

Az Internet jövője: egység vagy széttagol(ód)ás?

Sokan azok közül, akik részt vesznek az internet irányításában, aggodalmukat fejezik ki, mert szerintük veszélyben van az internet egysége. Az államok és a nagy technológiai cégek, a „Big Tech” döntései arra vezetnek, hogy a hálózat különböző felhasználói nem ugyanazt látják attól függően, hogy melyik országban tartózkodnak, milyen szolgáltatónál vannak csatlakozva, és milyen szoftvert futtatnak a gépükön, vagy milyen közösségi hálózaton van fiókjuk. A gazdasági és politikai folyamatok, amelyek esetleg, végső soron az internet széttagolásához vezethetnének, még messze nem érték el ezt a pontot. De így is komolyan lehet korlátozni az internet egyetemeségét. A tanulmányunk eredeti célja – az Európai Parlament felkérésére – ezeknek a folyamatoknak a feltárása és elemzése, beleértve az Európai Unió tevékenységének a hatását ezen a téren. Nem minden centrifugális tendencia kerülhető el – vagy akár kerülendő el. Így végül az alapvető jogok prizmáján keresztül elemeztük ezt az alakuló közproblémát. E cikkben a tanulmányunk főbb következtetéseit találják.

Kulcsszavak: *Internet szabályozása, geopolitika, cenzúra, transznacionális közszférák*

Köszönetnyilvánítás

A cikkben bemutatott kutatási eredmények az Európai Parlament STOA Bizottság, az Internet Society France, a CNRS Internet, Mesterséges Intelligencia és Társadalom Kutatóhálózat Internet Irányítását és Szabályozását kutató Munkacsoport és a Párizs 8 Vincennes Egyetem Média, Technológiák és Internacionalizáció Kutatóközpontja (CÉMTI) által támogatott kutatási projekt keretében jöttek létre. Székely Ivánnak különösen köszönjük a segítségét a cikk nyelvi lektorálásában.

Szerzői információ

Rossi, Julien, Párizs 8 Egyetem,

<https://orcid.org/0000-0003-3715-9720>

Perarnaud, Clément, Vrije Universiteit Brussel,

<https://orcid.org/0000-0002-6491-1466>

Musiani, Francesca, Centre Internet et société – CNRS,

<https://orcid.org/0000-0001-8343-6122>

Castex, Lucien, Afnic,

<https://orcid.org/0000-0002-1849-8308>

Így hivatkozzon erre a cikkre:

Rossi, Julien, Clément Perarnaud, Francesca Musiani, Lucien Castex. „Az Internet jövője: egység vagy széttagol(ód)ás?”. *Információs Társadalom* XXVI, 1. szám (2026): 66–80.

== <https://dx.doi.org/10.22503/inftars.XXVI.2026.1.12> ==

A folyóiratban közölt művek

a Creative Commons Nevezd meg! – Ne add el! – Így add tovább! 4.0

Nemzetközi Licenc feltételeinek megfelelően használhatók.

The Future of the Internet: Unity or Fragmentation?

Many actors in the field of Internet Governance fear that the unity of the Internet may be at risk. The decisions of both states and “Big Tech” corporations lead to a situation where different users of the network do not see the same thing, depending on which country they are in, which service provider they are connected to, what software they are running on their computers, or which social network they have an account on. The economic and political processes that could eventually lead to the fragmentation of the Internet have not yet reached this stage. But the unity of this network can still be seriously limited. The original aim of our study – at the request of the European Parliament – was to explore and analyse these processes, including the effects of the European Union’s actions in this field. Not all centrifugal tendencies can – or should – be avoided. Thus, we finally analysed this emerging public problem through the prism of fundamental rights. In this article, you will find the main conclusions of our study.

Keywords: *Internet governance, geopolitics, censorship, transnational public spheres*

Bevezetés

Egy felhasználó szemében az internet egy globális közszféra, amely átível a nemzetállamok és a nagy techvállalatok határain. Bármelyik országból hozzá lehet férni bármilyen más országban készült és tárolt tartalomhoz. Ezt akármilyen számítógéppel meg lehet tenni, teljesen függetlenül attól, hogy melyik cég fejlesztette azokat az applikációkat, amelyeket anet böngészésére használunk. Ezek a tartalmak egy olyan “kibertérben”, adott esetben „felhőben” (*cloud*) vannak, amiről úgy tűnik, mintha az anyagi, földrajzi világon kívül létezne; így esik gyakran szó a „dematerializációról”, amikor egy eredetileg fizikai helyen elérhető szolgáltatás a neten válik elérhetővé. Ezen a nem letéző helyen, ami csak az internetfelhasználó élményében válik területté, egyesek szerint anarchia uralkodik. Ott valósulhatna meg a „globális falu” utópisztikus ígérete. John Perry Barlow amerikai író és aktivista, aki részt vett az Electronic Frontier Foundation civil szervezet alapításában, 1996 februárjában egy „Kibertér Függetlenségi Nyilatkozatot” írt, amelyben a következőt követelte az állami hatalmaktól:

Ipari világ kormányai, fáradt hús-acél óriások! A kibertérből jövök, az Elme új otthonából! A jövő nevében arra kérem a múltat, hogy hagyjon minket békén! Nem látunk szívesen közöttünk. Nincs szuverenitásokat ott, ahol összegyűlünk!
(Barlow 1996).

Így szólt a szabadságról és az egyetemes emberiségről az az utópia, amely többek között Ted Nelson (1974) *Computer Lib/Dream Machines* című könyvében bontakozik ki, amelyről több, számítástechnikával foglalkozó történész számolt be (Musiani és Schafer 2011; Russell 2006; Turner 2008; Flichy 2001), és amiről Félix Tréguer 2019-ben állította, hogy “elesett” (Tréguer 2019). Az egyik oka ennek a csalódásnak az – főként, de nem kizárólagosan –, hogy a tekintélyelvű államok egyre hatékonyabban gyakorolják a hatalmukat a kibertérben is, sokszor a technológiai vállalatok együttműködésével.

Így a szilícium-völgyi utópiák bukásának az egyik oka, hogy valótlan az az állítás, ami szerint az internet a földrajzi világon kívül létezne. Kábelekből, gépekből, valamint műholdakból áll össze – aminek nem mellesleg komoly környezetszennyező hatása van (Flipo, Dobré és Michot 2013). Ezek a tárgyi eszközök a földrajzi valósághoz vannak kötve, nemzetállamok területén, amelyek mégis gyakorolják a hatalmukat (Firmino, Melgaço és Kloza 2018). Tény, hogy az interneten keringő adatok nem tartják be az államhatárokat. Ez nehezíti az állami szuverenitás gyakorlását. Így 2020-ban még az orosz hatóságok is elismerték a kudarcukat, amikor nem sikerült hatékonyan kitiltaniuk a Telegram titkosított csevegőapplikációt az ország területéről (Ermoshina és Musiani 2021). De 2024-ben Franciaországnak sikerült előzetes letartóztatás alá vonni Pavel Durovot, a Telegram alapítóját. A francia nyomozók azzal vádolják, hogy bűnrészes a platformon folytatott illegális cselekményekben, amelyeket többek között pénzmosásra, kábítószer-kereskedelemre és más bűncse-

¹ Szerzők fordítása az angolból.

lekményekre használtak (Kaufmann 2024). Ugyanebben az országban a hatóságok, Gérald Darmanin belügyminiszter telefonon adott utasítására, 2024 májusában kikapcsolták a TikTokot Új-Kaledóniában arra hivatkozva, hogy az ezen a közösségi médián keresztül terjesztett tartalmak gerjesztették az erőszakos függetlenségpárti lázadásokat a szigetcsoporton (Rosson 2024). Így nem csak a tekintélyelvű rezsimiek döntenek az internet egyetemességének korlátozásáról, hanem liberális demokráciák is, beleértve az Európai Uniót (EU) és annak tagállamait. Céges, gazdasági érdekek is szerepet játszhatnak. A 2000-es évek eleje óta rendszeresen korlátozzák a szellemi tulajdonjog által védett tartalmak forgalmát úgy, hogy azok ne –vagy csak nehezebben – legyenek elérhetőek azokon az országokon kívül, ahol a közvetítési jogok ezt engedélyezik (Lenert 2004). Továbbá a nagy techbirodalmak, mint a Meta vagy az Alphabet, érdekeltek abban, hogy a felhasználói minél inkább a saját zárt kertjükben maradjanak, aminek az az eredménye, hogy az egyik cég felhasználója nem mindig férhet hozzá egy másik cégnél tárolt vagy közvetített tartalomhoz.

Mindez azt az aggályt veti fel, hogy veszélyben lehet az internet egysége. Ezt a folyamatot nem lehet visszafejteni egyetlen központi akaratra. Bár részben bizonyos szereplők tudatos döntéseiből ered, sokszor számos, egymástól független tényező keresztüzében alakul, ezért bár angolul vagy franciául mindenképpen a „fragmentation” szóval lehet leírni, a magyar nyelv lehetőséget ad arra, hogy azt állítsuk, hogy egyszerre széttagolásról és széttagolódásról van szó, ami akár több, egymástól teljesen szétszakadt, úgynevezett „Splinternet”-hez² vezethetne.

Bár maga a szó 2001-ben jelent meg először a *Forbes* magazinban (Wayne Crews 2001), leginkább a 2010-es évek eleje óta jelennek meg újságírói és tudományos publikációk, amelyek a „Splinternet”, azaz a széttagolt-internet veszélyét tárgyalják (például Ananthaswamy 2011; Malcomson 2016; Drake, Cerf és Kleinwächter 2016; Mueller 2017; Lemley 2020). Tényleg széttagolódhatna különböző összeférhetetlen nemzeti vagy magáncéges „Splinternetekké”? Erre a kérdésre kereste a választ az Európai Parlament Testülete a Tudomány Jövőjéért³ (röviden: STOA Testület), amikor a kutatócsoportunkra bízta a feladatot, hogy írjunk jelentést a témáról, amiben arra is kértek, hogy fordítsunk figyelmet az Európai Unió (EU) politikáinak erre a jelenségre gyakorolt hatásaira. Ez lett a kezdőpontja egy többéves projektnek, amely a Francia Nemzeti Tudományos Kutatási Központ (CNRS) „Internet, Mesterséges Intelligencia és Társadalom Kutatóhálózat Internet Irányítását és Szabályozását kutató Munkacsoportja” keretében bontakozott ki. A kutatás eredményei először a STOA Testületnek egy 2022-ben átadott jelentésben jelentek meg (Perarnaud et al. 2022), amit később egy 2024 szeptemberében kiadott könyvben frissítettünk (Perarnaud et al. 2024). Ennek a munkának a főbb következtetéseit igyekszünk itt megfogalmazni.

Még mielőtt ezek szóba kerülhetnének, fontos az internet múltjából megérteni, ahogy egységes közszféraként formálódott meg. Ebből kiindulva pontosítjuk, hogy mit eredményezne az internet „széttagolása”, mivel ez akár a szakirodalomban is vitatott kérdés. Egyesek (például Mueller 2017) nagyon szűk technikai szemszögből definiálják ezt a folyamatot, ami teljesen figyelem kívül hagyja azokat a társadalmi

² Ez a szó az angol „to splinter” (széttagolni) ige és az Internet tulajdonnévből áll össze.

³ Angolul: STOA Panel on the Future of Technology.

tényezőket, amelyek ugyanúgy hatnak a felhasználó lehetőségeire, hogy ország- és nagyvállalati határtól függetlenül tudjon hozzáférni egy egységes online közzsférá-hoz. Ebből kiindulva felvázoljuk, hogy milyen geopolitikai és gazdasági folyamatok hatnak az internet infrastrukturális irányítására úgy, hogy valóban egyre nagyobb feszültség alá kerül annak egyetemessége – anélkül, hogy eddig valóban lehetne elszakadt „Splinternetekről” beszélni. Záró fejezetként az EU szerepét említjük, megmutatva azt, hogy a 2020-as évek első felében az internet széttagolása még csak egy alakuló közprobléma volt. Végül kimutatjuk, hogy végeredményben a vita arról szól, hogy egy állam meddig mehet el azért, hogy érvényesítse szuverenitását a „kibertérben”. A liberális alapjogi és alkotmányjogi hagyomány követése szerintünk azt eredményezheti csak, hogy az állam elfogadja, hogy akár a „fizikai” világban, akár az internet saját világában korlátozza a hatalmát annak érdekében, hogy óvja az alapvető szabadságokat a teljhatalom veszélyeitől, és ne tegye tönkre az internetet.

A „Splinternet”: kísérlet egy épülő közprobléma definíciójára

Az első példa, ami valószínűleg bárkinek az eszébe jut, amikor az internet széttagolásáról hall, az a kínai vagy az orosz. Kína a 2000-es évek eleje óta üzemelteti a „Nagy Kínai Tűzfalat”, és rendszeresen kísérletezik a globális internetszabványok helyett saját fejlesztésüket bevezetni a saját területén, ha nem sikerül nemzetközi szinten (Kim, Lee és Kwak 2020; Nanni 2022; Hoffmann et al. 2020). A lakosság nagyobb része helyi szolgáltatásokat használ, mint a Weibo vagy a QQ, részben azért, mert nem könnyű hozzáférni a nagyobb nyugati cégek szervereihez. Oroszországban is épül a helyi „Ru-Net”. A VKontakte nagy vonalakban a Facebook szerepét játssza, míg a Yandex a Google-ét. Az orosz hatóságok csak később kezdtek komolyabban foglalkozni az internet szabályozásával és korlátozásával. Az elején kudarcra jártak, és 2020-ban feladták a kísérletüket a Telegram blokkolására (Ermoshina és Musiani 2021), de az utóbbi években egyre hatékonyabban sikerül az orosz netcsendőrségnek (a *RosKomNadzornak*) blokkoló- és megfigyelőtechnológiákat telepíteni a nemzeti netes infrastruktúrára (Ermoshina, Loveluck és Musiani 2022).

Mindezek ellenére Milton Mueller szerint nem lehet az ilyen példánál valódi széttagolásról beszélni, mivel a bevezetett cenzúra nem teszi teljesen lehetetlenné a kommunikációt két IP-csomópont között. Ráadásul az internet soha nem volt *egyetlen* hálózat, hiszen rengeteg úgynevezett autonóm rendszerből – tehát egymástól független hálózathoz – áll össze, amelyek mind ugyanazokat a protokollokat használják annak érdekében, hogy tudjanak egymással kommunikálni. Így:

“Az internet hozzáférhetősége valójában nem bomlik szét és nem gyengül, hanem éppen hogy virálisan terjed. Bár mindegyik autonóm rendszer azzal a kapacitással és joggal rendelkezik, hogy szabályozza a kapcsolatát az internethez, a nyitottság a világ többi számítógépéhez továbbra is alapbeállítás ebben a környezetben. Nagy erőfeszítést követel egy autonóm rendszertől, ha korlátozni kívánja a hozzáférhetőségét a hálózathoz”⁴ (Mueller 2017, 25).

⁴ Szerzők fordítása az angol eredetiből.

Tény, hogy ha egy ország hatósága a helyi domainnév-szervereket egy adott domain törlésére kényszeríti, akkor még mindig lehet kapcsolatot teremteni, ha valaki tudja az adott célnak az IP-címét, vagy ha úgy módosítja a gépe konfigurációját, hogy az egy külföldi domainnév-szerverről kérje az adatot. Megoldást nyújtanak a virtuális magánhálózatok (VPN), valamint a TOR-hálózat is.

A számítógépes hálózatok működése réteges architektúrát követ, amit eredetileg az ISO fejlesztett és "OSI-modellként" határozott meg a 80-as években (Russell 2006): az alkalmazási rétegnek (például a web, az e-mailezés stb.) szüksége van az alsóbb rétegekre: a szállítási rétegre (ami két alkalmazás között kommunikációs munkamenetet hoz létre), a hálózati rétegre (ami minden adatot IP-csomagban szállít) és egy fizikai rétegre (maguk a kábelek vagy rádióhullámok). Vannak, akik Muellert követve úgy vélik, hogy csak abban a pillanatban van széttagolás, ha az alsó rétegek nem tudnak egymásnak üzenetet küldeni. Mivel a domainnév-rendszer (*Domain Name System*, DNS) az alkalmazási réteg része, ha azon a szinten történik cenzúra, az önmagában nem lehetetleníti el teljesen a kommunikációt... Az egyik megkérdezett válaszadónk – aki egy nemzeti domainnyilvántartónál mérnökként dolgozik – egy vele készített interjúban különbséget tett két jelenség, a széttagolás (franciául: *fragmentation*) és a súrlódás (franciául: *friction*) között. A súrlódás csak nehezíti a felhasználó életét, amikor hozzá akar férni egy adott szolgáltatáshoz, míg a széttagolás ezt teljesen ellehetetleníti. De van-e ebben igazi különbség társadalomtudományi – és politikai – szemszögből nézve?

Bár az internet technikailag internetprotokollt használó számítógépek hálózatainak a hálózata, az emberi felhasználók szemében egy virtuális globális közsféra (Abbate 2017). Így mindegy, hogy műszakilag miért nem tud valaki hozzáférni az internet valamelyik részéhez. Az a lényeg, hogy eltűnik egy kapcsolat, néha akkor is, ha elméletileg még megmarad ennek a lehetősége egy bizonyos szinten. Ahogy egy másik válaszadó – aki informatikus mérnökként részt vesz az internet szabványosítási folyamataiban – leszögezte: „sokak szerint a Facebook az internet, vagy a Google az internet, pedig ezek csak magántulajdonban lévő platformok, amelyek az internetre épültek”. De ennek semmi technikai szükségszerűsége nincsen. Ezért úgy döntöttünk a jelentésünkben, valamint a könyvünkben, hogy nem teszünk radikális különbséget a „széttagolás” és a „súrlódás” között. Az internetes közsféra széttagolása egy technikai és társadalmi jelenség. Egy nagy kontinuum van a teljesen globális és egységes hálózat, és a teljesen széttagolt, különböző, egymással egyáltalán nem kommunikáló részekből álló „Splinternet” között.

Két tényező kategória hat negatívan az internet egyetemessége szempontjából ezen az íven: politikai és gazdasági. Mindkettő nyomást gyakorol az internet műszaki rétegére, legalábbis egy bizonyos szintig. Az Európai Parlament felkérésére fel kellett mérnünk a „Splinternet” jelenségnek a mértékét, az EU hatását azonosítani, és javaslatokat tenni az STOA Testület tagjai számára, hogy hogyan kezeljék azt. Ehhez eredetileg azt terveztük, hogy az Ügykoalíciók Keretrendszer (Sabatier és Jenkins-Smith 1993) követve sikerül majd feltérképeznünk azokat az érdekképviseleti szereplőket, akik követeléseket fogalmaznak meg a témával kapcsolatban. Összesen 23 szereplővel beszéltünk a témáról, 20 interjú és egy rögzített workshop

során⁵, valamint 62 *policy papert* olvastunk át. De hamar arra a következtetésre kellett jutnunk, hogy amikor 2021 és 2022 között véghez vittük a kutatásunkat, az internet szétagolása még csak egy alakuló közprobléma volt (Gusfield 1994 kifejezése szerint); a „Splinternet”-et egyes szereplők inkább érvelési fegyverként használták bizonyos törvényjavaslatok ellen, mondván, hogy ezek kockáztatják az internet egyetemességét. De nem fűződtek hozzá pozitív követelmények, és nem létezett semmilyen koordinált stratégia vagy vita azon, hogy mit kellene tennie az EU-nak annak érdekében, hogy ezt a közproblémát megoldja. Így a joghoz fordultunk: igyekeztünk elemezni az akkor még vitatott európai törvényjavaslatokat, mint a NIS 2 irányelv vagy a digitális szolgáltatásokról szóló rendelet. De a sokszor egymásnak ellentmondó kezdeményezések sokaságával szembesülve így sem sikerült világos tendenciákra és törésvonalakra mutatni. Ezért a munkánk egy elméleti fordulatot vett: igyekeztünk elemezni, hogy miként lehetne jogilag megfogalmazni az internet szétagolását, és azt, hogy így milyen jogi keretek között tudnak politikai döntést hozni az ügyben a választott döntéshozók az EU-ban.

A szétagol(ó)dás politikai és gazdasági okai

Mivel, ahogy láttuk, az internet mindig is különböző független hálózatok összekapcsolásából állt össze, amelyek nyílt protokollok és egyéb szabványok betartásának köszönhetően tudnak egymással egy egységes, transznacionális és nagy cégeken átívelő közszférát létrehozni, egyúttal mindig is létezett feszültség a hálózatok egyetemessége és szétagolása között. Az utóbbi években, és különösen a 2010-es évek közepe óta a szakirodalom és az internet irányításával foglalkozó fórumok elkezdtek foglalkozni az internet szétagolásának veszélyével (Drake, Cerf és Kleinwächter 2016; Mueller 2017; Lemley 2020). Általában három tényezőt azonosítanak, amelyek az egyetemesség-szétagolás ív közötti feszültségre hatnak: (geo)politikai, gazdasági és műszaki tényezők. A könyvünkben átértelmeztük ezt a tipológiát: mivel a technika egy emberi és társadalmi tevékenység (Bijker 1995; Ellul 1954), nem lehet élesen elválasztani a műszakit a politikaitól és a gazdaságitól. Így azt vizsgáltuk, hogy a politikai és a gazdasági tényezők, amelyek a szétagolás irányába vihetik az internetet, láthatóak-e a hálózat műszaki rétegeiben. Egy cikk keretében nincs hely minden egyes tényezőt átfogóan áttekinteni, még azokat sem, amelyeket a jelentésben (Perarnaud et al. 2022), majd a könyvben (Perarnaud et al. 2024) taglaltunk. Ha az olvasó teljesebb leírásra lenne kíváncsi, ezekben a forrásokban megtalálja.

Lássuk először a politikai oldalt. Tunézia és Oroszország jó példa arra, hogy milyen hatásai lehetnek a korai politikai döntéseknek a hálózati nyitottság hosszabb távú rezilienciájára. Az első példában Zín el-Ábidín ben Ali diktatúrája alatt épült ki a helyi internet a 90-es évek végén. A hatóságok akkor arra kényszerítették az épülő internetszolgáltatók mérnökeit, hogy kizárólag egy pontnál kapcsolódjanak a külföldi autonóm rendszerekhez, egy a Belügyminisztérium felügyelete alatt lévő épületben (Goupy 2014). Ez nagyban megkönnyítette a helyi internet központosított

⁵ A válaszadók listája a jelentés 9. oldalán található (Perarnaud et al. 2022, 9).

vezérlését, megfigyelését és cenzúráját. Ezzel ellentétben az orosz internet Borisz Jelcin elnöksége alatt épült, viszonylag nagy szabadságban. 2020-ban még több mint 3 000 aktív internetszolgáltató üzemelt az országban. Ez nagyban megnehezítette a RoszKomNadzor munkáját, amelynek egy decentralizált megoldást kellett fejlesztenie a cenzúra és a megfigyelés alkalmazásához, és minden – sok ezer – szolgáltatót arra kényszerítette, hogy együttműködjön vele (Ermoshina, Loveluck és Musiani 2022). De IP-szinten nincsen széttagolás az orosz internet és a külvilág között, bár egyre nagyobbak azok a „súrlódások” amelyek a gyakorlatban azt eredményezik, hogy egyre nehezebb és kockázatosabb Oroszországból hozzáférni a globális nethez. Minden erőfeszítés ellenére nem lehet még teljesen elszakítani az orosz netet a külföldi hálózatoktól, mivel nagyon sok szolgáltatás és fontos források (szerverek, alkalmazások stb.) csak külföldről érhetőek el.

Erre a problémára igyekeznek megoldást találni az iráni hatóságok, amelyek a 2010-es években egy „Nemzeti Információs Rendszer” nevű stratégiát fejlesztettek. A cél az, hogy a rezsím számára se legyen negatív mellékhatása, ha a globális internetről lekapcsolják a helyi autonóm rendszereket, mint ahogy idén meg is történt, amikor az ország rövid háborúba keveredett Izraellel és az Egyesült Államokkal (Golshiri és Untersinger 2025). Ehhez, amellet, hogy drasztikusan korlátozták a fizikai összekapcsolási pontokat a külvilággal – gyakorlatilag csak három iráni hálózat van közvetlen kapcsolatban a külfölddel (Salamatian et al. 2021) –, egy nagy belső intranetet építettek. Kötelezővé tették a 10.x.x.x IP-címtartomány használatát az országon belül. Ezek az Internetmérnöki Munkacsoport (*Internet Engineering Task Force*, IETF a továbbiakban) RFC 1918 normája szerint helyi címek: csak a helyi hálózaton belül érhetőek el (Anderson 2012). Egy külföldön lévő felhasználó nem tudja ezeket a címeket elérni anélkül, hogy hozzáférne egy belső VPN-szerverhez, ami hidat nyújt a belső hálózathoz. Ennek a politikai döntésnek a másik következménye az, hogy sokkal könnyebb kikapcsolni a külső internetet: egyszerűen csak le kell tiltani azoknak a címeknek az elérését, amelyek nincsenek a 10.x.x.x tartományban. Amint sikerül függetlenné válni a külföldi szervereken lévő forrásoktól, és azokat például helyileg lemásolni vagy lecserélni iráni szolgáltatásokra, ez lehetővé teheti, hogy a rezsím lekapcsolhassa a helyi hálózatokat a külföldtől anélkül, hogy ez a lépés működésképtelenné tenné a helyi szolgáltatásokat, beleértve a helyi pénzügyi rendszereket.

Ahogy a bevezetésben említettük, a liberális demokráciák is néha korlátozzák az internet egyetemességét, ezek a döntések akár annak a műszaki rétegeire is hatnak. A szellemi tulajdonjog már a 2000-es évek elején elérte, bírói döntések után, hogy egyes tartalomszolgáltatók új technológiákat fejlesszenek ki, hogy ki tudják szűrni, melyik országból jönnek a látogatói. Ez lehetővé teszi, hogy csak azoknak továbbítsanak egy adott tartalmat, akik olyan országban vannak, amelyekhez megszerezték a közlési jogokat. Így jött létre a „geo-blocking” (Lenert 2004). Igaz, hogy ez viszonylag könnyen megkerülhető – például egy VPN-nel –, de ez mégis jelentősen a netes közszféra széttagolásának irányába hat. Egy másik gyakran említett példa az eredetileg európai – de egyre szaporodó (Greenleaf 2013) – adatvédelmi szabályok. Amikor 2014-ben az Európai Unió Bírósága (EUB) az elfeledtetéshez való

jogról szóló döntését meghozta⁶, sok kritika érte, amely szerint ez azt eredményezi, hogy onnantól fogva bizonyos keresőmotor-találatok nem lesznek elérhetőek az EU-ból (Tummarello 2016). Az Általános Adatvédelmi Rendelet (*General Data Protection Regulation*, a továbbiakban: GDPR) elfogadása is egyes kritikusai szerint széttagolást eredményezhet (Smolenskiy és Levshin 2021), hiszen az adatvédelmi jog szabályozza a személyes adatok továbbítását harmadik országok felé, ha azok nem rendelkeznek megfelelő garanciákkal. Így történt már több alkalommal, hogy Max Schrems, egy ausztriai aktivista, és a *None of Your Business* (az általa alapított civil szervezet, NOYB) kérelmére az EUB betiltotta a személyes adatok exportálását az Egyesült Államokba⁷. Ennek következtében számos amerikai felhőszolgáltató kezdett műszaki és jogi megoldásokat keresni ahhoz, hogy az EU-n belül tárolja az ottani ügyfeleinek az adatait.

Azonkívül az EU a közelmúltban több döntést hozott azzal a céllal, hogy az internet infrastruktúráját is szabályozza. Így a eIDAS 2 rendelet⁸ arra kényszeríti a webböngészőket, hogy elismerjék az EU-által minősített weboldal-hitelesítő tanúsítványokat. Ez eltér attól a gyakorlattól, amely szerint ezt a hitelesítőmechanizmust kizárólag magánszereplők (elsősorban böngészőfejlesztők és hitelesítő hatóságok) működtették annak érdekében, hogy ne legyen olyan centrális szereplő, aki egyedül hamisított tanúsítványt tud érvényesíteni. Egy másik példa a DNS4EU projekt, amivel az EU egy európai domainnév-szervert akar finanszírozni, amibe többek között „törvényes szűrési” kapacitás lenne beépítve⁹.

A vállalatok gazdasági okokból is hozzájárulhatnak a széttagolási tendenciához. Sok példát lehetne felsorolni, de a rövideg kedvéért csak két példát fogunk itt említeni: az úgynevezett “*zero-rating*”-szolgáltatások, és a csevegőprogramok interoperabilitásának a hiánya.

A *zero-rating*-szolgáltatás egy olyan ajánlat, ami abból áll, hogy bizonyos feltételek mellett a felhasználónak nem kell fizetnie az egyes online szolgáltatásokért. A Facebook Free Basics ehhez a kategóriához tartozik. Ez több országban lehetővé teszi, hogy egy bizonyos partner telefon- vagy internetszolgáltató ügyfelei ingyen tudjanak hozzáférni a Facebook és a cég által választott szolgáltatásokhoz, de nem az egész internethez. Ezt egyesek hevesen kritizálták, mivel teljesen ellentétes a netsemlegesség elvével, ami szerint maga a hálózat nem diszkriminálhat különböző tartalmak között (Szűts és Yoo 2015), így bizonyos országok, mint például India, be is tiltják ezt a gyakorlatot (Prasad 2018). Ha valaki csak egy *zero-rating*-szolgáltatáson keresztül juthat online szolgáltatáshoz, ez komolyan korlátozza az online lehetőségeit, és bezárja egy magáncég által választott információs tartományba, aminek kevés köze van ahhoz a szabad közszférához, amit az internet modellje ígért (Turner 2008; Tréguer 2019).

⁶ EUB 2014. május 13., Google Spanyolország, C-131/12 sz. ügy.

⁷ EUB 2015. október 6., Schrems 1, C-362/14 sz. ügy; EUB 2020. július 16., Schrems 2, C-311/18.

⁸ 1. cikk 44. bekezdés, 2024/1183 rendelet a 910/2014/EU rendeletnek az európai digitális személyazonosságai keret létrehozása tekintetében történő módosításáról.

⁹ Lásd a DNS4EU pályázati felhívást, CEF-DIG-2021-CLOUD-DNS-WORKS:

^h<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works>

A nagy techvállalatok abban érdekeltek, hogy a felhasználói minél több időt töltsenek a saját felületükön, és minél kevesebbet a konkurenciánál. A hegemonikus pozíciójukat annak köszönhetik, hogy egy bizonyos ponton sikerült kritikus nagyságú tömeget rávenni, hogy az ő szolgáltatásain keresztül tartsák a kapcsolatot, és így elkerülhetetlenné válhatnak. Bárki küldhet e-mailt bárkinek függetlenül attól, hogy ki birtokolja a szervereket, amelyeket az egymással levelezők használnak, mert mindenki közös nyílt és interoperábilis protokollt használ: SMTP, IMAP, POP... De akinek nincs Facebook-fiókja vagy X- (Twitter-) fiókja, nem tud üzenetet küldeni egy Facebook- vagy egy X-felhasználónak. Muszáj belépnie az adott cég zárt kertjébe, és elfogadnia a felhasználási feltételeit. Ez pedig nem mindig volt így. 2015-ig például a Facebook csevegőprogramja az XMPP-szabványt használta (Perarnaud et al. 2024, 32), ami lehetővé tette, hogy bárki, aki egy fiókkal rendelkezett egy másik XMPP-szerveren (mint például Jabber vagy Google Talk), csevegni tudott egy Facebook-felhasználóval anélkül, hogy belépett volna a Facebookba. Az XMPP elhagyása tisztán műszaki döntésnek tűnhet, de nem az: gazdasági döntés, ami bezárta a Facebook felhasználóit egy zárt kertbe, ezzel szűkítve a lehetőségeiket abban, hogy a cég közösségi hálózatán kívül tartsanak kapcsolatot. Ez is egy olyan „súrlódás”, ami a széttagolás felé lendít.

Ahogy említettük, akár a politikai oldalon, akár a gazdaságin, sok egyéb példát lehetne még sorolni, és ezek a jelentésünkben és a könyvünkben találhatóak. Ezek együttvéve olyan képet festenek, hogy bár amióta van internet, létezik a feszültség a kibertér egyetemessége és a széttagolása között, egyre nagyobb nyomás hat az utóbbi irányába. Így sem lehet igazi „Splinternetekről” beszélni, mert a legtöbb esetben az általunk jelentett akadályok megkerülhetőek. Még az iráni hálózat sem vált még teljesen szét a globális hálózattól, bár az ottani rezsim igyekszik ezt lehetővé tenni. De ahogy a „súrlódások” felhalmozódnak, a gyakorlatban sok felhasználó csak az internet egy töredékéhez juthat hozzá.

A széttagolás jogi értelmezése

E megfigyelésekből kiindulva azt kellett elemeznünk, hogy milyen lehetőségei vannak az EU-nak a beavatkozásra ebben a témában. Ez egyből egy normatív kérdéshez vezetett: valóban (mindig) rossz dolog a széttagolás? Mivel a jog mégis egy normatív tudományág, és ráadásul a STOA Testület arra kért, hogy fogalmazzunk meg ajánlatokat, kénytelenek voltunk a kérdéssel foglalkozni. Egy paradoxonnal kellett szembenéznünk: ha egyetértünk az EUB Schrems 1 és 2 döntéseivel – amelyek megsemmisítették az EU–Egyesült Államok egyezményeit a személyes adatok szabad áramlásáról –, mert fontosnak tartjuk, hogy ne lehessen elkerülni a adatvédelmi alapjogot védő szabályokat, és eközben minden esetben rossz dolognak tartjuk az internet széttagolásához vezető tényezőket, akkor ez egymásnak ellentmond.

Három forгатókönyvet elemeztünk:

- A status quo fenntartása, a jelenlegi uniós jog számos ellentmondásával és következetlenségével a széttagolás jelenségéhez való hozzáállásban;

-
- Az internet széttagolásának felkarolása: az EU nem korlátozná magát abban, hogy akadályokat állítson fel maga és harmadik országok között, és beavatkozna a helyi hálózatok infrastruktúrájába, hogy a saját érdekeit és politikai döntéseit érvényesítse, anélkül, hogy ezeket meg lehessen kerülni;
 - A következetes küzdelem a széttagolás ellen: ebben a forgatókönyvben az EU-nak felül kellene vizsgálnia számos jelenlegi politikáját annak érdekében, hogy szabályai semmilyen széttagolási hatást ne gyakoroljanak, miközben biztosítaná, hogy megtörje azokat a monopóliumokat, amelyek lehetővé teszik bizonyos vállalatok számára, hogy zárt kertekbe zárják be a felhasználóit, ezzel megtörve az internetes közszféra egységét.

Megállapításaink szerint egyik forgatókönyv sem felelt meg a jogi kereteknek, amelyek az EU tevékenységét szabályozzák. Vannak például egyes, a széttagolást erősítő tényezők, mint például a GDPR-ban szereplő adattovábbítási szabályok, amelyek az alapvető jogok hatékony alkalmazásának biztosítását szolgálják. Ezek az EU jogrendjében nem képeznek opciót. Így kidolgoztunk egy negyedik, az emberi jogokon alapuló megközelítést.

Az internet egysége és szabadsága szorosan kötődik a szólásszabadsághoz való joghoz. Ezt jól jelzi az Emberi Jogok Egyetemes Nyilatkozata 19. cikke:

“Minden személynek joga van a vélemény és a kifejezés szabadságához, amely magában foglalja azt a jogot, hogy véleménye miatt ne szenvedjen zaklatást, és hogy **határokra való tekintet nélkül** kutathasson, tájékozódhasson és terjeszthessen információkat és eszméket **bármilyen kifejezési módon**.”

A „bármilyen kifejezési módon” kifejezés, ami az Egyesült Nemzetek Szervezetének a nyilatkozat hivatalos magyar nyelvű fordításában szerepel, nem jól fejezi ki az eredeti szövegben található „through any media” (angolul), „por cualquier medio de expresión” (spanyolul) vagy „par quelque moyen d’expression que ce soit” (franciául) kifejezést, ami jobban hangsúlyozza a médiatípus szabad megválasztását. Így az internet választása egy vélemény kinyilvánításához, és annak a véleménynek a szabad áramlása a határokon át, része az egyetemes nyilatkozat által védett szólásszabadságnak. Ezt a szabadságot Európában, többek között az Emberi Jogok Európai Egyezménye (EJEE) 10. cikke, valamint az EU Alapjogi Chartája (Charta) 11. cikke tartalmazza, hangsúlyozva, hogy a véleménynyilvánítás jog, országhatárokra való tekintet nélkül. Eszerint a jogi vagy hatósági intézkedések, amelyek korlátozzák az internet egyetemességét, a véleménynyilvánítást korlátozzák, ami csak akkor jogszerű, ha – az EJEE szavait használva – „szükséges intézkedéseknek minősülnek egy demokratikus társadalomban”. Ezt a bíróságok tudják felülvizsgálni.

Vannak így esetek, amikor a szólásszabadság korlátozása legális. Így az EU Törvényszéke már jóváhagyta azokat a szankciókat, amelyek az orosz médiumokat sújtották, amikor Oroszország támadást indított Kijev ellen 2022 februárjában¹⁰. Ezeknek az intézkedéseknek a megfelelő végrehajtása beavatkozásokat igényelt az

¹⁰ EU Törvényszéke 2022. július 27., RT France, T-125/22 sz. ügy.

infrastruktúrába. Az internetszolgáltatóknak különféle (néha többé-kevésbé hatékony) eszközökkel kellett konfigurálniuk hálózataikat, hogy blokkolják a szankcionált médiaszolgáltatótól származó tartalmakat (ten Oever et al. 2024).

Másrészt az emberi jogi megközelítés lehetőséget ad az államoknak, hogy ne csak negatív szabadságként (Berlin 1969) kezeljék a felelősségüket a szólásszabadság – beleértve az internet egyetemessége – iránt, hanem pozitív szabadságként is. Ezt tette az EU többek között a digitális szolgáltatásokról szóló rendeletével, amely több rendelkezést tartalmaz, elismerve, hogy „a közvetítő szolgáltatók felelősségteljes és kellően gondos magatartása elengedhetetlen [...] ahhoz, hogy az uniós polgárok és más személyek gyakorolhassák az Európai Unió Alapjogi Chartájában [...] biztosított alapvető jogokat, különösen a véleménynyilvánítás és a tájékozódás szabadságát” (digitális szolgáltatásokról szóló rendelet, 3. preambulumbekzdés).

Összegzés

„Splinternet” még nincs, de egyre inkább felhalmozódnak azok a feszültségek, amelyek gyengítik az internet nyitottságát és egyetemességét. Ezekért nemcsak a tekintélyelvű államok felelősek – bár azok gyakran a jelenség élén állnak –, hanem a liberális demokráciák és a nagy techvállalatok is. Ez nem egy politikailag és jogilag semleges jelenség: ahogy láttuk, az internet egyetemességének korlátozása egyben a véleménynyilvánításnak is gátat vetett. Ebből kiindulva, ennek az alakuló közproblémának a kezelésében az EU az emberi jogok hagyományaira és eszközeire építhetne nagyobb koherenciát.

A társadalmi problémákra adott pusztán technikai megoldások sokszor illúziók (Morozov 2013). Ennek ellenére sok állam ebben a disztópikus küldetésében, hogy minden problémát technikai csodaeszközökkel győzzön le, akár a szabad online közsféra felbomlásához is vezethet. Egy olyan rohamnak vagyunk tanúi, amely először a DNS-rendszer szintjén vezet be cenzúrát, majd megakadályozza a közvetlen kapcsolatokat bizonyos IP-címekhez, végül betiltja a titkosítást vagy a VPN-eket, vagy akár egyfajta országos helyi hálózatot hoz létre, mint Iránban. Ez a féktelen rohanás szerintünk részben abból fakad, hogy képtelenek elfogadni, hogy bármilyen jogi és technikai intézkedést is hoznak egy jelenség – beleértve a komoly bűnözést is – leküzdésére, mindig lesznek hibái és megkerülési módjai ezeknek a technikáknak. Ez a folyamat arra vezethet, hogy az online szférában még a liberális államok is totális kontrollra hajtsanak, ami alapvetően és radikálisan ellentétes a jogállami alkotmányosság elvével, amely szerint magának a szuverénnek kell elfogadnia, hogy fékekkel és ellensúlyokkal korlátozza a saját hatalmát a szabadságok virágzása érdekében. Az internet decentralizált és nyitott koncepciója talán egy olyan fék- és ellensúly-mechanizmus az online közszférában, amit óvni kell a „megoldásfetisizta”¹¹ csábításoktól. Az emberi jogi kereten belül, ahogy már hosszú évtizedek gyakorlata bemutatta, még így is sokat lehet tenni annak érdekében, hogy „egy demokratikus társadalomban szükséges” intézkedéseket tegyen az

¹¹ Itt lefordítottuk Evgeny Morozov “solutionism” angol kifejezését.

állam fontos egyéb érdekek, például a magánélethez való jog vagy a közbiztonság védelmében.

Ennek a jogból és politikai elméletből kölcsönzött elemzési keretrendszernek az az előnye, hogy kihúz minket abból a patthelyzetből, ahol az egységes és a fragmentált internet támogatói (jó vagy rossz okokból) összeütköznek anélkül, hogy figyelembe vennék az alapvető folyamatokat, amelyek az internetet korunk egyik legfontosabb infrastruktúrájává tették.

Irodalom

- Abbate, Janet. "What and where is the Internet? (Re)defining Internet histories." *Internet Histories* 1, no. 1–2 (2017): 8–14.
<https://doi.org/10.1080/24701475.2017.1305836>
- Ananthaswamy, Anil. "Age of the splinternet." *New Scientist* 211, no. 2821 (2011. július 16): 42–45.
[https://doi.org/10.1016/S0262-4079\(11\)61710-7](https://doi.org/10.1016/S0262-4079(11)61710-7)
- Anderson, Collin. "The Hidden Internet of Iran: Private Address Allocations on a National Network." ArXiv. 2012.
<https://doi.org/10.48550/arXiv.1209.6398>
- Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. 1996. február 8.
<https://www.eff.org/cyberspace-independence>
- Berlin, Isaiah. "Two concepts of liberty." In *Four Essays on Liberty*, 118–72. Oxford: Oxford University Press, 1969.
https://cactus.utahtech.edu/green/B_Readings/1_Berlin_Two_Concpets_of_Liberty.pdf
- Bijker, Wiebe E. *Of bicycles, bakelites, and bulbs: toward a theory of sociotechnical change. (Inside technology)*. Cambridge, Mass: MIT Press 1995.
- Drake, William J., Vinton G. Cerf és Wolfgang Kleinwächter. "Internet Fragmentation: An Overview." Future of the Internet Initiative White Paper. World Economic Forum 2016.
https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf
- Ellul, Jacques. *La technique ou l'enjeu du siècle*. Paris: Armand Colin, 1954.
- Ermoshina, Ksenia, Benjamin Loveluck és Francesca Musiani. "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia." *Journal of Information Technology & Politics* 19, no. 1 (2022): 18–33.
<https://dx.doi.org/10.1080/19331681.2021.1905972>
- Ermoshina, Ksenia és Francesca Musiani. "The Telegram Ban: How Censorship 'Made in Russia' Faces a Global Internet." *First Monday* 26, no. 5 (2021).
<https://dx.doi.org/10.5210/fm.v26i5.11704>
- Firmino, Rodrigo, Lucas Melgaço és Dariusz Kloza. "The spatial bonds of WikiLeaks." *Government Information Quarterly* 35, no. 3 (2018): 389–397.
<https://dx.doi.org/10.1016/j.giq.2018.05.005>
- Flichy, Patrice. *L'imaginaire d'Internet*. Paris: Découverte, 2001.
- Flipo, Fabrice, Michelle Dobré és Marion Michot. *La face cachée du numérique: l'impact environnemental des nouvelles technologies*. Montreuil: Éditions L'Échappée, 2013.

- Golshiri, Ghazal és Martin Untersinger. "Iran's leaders cut internet access to outside world." *Le Monde*, 2025. június 20.
https://www.lemonde.fr/en/international/article/2025/06/20/iran-s-leaders-cut-internet-access-to-outside-world_6742544_4.html
- Goupy, Marie. "La bienveillante neutralité des technologies d'espionnage des communications: le cas tunisien." *Cultures & Conflits*, no. 93 (2014): 109–124.
<https://dx.doi.org/10.4000/conflits.18863>
- Greenleaf, Graham. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories." *Journal of Law, Information and Science* 23, no. 1 (2013).
- Gusfield, Joseph R. *The Culture of Public Problems: Drinking-Driving and the Symbolic Order*. 4. print. Chicago: University of Chicago Press, 1994.
- Hoffmann, Stacie, Dominique Lazanski és Emily Taylor. "Standardising the splinternet: how China's technical standards could fragment the internet." *Journal of Cyber Policy* 5, no. 2 (2020): 239–264.
<https://dx.doi.org/10.1080/23738871.2020.1805482>
- Kaufmann Balázs. "Letartóztatták a Telegram vezérigazgatóját Párizsban." 444. 2024. augusztus 25.
<https://444.hu/2024/08/25/letartoztattak-a-telegram-vezerigazgatojat-parizsban>
- Kim, Mi-jin, Heejin Lee és Jooyoung Kwak. "The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization." *International Journal of Information Management* 54 (2020): 102145.
<https://dx.doi.org/10.1016/j.ijinfomgt.2020.102145>
- Lemley, Mark A. "The Splinternet Lecture." *Duke Law Journal* 70, no. 6 (2020): 1397–1428.
- Lenert, Edward. "A Social Shaping Perspective on the Development of the World Wide Web: The Case of iCraveTV." *New Media & Society* 6, no. 2 (2004): 235–258.
<https://dx.doi.org/10.1177/1461444804041442>
- Malcomson, Scott. *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*. New York, USA: OR Books, 2016.
- Morozov, Evgeny. *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems That Don't Exist*. London, UK: Penguin Books Limited, 2013.
- Mueller, Milton. *Will the Internet fragment? sovereignty, globalization, and cyberspace. (Digital futures)*. Cambridge, UK; Malden, MA: Polity Press, 2017.
- Musiani, Francesca és Valérie Schafer. "Le modèle Internet en question (années 1970-2010)." *Flux* 85-86, no. 3 (2011): 62–71.
<https://dx.doi.org/10.3917/flux.085.0062>
- Nanni, Riccardo. "The 'China' Question in Internet Fragmentation: Evidence From the 'New IP'." *Global Cooperation Research* (blog). 2022. november.
<https://www.gcr21.org/publications/gcr/gcr-quarterly-magazine/qm-2-3/2022-articles/qm-2/3-2022-nanni-the-china-question-in-internet-fragmentation-evidence-from-the-new-ip?type=rss>
- Nelson, Ted. *Computer Lib/Dream Machines*. Független könyv, 1974.
- Perarnaud, Clément, Julien Rossi, Francesca Musiani és Lucien Castex. "Splinternets«: Addressing the renewed debate on internet fragmentation." Strasbourg: European Parliament - STOA Panel for the Future of Technology, 2022.
[https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2022\)729530](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2022)729530)

-
- Perarnaud, Clément, Julien Rossi, Francesca Musiani és Lucien Castex. “»Splinternets«: Addressing the renewed debate on internet fragmentation.” *L’avenir d’Internet : unité ou fragmentation ? Documents*. Bordeaux: Le Bord de l’Eau, 2024.
- Prasad, Revati. “Ascendant India, Digital India: How Net Neutrality Advocates Defeated Facebook’s Free Basics.” *Media, Culture & Society* 40, no. 3 (2018): 415–431.
<http://dx.doi.org/10.1177/0163443717736117>
- Rosson, Zach. “First-Time Culprit: France Blocks TikTok in New Caledonia.” *Access Now* (blog). 2024. június 5.
<https://www.accessnow.org/france-blocks-tiktok-new-caledonia/>
- Russell, Andrew L. “»Rough Consensus and Running Code« and the Internet-OSI Standards War.” *IEEE Annals of the History of Computing* 28, no. 3 (2006): 48–61.
<http://dx.doi.org/10.1109/MAHC.2006.42>
- Sabatier, Paul A. és Hank C. Jenkins-Smith (szerk.). *Policy change and learning: an advocacy coalition approach*. Theoretical lenses on public policy. Boulder, Colo: Westview Press, 1993.
- Salamatian, Loqman, Frédérick Douzet, Kavé Salamatian és Kévin Limonier. “The geopolitics behind the routes data travel: a case study of Iran.” *Journal of Cybersecurity* 7, no. 1 (2021): tyab018.
<https://dx.doi.org/10.1093/cybsec/tyab018>
- Smolenskiy, Mikhail és Nikolay Levshin. “GDPR implementation as the main reason for the regional fragmentation in the online mediasphere.” Szerkesztette D. Rudoy, A. Olshevskaya, és N. Ugrekhelidze. *E3S Web of Conferences* (2021) 273:08099.
<https://doi.org/10.1051/e3sconf/202127308099>
- Szűts, Zoltán és Jinil Yoo. “A netsemlegesség – törvényhozói, tartalomszolgáltatói, internetszolgáltatói és felhasználói olvasatok.” *Információs Társadalom* 15, 3. szám (2015): 41–62.
- ten Oever, Niels, Clément Perarnaud, John Kristoff, Moritz Müller, Max Resing, Arturo Filasto és Chris Kanich. “Sanctions and Infrastructural Ideologies: Assessing the Material Shaping of EU Digital Sovereignty in Response to the War in Ukraine.” *Policy & Internet* 16, no. 4 (2024): 692–710.
<https://dx.doi.org/10.1002/poi3.422>
- Tréguer, Félix. *L’utopie déçue: une contre-histoire d’Internet, XVe-XXIe siècle*. A venir. Paris: Fayard, 2019.
- Tummarello, Kate. “We Won’t Let You Forget It: Why We Oppose French Attempts to Export the Right To Be Forgotten Worldwide.” Electronic Frontier Foundation. 2016. november 29.
<https://www.eff.org/fr/deeplinks/2016/11/we-wont-let-you-forget-it-why-we-oppose-french-attempts-export-right-be-forgotten>
- Turner, Fred. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, Ill.: University of Chicago Press, 2008.
- Wayne Crews, Clyde. “On My Mind.” *Forbes*, 2001. április 2.
<https://www.forbes.com/forbes/2001/0402/036.html>