást alátámasztja egy 2023 júliusában közzétett esettanulmány is, mely szerint Szerbiában több orosz érdekeltségű médiafelület működik, többek között a „News Front”, melyen megjelent tartalmakra gyakran hivatkoznak más szerbiai és bosznia-hercegovinai médiumok is.<sup>74</sup> Az Unió és szövetségeseinek félelme, hogy az EU nyugat-balkáni terjeszkedésének megállítása érdekében Oroszország információs műveleteket alkalmaz etnikai feszültségek és befagyott konfliktusok szítására. Oroszország nyíltan támogatja Szerbiát Koszovóval kapcsolatos álláspontjában, de emellett információs hadviselést folytat a szerb társadalom és politikai elitek polarizálása érdekében. A nyugat-balkáni államok EU-taggá válása egyértelműen csökkentené az orosz befolyást a térségben. A Nyugat ezzel párhuzamosan információs kampányt indított, amelynek célja Szerbia és Oroszország közötti feszültség fokozása volt, különösen a lőszerexport ügyét illetően. A vádak szerint Szerbia közvetve 800 millió euró értékben szállított lőszert Ukrajnába.<sup>75</sup> Aleksandar Vučić, Szerbia elnöke válaszában kijelentette, hogy az export kizárólag az engedélyezett végfelhasználók számára történt, és hangsúlyozta, hogy Szerbia maradéktalanul betartja a fegyverexporttal kapcsolatos nemzetközi szerződéseket.<sup>76</sup> Vučić a Nyugat által felhozott vádakot politikai manőverként értékelte, és megerősítette, hogy Szerbia és Oroszország közötti kapcsolat továbbra is stabil, elutasítva bármiféle fegyverközvetítést Oroszország számára. Az ilyen információs műveletek az államok és szövetségi rendszerek döntéshozatali képességeit is célba vehetik, aláásva a biztonságpolitikai stabilitást.

Kína globális propaganda- és véleményformáló stratégiája a nyugati diskurzusdominancia gyengítését és saját narratíváinak terjesztését célozza, különösen a Globális Délen. 2008 óta évente több mint 1,5 milliárd dollárt fordít erre, miközben a Szinchua hírügynökség hálózatán napi 7300 tartalmat oszt meg, 15 nyelven, 200 millió követővel.<sup>77</sup> A „precíz kommunikáció” módszerével adatokat gyűjt és célzott üzeneteket juttat el a közönséghez. Kína ezen kívül befolyásolja a globális információs és kommunikációs technológiák szabványait, elősegítve a kiber-szuverenitás elvét, amely szerint az államok teljes ellenőrzést gyakorolnak a határokon belüli internetes infrastruktúra és adattartalom felett, szemben a nyitottabb, több

73 European Commission 2025:41.

74 Brey 2023, 8.

75 Radio Slobodna Evropa 2024.

76 Radio Slobodna Evropa 2024.

77 Bajčić 2023.

szerreplős (multi-stakeholder) globális internetirányítási modellel. Ezen eszközök segítségével Kína technikai infrastruktúráját biztosít fejlődő országok számára, miközben a kínai normákat népszerűsíti. Kína technológiai és infrastrukturális beruházásai – például Szerbiában a Nuctech szkennerei – szoros kapcsolatban állnak a kínai állammal, adatbiztonsági és geopolitikai aggodalmakat felvetve.<sup>78</sup> Az eszközök, melyek a szerb–bolgár határon kerültek telepítésre, biztonsági aggályokat vetnek fel, különösen az érzékeny adatok gyűjtése és a Kínai Kommunista Párt befolyása miatt.<sup>79</sup> A kínai technológia alkalmazása Szerbiában, különösen a kétoldalú megállapodások alapján történő vásárlások, a transzparencia hiányát vetik fel és geopolitikai feszültséget okozhatnak az EU és szövetségeseivel való kapcsolatban.

A geopolitikai környezetben tapasztalható kibertérbeli aktivitások egyértelművé teszik, hogy a kibervédelem nemcsak technológiai, hanem stratégiai és diplomáciai kérdés is. Miközben Szerbia hivatalos stratégiai célja továbbra is az Európai Unióhoz való teljes jogú csatlakozás, külpolitikája a gyakorlatban multivektorális. A biztonsági és védelmi kihívások hatékony kezelése szempontjából elengedhetetlen az EU-val és annak biztonsági struktúráival való együttműködés elmélyítése, különösen a közös kül- és biztonságpolitikához való igazodás terén, ami a csatlakozási folyamat egyik kulcsfontosságú követelménye.

## Összegzés

A modern információs technológiák fejlődése jelentős mértékben alakította át a társadalmi nyilvánosság szerkezetét és működését Szerbiában. Az internet és a digitális platformok elterjedése új lehetőségeket teremtett a közvélemény formálása, a politikai részvétel és az információáramlás szempontjából, ugyanakkor számos kihívást is felszínre hozott. A tanulmány elemezte a társadalmi polarizáció, a dezinformáció és a digitális térben megjelenő biztonsági fenyegetések – például kibertámadások, propaganda és álhírek – hatásait a társadalmi kohézióra és a politikai döntéshozatalra. A szerb digitális infrastruktúra fejlődése és a jogi környezet elemzése során a tanulmány hangsúlyozta, hogy az EU-s normákhoz való igazodás elengedhetetlen a hatékony szabályozási keretek megteremtéséhez. Miközben a jogszabályi keret szilárd alapot biztosít, az intézményi kapacitások fejlesztése elengedhetetlen ahhoz, hogy az állami szervek lépést tartsanak a technológiai változásokkal. Ennek érdekében elengedhetetlen a megfelelő képzések biztosítása az állami intézmények dolgozóinak, a rendvédelmi szervek és a bírói testület számára, továbbá az erőforrások bővítése, különösen a kiberbiztonsági intézmények és a nemzeti CERT-ek megerősítése terén. Kiemelt fontosságú az állami és civil szféra közötti együttműködés elmélyítése, főként a kiberfenyegetések kezelése és a lakossági tudatosság növelése érdekében. A médiapluralizmus biztosítása érdekében szükség van a médiatulajdon átláthatóságát célzó szabályozások szigorítására, valamint a közérdekű tájékoztatás támogatására. A digitális tér által kínált lehetőségek csak akkor használhatók ki teljes mértékben, ha biztosítják az egyenlő hozzáférést a digitális infrastruktúrához. A vidéki és

78 Gočanin 2023.

79 Gočanin 2023.

alacsony jövedelmű régiók fejlesztésével csökkenteni kell a digitális szakadékot, ami nemcsak a társadalmi kohézió erősítéséhez, hanem az ország gazdasági fejlődéséhez is hozzájárulhat. A digitális írástudás fejlesztése, széles körű oktatási kampányokkal kiegészítve, szintén kiemelkedően fontos a lakosság információs környezetben való eligazodásának elősegítése és a dezinformációval szembeni ellenállóképeség növelése érdekében. Az álhírek és propaganda elleni hatékony fellépés megvalósításához célzott oktatási programok és közösségi médiakampányok szükségesek, amelyek a kritikus gondolkodás erősítésére irányulnak. Nemzetközi szinten a regionális együttműködés elmélyítése kiemelten fontos a kiberbűnözés elleni közös fellépés előmozdítása érdekében, miközben szükség van a közösségi médiaplatformok átláthatóságának és felelősségvállalásának szabályozására is. A digitális tér jelentette kihívások és lehetőségek megfelelő kezelésével Szerbia nemcsak a társadalmi egyenlőség és a biztonság erősítéséhez járulhat hozzá, hanem hosszú távon gazdasági és politikai stabilitását is biztosíthatja.

#### FELHASZNÁLT IRODALOM

- Bajčić, Tamara: Kako Kina utiče na globalno javno mnjenje? Online: <https://www.danas.rs/vesti/politika/kako-kina-utice-na-globalno-javno-mnjenje/> (Letöltés ideje: 2024. 11. 29.)
- Bjeloš, Maja – Pavlović, Marija 2022. *Sajber bezbednost i ljudska prava na Zapadnom Balkanu: slučaj Srbije*. Beogradski centar za bezbednosnu politiku.
- Brey, Thomas 2023. *Ruski mediji na Balkanu i njihova uloga u agresorskom ratu protiv Ukrajine. Studija slučaja: RT Balkan*. Potsdam–Babelsberg: Friedrich-Neumann-Stiftung für die Freiheit.
- Castells, Manuel 2012. *Networks of outrage and hope : social movements in the Internet Age*. Polity Press, second edition.
- Európai Bizottság (n.é.). NIS 2 irányelv: hálózati és információs rendszerek biztosítása. Online: <https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive>
- European Commission 2024. *Commission Staff Working Document, Serbia 2024 Report*. SWD(2024) 695 final. Brussels, 30.10.2024. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024SC0695>
- European Commission 2025. *Commission Staff Working Document, Serbia 2025 Report*. SWD(2025) 755 final. Brussels, 4.11.2025. Online: [https://neighbourhood-enlargement.ec.europa.eu/serbia-report-2025\\_en](https://neighbourhood-enlargement.ec.europa.eu/serbia-report-2025_en)
- European Parliament 2021. *European Parliament resolution of 15 December 2021 on cooperation on the fight against organised crime in the Western Balkans*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0506>
- Freedom House 2024. *Freedom on the net 2024–Serbia*. Online: <https://freedomhouse.org/country/serbia/freedom-net/2024> (Letöltés ideje: 2024. 11. 29.)
- Gočanin, Sonja: Kinesku opremu instaliraju u Srbii, u EU preispituju, u SAD zabranjuju. Online: <https://www.slobodnaevropa.org/a/nuctech-oprema-srbija-kina-donacija-bezbednost/32674637.html> (Letöltés ideje: 2024. 11. 29.)
- Habermas, Jürgen: Towards a United States of Europe. Online: <http://www.signandsight.com/features/676.html> (Letöltés ideje: 2024. 11. 29.)
- International Press Institute. Serbia: KRIK journalists facing SLAPPs after publishing the profile of Judge Dušanka Đorđević in database. Online: <https://ipi.media/serbia-krik-journalists-lawsuit-judge-database/> (Letöltés ideje: 2024. 11. 29.)
- KRIK. Prosudi ko sudi. Online: <https://prosudikosudi.rs/sudija.php?id=201203195752&ime=Dusanka-Dordevic> (Letöltés ideje: 2024. 11. 29.)

- Kuehl, Daniel 2009. From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer-Stuart H. Starr-Larry K. Wentz (szerk.): Cyberpower and National Security. University of Nebraska Press.
- Media Ownership Monitor Serbia 2023. Online: <https://serbia.mom-gmr.org/en/owners/> (Letöltés ideje: 2024. 11. 29.)
- Milić, Marija: Prostori razvoja računarstva i IT industrije u Jugoslaviji. Online: <https://www.oblakodermagazin.rs/prostori-razvoja-racunarstva-i-it-industrije-u-jugoslaviji/> (Letöltés ideje: 2024. 11. 29.)
- Nacionalni CERT Republike Srbije – Regulatorno telo za elektronske komunikacije i poštanske usluge (n.é.). Online: <https://www.cert.rs/rs/cesto-postavljana-pitanja.html>
- NATO glossary of terms and definitions AAP-06 Edition 2019. Online: [https://www.coemed.org/files/stanags/05\\_AAP/AAP-06\\_2019\\_EF.pdf](https://www.coemed.org/files/stanags/05_AAP/AAP-06_2019_EF.pdf) (Letöltés ideje: 2024. 11. 29.)
- Navidiku: Kada je stigao prvi računar u Srbiju? Online: <https://www.navidiku.rs/firme/laptop-servis-racunara-beograd/kada-je-stigao-prvi-racunar-u-srbiju> (Letöltés ideje: 2024. 11. 29.)
- Radio Slobodna Evropa: Vučić o prodaji municije Ukrajini: Izvozimo samo ‘krajnjim korisnicima’. Online: <https://www.slobodnaevropa.org/a/vucic-ukrajina-srbija-oruzje-naoruzanje-izvoz/33007417.html> (Letöltés ideje: 2024. 11. 29.)
- Republički zavod za statistiku 2025. *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji*. Beograd: Republički zavod za statistiku.
- Simić, Lazar: Medijske pustinja u Evropi: kako je u EU i ko kupuje lokalne medije u Srbiji? Online: <https://localpress.org.rs/medijske-pustinja-u-evropi-kako-je-u-eu-i-ko-kupuje-lokalne-medije-u-srbiji/> (Letöltés ideje: 2024. 11. 29.)
- Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine. Online: [http://demo.paragraf.rs/demo/combined/Old/t/t2020\\_01/t01\\_0005.htm](http://demo.paragraf.rs/demo/combined/Old/t/t2020_01/t01_0005.htm) (Letöltés ideje: 2024. 11. 29.)
- Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine. Online: <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/strategija/2021/86/1/reg> (Letöltés ideje: 2024. 11. 29.)
- Tanjug, Euronews Srbija: U Skupštini usvojena izmena Liste kandidata za članove Saveta REM-a. Online: <https://www.euronews.rs/srbija/politika/194987/u-skupstini-usvojena-izmena-liste-kandidata-za-clanove-saveta-rem-a/vest> (Letöltés ideje: 2025. 11. 07.)
- Török Bernát- Zódi Zsolt 2022. *Az internetes platformok kora*. Budapest, Ludovika Kiadó
- Török Bernát: Donald Trump különös esete a szólásszabadsággal. Online: [https://telex.hu/velemeney/2021/01/16/szolasszabadsag-es-kozossegi-media?utm\\_source=mandiner&utm\\_medium=link&utm\\_campaign=mandiner\\_202101](https://telex.hu/velemeney/2021/01/16/szolasszabadsag-es-kozossegi-media?utm_source=mandiner&utm_medium=link&utm_campaign=mandiner_202101) (Letöltés ideje: 2024. 11. 29.)
- Ustav Republike Srbije 2006. Online: [https://www.paragraf.rs/propisi/ustav\\_republike\\_srbije.html](https://www.paragraf.rs/propisi/ustav_republike_srbije.html) (Letöltés ideje: 2024. 11. 29.)
- Zakon o informacionoj bezbednosti, 2016. Online: [https://www.paragraf.rs/propisi/zakon\\_o\\_informacionoj\\_bezbednosti.html](https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html) (Letöltés ideje: 2024. 11. 29.)
- Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala 2005. Online: [https://www.paragraf.rs/propisi/zakon\\_o\\_organizaciji\\_i\\_nadleznosti\\_drzavnih\\_organ\\_a\\_za\\_borbu\\_protiv\\_visokotehnoloskog\\_kriminala.html](https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organ_a_za_borbu_protiv_visokotehnoloskog_kriminala.html) (Letöltés ideje: 2024. 11. 29.)