Iustum Aequum Salutare
XX. 2024. 3. • 17–29.

‘KIBER GULÁG’ ÉS ‘DIGITÁLIS VASFÜGGÖNY’, AVAGY AZ INTERNETSZUVERENITÁS KÉRDÉSEI OROSZORSZÁGBAN*

Gosztonyi Gergely
habilitált egyetemi docens (ELTE ÁJK)

„Varázstalan világban végképp nem érdemes élni.”[1]

1. Bevezetés

Az Ukrajna területi integritásába a nemzetközi jogot sértő[2] orosz beavatkozás már tíz éve folyamatosan zajlik (a Krím annektálása, a donbászi háború), 2022. február 24-e mégis új helyzetet teremtett. Ezen a napon, amikor az Oroszországi Föderáció (a továbbiakban: Oroszország) rakétái több helyen becsapódtak Ukrajnában, kezdetét vette a második világháború utáni legnagyobb hagyományos európai katonai konfliktus,[3] az orosz–ukrán háború. Bár a hivatalos orosz megnevezése az eseményeknek a háború *(война)* helyett a szépelgő különleges katonai művelet *(специáльная воéнная операция)*, a szómágia nem tudja meg nem történtté tenni a nemzetközi háborús jog megsértését.[4] Az Orosz Szövetségi Kommunikációs, Információs Technológiai és

* A tanulmány a Bolyai János Kutatási Ösztöndíj támogatásával készült.

1 Pünkösti Árpád: „Újra és újra felháborodom; ez éltet.” Interjú Ferge Zsuzsával. *Népszabadság*, 2011. április 23., Hétvége melléklet, 8.

2 Hoffmann Tamás: War or Peace? – International Legal Issues concerning the Use of Force in the Russia-Ukraine Conflict. *Hungarian Journal of Legal Studies,* Vol. 63., N. 3. (2022) 206–235. https://doi.org/10.1556/2052.2022.00419

3 Serhii A. Shevcuk – Viktor I. Vyshnevskyi – Olena P. Bilous: The Use of Remote Sensing Data for Investigation of Environmental Consequences of Russia-Ukraine War. *Journal of Landscape Ecology,* Vol. 15., N. 3. (2022) 37. https://doi.org/10.2478/jlecol-2022-0017

4 International Federation for Human Rights: Ukraine, ‘war’ versus ‘special military operation’: why words matter in international law. *FIDH*, 2022. augusztus 8. https://tinyurl.com/4zazsf9n

Tömegtájékoztatási Felügyeleti Szolgálat, a *Roskomnadzor*[5] már 2022. február 26-án figyelmeztetett 10 független szerkesztőséget (Echo of Moscow, InoSMI, Media Zona, New Times, Dozhd, Svobodnay Pressa, Krym.Realii, Novaya Gazeta, Journalist és Lenizdat), hogy azonnal távolítsák el azon anyagaikat a felületeikről,[6] amelyek a hatóság álláspontja szerint hamis információkat tartalmaznak (hiszen a támadás, a háború vagy a hadüzenet szavak szerepelnek bennük), ellenkező esetben 5 millió rubeles pénzbüntetéssel (20 millió HUF) vagy az elérhetőség felfüggesztésével kell szembenézniük. Az ezután következő napokban villámgyors tempóban tettek az orosz hatóságok elérhetetlenné több tucat olyan médiumot, amelyek nem csupán a hivatalos álláspontot jelenítették meg tudósításaikban.

A helyzet a háború kezdete óta tovább rosszabbodott: az eredeti orosz villámháborús tervekhez képest jelentősen elhúzódó harci cselekmények, az immár Oroszország területét is több alkalommal elérő ukrán dróntámadások, Jevgenyij Prigozsin orosz oligarcha lázadása és halála, illetve a hivatásos katonai és a 2023 nyarán 27-ről 30 éves életkorra felemelt besorozott sorkatonai szolgálati állománnyal egyre csak növekvő számú orosz hadsereg veszteségei[7] mind-mind olyan kérdések, amelyek demokratikus körülmények között megingathatnák – megszakításokkal ugyan, de – az immár több mint húsz éve regnáló elnök, Vlagyimir Putyin hatalmát. Oroszországban azonban nem csupán a háborús helyzet teszi lehetetlenné a demokrácia működését: a negatív folyamatok jó pár éve a világ közvéleményének szeme előtt zajlanak. Ugyanígy állíthatjuk, hogy a véleménynyilvánítás szabadságát alapjaiban megkérdőjelező jogszabályokat sem 2022-ben kezdték elfogadni Oroszországban. Ugyan az orosz–ukrán háború felgyorsította az eseményeket, az orosz elit korábban is mindent megtett, hogy az orosz lakosság a hatalom számára kellemetlen hírekről ne értesülhessen. Innen pedig már csak egy lépés a propaganda, a hírhamisítás, a *fake news*, a *deepfake* és társainak olyan mértékű elterjedése, amelyek egy 21. századi hibrid háború[8] alapjait képezik:[9] „A fegy-

---

5 Роскомнадзор, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

6 Russia: With War, Censorship Reaches New Heights. *Human Rights Watch,* 2022. február 28. https://www.hrw.org/news/2022/02/28/russia-war-censorship-reaches-new-heights

7 A katonai veszteségek – a háború természetéből is adódóan – pontosan megállapíthatatlanok, és attól függően, hogy a háborús felek melyikének adatait nézzük, jelentősen eltérhetnek. Az orosz–ukrán háború első két éve alatt nyugati források 66.000 és 88.000 közé teszik az Ukrajnában elesett orosz katonák számát (és nagyjából 315.000 főre az elesett és megsérültekét összesen), míg Oroszország ezen adatoknak csak a töredékét ismeri el valósnak. How many Russian soldiers have died in Ukraine? Five charts illustrate the enormous losses. *The Economist,* 2024. február 24. https://tinyurl.com/5cy4zrve

8 Jójárt Krisztián szerint a hibrid hadviselés a csecsen gerillák által alkalmazott módszer, amely „ötvözte a gerilla harcmodort a szovjet és nyugati katonai doktrínák, valamint a modern technológia alkalmazásával." Jójárt Krisztián: A hibrid hadviselés orosz elméletének változása az ukrajnai tapasztalatok tükrében. *Hadtudomány,* 2019/1–2. 50.

9 Kelemen Roland – Farkas Ádám: A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. *In Medias Res,* 2022/1. 96–108.

verropogás mögött húzódó kommunikációs háború […] nem feltétlenül az objektív tájékoztatásról szól, hanem a félrevezetésről és a szívek megnyeréséről.”[10]

2. A kiber- vagy internetszuverenitás alapjai

Az internetszuverenitás kérdéskörének megértéséhez Hszi Csin-ping, a Kínai Népköztársaság elnökének 2015-ben, a második Internet Világkonferencia nevű rendezvényen elmondott beszédéhez kell visszanyúlnunk.[11] Ebben felszólította a világ összes országát, hogy tartsák tiszteletben egymás „kiberszuverenitását”, azaz annak jogát, hogy megválaszthassák a „saját” internetük fejlesztésének és szabályozásának módjait. Mindemellett – egyértelműen az Amerikai Egyesült Államokra utalva – visszautasította, hogy a kibertérben bármely ország hegemóniát szerezzen azzal, hogy ráerőszakolja a saját szabályozási és technológiai megoldásait más országokra. Ezen értelmezés szerint a 21. századi internetszabályozást a korai sajtószabályozásokhoz vagy műsorszolgáltatási szabályozásokhoz kellene hasonlatossá tenni, amikor is az államok megalkothatták a saját szabályaikat, majd szükség esetén egyeztethettek a környező, érintett országok vezetőivel.[12] Ahogy Andrew Keane Woods megjegyezte: „az államok továbbra is a legitim szabályok egyetlen legfőbb forrásai maradnak a különböző népek számára, amelyek különböző közösségi értékekkel és tapasztalatokkal rendelkeznek egy sokszínű bolygón.”[13] A probléma mindezzel ugyanakkor az, hogy a korábbi – jelentősen lokálisabb – kommunikációs környezettől jelentősen eltérő technológiai és fizikai adottságokkal rendelkező globális internet esetében nem biztos, hogy értelmezhetőek nemzetközi együttműködés nélkül az országhatárokat figyelembe vevő szabályozási megoldások.[14] Ebből következően viszont – Anupam Chander és Haochen Sun álláspontját osztva – az internetszuverenitás kérdései mindig és egyértelműen csupán a globális skálán értelmezhetőek.[15]

---

[10] Földes Márton: A világ legjobban dokumentált háborúja zajlik, de sokszor nem szabad hinnünk a szemünknek. *Heti Világgazdaság,* 2023. március 30. https://tinyurl.com/4dk3kmje

[11] N/A: China internet: Xi Jinping calls for ‘cyber sovereignty’. *BBC News,* 2015. december 16. https://www.bbc.com/news/world-asia-china-35109453

[12] Jack L. Goldsmith – Timothy Wu: *Who controls the Internet? Illusions of a borderless world*. Oxford, Oxford University Press, 2006. https://doi.org/10.1093/oso/9780195152661.001.0001

[13] Andrew Keane Woods: Litigating Data Sovereignty. *Yale Law Journal,* Vol. 128., N. 2. (2018) 369.

[14] Frank Pasquale azt veti fel, hogy az internet kapcsán a területi szuverenitás vagy a funkcionális szuverenitás fogalma használható-e jobban, illetve ezek miként keverednek folyamatosan az államok és az óriásplatformok vonatkozásában. Frank Pasquale: Two Visions for Data Governance. Territorial vs. Functional Sovereignty. In Anupam Chander – Haochen Sun (eds.): *Data Sovereignty. From the Digital Silk Road to the Return of the State*. Oxford, Oxford University Press, 2023. 35–48. https://doi.org/10.1093/oso/9780197582794.003.0002

[15] Anupam Chander – Haochen Sun: Introduction. Sovereignty 2.0. In: Chander–Sun (eds.) i. m. 21–22. https://doi.org/10.1093/oso/9780197582794.003.0001

3. Oroszország és az internetszuverenitás

A Riporterek Határok Nélkül (RSF) nemzetközi újságíró szervezet már a 2019-es éves jelentésében huszonhét olyan orosz törvényt tudott azonosítani, amelyek a véleménynyilvántás szabadságát korlátozzák az országban.[16] Ezek közül külön szükséges kiemelni a 2006. évi „Az információról, az információs technológiákról és az információ védelméről szóló törvény"[17] 2019-es módosítását, amely akár szabadságvesztéssel is sújthatja az illegális internetes tartalmakat megosztó felhasználókat.[18] A nemzetközi emberi bíróságok viszonylag következetes gyakorlata alapján kijelenthető, hogy a véleménynyilvánítás szabadságát érintő ügyekben ezen klasszikus büntetőjogi szankció használatától az államoknak inkább óvakodniuk kell.[19] Amennyiben a nemzeti joganyag mégis lehetővé teszi a használatát, akkor is meg kell felelnie a hármas-teszt gyakorlatának, azaz a beavatkozásnak „(a) alkalmasnak kell lennie az elérni kívánt jogszerű célok megvalósítására (megfelelőség vagy jogszerűség), (b) a lehető legkisebb mértékű beavatkozást jelentő eszköznek kell lennie (szükségesség), valamint (c) szigorúan arányban kell állnia az elérni kívánt jogi céllal (*stricto sensu* arányosság)".[20] A fent említett 2019-es RSF-jelentés kiegészítésében ráadásul bemutatják, hogy rövid két év alatt (2020–2021) újabb 16 hasonló jellegű törvényt került elfogadásra Oroszországban.[21]

Mindezekhez kiegészítésképpen hozzáadódik, hogy Oroszország ugyancsak 2019-ben – a 2013-as távközlésről szóló szövetségi törvény módosításaként[22] – elfogadta a szuverén internetről szóló törvényt is,[23] amely alapján:

---

16 Taking Control? Internet Censorship and Surveillance in Russia. *rsf.org*, 2019. november 27. 10–20. https://tinyurl.com/4pvv8y7u

17 Федерального закона от 27.07.2006 № 149-ФЗ „Об информации, информационных технологиях и о защите информации".

18 Andrei Richter: *Regulation of social media in Russia*. Strasbourg, European Audiovisual Observatory, 2021. 16.

19 Luzius Wildhaber: The right to offend, shock or disturb? Aspects of Freedom of Expression under the European Convention on Human Rights. *Irish Jurist*, Vol. 36., N. 1. (2001) 27.

20 Jan Oster: *Media Freedom as a Fundamental Right*. Cambridge, Cambridge University Press, 2015. 123–124. https://doi.org/10.1017/CBO9781316162736

21 Taking Control? Internet Censorship and Surveillance in Russia. Updated. *rsf.org*, 2021. augusztus 31. 9–18. https://tinyurl.com/3sh2wreh

22 A törvény elfogadásához vezető folyamatról és a törvény részletes szabályairól ld. Tölgyesi Beatrix: Az orosz „szuverén internet" törvényről. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 2020/2. 113–132. https://doi.org/10.32576/nb.2020.2.8 ; Russia: Growing Internet Isolation, Control, Censorship. Authorities Regulate Infrastructure, Block Content. *Human Rights Watch,* 2020. június 18. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

23 Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи" и Федеральный закон „Об информации, информационных технологиях и о защите информации".

– az internetszolgáltatóknak az ország webes forgalmát és információit kötelező államilag ellenőrzött pontokon keresztül vezetniük;[24]
– az orosz internetszolgáltatóknak kötelező mélységi tartalom-ellenőrzést (DPI) lehetővé tevő eszközöket telepíteniük, ezzel lehetővé téve az állami hatóságok számára, hogy megtalálják az általuk fenyegetőnek vagy veszélyesnek ítélt tartalmak eredeti forrását, és szükség esetén blokkolják azokat;
– a kormánynak joga van arra, hogy fenyegetés esetén fizikailag leválassza az orosz internetet a nemzetközi internethálózatról.[25]

Mindezeken felül a fenyegetőnek vagy veszélyesnek ítélt tartalmak homályos törvényi meghatározása miatt a hatóságok – az önkényes döntéshozatal problematikáját folyamatosan magában hordozó – feladata, hogy esetről-esetre eldöntsék, melyik helyzet követel nyomon követést, átirányítást vagy blokkolást. „A folyamat nem átlátható és visszaélések tárháza lehet”, jelentette ki a Human Rights Watch, kiemelve, hogy a jogszabály elfogadása „rossz hír Oroszország számára, és veszélyes precedenst teremt más országok számára”.[26]

Artyom Kozljuk, a *RoskomSvoboda,*[27] egy orosz internetszabadsággal foglalkozó civil szervezet vezetője a *Novaja Gazetá*nak adott 2021-es interjújában így fogalmazott: „Már most is számtalan lehetőség van arra, hogy bármilyen internetes erőforrást blokkoljanak, függetlenül annak méretétől, látogatottságától, irányától, domainzónájától vagy joghatóságától, rengeteg okból kifolyólag.”[28] Ezt alátámasztja, hogy Oroszország már korábban is gyakran élt a hatalom számára fenyegetőnek vagy veszélyesnek ítélt tartalmak kapcsán a blokkolás eszközével. Az állami hatóságok eszközei pedig változatosak voltak: alkalmaztak járulékos blokkolást, amikor a blokkolt IP-címen több oldal osztozott, köztük a megcélzott oldal is; túlzott blokkolást, amikor egy egész weboldalt blokkoltak egyetlen elfogadhatatlannak tartott lap vagy fájl miatt, vagy teljes körű blokkolást, amikor az internet egészét vagy egy részét blokkolták. Az Emberi Jogok Európai Bírósága (EJEB) mindegyik elé került, mérföldkőnek számító orosz ügyben megállapította az Emberi Jogok Európai Egyezményének (EJEE) 10. cikkének megsértését,[29] és egyértelműen kimondta, hogy a nemzeti eljárásokból hi-

[24] Oroszországban az ezen ellenőrzést kikerülő *Virtual Private Network* (VPN) használatra súlyos és elrettentő bírságok kiszabása is lehetséges. N/A: Госдума ввела штрафы за нарушение закона об анонимайзерах. *Meduza*, 2018. június 5. https://tinyurl.com/2p8m44eu

[25] Alexandra Ma: Russia officially introduced a ‚sovereign internet’ law to let Putin cut off the entire country from the rest of the web. *Insider*, 2019. november 1. https://tinyurl.com/54rfaj96

[26] Russia: New Law Expands Government Control Online. Wider Internet Surveillance. *Human Rights Watch,* 2019. október 31. https://tinyurl.com/28f692ah

[27] Роскомсвобода.

[28] Софья Кругликова: Что это вы тут надумали? *Новой газеты*, 2021. december 25. https://novayagazeta.ru/articles/2021/12/25/chto-eto-vy-tut-nadumali

[29] *Elvira Dmitriyeva v. Russia*, no. 60921/17 és 7202/18, 2019. április 30i ítélet; *Kablis v. Russia*, no. 48310/16 és 59663/17, 2019. április 30i ítélet; *Bulgakov v. Russia*, no. 20159/15, 2020. június 23i ítélet; *Engels v. Russia*, no. 61919/16, 2020. június 23i ítélet; *OOO Flavus and Others v. Russia*, no. 12468/15, 23489/15 és 19074/16, 2020. június 23i ítélet; *Vladimir Kharitonov v. Russia*, no. 10795/14, 2020. június 23-i ítélet; *Taganrog LRO and Others v. Russia,* no. 2401/10 és 19 másik, 2022. június 7-i ítélet; *OOO*

ányzott a szükséges legitimitás, mivel Oroszország vonatkozó törvényeinek a weboldalak blokkolásához rendelt szabályai nem biztosítottak megfelelő garanciákat a hatósági visszaélésekkel szemben. Az EJEB elvi éllel azt is kimondta, hogy „valamely weboldal elérésének teljes körű blokkolása olyan extrém intézkedés, amely egy újság- vagy televíziócsatorna-betiltáshoz hasonlítható."[30] Bár teljeskörűen nem állnak hivatalos adatok a rendelkezésünkre a blokkolások számát illetően, a *RoskomSvoboda* adatai szerint már az orosz–ukrán háború előtti 2021. évben nagyjából 200.000-re volt tehető az orosz hatóságok által blokkolt weboldalak száma.[31]

Az Európai Audiovizuális Megfigyelőközpont ugyanebben az évben úgy ítélte meg, hogy Oroszország a weboldalak blokkolása mellett az egyre jelentősebb összegű bírságok kiszabásának irányába is elindult:[32] a személyes adatok kezelésével összefüggésben immár 1-6 millió rubeles (4-24 millió HUF) bírság szabható ki első alkalommal, míg az ismételt jogsértés esetén az összeg 6-18 millió rubelre (24-72 millió HUF) emelkedik. 2021 augusztusában a *WhatsApp* még csak 4 millió rubeles (16 millió HUF), később – visszaesőként – a *Facebook* 15 millió rubeles (60 millió HUF), a *Twitter* a maximumhoz közelítő 17 millió rubeles (68 millió HUF) bírságot kapott.[33]

A szuverén internetről szóló törvény egyik legnagyobb figyelmet kapott szabálya – amely a Splinternet megvalósulását is elénk vetítheti –, hogy bizonyos fenyegetések esetén a *Roskomnadzor* átveheti az orosz internethálózat központi irányítását. A törvény 65. paragrafusának 1. pontja így fogalmaz: „A nyilvános hírközlő hálózat irányítását vészhelyzetekben a hírközlés területén a szövetségi végrehajtó szerv végzi, együttműködve a különleges célú hírközlő hálózatok és a nyilvános hírközlő hálózathoz kapcsolódó technológiai hírközlő hálózatok irányítóközpontjaival."[34] A vonatkozó vészhelyzetek között megtalálhatóak „A) a hálózat integritásának zavara (például ha a felhasználók között nem lehet kapcsolatot létesíteni); B) a hálózat stabilitásának meg-

---

Mediafokus v. Russia, no. 55496/19, 2023. január 17-i ítélet. Az egyes ügyeket részletesen ld. Gosztonyi Gergely: Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt. *In Medias Res*, 2021/1. 91–101.

30 *Vladimir Kharitonov v. Russia* i. m. 38.

31 Lena Masri: Explainer: Russia's internet crackdown. *Reuters*, 2022. március 31. https://www.reuters.com/world/europe/russias-internet-crackdown-2022-03-31

32 Richter i. m. 10–11.

33 A kiszabható pénzbírságok ráadásul exponenciálisan emelkednek, jelentős dermesztő hatást *(chilling effect)* okozva: az orosz–ukrán háború kitörése után az *Alphabet* 21,1 milliárd (!) rubeles (84,4 milliárd HUF) büntetést kapott, mivel a módosított Büntető Törvénykönyv 207. paragrafusának 3. bekezdése szerint hamis információkat engedett terjeszteni a platformjain (Google, YouTube) az orosz fegyveres erőkről. A bírság mértékét a Google oroszországi éves forgalmának arányában számították ki. N/A: Russia fines Google $370 million for repeated content violations, regulator says. *Reuters*, 2022. július 18. https://tinyurl.com/5n7n6jhk . Az orosz állam által hamis híreknek tekintett információkkal kapcsolatos részletes jogi háttérről ld. Elena Sherstoboeva: Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty. *International Communication Gazette,* Vol. 86., N. 1. (2024) 40. https://doi.org/10.1177/17480485231220141

34 Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи" и Федеральный закон „Об информации, информационных технологиях и о защите информации" (23. lj.), Статья 65.1.

bomlása (például ha a berendezések nem működnek megfelelően vagy természeti vagy ember okozta katasztrófák miatt működésképtelenné válnak); és C) a hálózat működésének biztonsága (például ha hackerek támadják a hálózatot, és az internetszolgáltatók nem tudnak ellenállni a támadásnak, vagy ha maguk az internetszolgáltatók okoznak fennakadást)”.[35] Ezen helyzetek bekövetkezése esetén a *Roskomnadzor* megtilthatja a távközlési üzeneteknek Oroszország területén kívül elhelyezkedő kommunikációs hálózatokon keresztül történő továbbítását, azaz az üzenetek csak orosz szervereken keresztül kerülhetnek egyik helyről a másikra.[36] Oroszország a hírek szerint néhány évig többször is próbálgatta a technológiát, és végül felhúzta a ‘digitális vasfüggönyt’, amikor 2021. június 15. és július 15. között – teszt jelleggel – sikeresen[37] megvalósította az ország fizikai leválását a nemzetközi internethálózatról.

4. Internetszuverenitás és weboldal blokkolások a háború árnyékában

A háború kitörése után egyértelműnek tetszik, hogy az orosz hatóságok minden eszközt felhasználtak, hogy az orosz lakosság jelentős részét elzárják a háborúval kapcsolatos negatív hírektől. Mindennek többféle eszközét vetették be az állami szervek a klasszikus cenzúrától kezdve a weboldalak blokkolásán át egészen az internetforgalom és internetes tartalmak állami megfigyeléséig.[38]

A nemzetközi internethálózat „nyitott, ingyenes, globális, interoperábilis, megbízható és biztonságos”[39] voltának egyik biztosítéka, hogy a webes forgalom millió és millió szerveren és számítógépen keresztül fut át, azaz kevés vagy minimalizált számú az úgynevezett hálózati fojtópont *(network choke point)* van, ahol a hálózat teljes vagy jelentős mennyiségű tartalma áramolna át.[40] A hálózattervezők mindent megtesznek az ilyen csomópontok kiküszöböléséért, mivel ezek jelentős támadási pontot kínálnak akár a crackereknek, akár a hardverhibáknak, akár az állami ellenőrzésnek. A potenciális hálózati fojtópontok száma egy országban azt tükrözheti, hogy „egy kormány milyen könnyen képes beavatkozni az internetforgalomba akár a kiberbiztonság, akár az ország polgárai kommunikációs szabadságának elnyomása érdekében.”[41] Az orosz

---

[35] Alena Epifanova: *Deciphering Russia’s ‘Sovereign Internet Law’: Tightening Control and Accelerating the Splinternet*. Berlin, Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V., 2020. 6.

[36] Technikailag ez jelenti az ország fizikai leválasztását az internetről.

[37] Ashley Collman: Russia disconnected itself from the rest of the internet, a test of its new defense from cyber warfare, report says. *Insider,* 2021. július 23. https://tinyurl.com/nhfdhw85

[38] Jelen tanulmány csak az Oroszországon belüli módszerekkel foglalkozik. Az orosz állam Ukrajna területén használt weboldal blokkolásairól és internetes forgalomelterelési technikáiról ld. Anastasiya Zhyrmont: #KeepItOn: Who is shutting down the internet in Ukraine? *AccessNow,* 2022. december 15. https://tinyurl.com/3n48xwa6

[39] A declaration for the future of the Internet, 2022. https://tinyurl.com/nh9jswzw

[40] Andrei Robachevsky – Christine Runnegar – Karen O’Donoghue – Mat Ford: The Danger of the New Internet Choke Points. *Internet Society,* 2014. február 14. 2. https://tinyurl.com/2vdbtrxs

[41] Monique Clement: Choke points and censorship: Protecting free flow of information on internet. *Arizona State University News,* 2018. szeptember 10. https://tinyurl.com/3fe79zky . Részletesen ld. Kirtus G. Leyba – Benjamin Edwards – Cynthia Freeman – Jedidiah R. Crandall – Stephanie Forrest:

szuverén internet-törvény ezen cenzurális ellenőrzést valósítja meg azzal, hogy az internetszolgáltatóknak az ország webes forgalmát és információit kötelező államilag ellenőrzött pontokon keresztül vezetniük, így fennáll annak a veszélye, hogy az orosz hatóságok nem csupán az egyértelműen jogellenes tartalmak megakadályozására, hanem a hatóságok álláspontja szerint veszélyes vagy zavaró jogszerű tartalmakba is be tudnak avatkozni. Ez utóbbi esetben pedig egyértelműen a véleménynyilvánítás szabadságának elhalványodásáról tudunk beszélni.

Bár technikai jellegűnek tűnik, de a szuverén internet-törvény lehetővé tette egy orosz nemzeti domainnév-rendszer (DNS, *Domain Name System*) létrehozását is.[42] A törvény 14. paragrafusának 2. bekezdése alapján az erre vonatkozó szabályokat, „a vele szemben támasztott követelményeket, a létrehozására vonatkozó eljárást, beleértve a benne foglalt információk kialakítását, valamint a használatára vonatkozó szabályokat, beleértve az információkhoz való hozzáférés biztosításának feltételeit és eljárását" újfent a *Roskomnadzor* határozza meg. 2019-ben ezt többen úgy értelmezték, mint egy újabb lépést az online izoláció irányába, hiszen „alapvetően szétttördeli a globális DNS-t, és ennek következtében aláássa és szétttördeli magának az internetnek a globális jellegét."[43] A valóságban a leválás helyett az elmúlt pár évben (még csak) egy párhuzamos – általuk védelminek nevezett – struktúrát építettek ki Oroszországban, arra való hivatkozással, hogy amennyiben egy külföldi hatalom – jelesül a világ legtöbb DNS gyökérszerveréért felelős Amerikai Egyesült Államok[44] – valamilyen módon beavatkozna az internetforgalomba, akkor lehetőség legyen fenntartani az orosz internethálózatot.

Ezen párhuzamos struktúrával kapcsolatos jelentős problémával lehetett szembesülni 2024. január 30-án, amikor is az orosz internet több órán át nem működött.[45] Ez a gyakorlatban azt jelentette, hogy a .ru felső szintű tartományt (TLD, *top-level domain*) használó weboldalak elérhetetlenek voltak mind Oroszországból, mind pedig külföldről. Ez pedig nem más, mint az a helyzet, amikor az orosz állampolgárok elzárva kell létezzenek a digitális világtól, amire nem egy távoli analógia, hogy Oroszország a 'kiber Gulágra' küldi lakosait, távol a felforgatónak vélt információktól, kontrollálva életük minél nagyobb szeletét.

Borders and gateways: measuring and analyzing national as chokepoints. In: Jay CHEN – Jennifeer MANKOFF – Carla GOMES (eds.): *Compass '19: Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*. New York, Association for Computing Machinery, 2019. https://doi.org/10.1145/3314344.3332502

42 Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи" и Федеральный закон „Об информации, информационных технологиях и о защите информации" (23. lj.), Статья 14.2.

43 N/A: Mandating Certain Types of Connections Is Risky. *Internet Society,* 2023. december 1. https://www.internetsociety.org/resources/internet-fragmentation/russias-national-dns

44 Sara JELEN: DNS Root Servers: What Are They and Are There Really Only 13? *SecurityTrails Blog,* 2021. július 30. https://securitytrails.com/blog/dns-root-servers

45 N/A: Mass Blackout Takes Russian Internet Offline. *The Moscow Times,* 2024. január 30. https://tinyurl.com/5um6ysrz

Mivel a probléma érintette a nagy orosz szolgáltatókat is, ezért – hivatalos magyarázat hiányában – többféle teória is lábra kelt a következő napokban. Ezek közül az egyik magyarázat szerint a leállás egy ki nem kényszerített hiba volt, mivel „a hatóságok tesztelték az elszigetelt orosz internet működőképességét.”[46] Ez összefüggésben lehet az orosz internet fizikai leválasztásának tesztelésével, amit – a 2022-es évet kihagyva – 2023 kora nyarán ismét elvégzett Oroszország.[47] Alexander Amzin álláspontja szerint ezen állami hibának az egyik oka az is lehet, hogy „az ukrajnai invázió nemcsak megerősítette az oroszországi internetes elnyomást, hanem céltalanná és kaotikussá is tette azt.”[48] Ebbe pedig könnyen belefér az, hogy a hatóságok próbálkoznak a tesztelés során többféle technológiai megoldással, és nem veszik figyelembe az esetleges következményeket.

Ha az internetszuverenitás kapcsán a fentieknél kisebb léptéket keresünk, fordulhatunk a *Roskomnadzor* hivatalos adatbázisához,[49] ám az adatbázis nem különösebben felhasználóbarát, ha összehasonlító adatokat keresne rajta valaki. Ráadásul a *RoskomSvoboda* saját adatbázist[50] működtet, hogy az érdeklődők a valós adatokhoz juthassanak hozzá. Ebben azt láthatjuk, hogy 2022 februárjának végétől a weboldalblokkolások száma emelkedésbe kezdett: a *RoskomSvoboda* blokkolt weboldalakat listázó adatbázisában majdnem 250.000 oldal volt megtalálható csak a 2022. évre vonatkozóan. A legtöbb, majdnem 80.000 blokkolást az Orosz Szövetségi Adóhivatal[51] rendelte el, de a leginkább figyelemre méltó mégis az a 3.503 darab blokkolás, ahol az ismeretlen *(неизвестно)* címke szerepel, azaz nem ismerhető meg, hogy melyik állami szerv áll a blokkolás mögött.[52] Ahol mégis, ott a blokkolást elrendelő állami hivatalok között megtalálható a *Rospotrebnadzor,* az Orosz Szövetségi Fogyasztóvédelmi és Emberi Jólét Felügyeleti Szolgálat[53] ugyanúgy, mint a *Rosdravnadzor,* az Orosz Szövetségi Egészségügyi Felügyeleti Szolgálat[54] vagy a *Rosmolodezh,* az Orosz Szövetségi Ifjúsági Ügyek Ügynökség[55]. Bár az EJEB többször is kimondta, hogy a blokkolási intézkedéseket elsősorban bíróságnak vagy független bírói szervnek kell elrendelnie,[56]

---

46 Kevin Rothrock: The Russian Internet’s domain problems and how the war in Ukraine narrows the Kremlin’s options for online controls. *Meduza*, 2024. február 1., https://tinyurl.com/52unzpcs

47 Uo.

48 N/A: Масштабный сбой в российском интернете, вероятно, связан с активным строительством Чебурнета — «суверенного интернета». *Meduza,* 2024. január 31. https://tinyurl.com/3hcmutc2

49 https://eais.rkn.gov.ru

50 https://reestr.rublacklist.net

51 Федеральная налоговая служба.

52 How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine. *Open Observatory of Network Interference,* 2023. február 24. https://tinyurl.com/mr464kpb

53 Роспотребнадзор, Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека.

54 Росздравнадзор, Федеральная служба по надзору в сфере здравоохранения.

55 Росмолодёжь, Федеральное агентство по делам молодёжи.

56 *OOO Flavus and Others v. Russia* 39.

az adatbázisban számos orosz hatóság intézkedése található meg.[57] Ráadásul 2022-ben a külföldi ügynökökről szóló törvény módosítása lehetővé tette az Igazságügyi Minisztérium számára, hogy bírósági határozat nélkül blokkolja a kijelölt „külföldi ügynökök" weboldalait.[58]

A blokkolások a nagy nyugati online óriásplatformokat is érintik. Röviddel a háború kitörése után Oroszország blokkolta a *GoogleNews*-t és a *Twitter*-t is, mert az ukrajnai inváziót szóló, álláspontjuk szerint „nem hiteles" információkra hivatkoztak, és mert a platformok intézkedéseket hoztak a háborúval kapcsolatos orosz dezinformáció terjedésének visszaszorítására.[59] A *Roskomnadzor* hasonló intézkedés alkalmazásával fenyegette meg a *TikTok*-ot is, amely nem várta meg a döntést, hanem saját maga függesztette fel a *livestreaming*et és a feltöltési lehetőséget Oroszországban.

2022 márciusában a *Meta* az orosz–ukrán háború kapcsán bizonyos esetekben felfüggesztette a gyűlöletbeszéddel kapcsolatos közösségi alapelveit,[60] és úgy nyilatkozott, hogy „ideiglenesen engedélyeztük a politikai véleménynyilvánítás olyan formáit, amelyek normális esetben megszegnék a szabályainkat, mint például az erőszakos beszéd, például a »halál az orosz megszállókra«".[61] Erre reakcióképpen az orosz főügyészség kérelmére a *Roskomnadzor* blokkolta a *Facebook*hoz és az *Instagram*hoz való hozzáférést[62] Oroszországban azzal az indokkal, hogy egyrészt a platformokon lehetséges az orosz hadsereggel szembeni gyűlöletbeszéd, másrészt pedig a *Meta* az országgal szemben diszkriminatív gyakorlatot folytat, mivel blokkolja az egész Európai Unióban a *Russia Today* (RT) és a *Szputnyik* elérését.[63] A megfellebbezett blokkolási döntést az elsőfokú orosz bíróság helybenhagyta, és emellett az ítéletben egyetértett az orosz ügyészség kérelmével, miszerint a bíróság állapítsa meg, hogy a vállalat az orosz Büntető Törvénykönyv 282. paragrafusának 2. bekezdése alapján „szélsőséges

---

57 Összevetésképpen érdemes megjegyezni, hogy Törökországban is „több mint 15 intézmény és szervezet kapott felhatalmazást arra, hogy különböző szabályozások alapján hozzáférés-korlátozó végzéseket bocsásson ki vagy kérjen, és e hatáskörök többségét bírósági jóváhagyáshoz nem kötött közigazgatási blokkolási végzések benyújtásán keresztül gyakorolták". Yaman AKDENIZ – Ozan GÜVEN: *Web 2019: An Iceberg of Unseen Internet Censorship in Turkey.* Istanbul, İfade Özgürlüğü Derneği – Freedom of Expression Association, 2020. 4–8.

58 *Freedom on the Net 2023. Russia Country Report.* Freedom House, 2023. október 3. https://freedomhouse.org/country/russia/freedom-net/2023

59 Russell BRANDOM: Russia blocks Twitter as Ukraine invasion escalates. *The Verge,* 2022. február 26., https://tinyurl.com/4k7k3wsh

60 https://transparency.fb.com/hu-hu/policies/community-standards/hate-speech

61 Munsif VENGATTIL – Elizabeth CULLIFORD: Facebook allows war posts urging violence against Russian invaders. *Reuters,* 2022. március 11. https://tinyurl.com/mvfufsj8

62 Érdekesség, hogy az ügyészség kérelme a WhatsApp üzenetküldő szolgáltatásra nem vonatkozott.

63 A részletes jogi eljárásról ld. Gergely Ferenc LENDVAI: Media in War: An Overview of the European Restrictions on Russian Media. *European Papers,* Vol. 8., N. 3. (2023) 1235–1245. https://doi.org/10.15166/2499-8249/715; András KOLTAY: Censorship as a Tool Against State Disinformation: The Freedom of Expression Implications of the Russian–Ukrainian War. *Journal of International Media & Entertainment Law,* 2023, 10(1), 1–53.; Joan BARATA – Jordi CALVET-BADEMUNT: The European Commission's Approach to DSA Systemic Risk is Concerning for Freedom of Expression. *Tech Policy Press,* 2023. október 30. https://tinyurl.com/4h9s2ujm

tevékenységet folytat”.[64] Mivel a *Meta* ezen döntés ellen is fellebbezéssel élt, 2022 júniusában a Moszkvai Városi Bíróság továbbra is fenntartotta az orosz igazságszolgáltatás korábbi döntését, így az orosz fiatalok körében kiemelten népszerű *Instagram* elérhetősége továbbra is blokkolva van az országban.

Érdemes megemlíteni, hogy a *YouTube* – annak ellenére, hogy szintén felfüggesztette az orosz állami propagandát sugárzó csatornák terjesztését – nem került fel a blokkolt weboldalak listájára. Több szakértő álláspontja szerint ennek legfőbb oka a szolgáltatást használók száma: míg a *Twitter*-t az orosz internetfelhasználók csak nagyjából 6%-a, a *Facebook*-ot pedig 25%-a használta, ez az arány a *YouTube* esetében 45%-os.[65]

Ráadásul a külföldi alkalmazások blokkolása lehetőséget terem a helyi alternatívák megerősödésére, ami egyrészt Oroszországban egy már jó ideje tartó folyamat, másrészt pedig „csökkentheti a külföldi alkalmazások blokkolásának költségeit.”[66] Bár nem következett be a *Reddit*-en terjedő ironikus mém,[67] miszerint a *LinkedIn*-t a *LeninkedIn,* a *Tinder*-t a *Putinder,* a *Google*-t a *Gogol* vagy a *Spotify*-t a *Spotnik* alkalmazások váltsák fel, az orosz közösségi média alkalmazások egy meghatározott arányig képesek kiváltani a nyugati cégek által kínáltakat. A *VKontakte*-t *(ВКонтакте)* az orosz internetfelhasználók 54%-a, az *Odnoklassniki*-t *(Одноклассники)* a 38%-a, míg a *MoiMir*-t *(МоёМир)* a 44%-a használja.[68] Mindegyik mögött felsejlik Alisher Usmanov üzbég–orosz „Kreml-barát oligarcha, aki különösen szoros kapcsolatban áll Vlagyimir Putyin orosz elnökkel.”[69] Így keveredik véglegesen össze a politika, a média és a háború világa a szemünk előtt, amely összefüggéseket az autoriter államok gyakran rejtenek el szépen csengő nyugatellenes jelszavak mögé. Úgy tűnik, Oroszország tényleg a „Kiber Gulágra” küldi a külvilág és a nem propagandahírek iránt érdeklődő állampolgárait.

5. Zárszó helyett

David Bromel 2022-ben így fogalmazott: „az internet első évei hatalmas buli volt – vad és veszélyes. De most a bulinak vége, és minden vendégnek segítenie kell a takarítás-

---

64 Ráadásul a vállalatot a *Rosfinmonitoring,* az Orosz Szövetségi Pénzügyi Ellenőrző Szolgálat (Росфинмониторинг, Федеральная служба по финансовому мониторингу) 2022 októberében felrakta a terrorista és szélsőséges szervezeteket tartalmazó listájára, ellehetetlenítve ezzel oroszországi működését.

65 Billy Perrigo: Why YouTube Has Survived Russia’s Social Media Crackdown—So Far. *Time,* 2022. március 23. https://time.com/6156927/youtube-russia-ukraine-disinformation

66 Chander–Haochen i. m. 16.

67 https://www.reddit.com/r/memes/comments/tryzi0/go_to_googlag

68 Karl Kangur: Social Media in Russia. *Dreamgrow,* 2023. január 1. https://www.dreamgrow.com/social-media-in-russia/

69 A Tanács (EU) 2022/336 végrehajtási rendelete (2022. február 28.) az Ukrajna területi integritását, szuverenitását és függetlenségét aláásó vagy fenyegető intézkedések miatti korlátozó intézkedésekről szóló 269/2014/EU rendelet végrehajtásáról. HL L 58., 2022.2.28., 1–18.

ban."[70] Mindez alatt Bromel azt értette, hogy a korábbi, szinte szabályozhatatlannak és szabályozatlannak tekintett új kommunikációs teret bizony szabályokkal kell rávenni arra, hogy azon alapértékek, amelyeket társadalmaink magukénak vallanak, az online térben is érvényesülhessenek. Ám a kétezertízes évek közepétől egyre erősödő állami szabályozási igény bizony magával hozta azt is, hogy „a globális normák drámaian eltolódtak a digitális szférában történő nagyobb kormányzati beavatkozás irányába."[71]

Szerte a világban pedig egyre több autoriter vagy erősen autoriter jellegű állam próbálgatja az internet határokon átnyúló jellegének és a globális közösségnek határait. A kérdés pedig így az, hogy az államok hagyományos területi szuverenitása milyen mértékben érvényeül és érvényesíthető a kibertérben. Ahogy Pia Hüsch fogalmazott a kérdés kapcsán: „A kibertér egyedi jellemzői még egy újabb nehézségi szintet adnak az állami szuverenitás megértésének kihívásához, így az államok alapvetően nem értenek egyet abban, hogyan közelítsék meg a szuverenitást a kibertérben."[72]

Az internethálózathoz és az internetes tartalmakhoz való hozzáférést „a véleménynyilvánítás szabadságához fűződő emberi jog gyakorlásának fényében kell vizsgálni, mint az információk és eszmék befogadásának és továbbításának eszközét."[73] Ennek függvényében az állampolgárok elzárása az információktól egyértelműen beavatkozás a véleménynyilvánítási szabadságukba, és mint ilyen, mindenképpen számot tarthat a figyelmünkre. Ahogy fentebb láthattuk, Oroszország az információk elzárása érdekében az eszközök széles tárházát alkalmazza: a klasszikus cenzúrától kezdve a weboldalak blokkolásán át egészen az internetforgalom és internetes tartalmak állami megfigyeléséig.[74] A digitális világgal kapcsolatban a legfőbb kérdés, amelyre az autoriter vezetők választ keresnek, hogy lehet-e olyan megoldás a 21. században, amely egyszerre biztosítja a gazdasági nyitottságot és a fejlődést, ugyanakkor az információs zártságot is?

Biztató jelek vannak a nemzetközi közösség részéről: 2024 elejéig 70 ország látta el kézjegyével a 2022-ben elfogadott nyilatkozatot az internet jövőjéről, amely egy megbízható és kiszámítható internet jövőképét és elveit határozza meg.[75] Ebben az aláírók felszólítják a világ kormányait, hogy – többek között – a) tartózkodjanak a kormány által elrendelt internetlezárásoktól vagy a belföldi internet-hozzáférés teljes vagy rész-

---

[70] David Bromel: *Regulating free speech in a digital age. Hate, harm and the limits of censorship*. Cham, Springer, 2022. 217. https://doi.org/10.1007/978-3-030-95550-2

[71] *Freedom on the Net 2021. The Global Drive to Control Big Tech*. Freedom House, 2021. szeptember 16. 11. https://tinyurl.com/3tr7j2uj

[72] Pia Hüsch: Error 404: No Sovereignty Analogy Found. In: Angelo Golia Jr. – Matthias C. Kettemann – Raffaela Kunz (eds.): *Digital Transformations in Public International Law*. Baden-Baden, Nomos, 2022. 29. https://doi.org/10.5771/9783748931638-25

[73] Marijana Mladenov – Tamara Staparski: Human rights approach to internet access with a special emphasis on the case-law of the European Court of Human Rights. *Revija za evropsko pravo,* Vol. 24., N. 1. (2022) 34.

[74] Jelen tanulmány csak az Oroszországon belüli módszerekkel foglalkozik. Az orosz állam Ukrajna területén használt weboldal blokkolásairól és internetes forgalomelterelési technikáiról ld. Anastasiya Zhyrmont: #KeepItOn: Who is shutting down the internet in Ukraine? *AccessNow,* 2022. december 15. https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine

[75] Oroszország nincs az aláírók között.

leges korlátozásától, és b) – a hálózatsemlegesség elveivel összhangban – tartózkodjanak a jogszerű internetes tartalmakhoz, szolgáltatásokhoz és alkalmazásokhoz való hozzáférés blokkolásától vagy korlátozásától.[76] A világ számára létfontosságú lenne, hogy egyes államok ne taszíthassák polgáraikat a digitális sötétségbe.[77] Orosz analógiával élve: ne hozhassanak létre ‘digitális vasfüggönyöket’ vagy ‘kiber Gulágokat’, mert annak rövid- és hosszútávon is visszafordíthatatlan társadalmi és gazdasági következményei lesznek.

[76] A declaration for the future of the Internet, 2022. 2. https://tinyurl.com/nh9jswzw (39. lj.)

[77] Shilpa Jain – Adithya Anil Variath: Internet shutdowns and virtual curfews: searching for rights in digital darkness. *CASIHR Journal on Human Rights Practice,* Vol. 4., N. 2. (2020) 35–48.