

NEW YORKI EGYETEM  
NEMZETKÖZI JOGI ÉS POLITIKAI  
FOLYÓIRAT

---

---

VOL. 54Ősz 2021No.1

---

---

A PEKINGI HATÁS: KÍNA  
DIGITÁLIS SELYEMÚTJA  
MINT TRANSZNACIONÁLIS ADATKEZELÉS\*

MATTHEW S. ERIE† & THOMAS STREINZ‡

I.	BEVEZETÉS .....	3
II.	KÍNA TRANSZNACIONÁLIS HATÁSA AZ ADATOKRA KORMÁNYZAT11	
	A. <i>A pekingi hatás</i> .....	14
	B. <i>Kína megközelítése az adatkezeléshez: Az adatok lokalizálása az adatszuverenitásra való törekvésben</i> 24	

---

\* Ez a cikk a Harvard Law School, a Hertie School of Governance és a New York University School of Law U.S.-Asia Law Institute előadásából származik. A szerzők köszönetet mondanak Alvarez, Anu Bradford, Maria Adele Carrai, Prasenjit Duara, Rebecca Hamilton, Benedict Kingsbury, Aynne Kokas, Elisa Oreglia, Shitong Qiao és Katharin Tai korábbi vázlatokhoz fűzött észrevételeikért. A szerzők köszönetet mondanak továbbá a N.Y.U. J. Int'l L. & Pol. diákszerkesztőknek a hozzájárulásukért. Minden kínai fordítás Matthew Erie fordítása, hacsak másképp nem jelezzük. Minden hiba a szerzőké.

† a Keleti Intézet modern kínai tanulmányok docense és az Oxfordi Egyetem Társadalmi-jogi Tanulmányok Központjának munkatársa. E-mail: matthew.erie@law.ox.ac.uk. Ez a cikk az Európai Kutatási Tanács által finanszírozott "Kína, jog és fejlődés" projekt része (803763 számú támogatás).

‡ A New York University School of Law adjunktus professzora és a Guarini Global Law & Tech ügyvezető igazgatója. E-mail: thomas.strein@law.nyu.edu. Ez a cikk a Guarini Global Law & Tech globális adatjogi projektjének, valamint a Nemzetközi Jogi és Igazságügyi Intézet (IJL) infrastruktúrák mint szabályozás (In- fraReg) és a Megareguláció és nemzetközi jogi rendezés (MegaReg) projektjeinek meglátásaira támaszkodik.

C.	<i>Kína változó szerepe a globális adatszolgáltatásban</i>	
	<i>    Irányítási intézmények</i> .....	35
D.	<i>Kína növekvő jelentősége az infrastruktúrában</i>	
	<i>    Adatkezelés</i> .....	42
III.	<b>KÍNA DIGITÁLIS SELYEMÚTJA</b> .....	48
A.	<i>A digitális eszközök fizikai komponenseinek szállítása</i>	
	<i>    Infrastruktúra</i> .....	50
B.	<i>A kínai technológiai vállalatok mint infrastrukturális szereplők</i> .....	53
C.	<i>A DSR jogi és intézményi irányítási infrastruktúrája</i> .	61
IV.	<b>DIGITÁLIS SELYEMÚT ESETTANULMÁNY: PAKISZTÁN</b> <sup>66</sup>	
A.	<i>Digitális összeköttetés Pakisztánon belül és azon túl</i> .....	67
B.	<i>Kínai felügyeleti infrastruktúra az intelligens és Biztonságos városok</i> .....	71
C.	<i>Pakisztán kialakulóban lévő adatkezelési rendszere</i> .....	75
V.	<b>A PEKINGI HATÁS ÉRTÉKELÉSE: DATA SZUVERENITÁS ÉS DIGITÁLIS FEJLŐDÉS</b> .....	83
A.	<i>Az adatszuverenitás</i> .....	<i>vonzereje és korlátai</i> <sup>84</sup>
B.	<i>A digitális selyemút és a digitális fejlődés</i> .	89 VI.
	<b>KÖVETKEZTETÉS</b> .....	91

*Kína a feltörekvő piacok digitális infrastruktúrájának biztosításával alakítja a transznacionális adatkezelést. A jelenség uralkodó magyarázata a digitális tekintélyelvűség, amelynek révén Kína nemcsak technológiáját, hanem értékeit és kormányzási rendszerét is exportálja a fogadó államokba. A digitális tekintélyelvűséggel kapcsolatos egyméretű tézissel ellentétben ez a cikk a "pekingi hatás" elméletét vázolja fel, amely a "push" és "pull" tényezők kombinációja, és amely megmagyarázza Kína növekvő befolyását a határain túli adatkezelésben. A feltörekvő gazdaságok kormányai kínai digitális infrastruktúrákat követelnek, és az adatszuverenitásra és a digitális fejlődésre törekedve utánozzák Kína adatkezelési megközelítését. Kína "digitális selyemútja", a digitális infrastruktúra fizikai összetevőinek (pl. optikai kábelek, antennák és műholdak) kiépítésére irányuló hatalmas erőfeszítés, amely az ilyen fejlődő államokban a digitális ökoszisztémák interoperabilitásának fokozását szolgálja, a pekingi hatás megvalósulását jelenti. Ennek fő mozgatórugói a kínai technológiai vállalatok, amelyek egyre inkább telekommunikációs és e-kereskedelmi szolgáltatásokat nyújtanak világszerte. A pekingi hatás ellentétben áll a brüsszeli hatással, amely szerint a vállalatok globális működése az Európai Unió szabályozása felé húz. Eltér az Egyesült Államok azon törekvéseitől is, hogy a nemzetközi gazdasági jog eszközeivel alakítsa a globális adatkezelést. A normatív dokumentumok tanulmányozása és egy kulcsfontosságú fogadó államban végzett empirikus terepmunka alapján elmagyarázzuk, hogyan működik a pekingi hatás a gyakorlatban, és felmérjük a fejlődő országokra gyakorolt hatását. Azzal érvelünk, hogy az adatszuverenitás illuzórikus, mivel a kínai pártállam különböző mértékben tartja fenn az ellenőrzést a kínai*

*a digitális infrastruktúrát szolgáltató vállalkozások, és a digitális fejlesztési stratégiáknak megfelelő jogi infrastruktúrák fejlesztését szorgalmazzák.*

## I. BEVEZETÉS

A Kínai Népköztársaság (KNK vagy Kína) globális kormányzásban betöltött szerepe a XXI. században egyre inkább előtérbe kerül, mivel a KNK kiterjedt Övezet és Út Kezdeményezése (BRI) a globális gazdasági rendezés új modelljeként került a középpontba.<sup>1</sup> A BRI infrastrukturális projektek széles skáláját öleli fel, hogy javítsa az áruk, a munkaerő, a tőke és az energia mozgását Kína és a Vanuatutól Venezueláig terjedő országok között, szárazföldi, tengeri, sőt úrkapcsolatokat teremtve. Az ilyen infrastrukturális projektek potenciálisan jelentős helyi és regionális hatásokkal járhatnak, és összességében elősegíthetik a Kínától függő értékláncok kialakulását. E folyamat részeként a cégek döntő mértékben támaszkodnak az információs és távközlési technológiára a decentralizált vagy "szétválasztott" termelési hálózatok működtetése érdekében.

1. Lásd NADE`GE ROLLAND, NAT'L BUREAU OF ASIAN RSCH „CHINA'S VISION FOR A NEW WORLD ORDER, 3, 6, 48-49 (2020) (azzal érvelve, hogy Kína par- tális hegemoniára törekszik a "globális Dél" felett); Julien Chaisse & Mitsuo Matsushita, *China's 'Belt and Road' Initiative: Mapping the World Trade Normative and Strate- gic Implications*, J52. WORLD TRADE (163,2018167) (megállapítva, hogy Kína "radikálisan új megközelítésre törekszik a nemzetközi kereskedelem és beruházás tekintetében"); Ju- lien Chaisse, *Introduction: China's International Investment Law and Policy Re- gime- Identifying the Three Tracks*, in CHINA'S INTERNATIONAL INVESTMENT STRATEGY: BILATERAL, REGIONAL, AND GLOBAL LAW AND POLICY 1, 12 (Julien Chaisse szerk., 2019) (megállapítva, hogy Kína hosszú távon szabályalkotó lesz); BRUNO M. BELT AND ROAD: A CHINESE WORLD ORDER 189170, (2018) (azzal érvelve, hogy Kína a nyugati globalizációval szemben alternatív értékrendet képvisel). De lásd Gregory Shaffer & Henry Gao, *A New Chinese Economic Order?*, 23 J. INT'L ECON. L. 607, 609 (2020) (azzal érvelve, hogy a kínai modell újrahasonosítja a nyugati jogot és intézményeket); Matthew S. Erie, *Chinese Law and Development*, 62 HARV. INT'L L.J. 51, 54-56 (2021) (felhívja a figyelmet Kína joggal és fejlődéssel kapcsolatos megközelítésére, valamint a nemzetközi gazdasági és kereskedelmi jog eszközei mellett az extralegális és nem jogi normák jelentőségére); Jiangyu Wang, *China's Governance Approach to the Belt and Road Initiative (BRI): Relations, Partnership, and Law*, 14 GLOB. TRADE & CUSTOMS J. 222, 224 (2019) (a globális kereskedelemmel és beruházásokkal kapcsolatos kínai megközelítést rugalmasnak, pragmatikusnak és eredményorientáltnak minősíti); Prasenjit Duara, *The Chi- nese World Order in Historical Perspective: The Imperialism of Nation-States or Soft Power*, CHINA2 & WORLD: ANCIENT & MOD. SILK ROAD 1, 1 (2019) (a BRI-t a nemzetállami imperializmuson belül helyezi el).

transznacionálisan.<sup>2</sup> E célból és más célokból Kína a hagyományos infrastrukturális projektjei mellett digitális kiegészítőket épít, amelyeket "Digitális Selyemút" (DSR) (*shuzi sichou zhilu*) néven csomagolnak, hogy a nemzetközi kommunikáció és adatforgalom szempontjából összeköttetést biztosítsanak.<sup>3</sup> Ez a digitális infrastruktúra kiegészíti a szárazföldi Selyemút gazdasági övezetét és a XXI. századi tengeri selyemutat, amelyek a fizikai áruk nagyobb szállítási kapacitásának biztosításával biztosítják az összeköttetést.

Ez a cikk azt vizsgálja, hogy a DSR befolyásolja-e és milyen mértékben az adatkezelést Kínán kívül. A hagyományos vélekedés szerint Kína exportálja a technológiai irány "modelljét", amit az elemzők "digitális tekintélyelvűségnek" neveznek.<sup>4</sup> Úgy véljük, hogy ez a magyarázat több okból is elégtelen, többek között azért, mert feltételezi, hogy létezik egy kínai modell, és hogy ez a minta problémamentesen átültethető más joghatóságokba. Ehelyett a mi válaszuk erre a kérdésre az, amit mi "pekingi hatásnak" nevezünk: a push és pull tényezők kombinációja, amely megmagyarázza Kína növekvő befolyását a "transznacionális adatkezelésben". A "transznacionális adatkezelés" alatt azokat a szabályokat, normákat, gyakorlatokat és infrastruktúrákat értjük, amelyek a digitalizált információk (azaz az adatok) gyűjtését, tárolását, továbbítását, felhasználását és az azokhoz való hozzáférést szabályozzák a nemzeti határokon túl.<sup>5</sup> Az internet globális irányításáról szóló diskurzusának kiterjesztéseként, amelyben Kína következetesen kiállt a "kiber-szuverenitás" mellett, Kína a belső adatkezelési rendszerében az "adat- szuverenitást" hangsúlyozza, és ezzel az adatáramlások feletti kormányzati ellenőrzés legitimitását erősíti meg.<sup>6</sup> Az Európai Unióval és az Egyesült Államokkal ellentétben Kína nagyrészt nem használta fel a jogi eszközöket más országok adatkezelési rendszereinek közvetlen befolyásolására. A DSR-en keresztül azonban a kínai vállalatok egyre inkább biztosítják a digitális infrastruktúrát, amely minden adatkezelési rendszer szerves részét képezi. Az olyan fejlődő országok, amelyek egyre növekvő de-

---

2. Lásd RICHARD BALDWIN, THE GREAT CONVERGENCE: INFORMATION TECHNOLOGY AND THE NEW GLOBALIZATION 4-5, (102016) (tárgyalja, hogy a globális egy második és harmadik szétválasztást igényelt, amely a munkát és a munkavállalókat nemzetek között terjeszti).

3. Lásd a 183-87. lábjegyzethez tartozó alábbi szöveget.

4. Lásd a 39-41. lábjegyzeteket.

5. Lásd a 28-38. lábjegyzeteket kísérő *infra* szöveget.

6. Lásd a 130-31. és 360-68. lábjegyzeteket.

az ilyen infrastruktúrák megbízói különösen vonzóknak találhatják az "adatszuverenitás" lehetőségét.

Azt állítjuk azonban, hogy az "adatszuverenitás" a legtöbb fejlődő ország számára illuzórikus, mivel az adatok hatékony szabályozásának hatalma az összes releváns digitális infrastruktúra ellenőrzésétől függ, amelynek nagy részét egyre inkább a kínai technológiai vállalatok biztosítják, amelyek viszont - különböző mértékben - a Kínai Kommunista Párt (KKP) befolyása alatt működnek. Következésképpen, bár egyes BRI-államok többé-kevésbé "zárt" adatkezelési környezetek felé vonzódnak (abban az értelemben, hogy bizonyos fokú kormányzati ellenőrzést tesznek lehetővé mind az országon belüli, mind a határokon átnyúló adatáramlás felett), végső soron mégis "nyitottak" maradnak a Kínai Népköztársaság beavatkozására és nyomására. Az, hogy a kormányok milyen mértékben tudják ellensúlyozni a digitális területen a folyamatos és növekvő kínai befolyást, nem csak a Kínától való relatív hatalmuktól, valamint pénzügyi és infrastrukturális függőségüktől függ, hanem a hazai jogi és politikai rendszereik erősségétől is.<sup>7</sup> A kérdés tehát az, hogy a kisebb államok hogyan vagy egyáltalán meg tudják-e húzni a határt a saját és a Kína által formált uralom között.

A DSR és annak a Kínán kívüli adatkezelésre gyakorolt hatása összefonódik a hatalmas kínai elektronikus kereskedelmi és információs és távközlési (IKT) technológiai vállalatok globális terjeszkedési stratégiáival. Az Alibaba a kis- és középvállalkozások (kkv-k) globális e-kereskedelmi platformjaként pozícionálta magát, és ezt a stratégiát az elektronikus világkereskedelmi platformon (eWTP) keresztül nemzetközivé teszi.<sup>8</sup> Az olyan vállalatok, mint a Huawei és a ZTE olyan hálózati berendezéseket biztosítanak, amelyek alapvető fontosságúak a szélessávú internet és a "dolgok internete" alkalmazásokhoz az "intelligens" és "biztonságos" városokban.<sup>9</sup> A TenCent Weixin (WeChat) közösségi médiaplatformja és a ByteDance TikTok videomegosztó alkalmazása megkönnyíti a kommunikációt a felhasználók milliárdjai között világszerte. Az elmúlt években e vállalatok belépése az amerikai, brit, európai és japán piacokra széles körű vitákat váltott ki, amelyek többnyire a magánélet védelmével és a nemzetbiztonsággal kapcsolatos aggályok köré csoportosultak, de a technológiai és gazdasági helyek kérdéseit is érintették.

7. Lásd a 369-76. lábjegyzeteket kísérő *infra* szöveget.

8. Lásd a 220-223. lábjegyzeteket kísérő *infra* szöveget.

9. Lásd a 296-317. lábjegyzeteket kísérő *infra* szöveget.

gemony.<sup>10</sup> Míg a kínai vállalatoknak a nyugati államok piacain való jelenlétére jelentős figyelmet fordítottak,<sup>11</sup> a mai napig kevés elemzés készült a fejlődő országokra gyakorolt hatásokról, ahol Kína digitális jelenlétével kapcsolatban egészen más dinamika alakul ki.<sup>12</sup>

A BRI keretében Kína nem csak néhány érett európai piacra, hanem elsősorban a feltörekvő gazdaságokba szállít infrastruktúrát és tőkét. A BRI a hagyományos infrastrukturális projektek, mint az autópályák, vasutak és erőművek mellett a DSR, a digitális infrastruktúra (azaz az adatok továbbítására, tárolására és feldolgozására szolgáló infrastruktúra) elemeit is magában foglalja. Ezek a digitális infrastruktúrák fizikai elemek (pl. optikai kábelek, antennák és adatközpontok) és nem fizikai elemek (pl. átviteli szabványok) összességei,

10. *Lásd általában* KAI-FU LEE, *AI SUPER-POWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER* (2018) (bemutatja, hogyan vált Kína a mesterséges intelligencia terén az Egyesült Államok fölé kerekedő domináns vezetővé); REBECCA

A. FANNIN, *TECH TITANS OF CHINA: HOW CHINA'S TECH SECTOR IS CHALLENGING THE WORLD BY INNOVATING FASTER, WORKING HARDER & GOING GLOBAL* (2019) (azzal érvelve, hogy a kínai Szilícium-völgy a technológia, a vízi-tőke és a mesterséges intelligencia terén vetekszik a Nyugattal, és az Egyesült Államokat megelőzheti a vezetésben); WINSTON MA, *THE DIGITAL WAR: HOW CHINA'S TECH POWER SHAPES THE FUTURE OF AI, BLOCKCHAIN AND CYBERSPACE* (2021) (azzal érvel, hogy Kínában egy újabb digitális forradalom küszöbén állunk, amely Kínát az USA, Európa és Japán kihívójává teszi a digitális gazdaságban).

11. *Lásd általában* Karl P. Sauvant, *Is the United States ready for FDI from China? Áttekintés, in* INVESTING IN THE UNITED STATES: KÉSZEN ÁLL-E AZ USA A KÍNÁBÓL ÉRKEZŐ FDI-RE? (Karl P. Sauvant szerk., 2009) (adatok segítségével mutatja be a kínai befektetések növekedését a Kanadát és az Egyesült Államokat is magában foglaló országokba irányuló közvetlen külföldi befektetéseken keresztül); JI LI, *THE CLASH OF CAPITALISMS?: CHINESE COMPANIES IN THE UNITED STATES* (2018) (a kínai közvetlen külföldi befektetéseket az Egyesült Államokban övező főbb debátumok tárgyalása olyan példák segítségével, mint a Lenovo, a Bank of China és a Huawei Egyesült Államokban végzett beruházási tapasztalatai); Jeffrey N. Gordon & Curtis J. Milhaupt, *China as a "National Strategic Buyer": Toward a Multilateral Regime for Cross-Border M&A*, COLUMBIA BUS. L. REV. (amely azt tárgyalja, hogy Kína növekvő jelenléte a határokon átnyúló M&A-ügyekben meghaladta az Egyesült Államokat, és új rendszerre lesz szükség ahhoz, hogy számot adjon "felemelkedéséről" ezen a területen).

12. Természetesen vannak kivételek. *Lásd pl.* „IGINIO GAGLIARDONE, *CHINA, AFRICA, AND THE FUTURE OF THE INTERNET* (2019) (az afrikai államokban az információs és kommunikációs technológiák alakítására irányuló kínai stratégiák elemzése); STEVEN FELDSTEIN, *THE RISE OF DIGITAL REPRESSION: HOW TECHNOLOGY IS RESHAPING POWER, POLITICS, AND RESISTANCE* (2021) (a kínai digitális elnyomás vizsgálata Thaiföldön, Etiópiában és a Fülöp-szigeteken).

hálózati protokollok és digitális azonosítók).<sup>13</sup> Mivel a fejlődő országok digitális infrastruktúrája gyakran kezdetleges, a kínai cégek tevékenységeinek hatása ezeken a piacokon nagyobb következményekkel járhat, mint a nyugati poszt-indusztériális társadalmakban való jelenlétük, különösen azokban, ahol a technológiai ágazatban szigorú beruházási rendszer van érvényben.<sup>14</sup>

A pekingi hatás elmélete megragadja, hogy Kína hogyan befolyásolja az adatkezelést transznacionális szinten, és különösen azt, hogy a kínai vállalatok milyen mértékben alakítják a digitális infrastruktúrát egy fejlődő országban a DSR keretében. A DSR ~~eredés~~ kínai és angol nyelvű normatív dokumentumok - köztük törvények, rendeletek, ágazati jelentések és esetek - gondos elemzésén alapul, amelyet kínai médiaelemzésekkel egészítünk ki, elsősorban a kínai vállalatok fejleményeinek nyomon követése érdekében. A DSR-rel kapcsolatos agytrösztök kutatásaira, <sup>15</sup>bizottsági jelentésekre <sup>16</sup>és a különböző tudományágakból származó, a DSR-ről szóló új tudományos munkákra is támaszkodunk.<sup>17</sup> Továbbá kiegészítettük elméleti

13. Lásd általában Martin Hilbert & Priscila ~~W.~~ *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE 60 (2011) (a digitális technológiák dominanciájának leírása a távközlés és az információ tárolása és feldolgozása terén).

14. A koronavírus-járványt követően a fejlett és a fejlődő országok között egyre inkább eltérnek a kínai befektetésekkel kapcsolatos nézetek, és az utóbbiak sokkal nyitottabbak a kínaiakkal való további üzletelésre. Lásd BRUNSWICK, UNDERSTANDING GLOBAL OPINION OF CHINESE BUSINESSES: A GROWING DIVIDE BETWEEN DEVELOPED AND EMERGING MARKETS 3, 9 (2020) (23 olyan ország általános lakossága körében, ahol kínai befektetések történtek, a feltörekvő gazdaságokból származó válaszadók 80%-a bízott a kínai vállalatokban, ami 3 százalékpontos növekedést jelent 2018-hoz képest, míg a fejlett gazdaságokból származó válaszadóknak csak 51%-a, ami 5 százalékpontos csökkenést jelent a kínai vállalatokban való bizalomhoz 2018, képest).

15. DANIELLE CAVE ET AL. „AUSZTRÁL STRATÉGIAI POLITIKAI INTÉZET, ISSUES PAPER: MAPPING CHINA'S TECHNOLOGY GIANTS (2019); SEN GONG ET AL., K4D, FELTÖREKVŐ KÉRDÉSEKRŐL SZÓLÓ JELENTÉS: AZ ÖV ÉS ÚT KEZDEMÉNYEZÉS DIGITÁLIS ÖSSZEKÖTTETÉSBE ÉS INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS TECHNOLÓGIÁKBA TÖRTÉNŐ BERUHÁZÁSAINAK HATÁSA AZ SDG-K ELÉRÉSÉRE (2019).

16. AMERIKAI-KÍNAI GAZDASÁGI ÉS GAZDASÁGI BIZTONSÁG. REV. COMM'N, REPORT 2018 TO CONGRESS 441-60 (egy egész fejezetet szentel Kína csúcstechnológiai fejlődésének és a "következő generációs összekapcsolhatóságnak").

17. Hong Shen, *Digitális selyemút építése? Situating the Internet in China's Belt and Road Initiative*, 12 INT'L J. COMM. 2683, 2685 (2018) (a kínai internetes vállalatok szerepének vizsgálata a DSR előmozdításában); Chan Jia Hao & Deepakshi Rawat, *China's Digital Silk Road: The Integration of Myanmar*, in RSIS84 COMMENTARIES (2019), <https://perma.cc/RK4X-YAKG> (Kína szerepének vizsgálata Mianmar digitalizálásában); THE DIGITAL SILK ROAD: PERSPECTIVES

a munkát empirikus kutatással, azáltal, hogy 2017 és 2020 között Pakisztánban, a kínai DSR egyik kulcsországában országon belüli inter-views-ot végez, ami talán az első olyan terepmunka, amely a DSR helyi hatását vizsgálja egy BRI-partnerállamban. Az elméleti és empirikus munka ilyen mértékű összekapcsolása azért jelentős, mert a BRI-t, beleértve a DSR-t is, köztudottan nehéz tanulmányozni az alapvető anyagok - különösen az olyan normatív dokumentumok, mint az államközi kötelezettségvállalásokat felvázoló egyetértési memorandumok - hozzáférhetetlensége miatt. E források többsége a kereskedelmi titoktartástól a nemzetbiztonságig terjedő okok miatt nem kerül nyilvánosságra. Terepmunkánk empirikus betekintést nyújt a helyszíni fejleményekbe, hogy a BRI-t, amelyet gyakran nagyra törő törekvések jellemeznek, hozzáférhetőbbé és elemezhetőbbé tegyük.

Ebben a cikkben reméljük, hogy összekapcsoljuk és bevonjuk a különböző interdiszciplináris és intradiszciplináris tudományterületek szakirodalmát. A transznacionális adatkezelésre összpontosítva a jogtudósok által a kiberjog, az adatvédelmi és magánéletvédelmi jog, az információs jog és a távközlési jog különböző, de egymást átfedő rubrikái alatt szokásosan tárgyalt kérdések egész sorát hozzuk össze, többek között összehasonlító szemszögből is. Emellett olyan interdiszciplináris megközelítést tesz szükségessé, amely integrálja a kommunikációval és az internettanulmányokkal foglalkozó tudósok fontos munkáját.<sup>18</sup> Az infrastruktúra jelentőségének kiemelésével az internetirányítással foglalkozó<sup>19</sup> kutatók megállapításait visszhangozzuk, és eleget teszünk annak a felhívásnak, hogy az infrastruktúrakutatás interdiszciplináris területének meglátásait integráljuk a jogi elemzésbe.<sup>20</sup> A DSR Pakisztánra gyakorolt hatásáról szóló esettanulmányunk a jog és a fejlődés kapcsolatával kapcsolatos régóta fennálló kérdésekre kíván válaszolni azzal az innovációval, hogy a KNK - nem a PRC

---

FROM AFFECTED COUNTRIES (Rogier Creemers, szerk., 2021) (a digitális selyemút működésének és hatásának leírása Kambodzsában, Iránban, Indiában és Etiópiában).

18. ROHINTON P. MEDHORA ET AL., DATA GOVERNANCE IN THE DIGITAL AGE (Centre for International Governance Innovation szerk., 2018).

19. Laura DeNardis & Francesca Musiani, *Governance by Infrastructure*, in THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 3-21 (Francesca Musiani et al. szerk., 2014); MILTON MUELLER, WILL THE INTERNET FRAGMENT?: SOVEREIGNTY, GLOBALIZATION AND CYBERSPACE (2017); DAVID D. CLARK, DE-SIGNING AN INTERNET (2018).

20. Benedict Kingsbury, *Infrastructure and InfraReg: On Rousing the International Law 'Wizards of Is'*, CAMBRIDGE INT'L L.J. (171,2019177).

a hagyományos "fejlett országok"<sup>21</sup> - a fejlesztési menetrendet irányítják.<sup>22</sup> Végezetül cikkünk alapvetően Kína globális hatalommá válásával foglalkozik, ami olyan nagy jelentőségű téma, amely a tudományágak széles köréből - többek között a nemzetközi jog és a globális kormányzás, a nemzetközi politika és a nemzetközi kapcsolatok, valamint a Kína-tanulmányok - megfelelő érdeklődést vált ki.<sup>23</sup>

Az intrapolitikai és interdiszciplinaritás iránti elkötelezettség a folyamatban lévő nagyszabású kutatási projektjeinket is érinti, amelyekből ez a cikk merít. A "Kína, jog és fejlődés" projekt a jog szerepét vizsgálja a KNK globális fejlődésében.<sup>24</sup> Ez a

---

21. Lásd általában David M. Trubek & Marc Galanter, *Scholars in Self-Estrangement: Some Reflections on the Crisis in Law and Development Studies in the United States*, 4 WIS. L. REV. 1062 (1974) (a jog és a fejlődés tanulmányozása során felmerülő problémák vizsgálata); JAMES A. GARDNER, LEGAL IMPERIALISM: AMERICAN LAWYERS AND FOREIGN AID IN LATIN AMERICA (1980) (azzal érvelve, hogy a jogi reformot a fejlődés előfeltételének tekintő amerikai erőfeszítések kudarcot vallottak); Brian Tamanaha, *The Lessons of Law-and-Development Studies*, AM89.

J. INT'L L. 470 (1995) (tárgyalja, hogy a modernizációs elmélet és a függőségi elmélet hogyan befolyásolta a jog és fejlődés irodalmát); Michael Trebilcock & Jing Leng, *The Role of Formal Contract Law and Enforcement in Economic Development*, 92 VA. L. REV. 1517 (2006) (a formális szerződési jog és a szerződésérvényesítés intézményeinek a gazdasági fejlődésben betöltött szerepével foglalkozik); THE NEW LAW AND ECONOMIC DEVELOPMENT (David M. Trubek & Alvaro Santos szerk., 2006) (a jog és a fejlődés iránti érdeklődés történetét és a fejlesztéspolitikai kezdeményezések mögött álló változó racionalitásokat tárgyalja); David M. Trubek, *Law and Development: Scholars in Self-Estrangement" után negyven évvel*, 66 UNIV. TORONTO L.J. 301 (2016) (a jog és fejlesztés területének feltérképezése az 1970-es évek óta).

22. Kína aktívabb volt Afrikában, mint más régiókban, az iparpolitikai innováció előmozdításában, beleértve a technológiát is. Lásd általában CHINA RETURNS TO AFRICA: A RISING POWER AND A CONTINENT EMBRACE (Chris Alden et al. eds., 2008) (Kína Afrikával való bővülő kapcsolatainak elemzése); DEBORAH BRANT UTIGAM, THE DRAGON'S GIFT: THE REAL STORY OF CHINA IN AFRICA (2009) (Kína növekvő jelenlétének és befolyásának elemzése Afrikában).

23. DAVID SHAMBAUGH, CHINA GOES GLOBAL: THE PARTIAL POWER 6-7 (2013) (azzal érvelve, hogy Kína széles, de sekélyes globális lábnyommal rendelkezik). De lásd ANDRE GUNDER FRANK, REORIENTING THE 19TH CENTURY: GLOBAL ECONOMY IN THE CONTINUING ASIAN AGE 4 (Robert A. Denemark ed., 2015) (újra megvizsgálja az Európa és Ázsia közötti "nagy eltérést", hogy Ázsiát, és különösen Kínát, mint a világtörténelem gazdasági súlypontját hangsúlyozza); KISHORE MAHBUBANI, HAS CHINA WON?: THE CHINESE CHALLENGE TO AMERICAN PRIMACY (132020) ("Kínának ugyanolyan jó esélye van, mint Amerikának arra, hogy a világ meghatározó befolyásává váljon.").

24. Lásd Erie, *Supra* note 1 (elemezve, hogy Kína hogyan használja a jogi és nem jogi rend integrált modelljét a gazdasági növekedés előmozdítására). További információért

A cikk osztja ezt a törekvést, és rávilágít arra, hogy a DSR a BRI részeként hogyan befolyásolja a fogadó államok adatkezelését, hangsúlyozva ezzel a digitális infrastruktúrák gazdasági, társadalmi és kulturális következményeinek hatékony szabályozására szolgáló hazai jogi eszközök fontosságát. Ez a felismerés kapcsolódik az "InfraReg projekt" egy bizonyos irányzatához, amely felismeri az infrastruktúrák szabályozási hatásait - amelyek a várostudományokban és a tudományos és technológiai tanulmányokban (STS) gyakoriak, de a jogtudományban kevésbé vizsgáltak -, és felteszi a kérdést, hogy a jog szabályozza-e és hogyan szabályozza ezeket az infrastruktúrákat.<sup>25</sup> Amint ez a cikk bemutatja, a BRI-államok nemzetközi és hazai internetpolitikája mélyen összefonódik az olyan fizikai infrastruktúrákkal, mint a földi és víz alatti üvegszál kábelek, az Internet Exchange Points és a szélessávú mobilhálózatokhoz szükséges antennák. Ezenkívül az "intelligens" és "biztonságos" városokban bevezetett "tárgyak internete" technológiák átalakító hatással lehetnek a polgárok életére és életvitelére.<sup>26</sup> Mindezen technológiák közös nevezője az adat. Az adatokhoz való hozzáférést és az adatok felhasználását alapvetően a digitális infrastruktúrák szabályozzák, de egyre inkább jogi szabályozás tárgyává és a különböző léptékű rendezés eszközévé is válnak - olyan szempontok, amelyeket a "Globális adatjog" projekt vizsgálni kíván.<sup>27</sup> A DSR kínai fejlesztésével összefüggésben azt tapasztaljuk, hogy az Európai Unió és az Egyesült Államok által követett megközelítésekhez képest hiányzik a transznacionális jogi rendezés a digitális területen. Kína inkább a digitális infrastruktúrák kínai vállalatok általi kiépítésével, karbantartásával és működtetésével valósítja meg az infrastrukturális rendezést, ami átalakítja a feltörekvő gazdaságok digitális jövőbe való átmenetének feltételeit.

A cikk további része a következőképpen épül fel: A II. rész Kína nemzetek közötti adatkezelésre gyakorolt hatását elemzi. A digitális tekintélyelvűséggel ellentétben kidolgozzuk a "pekingi hatásról" szóló beszámolóinkat, majd bemutatjuk, hogy Kína hogyan befolyásolja az adatkezelést határain túl. Kína hazai adatai

---

a projektről lásd: CHINA, LAW & DEVELOPMENT, <https://perma.cc/7GNQ-YU6N> (utolsó látogatás 202129., szeptember).

25. A projektről bővebben lásd INFRAREG, [www.iilj.org/infrareg](http://www.iilj.org/infrareg) (utolsó látogatás 202129., szeptember).

26. *Lásd az alábbi IV.B. szakaszt.*

27. A projektről bővebben lásd: GLOBAL DATA LAW, [www.guariniglobal.org/global-data-law](http://www.guariniglobal.org/global-data-law) (utolsó látogatás 202129., szeptember).

az irányítási rendszer területi adatlokalizációs követelményeket alkalmaz az adatszuverenitásra való törekvés érdekében. A fejlődő országok vonzza az adatáramlás feletti kormányzati ellenőrzés ígérete és Kína digitális gazdaságának látszólagos gazdasági sikere. Ezt a hatást erősíti, hogy Kína az adatszuverenitás mellett érvel a különböző globális adatkezelési intézményekben, és erősíti, hogy a kínai vállalatok egyre inkább digitális infrastruktúrát biztosítanak a fejlődő országokban, és befolyásolják a feltörekvő digitális technológiák műszaki szabványainak meghatározását. A III. rész bemutatja, hogyan valósul meg a pekingi hatás a DSR összefüggésében. A DSR egy átfogó jogi struktúra helyett számos nem kötelező erejű két- és többoldalú eszközre támaszkodik a Kína és a DSR-nek otthont adó államok közötti nemzetközi koordináció érdekében, amelyek meghatározzák az összekapcsolhatóság, a szuverenitás és a létrehozott nemzetközi intézmények közötti kapcsolatot. A IV. rész Pakisztánra mint esettanulmányra összpontosít, hogy megvizsgálja, hogyan befolyásolja Kína a DSR keretében az adatkezelést egy fogadó államban. A DSR digitális összeköttetést biztosít a Kína-Pakisztán gazdasági folyosó (CPEC) keretében, és a kínai technológiai vállalatok számos biztonságos város projektben vesznek részt Pakisztánban. Ugyanakkor Pakisztán adatkezelésre vonatkozó jogi infrastruktúrája nem rendelkezik megfelelő biztonsági intézkedésekkel, és a kínaihoz hasonlóan a nemzetbiztonságot helyezi előtérbe a polgárok adatainak védelmével szemben. Az V. rész a pekingi hatást a DSR-nek a fogadó államok digitális fejlődésére gyakorolt hatásával összefüggésben értékeli. Az adatszuverenitás a legtöbb fejlődő ország számára tarthatatlan, és a digitális infrastruktúra kiépítése megfelelő jogi infrastruktúra nélkül valószínűleg nem lesz fenntartható. A VI. rész zárszava.

## II. KÍNA TRANSZNEMZSIÁLIS HATÁSA AZ ADATKEZELÉSRE

Mielőtt elmagyaráznánk, hogy a KNK hogyan alakítja egyre inkább az adatokat

A pekingi hatáson keresztül a transznacionális kormányzásról, tisztázzuk terminológiánkat. Az "adatkezelés", a "transznacionális" és az "infrastrukturális" kifejezéseket olyan megkülönböztető módon használjuk, amely eltérhet a máshol használtaktól. *Adatkezelés* alatt a digitalizált információk (azaz az adatok) gyűjtését, tárolását, továbbítását, használatát és a hozzájuk való hozzáférést szabályozó szabályokat, normákat, gyakorlatokat és infrastruktúrákat értjük.<sup>28</sup> Ez az adatközpontú kon-

<sup>28</sup> Ez a meghatározás eltér az "adatkezelés" és az "adatkezelés" vállalati környezetben való használatától. *Lásd: Vijay Khatri & Carol V. Brown, Design-*

A jogtudományi koncepció tágabb, mint a szűkebb felfogás, amely csak bizonyos típusú információkra és azok jogi szabályozására összpontosítana. Az összes adatot felölelve az adatkezelés e dokumentumban használt koncepciója magában foglalja az olyan adatkategóriákat, amelyekre hagyományosan bizonyos speciális jogi szabályok vonatkoznak, valamint minden olyan adatot, amelyre nem léteznek ilyen szabályok. Például az adatkezelés magában foglalja az adatvédelmi és a magánélet védelmére vonatkozó jogszabályok által védett személyes adatokat; bizonyos szellemi tulajdonjogok által védett információkat; a szöveges, vizuális vagy hanginformációkat, amelyeket a nemzetközi emberi jogi jog és a hazai alkotmányjog alapján a véleménynyilvánítás szabadsága véd. Az adatkezelés azonban olyan adatokkal is foglalkozik, amelyekre nem léteznek ilyen speciális szabályok. Például a nem személyes, tényszerű adatok, amelyeket egy érzékelő gyűjtött össze egy adott helység időjárásáról.<sup>29</sup> A formális jogon túllépve az adatkezelés fogalma magában foglalja az adatok kezelésére vonatkozó társadalmi vagy kulturális normákat, valamint az intézményi gyakorlatokat is. Elismerjük a (jogilag nem kötelező erejű) technikai szabványok óriási gyakorlati jelentőségét is.<sup>30</sup> Ezeket a szabványokat hivatalos szabványalkotó szervezetek, technológiai vállalatok konzorciumai vagy akár egyetlen fejlesztő is kiadhatják.<sup>31</sup> Az ilyen adatokkal kapcsolatos szabványok foglalkozhatnak az adatok kezelésével (mint például a Nemzetközi Szabványügyi Szervezet (ISO)27701 információbiztonsági szabványa),<sup>32</sup> de meghatározhatják azokat a formátumokat is, amelyekben az adatok tárolhatók.

---

*ing Data Governance*, 53 COMM. ASS'N COMPUTING MACH. 148 (2010), <https://perma.cc/SML2-R7BH> (megkülönböztetve az adatkezelés mint az informatikával kapcsolatos döntési területek és elszámoltathatósági mechanizmusok, valamint az adatkezelés mint a döntések meghozatala és végrehajtása közötti különbséget).

29. *De lásd* Nadezhda Purtova, *The Law of Everything*, 10 L., INNOVATION & TECH. 40 (2018) (amellett érvel, hogy a személyes és nem személyes adatok közötti különbséget el kell hagyni, és minden adatfeldolgozást jogi szabályokkal kell irányítani).

30. A félreértések elkerülése végett, a jogelméletben a szabályok/normák megkülönböztetése nem ezeket a normákat kívánja megvilágítani. Valójában az adatkezelési szabványok magukban foglalhatják a jogtudományi értelemben vett szabályokat, szabványokat és elveket.

31. *Lásd* C. Bradford Biddle, *No Standard for Standards: Az IKT-szabványok fejlesztésének ökoszisztémájának megértése*, in: THE CAMBRIDGE HANDBOOK OF TECHNICAL STANDARDIZATION LAW: COMPETITION, ANTITRUST, AND PATENTS (Jorge L. Contreras szerk., 2017) (az információs és kommunikációs technológiai iparág különböző szabvány-fejlesztési modelljeinek vizsgálatára).

32. *Lásd* Eric Lachaud, *ISO/IEC szabvány:27701 A GDPR-tanúsítás veszélyei és lehetőségei*, 6 EUR. DATA PROT. L. REV. 194 (a vonatkozó ISO-szabványok és a GDPR-tanúsítási rendszerek közötti kapcsolatról).

(mint például az Adobe PDF formátum), az adatátvitel protokolljainak fenntartása (mint például az internet alapját képező TCP/IP protokoll), vagy a tervezési specifikációk létrehozása a teroperabilitás biztosítása érdekében (mint például a vezeték nélküli távközlés negyedik generációs LTE szabványa).

A *transznacionális adatkezelés* használata túlmutat a határokon átnyúló adatáramlás szabályozásának gondolatán. Számításaink kiterjednek azokra a különböző módokra, amelyekkel egy hazai adatkezelési rendszer hatással lehet másokra, valamint a nemzetközi jog vagy más nemzetközi normák és szabványok használatára a határokon átnyúló adatkezelés alakítása érdekében. A hazai adattörvényeknek lehetnek szándékolt vagy nem szándékolt tovagyűrűző hatásai, például a területi adatlokalizációs követelmények által okozott hatások.<sup>33</sup> Egyes adattörvények kifejezetten vagy hallgatólagosan területi hatályon kívüli alkalmazásra is alkalmasak.<sup>34</sup> Emellett egyes hazai adattörvények egy másik ország adattörvénye "megfelelőségének" egyoldalú vagy kétoldalú értékelésére támaszkodnak az adatok transznacionális szabályozása érdekében.<sup>35</sup> A transznacionális adatkezelés mindezen "jogi technológiai" leginkább úgy értelmezhető, mint az adatok feletti hatékony joghatósági ellenőrzés gyakorlására irányuló kísérletek. A nemzetközi jog - akár külön adatvédelmi vagy kiberbiztonsági szerződések formájában, akár a nemzetközi öko- nomikus jog keretében tett kötelezettségvállalások révén - szintén alakíthatja a különböző joghatóságok adatszabályozási módozatait.<sup>36</sup> Azonban az adatok nemzetek közötti, egyre nagyobb mértékű, akár a nemzeti, akár a nemzetközi jogban gyökerező jogi eszközökkel történő transznacionális szabályozása olyan transznacionális adatkezelési eszközökre rétegződik, amelyek nem jogilag kötelező erejűek, de nem kevésbé, vagy akár még inkább szabályozó hatással bírnak. Ez különösen igaz a technikai szabványokra, de vonatkozhat bizonyos, a gyakorlatban széles körben betartott iránymutatásokra és elvekre is. Végül soron bármely adatkezelési keretszabályozás szabályozási hatása csak a gyakorlati végrehajtás vizsgálatával állapítható meg.

Végül különbséget teszünk a "jogi" és az "infrastrukturális" adatkezelés között. Ez bizonyos mértékig visszhangozza azt a felismerést, amelyet Lawrence Lessig népszerűsített a "kód" kifejezéssel.

---

33. *Lásd a 112-24. megjegyzéseket kísérő infra szöveget.*

34. *Lásd a 101-12. megjegyzéseket kísérő infra szöveget.*

35. *Lásd az 57-58. és az 57-58. megjegyzéseket kísérő infra szöveget.* 126.

36. *Lásd a 132-42. megjegyzéseket.*

az 1990-es években a "jog",<sup>37</sup> de mi itt tágabb értelemben használjuk, és jobban igazodunk a XXI. századi digitális környezethez. Technológiai szempontból Lessig akkoriban írt, amikor az internet kereskedelmi forgalomba került, és a világháló beindult. Napjainkra az internet mindenütt behatolt a társadalmakba és a gazdaságokba - a digitális megosztottság ellenére -, és túllépett eredeti kommunikációs funkcióin, hogy más digitális technológiák alapvető infrastruktúrájává váljon. Laura DeNardis elemzése szerint: az internet mindenben benne van.<sup>38</sup> Politikai szempontból Lessig normatív keretét az amerikai alkotmány adta. Ez a keret nem képes befogadni egy olyan többpólusú tájképet, amelyben a globális hatókörű digitális technológiákat külföldi (az Egyesült Államok szempontjából) vállalatok és kormányok fejlesztik és alkalmazzák transznacionálisan. Másképp fogalmazva, ez nem képes figyelembe venni a pekingi hatást.

#### A. A pekingi hatás

Ebben a szakaszban elméleti beszámolót dolgozunk ki annak bemutatására, hogy Kína hogyan befolyásolja egyre inkább az adatkezelést határain túl. Az egyik hagyományos magyarázat arra, hogy Kína hogyan befolyásolja a technológiai fejlődést a határain kívül, a "digitális tekintélyelvűség". Ez a nézet azt állítja, hogy ahogy Kína olyan technológiai megközelítést alakított ki, amely fokozza a társadalom feletti ellenőrzését, háttérbe szorítja az ellenzékiet és az elküldötteket, propagandát és dezinformációt terjeszt, és elősegíti a gazdasági cserét liberális emberi jogok nélkül, úgy Kína is átülteti a határain túlra a reprezentatív uralom ilyen technológiai alapú eszközeit.<sup>39</sup> Konkrétan, e szerint a

37. Lásd LAWRENCE LESSIG, CODE: ÉS A KIBERTÉR EGYÉB TÖRVÉNYEI (31999). Azt a felismerést, hogy a fizikai tárgyaknak szabályozási hatásai (és a hozzájuk kapcsolódó "politika") lehetnek, általában Langdon Winner társadalomtudósnak tulajdonítják, *Do Artifacts Have Politics?*, DAEDALUS 109 (1980) 121.

38. Lásd általában LAURA DENARDIS, AZ INTERNET MINDENBEN: SZABADSÁG ÉS BIZTONSÁG EGY KIKAPCSOLÁS NÉLKÜLI VILÁGBAN (2020) (az internet szabályozási hatásának következményeit vizsgálva).

39. Lásd általában: *Digitális tekintélyelvűség és a szólásszabadság globális fenyegetése: Meghallgatás a Cong.-Exec. Comm'n on China, 115th Cong.* (2018) (összefoglaló), <https://perma.cc/V2EC-XS8T>; DEMOCRATIC STAFF OF S. COMM. ON FOREIGN RELS. „116TH CONG. „THE NEW BIG BROTHER: CHINA AND DIGITAL AUTHORITARIANISM (2020), <https://perma.cc/P2K6-CXMX>; LYDIA KHALIL, LOWLY INST. „DIGITAL AUTHORITARIANISM, CHINA AND COVID (2020), <https://perma.cc/3ZY3-5EHB>; DIMITAR LILKOV, WILFRIED MARTENS CTR. FOR EUR. STUD., MADE IN CHINA: TACKLING DIGITAL AUTHORITARIANISM (2020),

A nem demokratikus államok kormányai és vállalatai a megfigyelésre, cenzúrára, társadalmi manipulációra, kibernetikai zaklatásra, az internet elzárására és célzott üldözésre támaszkodnak e célok elérése érdekében.<sup>40</sup> A digitális tekintélyelvűség tézise népszerűvé vált a demokratikus értékeket világszerte népszerűsítő agytrösztök körében.<sup>41</sup> A Kínáról szóló tudományos irodalomban is meghatározóvá vált, különösen a "Kína-modell" jegyében.<sup>42</sup>

Bár nem vitatjuk a "digitális tekintélyelvűség" szakirodalmának számos megállapítását, úgy véljük, hogy az érvelés mögött három problémás feltételezés húzódik meg. Először is, a tézis egy "Kína-modellt" feltételez. A szakirodalomban nincs konszenzus arról, hogy mi a kínai modell, és a definíciók az autokráciától a meritokratikus kísérletig terjednek.

---

<https://perma.cc/4LAY-EWSK>; ALINA POLYAKOVA & CHRIS MESEROLE, BROOKINGS INST., EXPORTING DIGITAL AUTHORITARIANISM: THE RUSSIAN AND CHINESE MODELS (2019), <https://perma.cc/6XJH-LB4T>; Tiberia Dragu & Yonatan Lupu, *Digital Authoritarianism and the Future of Human Rights*, INT'L ORG. (2021); Valentin Weber, *Understanding the Global Ramifications of China's Information-Control Model*, in ARTIFICIAL INTELLIGENCE, CHINA, RUSSIA, AND THE GLOBAL ORDER 76 (Nicholas D. Wright ed., 2019); Naazneen Barma, Brent Durbin, & Andrea Kenall-Taylor, *Digital Authoritarianism: Finding Our Way Out Of The Darkness*, WAR ON THE ROCKS (2020, február), <https://perma.cc/74CW-2NDE>; Fredrik Erixon & Hosuk Lee-Makiyama, *Digital Authoritarianism: Human Rights, Geopolitics and Commerce* (Eur. Ctr. for Int'l Pol. Econ., Occasional Paper, No. 5/2011, 2011), <https://perma.cc/9SJW-C4NP>.

40. Steven Feldstein, *When It Comes to Digital Authoritarianism, China Is A Challenge - But Not The Only Challenge*, WAR ON THE ROCKS (2020. február 12.), <https://perma.cc/98HA-NK9Y>.

41. Lásd pl. Adrian Shabaz, *The Rise of Digital Authoritarianism*, FREEDOM HOUSE, <https://perma.cc/4RZT-J8TK> (utolsó látogatás: 2020. november 24.) ("[A] cohort of countries is moving towards digital authoritarianism by embracing the Chinese model of extensive censorship and automated surveillance systems"); Erol Yayboke & Samuel Brannen, *Promote and Build: A Strategic Approach to Digital Authoritarianism*, CTR. FOR STRATEGIC & INT'L STUD. (2020. október 15.), <https://perma.cc/MZ2Q-KVEP> (kiemelve a digitális tekintélyelvűség határokon átnyúló eszközeit és technikáit).

42. Lásd pl. Andrea Kendall-Taylor, Erica Frantz, & Joseph Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, 99 FOREIGN AFF. 103, (1042020) (a "digitális autokráciák" leírása); Willem Gravett, *Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa*, 20 AFR. HUM. RTS. L.J. 125, 125 (2020) ("A digitális kormányzás e "kínai modellje" az állami cenzúra messzemenő rendszerének izléses álcája").



"Pekingi hatás." Ezt a kifejezést Anu Bradford "Brussels Effect"-je ihlette, amely az uralkodó elmélet annak megértésére, hogy a jognak milyen szabályozási hatásai lehetnek a származási joghatóságán kívül.<sup>47</sup> A brüsszeli hatás azt állítja, hogy a vállalatok akkor is az európai jog felé húzódnak, ha jogilag nem kötelesek ezt tenni. Ahogy Bradford kifejti, ez a dinamika a David Vogel által elemzett "kaliforniai hatáshoz" hasonló dinamika.

Amerikai szabályozási rendszerek, ahol a vállalatok alkalmazkodnak a kaliforniai környezetvédelmi előírásokhoz, ami "versenyfutást eredményez a csúcsra".<sup>48</sup> Bradford legfontosabb felismerése, hogy ezek a dinamikák globálisan is lejátszódnak, mivel az Európai Unió számos szabályozási területen átvette a globális szabályozó szerepét. E hatás bekövetkezésének előfeltételei a következők: piaci erő, szabályozási kapacitás, viszonylag magas normák, az érintett fogyasztói piac rugalmatlansága, valamint a vállalatok egységesség iránti preferenciája.<sup>49</sup>

Az Európai Unió adatvédelmi rendszerét gyakran a brüsszeli hatás egyik legfontosabb példaként mutatják be.<sup>50</sup> Az Európai Unió általános adatvédelmi rendelete (GDPR) joghatóságot biztosít az európai személyes adatok feldolgozása felett, függetlenül attól, hogy hol történik a feldolgozás.<sup>51</sup> A cégek nem kerülhetik el egyszerűen az európai adatvédelmi rendelet hatályát.

---

47. ANU BRADFORD, A BRÜSSZELI HATÁS: HOGYAN URALJA AZ EURÓPAI UNIÓ A VILÁGOT 25 (2020). Ez a könyv kibővíti az eredetileg Anu Bradford, *The Brussels Effect (A brüsszeli hatás)* című könyvében kifejtett érvelést, 107 nw. U. L. REV. 1, 3 (2012)).

48. *Lásd általában* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 248 (1995) (a kaliforniai környezetvédelmi szabályozások államon kívüli hatását tárgyalja).

49. *Lásd* BRADFORD, THE BRUSSELS EFFECT (2020), *Supra* 47. lábjegyzet, 25-66. o. (a globális szabályozói szerepvállalás előfeltételeinek tárgyalása).

50. *Lásd id.* 131-47. o. (az Európai Unió GDPR-politikájának hatását vizsgálva); Cedric Ryngaert & Mistale Taylor, *The GDPR as Global Data Protection Regulation?*, 114 AM. J. INT'L L. UNBOUND 5, 9 (2020) (az uniós adatvédelmi intézkedések globális kihatásainak elismerése).

51. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (április)27 a2016 természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet), HL2016 (L 119.), 1. cikk1. 3 [a továbbiakban: általános adatvédelmi rendelet]. A GDPR az adatkezelésre a helytől függetlenül alkalmazandó, amennyiben azt az EU-ban letelepedett adatkezelő végzi. A GDPR az EU-ban nem letelepedett adatkezelő által végzett adatkezelésre is vonatkozik, amennyiben az áruk vagy szolgáltatások nyújtásával vagy az EU-ban tartózkodó érintettek viselkedésének nyomon követésével kapcsolatos. Ezek a joghatósági jellemzők a GDPR globális hatókörét biztosítják.

törvényt az adatok de-lokalizációja révén, és így mindenhol az európai adatvédelmi jognak való megfelelés mellett dönthetnek.<sup>52</sup> A GDPR magas költségekkel jár a meg nem felelés esetén, mivel a GDPR megsértése esetén a globális forgalom akár négy százalékát kitevő szankciókkal fenyeget.<sup>53</sup> Mivel a globális technológiai vállalatoknak meg kell felelniük a GDPR-nak, amikor az európai piacot szolgálják ki, dönthetnek úgy, hogy mindenhol betartják a rendelet szabályait. Bár a Facebook kezdetben úgy reagált a GDPR hatályba lépésére, hogy a nem európai felhasználói adatokat a GDPR joghatósági körén kívülre helyezte,<sup>54</sup> végül a GDPR-t mint globális szabványt támogatta, és végül mindenhol a GDPR-nak megfelelő beállításokat kínált a felhasználóinak (bár nem alapértelmezetten).<sup>55</sup>

Bradford tézise befolyásolta a globális adatszabályozás körüli vitát. Paul Schwartz azzal érvelt, hogy Bradford egyoldalú szabályozási globalizációra vonatkozó ak-tézise túlbecsüli az Európai Unió egyoldalú hatalmát, hogy diktálja a globális adatvédelmi szabályozás feltételeit.<sup>56</sup> A személyes adatok határokon átnyúló továbbítására vonatkozó GDPR-korlátozások bonyolult tárgyalásokhoz vezettek a hőn áhított "megfelelőségi" státusz megszerzése érdekében, amely lehetővé teszi a személyes adatok exportját az Európai Unióból harmadik országokba.<sup>57</sup> Japán biztosította az első pro forma kétoldalú, nem pedig egyoldalú elismerést az Európai Unióval, míg az Európai Unió és az Egyesült Államok hosszadalmas vitát folytat az amerikai adatvédelmi jogszabályok megfelelőségéről.<sup>58</sup> Schwartz azt állítja, hogy

---

52. Lásd Thomas Streinz, *Data Governance in International Economic Law*: (publikálatlan kézirat) (a szerzőnél) (a stratégiai beépítés és az adatkezelés közötti kölcsönhatást tárgyalja).

53. GDPR, *fentebb* említett cikk. 51,82.

54. Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, GUARDIAN (Apr. 201819), <https://perma.cc/DZ2V-LRWC>.

55. Heather Kelly, *Facebook Will Push Privacy Alert to Users Outside EU Ahead of GDPR*, CNN BUS. (201824., május), <https://perma.cc/672M-RVVB>.

56. Paul Schwartz, *Globális adatvédelem*: N94.Y.U. L. REV. 771,774 (2019).

57. GDPR, *fentebb* említett cikkek51., 44, 45.

58. Lásd Paul Schwartz, *Supra* note 56, 786-93. o. (a megfelelőség elérésének különböző nemzeti megközelítéseiről); lásd még HENRY FARRELL & ABRAHAM

L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 125-60 (2019) (a transzatlanti adatpolitika elemzése). Az Európai Unió Bírósága a C-362/14. sz. ügyben, Maximillian Schrems kontra Data Prot. Comm'r, ECLI:EU:C:2015:650 (20156., október). A jogutód "adatvédelmi pajzs" szenvedett

az országok nem elsősorban a globális egységességért lobbizó cégek, hanem az adatvédelemmel kapcsolatos növekvő globális konszenzus miatt követhetik az európai adatvédelmi rendszert. Ez a konszenzus olyan nemzetközi megállapodásokban nyilvánul meg, mint az Európa Tanács adatvédelmi egyezménye és számos nem kötelező erejű, de mégis befolyásos globális adatvédelmi eszköz, amelyek az Egyesült Államok ágazati megközelítésével szemben az Európai Unió megközelítését átfogó jellege miatt vonzónak ismerik el. Schwartz nem cáfolja Bradford beszámolóját, de hasznos módon bonyolítja azt, rámutatva a nyomás és a húzás eltérő dinamikájára, és előtérbe helyezve a befolyásolási mechanizmusok szélesebb körét, különösen a nemzetközi megállapodásokat.

Bradford és Schwartz munkájára építve vizsgáljuk Kína befolyását a globális adatkezelésre a DSR összefüggésében. Bradford arra a következtetésre jut, hogy Kína még nem gyakorol olyan szabályozási befolyást, mint amelyet az Európai Unió tanúsított, vagy más szóval, a pekingi hatás nem valószínű a közeljövőben.<sup>59</sup> Egyetértünk azzal, hogy Kína nem valószínű, hogy Bradford elképzelése szerint pekingi hatást vált ki. Bár Kína kétségtelenül rendelkezik a piac méretével ahhoz, hogy a világ minden tájáról vonzza a vállalatokat, a <sup>60</sup>piac mérete önmagában nem elegendő ahhoz, hogy egy állam nemzeti jogszabályainak globális betartására készítse a világot. A szabályozás minősége kulcsfontosságú tényező. Ebben a tekintetben a kínai joggal szembeni szokásos kritika az, hogy a könyvek ellenére is gyenge a végrehajtása.<sup>61</sup> Továbbra is látható, hogy

---

ugyanaz a sors jutott a C-311/18. számú, Data Prot. Comm'r kontra Facebook Ireland Ltd., ECLI:EU:C:2020:559 (2020. júli.).

59. Lásd Bradford, *The Brussels Effect* (2012), *fenti jegyzet* 47.(49"Eltart egy ideig, amíg Kína felváltja az EU-t, mint a de facto globális szabványok forrását."); BRADFORD, *THE BRUSSELS EFFECT* (2020), *fenti jegyzet* 47., 266. o. (a brüsszeli hatáshoz hasonló "pekingi hatás" valószínűtlensége mellett érvel); lásd még Alan Beattie, *Technology: How the US, EU and China Compete to Set Industry Standards*, FIN. TIMES (2019. július 24.), <https://perma.cc/NLH3-3JAU> (tárgyalja, hogy mind a GDPR, mind az EU aggályoskodott a kínai vállalatok által elkövetett esetleges adattovábbítási jogsértések miatt).

60. A Világbank mérései szerint Kína az EU-val majdnem holtversenyben a világ második legnagyobb gazdasága a GDP alapján, az USA után. Lásd: *GDP (folyó USD) - Európai Unió, Egyesült Államok, Kína*, WORLD BANK, <https://perma.cc/55KM-T8M6> (utolsó megtekintés: 2020. augusztus).

61. Lásd Donald C. Clarke, *Rejtélyes megfigyelések a kínai jogban*: COHEN tiszteletére 93, 93 (C. Stephen Hsu szerk., 2003) (a kínai jogrendszer számos olyan rejtélyes jellemzőjét figyeli meg, amelyek meghiúsítják a kínai jogalkalmazók és a kínai jogalkalmazók számára a jogalkalmazók és a kínai jogalkalmazók számára a jogalkalmazók és a kínai jogalkalmazók közötti

hogy Kína szabályozási kapacitása kifejezetten az adatkormányzás terén szenved-e a nem megfelelő végrehajtástól, amely a múltban a kínai jogokat akadályozta. Kína adatkezelési rendszere még mindig kialakulóban van. Bár a rendszer nagyfokú átfogóságra és kifinomultságra törekszik - a kiberbiztonsági törvény és a kísérő intézkedések sok tekintetben fejlettebbek, mint az analóg amerikai jogszabályok - , a rendszerrel és a végrehajtás módjával kapcsolatban továbbra is számos kétértelműség van.<sup>62</sup>

A legfontosabb ok, amiért Kína valószínűleg nem fogja megismételni a brüsszeli hatást, az az, hogy a külföldi digitális gazdasággal foglalkozó vállalatok nem támogatják az adatkezelés kínai megközelítésének globalizációját. A vállalatok elvileg előnyben részesíthetik a globális adatkormányzás egységességét, de ez az eltérő rendszerek és a hozzájuk kapcsolódó költségek arányosságától függ. Bár az Európai Unió GDPR-je és Kína kialakulóban lévő adatkezelési keretrendszere között jelentős átfedések vannak,<sup>63</sup> továbbra is vannak olyan különbségek, amelyek miatt a globális vállalatok számára nem megvalósítható vagy nem kívánatos az egységes vállalati szintű szabvány. A globális technológiai vállalatok inkább a széttagolt területet részesíthetik előnyben, ahol az ügyfeleket az adott nemzeti jog szerint szolgálják ki ahelyett, hogy a költséges hazai adatkezelési kereteket globálisan felerősítenék. Az adatok bizonyos mértékig rugalmas szabályozási célpontok (a pénzügyi tőkétől nem eltérően), és az adatkezelés globális egységessége iránti üzleti preferenciának vannak korlátai. A széttagolt rendszer sem technológiailag nem lehetetlen, sem pedig nem feltétlenül megfizethetetlenül költséges. Az eltérő gyártási szabványokkal ellentétben, amelyek gyakran jelentős átállási költségekkel járnak, a multinacionális vállalatok viszonylag gyorsan és költséghatékony módon változtathatják meg az adattárolás és -feldolgozás módját. Ez lehet a sorsa a

---

ile magyarázat); RANDALL PEERENBOOM, CHINA'S LONG MARCH TOWARD RULE OF LAW 323, 323 (2002) (azzal érvelve, hogy nem a bírák döntenek egy ügyben); lásd még BRADFORD, THE BRUSSELS EFFECT (2020), *Supra* 47. lábjegyzet, 31. o. (idézve Kína "hatékony és független, a nemzeti piaci szabályokat ezen a területen felügyelő üzleti intézmények hiányát").

62. Lásd Jeanne Huang, *A transznacionális személyes adatokra alkalmazandó jog*: L.J. 1283 (2020) (megjegyezve, hogy Kína adatkezelési rendszere egyenlőtlen végrehajtástól szenved); lásd a kínai adatkezelési keretrendszer további tárgyalását a 85-116. lábjegyzet alatti szövegben.

63. Lásd BRADFORD, THE BRUSSELS EFFECT (2020), *Supra* 47. lábjegyzet, 153. o. (megállapítva, hogy a kiberbiztonsági törvény "legalábbis külsőleg" utánozza a GDPR-t).

a brüsszeli hatás: ha az Európai Unió adatvédelmi rendszere által megszabott költségek meghaladják a globális egységességből származó előnyöket, akkor a vállalatok a különböző piacokra szánt termékeiket feldarabolják.<sup>64</sup> Bár az Európai Unió esetében ez még nem valósult meg, a kínai adatkezelési rendszerrel kapcsolatban ez az uralkodó vállalati stratégia.<sup>65</sup>

Vannak más mechanizmusok is, amelyeken keresztül Kína befolyást gyakorol a külföldi adatkezelési rendszerekre. Kína belföldi adatkezelésre vonatkozó megközelítése és az "adatszuverenitás" ígérete - ez egy tág fogalom, amelyet az alábbiakban<sup>66</sup> részletesen megvizsgálunk - vonzó egyes kormányok számára, amelyek saját belföldi rendszereikben utánozzák azt, még akkor is, ha a Kínai Népköztársaság erre vonatkozó kifejezett előírása nem áll fenn. Ezenfelül jelentős kereslet mutatkozik a kínai vállalatok által egyre inkább globálisan kínált digitális infrastruktúrák iránt, amelyek így külföldön is bekapcsolódnak a hazai adatkezelési rendszerekbe. Ez a két dinamika egybeesik azzal, hogy Kína határozottan támogatja az adatszuverenitást az internetirányítási intézményekben, és hogy a kínai vállalatok egyre nagyobb befolyást gyakorolnak a műszaki szabványok meghatározásában. A pekingi hatás megragadja ezeket a fejleményeket, megmagyarázza a mozgatórugóikat, és hasznos lehet az ellenstratégiák kidolgozásában.<sup>67</sup>

Bár Kína nem mutatja a pekingi hatás Bradford-féle változatát, azt sugalljuk, hogy már most is létezik egy másfajta pekingi hatás, amely valószínűleg tovább fog növekedni. Három olyan mechanizmust tételezünk fel, amelyek mindegyike a push és pull dinamika kombinációja, és amelyeken keresztül Kína befolyásolja a transznacionális adatkezelést: Először is, a külföldi kormányok utánozzák Kína adatkezelési megközelítését és az adatszuverenítésre vonatkozó ígéretét, amit elősegít, hogy Kína ezt a koncepciót a globális internetirányítási intézményekben és más helyszíneken népszerűsíti.

---

64. Lásd Thomas Streinz, *The Limits of the Brussels Effect in the Digital Domain* (kiadatlan kézirat) (a szerzőnél) (azzal érvelve, hogy az uniós jognak a digitális területre gyakorolt hatása nem tekinthető magától értetődőnek); lásd még Jens Frankenreiter, *The Missing 'California Effect' in Data Privacy Law*, YALE J. REGUL. (megjelenés előtt) (empirikusan bemutatva, hogy a differenciálás költségei kevésbé fontosak lehetnek, mint azt általában feltételezik, legalábbis az adatvédelmi jogban).

65. Lásd a 123-24. megjegyzéseket kísérő *infra* szöveget.

66. Lásd az alábbi V.A. szakaszt.

67. Lásd az alábbi V. szakaszt.

Másodsor, a kínai szereplők egyre fontosabb szerepet játszanak a digitális technológiai szabványok meghatározásában.<sup>68</sup> A "Made in China 2025" terv által ösztönözve, amely az ország önállóságát kívánja biztosítani a csúcstechnológiai ágazatokban, a kínai vállalatok, különösen a Huawei, vezető szerepet játszanak a globális 5G-szabvány kidolgozásában.<sup>69</sup> Kína a digitális technológiai szabványok terén tanúsított magabiztossága része innovációs stratégiájának, és arra épül, hogy saját műszaki és ipari szabványait használja a tengerentúli fizikai infrastrukturális projektjeiben.<sup>70</sup> A digitális technológiai szabványok a határokon átívelnek a nemzetközi szabványügyi szervezetek általi elfogadás révén, vagy ha a multinacionális vállalatok az interoperabilitás biztosítása érdekében egy közös szabvány felé orientálódnak.<sup>71</sup> Különösen ebben a tekintetben a külföldi vállalatok továbbra is érdekelték a Kínával való együttműködésben. Nem biztos, hogy a kínai jog felé vonzódnak - ahogyan a brüsszeli hatás az EU számára posztulálja.

68. Shin-yi Peng, *A szabvány mint a technológiai vezetés eszköze? China's ICT Standards in the Context of the International Economic Order*, in CHINA IN THE INTERNATIONAL ECONOMIC ORDER (Lisa 129Toohey et al. eds., 2015) ("China's rise as a global manufacturing center, combined with its growing technological capabilities, even increasingly enables China to force its own standards on the international economic order."); U.S.-CHINA BUS. COUNCIL, CHINA IN INTERNATIONAL STANDARDS SETTING: USCBC RECOMMENDATIONS FOR CONSTRUCTIVE PARTICIPATION (2020), <https://perma.cc/J3YQ-PMA5> (felvázolja Kína céljait a nemzetközi szabványok meghatározásában).

69. Lásd Paul Triolo & Allison Sherlock, "New Infrastructure" - China's Race for 5G and Networked Everything Has a New Catchphrase, SUPCHINA (2020. július 1.), <https://perma.cc/Q3QD-UUPM> (kifejtve, hogy Kína vezető szerepet tölt be a globális 5G szabványok meghatározásában). De lásd Diester Ernst, *Competing in Artificial Intelligence Chips: China's Challenge amid Technology War*, CTR. FOR INT'L GOVERNANCE INNOVATION (202026., márc.), <https://perma.cc/YY4F-92PE> (Kína külföldi félvezetőkre való támaszkodásának tárgyalása).

70. Lásd általában Olivier Peyrat, *Normes: Un outil cache de la stratégie économique chinoise* [Normák: A kínai gazdasági stratégia rejtett eszköze], 6 LE JOURNAL DE L'ÉCOLE DE PARIS DU MANAGEMENT (201230) (a kínai gazdasági stratégia rejtett eszköze).

Kína befolyásos szerepe a nemzetközi szabványok befolyásolásában); Pierguiseppe Pusceddu, Hic sunt dracones? A kínai innovációs politika jogi kereteinek feltérképezése: Standardization and IPRs, 51 INT'L REV. INTELL. PROP. & COMPETITION L. 559 (2020) (Kína "belföldi innovációs politikájának" tárgyalása, amely a kínai tulajdonú technológia, szabványok és szellemi tulajdonjogok fontosságát hangsúlyozza, és nyomon követi Kína innovációs politikájának jogi keretének általános fejlődését az 1950-es évek óta).

71. Lásd Biddle, *Supra* 31. lábjegyzet, 17. o. (az IKT-szabványok kialakulásának magyarázata).

a kínai technológiával való átjárhatóság fenntartása érdekében a közös műszaki szabványok felé irányuló jogszabályok.<sup>72</sup>

Harmadszor, a kínai vállalatok digitális infrastruktúrákat és platformokat biztosítanak a DSR mentén fekvő fogadó országokban, ezáltal alakítva azokat a feltételeket, amelyek mellett ezek az országok a digitálisan közvetített gazdaságok és társadalmak felé haladnak. A feltörekvő gazdaságok növekvő keresletet mutatnak a kínai technológiai vállalatok által biztosított digitális infrastruktúra iránt - ez a folyamat paradox módon alááshatja a fogadó állam adatszuverenitásra irányuló törekvéseit.<sup>73</sup> Miközben tehát érzékelhetők bizonyos tolóerők, a húzóerők erejét nem szabad alábecsülni.

Összefoglalva, Peking nem Brüsszel. Kína adatkezelési rendszere nem rendelkezik azokkal a jellemzőkkel, amelyek az Európai Unió GDPR-jét *globális* adatvédelmi rendelettel való átalakításában szerepet játszottak. A pekingi hatás más mechanizmusokat és dinamikát foglal magában. Eredménye nem a Kínai Népköztársaság hazai adatkezelési jogszabályainak Kína-modellként történő lemásolása, vagy összehasonlító jogi kifejezéssel élve "jogi átültetés", hanem az adatok feletti kormányzati és területi ellenőrzés alapjául szolgáló adatkezelési elvek megerősítése, amely különböző és erősen kontextusfüggő hazai adattörvényekben realizálódik.<sup>74</sup> A kínai technológiai vállalatok a helyi jog viszonylagos fejlettségétől függően kihasználhatják a fogadó állam jogrendszerét, amelyek különleges piaci hozzáférést és működési szabadságokat biztosítanak számukra. Természetesen a kínai technológiai vállalatok nem egyedülállóak a feltörekvő piacokra való behatolásuk és a digitális infrastruktúrával való ellátásuk terén;<sup>75</sup> a kínai pártállammal való összefonódásuk azonban megkülönbözteti a kínai esetet, és egyedivé teszi a pekingi hatást.<sup>76</sup> A következőkben

---

72. *Lásd* Bureau of Industry and Security, Commerce, Temporary General License, Fed84. Reg. 23,468 (201922., május) (kodifikálandó: C15.F.R. pts. 762744,) <https://perma.cc/X2BD-CUFY> (az 5G szabványosítás céljából a Huawei-jel való együttműködés engedélyezése).

73. *Lásd* ennek az állításnak a tárgyalását az V. szakaszban.

74. *Lásd* a IV.C. szakaszban a pakisztáni belföldi adatkezelési keretrendszer (közvetett) kínai befolyás alatt történő megvitatását.

75. A Hewlett Packard például megfigyelési technológiát biztosított az ujjurok megfigyelésére. *Lásd* Liza Lin & Josh Chin, *U.S. Tech Companies Prop Up China's Vast Surveillance Network*, WALL ST. J. (201926., nov.), <https://perma.cc/Y4EF-6XF6>; *lásd még* az alábbi IV.B. szakaszt.

76. *Lásd* az alábbi IV.C. szakaszt.

A következő részben részletesebben kifejtjük a Beij-ing-hatás három mechanizmusát, kezdve Kína adatkezeléssel kapcsolatos megközelítésével, és összehasonlítjuk és szembeállítjuk Kína transznacionális adatkezelésre gyakorolt hatását az Európai Unió és az Egyesült Államok szerepével.

B. *Kína megközelítése az adatkezeléshez: Az adatok lokalizálása az adatszuverenitásra való törekvésben*

Kína más joghatóságoktól kölcsönzött, és saját megközelítést alakított ki az adatkezelésre vonatkozóan. A "kiber-szuverenitás" (*wangluo zhuquan*) gyakorlása - az internet feletti nemzeti joghatóság érvényesítése révén - központi szerepet játszik Kína adatkezelési rendszerében, és meghatározza, hogy a kínai polgárok hogyan érintkeznek a külvilággal és fordítva.<sup>77</sup> A Kínai Népköztársaság adatkezelési keretrendszerét a kettős cél vezérli: elsősorban a nemzetbiztonság védelme, ugyanakkor a gazdasági növekedés elősegítése. Még a KKP főtitkára és a KNK elnöke, Xi Jinping is támogatja azt, amit a World Economic Forum "negyedik ipari forradalomnak" nevez: a digitális, a biológiai és a fizikai világ összekapcsolását.<sup>78</sup> A Kínai Népköztársaság kormánya a kínai technológiai óriáscégekkel együtt a digitális technológiák, különösen a nagy adatelemzés és a mesterséges intelligencia/gépi tanulás alkalmazásai segítségével alakította át az ország társadalmi kormányzását.<sup>79</sup> Innovációk

77. Lásd Rogier Creemers, *China's Conception of Cyber Sovereignty*: (2020. február 5.), <https://perma.cc/FC73-GBUM> (idézi az Államtanács Hivatalának az *internetről szóló fehér könyvét* (2010), amely először mutatta be a kiber-szuverenitást).

78. Xi Jinping, *Zhonghua renmin gongheguo zhongyang renmin zhengfu* (中华人民共和国中央人民政府) [KNK kormánya], *Rang meihao yuanjing bian wei xianshi: zai jin zhuan guojia ren yuehanneisibao huiwu da (让美好愿景变为现实 - 引领全球发展大方向)* [Rang meihao yuanjing bian wei xianshi: zai jin zhuan guojia ren yuehanneisibao huiwu da] (Speech at the BRICS Countries in Johannesburg) (2018. július), <https://perma.cc/CKJ9-6E8D> (a nagy adatok, a mesterséges intelligencia és más csúcstechnológiák technológiai forradalmáról beszél). A "Made in China 2025" terv része ennek a célnak. A "negyedik ipari forradalom" elnevezést a WEF alapítója, Klaus Schwab alkotta meg. Klaus Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, WORLD ECON. F. (2016. jan.), <https://perma.cc/RWR8-3TJP>.

79. ZHONGGUO XINXI TONGXIN YANJIUYUAN ANQUAN YANJIUSUO (中国信息通信研究院安全研究所) [CHINA ACADEMY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY, SECURITY RESEARCH BUREAU] [KINAI INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS TECHNOLÓGIAI AKADÉMIA, BIZTONSÁGI KUTATÁSI IRODA] DASHUJU AN- QUAN BAIPISHU (大数据安全白皮书) [BIG DATA SECURITY WHITE PAPER] [NAGY ADATBIZTONSÁGI FEHÉR KÖNYV]. 1

A Kínában ma már általánosan elterjedt eszközök közé tartozik a készpénzmentes társadalom,<sup>80</sup> a szociális hitelrendszer,<sup>81</sup> az "egészségügyi kódex", amely a fertőző betegségeket figyeli,<sup>82</sup> és az online bíróságok a vitás ügyek kezelésére.<sup>83</sup> A digitalizációnak a pekingi társadalmi stabilitási prioritásokkal összhangban történő alakítására irányuló összehangolt erőfeszítések ellenére vagy éppen azért, mert Kína rendelkezik a legnagyobb e-kereskedelmi piaccal, a legtöbb internet-felhasználóval és a leggyorsabban növekvő technológiai vállalatokkal a világon.<sup>84</sup>

Ebben a cikkben nem nyújtunk teljes körű beszámolót Kína fejlődő adatkezelési keretrendszeréről.<sup>85</sup> Ehelyett inkább azokra az elemekre összpontosítunk, amelyek a transznacionális hatások szempontjából kiemelkedőek.

---

(2018) (a nagy adatokat "alapvető stratégiai erőforrásnak és a társadalmi alaptermelés kulcsfontosságú tényezőjének" nevezi).

80. Rui Zhong, *China Can't Afford a Cashless Society*, FOREIGN POL'Y (Sept. 201811.), <https://perma.cc/8Y82-NEAT> (a kínai digitális fizetéseket kísérő problémák megvitatása).

81. Az értékelések jelentősen eltérnek. Lásd pl. Yu-Jie Chen, Ching-Fu Lin, & Han-Wei Liu, "Rule of Trust": *The Power and Perils of China's Social Credit Megaproject*, 32 COLUM. J. ASIAN L. 1, 3 (2018-2020) (azt állítva, hogy a szociális hitelrendszer "bizalomuralma" aláássa a KNK kormányának "jogállamiságra" irányuló célját); Liav Orgad & Wessel Reijers, *How to Make the Perfect Citizen? Lessons from China's Model of Social Credit System*, EUR. U. INST. RSCAS, Work- ing Paper 2020/28 (a "kibernetikus állampolgárság" kínai modelljének leírása, valamint a nyugati rendszerekkel való párhuzamosságok és eltérések); Rogier Creemers, *China's Social Credit System: An Evolving Practice of Control* (2018. május 9.), <https://perma.cc/TN2R-TGQM> (a szociális hitelrendszert a lakosság ellenőrzésének egyik mechanizmusának tekinti); Xin Dai, *Towards a Reputation State: A Comprehensive View of China's Social Credit System Project*, in SOCIAL CREDIT RAT- ING 139, 139-40 (Oliver Everling szerk., 2020) (arra utalva, hogy a szociális hitelrendszer potenciálisan átalakíthatja a kormányzást Kínán belül).

82. "Geren jiankang xinxi ma" xilie guojia biao zhun jiedu (《个人健康信息码》系列国家标准解读) [A "Személyes egészségügyi információk kódexére" vonatkozó nemzeti szabványsorozat értelmezése], ZHEJIANG BIAOZHUN XINXI PINGTAI (浙江标准信息平台) [ZHEJIANG STANDARDS INFORMATION PLATFORM] (2022., május), <https://perma.cc/74PV-EAYA>.

83. Jason Tashea, *China's All-Virtual Specialty Internet Courts Look Set to Expand into Other Areas of the Law*, A.B.A. J. (Nov. 2019), <https://perma.cc/G7B3-GXYS>.

84. Lásd Jeff Desjardins, *China's Home-Grown Tech Giants Are Dominating Their US Competitors*, BUS. INSIDER (2018. február 7.), <https://perma.cc/9ABP-H5TP> (bemutatja, hogy a Baidu, az Alibaba, a Tencent és a Xiaomi a nemzetközi piaci penetráció tekintetében megelőzte a Google-t, az Apple-t, a Facebookot és az Amazont).

85. Egyre nagyobb az összehasonlító jogi szakirodalom, amely az Egyesült Államok, az Európai Unió és Kína adatkezelésének különböző megközelítéseit vizsgálja. Pl. Henry S. Gao, *Data Regulation with Chinese Characteristics*, in BIG DATA AND GLOBAL TRADE LAW (245 Mira Burri szerk., 2021); Emmanuel

megmutatja, hogy Kína hogyan gyakorolja az adatok feletti joghatósági ellenőrzést azáltal, hogy bizonyos adatkategóriák területi adatlokalizációját írja elő. Ez hasonlóságokat mutat, ugyanakkor fontos különbségeket is mutat az Európai Uniónak a GDPR szerinti megközelítésével, amely az extraterritoriális alkalmazás elemeit tartalmazza, és a külföldi joghatóságokat egyoldalú "megfelelőségi értékelésnek" veti alá. A közelmúltban az Egyesült Államok is érdeklődést mutatott a kínai technológiai vállalatokra irányuló célzott adatlokalizáció iránt.<sup>86</sup> Kína rendszere azonban, beleértve a területi adatlokalizációra vonatkozó megközelítését is, továbbra is sajátos marad.

Kína adatkezelési rendszere folyamatosan fejlődik, és számos egymást átfedő területet foglal magában, beleértve a távközlési szabályozást, az online tartalomkezelést, a határokon átnyúló adatáramlást, a titkosítást és a kritikus infrastruktúrák biztonságát.<sup>87</sup> Az ezeket az egymást átfedő területeket szabályozó szabályok nem tisztán jogi jellegűek; a jogszabályok és szabályozási intézkedések mellett a nem jogilag kötelező érvényű szabványok (nem összetévesztendő a technikai szabványokkal) és stratégiák is fontos szerepet játszanak, eltérő hatókörrel.<sup>88</sup> A "Tizenharmadik ötéves informatizációs terv" (2016) például számos célkitűzést fogalmaz meg a társadalom minden területének "informatizálására".<sup>89</sup> Ezek mentén

Pernot-Leplay, *Kína megközelítése az adatvédelmi joggal kapcsolatban: Harmadik út a USA és az EU?*, PA8. ST. J.L. & INT'L AFF. 50 (2020); Huang, *Supra* note. 62.

86. 2019 ősze óta az Egyesült Államokban történő külföldi befektetésekkel foglalkozó bizottság (CFIUS) vizsgálja a Bytedance által 2017 novemberében a Musical.ly felvásárlását, amely később beolvadt a TikTokba; a kérdés, hogy a TikTok továbbít-e adatokat az amerikai felhasználókról Kínába, a jelentések szerint a vizsgálat egyik fő fókuszában áll. *Lásd* Robert McMillan et al., *TikTok User Data: TikTok: Mit gyűjt az alkalmazás és miért aggnak az amerikai hatóságok?*, WALL ST. J. (2020. július 7.), <https://perma.cc/3539-RNDA>; *lásd még* Class Action Complaint, Hong v. Bytedance, Inc., WL (20196481689N.D. Cal.) ("A TikTok titokban hatalmas mennyiségű magánjellegű és személyazonosításra alkalmas felhasználói adatot porszívózott fel és továbbított kínai szerverekre, amelyek felhasználhatók az Egyesült Államokban élő felhasználók helyének és tevékenységeinek azonosítására, nyilvántartására és nyomon követésére most és a jövőben."). *De lásd* Pellaeon Lin, *TikTok and Douyin Explained*, CITI-ZEN LAB (Mar. 22, 2021), <https://perma.cc/YZ6U-W3KE> (nem talált nyílt adatátvitelt a kínai kormánynak, és nem talált kapcsolatot a Kínán belüli szerverekkel, ugyanakkor nem zárta ki a ByteDance-en keresztül történő adathozzáférést).

87. Samm Sacks, *China's Emerging Cyber Governance System*, CTR. FOR STRATEGIC & INT'L STUD., <https://perma.cc/5JBA-A6QK> (utolsó látogatás: 2020. május 28.).

88. *Id.*

89. "'Shisanwu' guojia xinxihua guifan de tongzhi" ("十三五"国家信息化规范的通知) [Közlemény a tizenharmadik ötéves in-

sorok, jogszabályok, intézkedések és szabványok sora ad egyre konkrétabb útmutatást arra vonatkozóan, hogy az adatokat hogyan kell kezelni a KNK stratégiai céljainak elérése érdekében.

Több kormányzati ügynökség is felelős e különböző típusú normatív dokumentumok közzétételéért. A legfontosabb ügynökségek a Közbiztonsági Minisztérium (MPS), amelynek feladata az internet biztonságának fenntartása, az Ipari és Informatikai Minisztérium (MIIT), az internet központi szabályozója, valamint a Kínai Kibertér Adminisztráció (CAC), amelyet 2011-ben hoztak létre az online tartalmak szabályozásának felügyeletével, és egyre nagyobb hatáskörrel rendelkezik.<sup>90</sup> E hármasság alatt, nemzeti szinten számos további ügynökség rendelkezik bizonyos mértékű felügyelettel az adatkezelési kérdések felett, többek között a Nemzeti Fejlesztési és Reformbizottság, a Pénzügyminisztérium, a Kínai Népbank és a Tudományos és Technológiai Minisztérium.<sup>91</sup> Kína nagy technológiai vállalatai és egyre több agytröszt is igyekszik alakítani Kína adatkezelési politikáját. A tartományi szintű (kormányzati, vállalati és tudományos) szervek saját érdekeiket képviselhetik, amelyek nem mindig tükrözik az országos szintű hatóságok érdekeit. Ezért számos hang és iparági igény határozza meg, hogy a különböző típusú adatokat hogyan kell tárolni, feldolgozni, felhasználni és továbbítani.<sup>92</sup>

Kína adatkezelési rendszerének legfontosabb jogszabálya a kiberbiztonsági törvény (2017).<sup>93</sup> A kiberbiztonsági törvény központi eleme

---

formázási terv] [az Államtanács által kihirdetve, 201627., dec.), <https://perma.cc/D5ZE-VZKY>.

90. Lásd Gao, *Supra* 85. lábjegyzet, 249. o. (a CAC, a MIIT és az MPS létrehozását és hatalomra jutását tárgyalja).

91. Lásd Weishan Miao, Min Jiang & Yunxia Pang, *Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994-2017)*, 15 INT'L J. COMM. 2010-162003, (2021) (a PCR internetszabályozásában részt vevő kormányzati<sup>71</sup> szervek katalógizálása, valamint a központi-perifériás dy-namika és az ügynökségek közötti együttműködés azonosítása).

92. Samm Sacks, Paul Triolo & Graham Webster, *Beyond the Worst-Case Assumptions on China's Cybersecurity Law*, NEW AMERICA, <https://perma.cc/BXG4-E5Q4> (utolsó látogatás 202017., augusztus).

93. Zhonghua Renmin Gongheguo Wangluo Anquanfa (中华人民共和国网络安全法) [A Kínai Népköztársaság kiberbiztonsági törvénye] [kihirdette az Állandó Bizottság. Nat'l People's Cong., 2017], nov., hatályos 2016, 2017. június). 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 6 [a továbbiakban: kiberbiztonsági törvény].

Törvény az általa "személyes információnak" és "fontos adatnak" nevezett adatok kezelése. A "személyes információ" nagyjából arra vonatkozik, amit a GDPR "személyes adatnak" vagy olyan információnak nevez, amely egy azonosított vagy azonosítható természetes személyre vonatkozik.<sup>94</sup> A "fontos adatok" tágan értelmezve olyan adatok, amelyek szorosan kapcsolódnak a nemzetbiztonsághoz, a gazdasági biztonsághoz vagy a társadalmi stabilitáshoz.<sup>95</sup> Kínában erőteljes feketepiac működik, amely adatlopás, adateltérítés, csalás és más adatalapú bűncselekmények révén kereskedik az adatokkal.<sup>96</sup> Kína adatkezelésre vonatkozó megközelítése a személyes adatok nem állami szereplők általi jogellenes felhasználását célozza, de nincsenek megfelelő akadályai a magánéletbe való kormányzati beavatkozásnak.<sup>97</sup> 2020 májusában a tizenharmadik Nemzeti Népi Kongresszus (NPC), a kínai rendszer legfőbb jogalkotó szerve, harmadik ülészaka elfogadta a polgári törvénykönyvet, a KNK első olyan törvénykönyvét, amely tovább pontosítja, hogy a személyes adatok védelmét a

94. GDPR, *fentebb* említett cikk51., 4(1).

95. "Shuju Anquan Guanli Banfa (Zhengqiu Yijiangao)" Gongkai Zhenqiu Yijian De Tongzhi (《数据安全管理办法（征求意见稿）》公开征求意见的通知) [Nyilvános közlemény for Seering Comments on the "Measures on Data Security Management" (Measures on Data Security Management) (Hozzászólásra váró tervezet)], (kihirdetve az Állami Internet Info. Off. által, 201928., június), 38. cikk (5) bekezdés, <https://perma.cc/FXN3-CUNR>.

96. Huang Shujing (黄姝静), Shuju Heishi Changjue, Yinsi Pin Zao Xielou, Ruhe Lifa Du Shang Geren Xinxi Loudong (《数据黑市猖獗，隐私频遭泄露，如何立法堵上个人信息漏洞》 [Az adatok A feketepiac burjánzik, és az adatok gyakran kiszivárognak. Hogyan lehet a törvényhozás későn betönni a személyes adatok kiskapuit?]) CAIJING ZAZHI (财经杂志) [CAIJING MAGAZIN], 2020. május 29., <https://perma.cc/2CKY-MD4U> (egy olyan példával szolgál, amikor a Wuhanban kitört koronavírus járvány csúcspontján Wuhan város 7000 lakosának személyes adatai szivárogtak ki a közösségi média alkalmazásokon keresztül).

97. *Lásd pl.* a kiberbiztonsági törvény, 93. látjegyzet, 93. cikk. 12. cikk (megkülönbözteti az államot, mint "az állampolgárok, jogi személyek és más szervezetek azon jogainak védelmét, hogy a hálózatokat a törvényeknek megfelelően használják", az "[a]zokat használó személyeknek és szervezeteknek be kell tartaniuk az alkotmányt és a törvényeket"); *lásd még* Xu Ridan (徐日丹), Zuigao Renmin Jianchayuan Guanyu Banli Qinfan Gongmin Geren Xinxi Xingshi Anjian Shiyong Falu" Ruogan Wenti de Jieshi (最高人民法院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) [Supreme People's Procuratorate Interpretation of Several Issues Concerning the Application of Laws in Handling Criminal Cases Infring Citizens' Personal Information], JIANCHA RIBAO (检察日报) [PROCURATORATE DAILY], May 10, <https://perma.cc/TT52-FPVB> (2017, megállapítva, hogy "számos esetben a polgárok személyes adatainak kiszivárgását belső személyek (*neibu rennyuan*) követik el", kiemelve a magánszereplőket, akik közül néhányan vállalatok, bankok és más pénzügyi intézményeken belülről tevékenykednek).

törvény.<sup>98</sup> 2021 júniusában a tizenharmadik NVB Állandó Bizottságának huszonkilencedik ülésén elfogadták a KNK adatbiztonsági törvényét.<sup>99</sup> 2021 augusztusában a harmincadik ülés elfogadta a személyes információvédelemről szóló törvényt.<sup>100</sup>

A közelmúltig Kína adatkezelési rendszere nagyobb mértékben hangsúlyozta a területiséget, mint az adatkezelés más megközelítései. A GDPR például joghatóságot biztosít az európai személyes adatok feldolgozása felett, függetlenül attól, hogy a feldolgozás hol történik.<sup>101</sup> A GDPR az Európai Unióban letelepedett minden adatkezelőre vonatkozik, és még azokra is, akik nem az Unióban letelepedtek, ha az Európai Unióban kínálnak árukat vagy szolgáltatásokat, vagy figyelemmel kísérik az érintettek viselkedését. Ezek a joghatósági jellemzők hozzájárulnak a GDPR globális hatóköréhez. Ezzel szemben a Kínai Népköztársaság kiberbiztonsági törvénye nem tartalmaz ilyen extraterritoriális elemeket; alkalmazása a "hálózatok építésére, üzemeltetésére, karbantartására és használatára, valamint a kiberbiztonsági felügyeletre és irányításra korlátozódik a Kínai Népköztársaság szárazföldi területén belül".<sup>102</sup> A kiberbiztonsági törvény egyetlen kifejezett extraterritoriális eleme az állam azon felelősségére vonatkozik, hogy figyelemmel kíséresse, megelőzze és kezelje a kiberbiztonsági kockázatokat és fenyegetéseket, amelyek mind az országon belülről, mind azon kívülről erednek.

98. Zhonghua Renmin Gongheguo Minfadian (中华人民共和国民法典) [A Kínai Népköztársaság Polgári Törvénykönyve], kihirdetve a Nat'l People's Cong. által, 2020. május 28., hatályos 2021. január 1., art. 111, ZHONGHUA RENMIN GONGHEGUO ZHUDI LING 45 (中华人民共和国主席令第45号) [ORDER OF THE PRESIDENT OF THE PEOPLE'S REPUBLIC OF CHINA NO. 45] <https://www.pkulaw.com/chl/aa00daeb5a4fe4ebdfb.html> (kimondja, hogy a természetes személy magánjellegű adatait a törvény védi).

99. Zhonghua Renmin Gongheguo Shuju Anquanfa (中华人民共和国数据安全法) [a Kínai Népköztársaság adatbiztonsági törvénye], amelyet az Állandó Bizottság hozott. Nat'l People's Cong., június hatályos 10, 2021, szept. ZHONGGUO1, 2021, REN DAWANG (中国人大网) [GENERAL OFFICE OF THE STANDING COMM. NAT'L PEOPLE'S CONG. NEWS], <https://perma.cc/H882-YZ3Q>.

100. Zhonghua Renmin Gongheguo Geren Xinxi Baohufa (中华人民共和国个人信息保护法) [A Kínai Népköztársaság személyi adatok védelméről szóló törvény], amelyet az Állandó Bizottság hozott. Nat'l People's Cong., aug. hatályos 20, 2021, nov. ZHONGGUO1, 2021, REN DAWANG (中国人大网) [GENERAL OFFICE OF THE STANDING COMM. NAT'L PEOPLE'S CONG. NEWS], <https://perma.cc/B3KH-5V8C>.

101. GDPR, *fentebb* említett cikk. 51,3.

102. Cybersecurity Law, *supra* note art. 93,2.

a Kínai Népköztársaság szárazföldi területe.<sup>103</sup> Más szóval, míg az adattárolás és -feldolgozás területi jellege a GDPR alkalmazási köre szempontjából nagyrészt lényegtelen, a kínai kiberbiztonsági törvény esetében továbbra is ez a központi kritérium.

Az Európai Unióval, vagy akár az Egyesült Államokkal ellentétben Kína történelmileg idegenkedik a belső jogának extraterritoriális alkalmazásától.<sup>104</sup> Ennek történelmi okai lehetnek,<sup>105</sup> de eredhet Kína külpolitikájából is, amely hagyományosan a be nem avatkozást hangsúlyozza.<sup>106</sup> Vannak azonban arra utaló jelek, hogy Kína vonakodása saját jogának extraterritoriális alkalmazásával szemben változhat.<sup>107</sup> A KNK adatbiztonsági törvénye például túlmutat a kiberbiztonsági törvényen azzal, hogy a KNK-n kívül található jogalanyokra és személyekre is vonatkozik, ha adataik sértik a nemzetbiztonságot, a közérdeket és az emberek jogos érdekeit Kínában.<sup>108</sup> Hasonlóképpen, és a GDPR példáját követve a

---

103. *Id.* art. 5.

104. *Lásd általában* TONYA L. PUTNAM, COURTS WITHOUT BORDERS: LAW, POLITICS, AND U.S. EXTRATERRITORIALITY (2016) (megállapítva, hogy a második világháború utáni korszak nagy részében az USA szövetségi bíróságain keresztül gyakran szabályozta a területén kívüli tevékenységeket); KEVIN E. DAVIS, BETWEEN IMPUNITY AND IMPERIALISM: THE REGULATION OF TRANSNATIONAL BRIBERY 203-07 (2019) (annak leírása, hogy az Egyesült Államok külföldi korrupciós gyakorlatokról szóló törvénye (FCPA) hogyan feszíti ki a territorialitás elvét). *De lásd* William S. Dodge, *The New Presumption Against Extraterritoriality*, 133 HARV. L. REV. 1582, 1589-1604 (2020) (az extraterritorialitás elleni vélelem alakulásának leírása az amerikai jogban).

105. *Lásd általában* Benjamin H. Williams, *Az amerikai állampolgárok védelme Kínában: Extraterritorialitás*, 16 AM. J. INT'L L. 43 (1922) (a kínai szerződéses kikötőkben és a külföldi állampolgárokkal való bánásmódban az extraterritoriális jogérvényesítésből eredő kérdések leírása).

106. *Lásd* MARC LANTEIGNE, KÍNA KÜLPOLITIKÁJA: AN INTRODUCTION (3d191 ed. 2015) (megjegyezve Kína hagyományos antipátiáját a beavatkozással szemben Oroszország ukrajnai szerepvállalása kapcsán); COURTNEY J. FUNG, CHINA AND INTERVENTION AT THE UN SECURITY COUNCIL: RECONCILING STATUS 2, 6 (2019) (kiemelve Kína határozottan beavatkozásellenes álláspontját az ENSZ-ben). *De lásd: KÍNA ÚJ SZEREPE AZ AFRIKAI POLITIKÁBAN: A NEM-BEAVATKOZÁSTÓL A STABILIZÁCIÓIG?* 6-12 (Christof Hartmann & Nele Noesselt szerk., 2019) (dokumentálva Kína növekvő szerepvállalását az afrikai politikában).

107. *Lásd általában* Zhengxin Huo & Man Yip, *Extraterritoriality of Chinese Law: CHINESE J. COMPAR. L.* 1 (2021) (bemutatva, hogy Kína hogyan építi ki saját extraterritoriális rendszerét érdekei védelmére).

108. *Lásd a Kínai Népköztársaság adatbiztonsági törvényét, lásd a fenti lábjegyzetet* 99., 2.

A személyes adatok védelméről szóló törvényt úgy alakították ki, hogy az a személyes adatok ex-triterritoriális kezelésére is vonatkozzon, ha a cél a termékek vagy szolgáltatások nyújtása természetes személyeknek a KNK határain belül, vagy az ottani tevékenységük elemzése vagy értékelése során.<sup>109</sup> Ez a fajta extraterritorialitás végrehajtási kihívásokat jelent.<sup>110</sup> Míg Kína igyekezett végrehajtani néhány új extraterritoriális jogszabályát,<sup>111</sup> még nem tudni, hogy az új adatkezelési rendszerének extraterritoriális rendelkezéseit hogyan és miként fogja-e végrehajtani.

Kína adatkezelési rendszere az adatszuverenitás megteremtése érdekében az adatok lokalizálásának különböző formáit követeli meg. Konkrétan a jelenlegi kiberbiztonsági törvény előírja a "területi adatokat": A "kritikus információk üzemeltetőinek", például az internetszolgáltatóknak és a közösségi médiaplatformoknak a "személyes információkat" vagy "fontos adatokat" Kína területén belül kell tárolniuk.<sup>112</sup> A területi adatlokalizáció jelentős következményekkel jár a Kínában működő, határokon átnyúló üzleti tevékenységet folytató külföldi vállalkozások számára, mivel jelentős megfelelési költségekkel kell szembenézniük, ha Kínán belül kell elhelyezniük adattároló létesítményeiket, szervereiket és felhőalapú szervereiket, feltéve, hogy a "kritikus információszolgáltatók" széles körébe tartoznak.<sup>113</sup> A személyes adatok áramlásáról szóló rendelet értelmében továbbá a fontos adatoknak a kínai szárazföldön kívülre történő továbbítása csak akkor lehetséges, ha az üzleti követelmények miatt szükséges, és biztonsági értékelésnek van alávetve.<sup>114</sup> Az ezzel kapcsolatos időbeli késedelmek és költségek miatt a multinacionális

109. *Lásd a Kínai Népköztársaság személyes adatok védelméről szóló törvényét, supra note art100, 3.*

110. *Lásd Benjamin Greze, A GDPR területenkívüli végrehajtása: 9 INT'L DATA PRIV. L. 109, 110-11 (2019) (azzal érvelve, hogy a GDPR globális joghatósági igénye természeténél fogva nehezen érvényesíthető).*

111. *Lásd pl. , William Yang, Hong Kong: National Security Law Targets Overseas Activists, DEUTSCHE WELLE (2020. augusztus 18.), <https://perma.cc/34VX-3RWA> (beszámoló arról, hogy a hongkongi hatóságok hogyan próbálták letartóztatni az amerikai állampolgárokat Hongkongon kívül).*

112. *Cybersecurity Law, supra art93, 37.*

113. *Lásd Geren Xinxu Chujing Anquan Pinggu Banfa (Zhengqiu Yijian Gao) (个人信息出境安全评估办法 (征求意见稿)) [Measures for Security Assessment of Personal Information Crossing Borders] (bizottsági tervezet)] (kiadta a Kínai Kibertér Adminisztráció, 201913., június), cikk. 3[a továbbiakban Measures for Security Assessment], <https://perma.cc/92VS-QYPW>.*

114. *Xinxu Anquan Jishu - Ge Ren Xinxu Anquan Guifan (信息安全技术—个人信息安全规范) [Információbiztonsági technológia -*

tionálisok az adatok helyi tárolását és feldolgozását alapértelmezett megoldásként fogadták el.<sup>115</sup> A kínai területi adatlokalizációs követelmények pontos hatályát a kiberbiztonsági törvényben és a végrehajtási előírásokban rejülő kétértelműség miatt sok vita övezte.<sup>116</sup>

Kína adatlokalizációs követelményei nemcsak arra vonatkoznak, hogy hol tárolják és dolgozzák fel az adatokat, hanem arra is, hogy ki által. A felhőszolgáltatóknak nemcsak a vonatkozó fizikai infrastruktúrákat (pl. adatközpontokat) kell a kínai szárazföldön elhelyezniük, hanem az ilyen infrastruktúrák tulajdonjogát és ellenőrzését is kínai jogalanyoknak kell gyakorolniuk.<sup>117</sup> E követelmények pénzügyi és reputációs költségei ellenére egyes multinacionális vállalatok nem hajlandók lemondani a kínai piacról, még akkor sem, ha továbbra is fenntartásaik vannak az adatok lokalizációjával kapcsolatban.<sup>118</sup> A vállalatok szolgáltatói, köztük a külföldi ügyvédi irodák, akik hozzáférhetnek a

---

Personal Information Security Specification] (a Nat'l Info. Sec. Standardization Tech. Comm., 2019. dec. 29., hatályos: 2018. június 1.), art. 8(7), <https://perma.cc/HG7U-Q8P5>.

115. Vö. biztonsági értékelési intézkedések, 113. lábjegyzet (a külföldre irányuló adatexportra vonatkozó követelmények átfogó és pontatlan jellegének kifejtése).

116. *Lásd pl. az Egyesült Államok közleménye, Kína által elfogadott és kidolgozás alatt álló intézkedések a kiberbiztonsági törvényével kapcsolatban*, WTO Doc. S/C/ W/374 (2017. szeptember 25.), <https://perma.cc/4KE7-27FM> (megállapítva, hogy a kiberbiztonsági törvény adatlokalizációra vonatkozó rendelkezései "jelentős negatív hatással vannak a szolgáltatások kereskedelmére"). *De lásd Li Yi & 李毅 Wang Di 王迪, Shimao zuzhi beijing xia Zhongguo shuju bendihua cunchu yaoqiu de Pingxi [A Critique of China's data localization requirements under the WTO]*, 4 CHONGQING YUODIAN DAXUE XUEBAO (SHEHUI KUOXUEBAN) (重庆邮电大学学报(社会科学版)). [CHONGQING POST & TELECOMM. J. (SOC. SCI. EDITION)] 41-4234, (2019) (azzal érvelve, hogy Kína adatlokalizációs követelményei összhangban vannak WTO-kötelezettségvállalásaival).

117. Az adatközpont-szolgáltatásokhoz internetes adatközpont hozzáadott értékű távközlési szolgáltatási engedélyre (IDC VATS) van szükség, amely a külföldi vállalatok számára nem elérhető. *Kína: Mít jelent ez az Ön kínai vállalkozása számára?*, DLA PIPER: PRIVACY MATTERS (201628. december), <https://perma.cc/HWM4-HZGQ>.

118. USA-KÍNA BUSZ. COUNCIL, TECHNOLOGY SECURITY AND IT IN CHINA: BENCHMARKING AND BEST PRACTICES (2016), <https://perma.cc/L772-WSX8> (megállapítva, hogy a vállalati tagok 43%-a "nagyon aggódik" az információáramlással és a technológiai biztonsággal kapcsolatos kínai politikák miatt). Kivételesen a Google híresen elhagyta a kínai piacot. *Lásd Henry Gao, Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS*, ASIAN J. WTO & INT'L HEALTH L. & POL'Y (3492011) (megvizsgálja, hogy Kína cenzúra-követelései összhangban vannak-e a WTO-jog szerinti kötelezettségvállalásaival).

bizalmas információk, hasonló követelményekkel kell szembenézniük.<sup>119</sup> Ugyanez igaz a Kínában működő felhőszolgáltatókra is. Az Apple például arra kényszerült, hogy a kínai felhasználók iCloud-fiókjait egy kínai partnercégen, az AIPO Cloud (Guizhou) Technology Co. Ltd. (G CBD), hogy megfeleljen a kiberbiztonsági törvénynek.<sup>120</sup> Hasonlóképpen a világ vezető felhőszolgáltatója, az Amazon Web Services (AWS) is kénytelen volt megválni bizonyos fizikai infrastruktúrák kínai működtetésétől.<sup>121</sup> Ellentmondásos, hogy a felhőszolgáltatókra vonatkozó adatlokalizációs követelmény a felhőben tárolt titkosított adatok visszafejtésére szolgáló titkosítási kulcsokra is vonatkozik.<sup>122</sup>

Míg egyesek figyelmeztettek a kínai területi adatlokalizációs igények lehetséges tovaryűrűző hatásaira, például amikor az amerikai felhasználói fiókok véletlenül kínai szerverekre kerülnek, az <sup>123</sup>ilyen tovaryűrűző hatások vitathatatlanul nem törvény által előre meghatározottak. Más szóval, lehetséges, hogy a globális technológiai vállalatok csak a kínai szárazföldi Kínában felelnek meg a kínai adatkezelési rendszernek, míg máshol másként működnek. Ez azért kulcsfontosságú, mert korlátozza a kínai adatkezelési keretrendszer globális alkalmazását. A Zoom videokommunikációs vállalatot a koronavírus-járvány idején ért incidens tanulságos ebből a szempontból. A kínai hatóságok értesítették a Zoomot a Tiananmen téri tüntetések négy közelgő megemlékezéséről, és követelték a Tiananmen téri tüntetések megszüntetését.

---

119. Ezek a követelmények a kínai irodával rendelkező külföldi ügyvédi irodákra is vonatkoznak. Az amerikai ügyvédek az ügyvédi titoktartási kötelezettségükkel szemben a kínai bűnüldöző szervek részéről nyomást gyakorolhatnak rájuk, hogy átadják az ügyfelek adatait. Ez a megfigyelés Matthew Erie pekingi ügyvédi gyakorlatának tapasztalatain alapul.

120. *Learn More About iCloud in China Mainland*, APPLE (2020. május 26.), <https://perma.cc/DM7W-7KRH> (utolsó látogatás 202017., aug.).

121. Jon Russell, *AWS isn't exiting China, but Amazon did sell physical assets to comply with Chinese law*, TECHCRUNCH (Nov. 201714.), <https://perma.cc/37WU-LVZ7>.

122. Stephen Nellis & Cate Cadell, *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, REUTERS (201824., február), <https://perma.cc/64XC-MK7J>.

123. Lásd Aynne Kokas, *Cloud Control: (2019. 26,1júli.)*, <https://perma.cc/D4KG-GWDE> (az amerikai felhasználók adatainak kínai szerverekre történő migrációjának hatásairól); Aynne Kokas, *Platform Patrol: 2017 China, the United States, and the Global Battle for Data Security*, 77 J. ASIAN STUD. 923, 926 (2018) (az amerikai székhelyű Apple ID-k kínai szerverekre történő áthelyezéséről).

a találkozók és a fogadói számlák a kínai törvények betartatása érdekében. A Zoom igyekezett megállapítani, hogy a résztvevők fizikailag a kínai szárazföldön tartózkodtak-e, és így a Kínai Népköztársaság területi joghatósága alá tartoznak-e. Azokat a találkozókat, amelyek esetében a Zoomnak közvetett bizonyítékai voltak arra, hogy a felhasználók Kínában tartózkodtak, leállította, és az összes fogadói fiókot megszüntette. A cenzúra e cselekménye azonban területen kívüli hatásokkal járt, mivel több házigazda székhelye nem a kínai szárazföldön volt - egy Hongkongban és négy az Egyesült Államokban. A Zoom később bocsánatot kért, és ígéretet tett arra, hogy olyan technológiát fejleszt ki, amely lehetővé teszi az egyes felhasználók földrajzi elhelyezkedésén alapuló blokkolását, ahelyett, hogy az egész találkozó lezárásával területen kívüli tovagyrúzó hatásokat váltana ki.<sup>124</sup>

Ezek a küzdelmek tükrözik azokat a kompromisszumokat, amelyek akkor merülnek fel, amikor a kormányok megpróbálják gyakorolni az adatok feletti joghatósági ellenőrzést, miközben a határokon átnyúló adatáramlás kereskedelmi érdekeit is figyelembe veszik. Ez a kompromisszum az Európai Unióban is látható, ahol a GDPR korlátozza a személyes adatoknak az Európai Unióból harmadik országokba történő továbbítását, ami bonyolítja a transzatlanti adatkapcsolatokat.<sup>125</sup> Az Európai Unió harmadik országok adatvédelmi rendszereinek megfelelőségi értékelései arra ösztönzik a többi országot, hogy az adatvédelmi törvényeket a GDPR mintájára alkossák meg, és ezzel de facto növelik a GDPR joghatósági hatókörét.<sup>126</sup> Az Európai Unió nem egyedül használja ki a jogrendszerét arra, hogy a saját jogszabályaihoz való közeledésre ösztönözze. Az Egyesült Államok CLOUD-törvénye, amely a bűnüldözés érdekében az adatokhoz való transznacionális hozzáférést szabályozza, felhatalmazza az Egyesült Államokat arra, hogy csak olyan más országokkal kössön megállapodást, amelyek "a magánélet és a polgári szabadságjogok szilárd anyagi és ~~es~~ jogi védelmét" biztosítják, hasonlóan az Egyesült Államok által preferáltakhoz.<sup>127</sup> A törvényhozás története a

124. *Politikáink javítása a globális együttműködés további lehetővé tételével*, ZOOM (202011., jún.), <https://perma.cc/S63T-FHSD>.

125. GDPR, *fentebb* 51. lábjegyzet, cikk. 44. cikk; *lásd még*: C-311/18. sz. ügy, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (2020. július 16.) (a Privacy Shield érvényesítésében, amely lehetővé tette a határokon átnyúló adatáramlást az EU-ból az USA-ba).

126. Ilyen konvergencia hiányában a vállalatok az adatok lokalizációjához folyamodhatnak, hogy elkerüljék az EU által a személyes adatok határokon átnyúló továbbítására vonatkozóan előírt szigorú szabályokat. *Lásd általában* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, J23. INT'L ECON. L. (7712020) (azzal érvelve, hogy az adatlokalizáció csak bizonyos vállalatok számára megvalósítható, és végső soron nem kívánatos).

127. Amint azt a DOJ a CLOUD Act fehér könyvében kifejti, a releváns kritériumok közé tartoznak a számítógépes bűnözésre és az elektronikus bizonyítékokra vonatkozó megfelelő anyagi és eljárási jogszabályok, például a Budapesti Egyezményben felsoroltak; - a számítógépes bűnözésre és az

2021] *A PEKINGI HATÁS* 35  
elektronikus bizonyítékokra vonatkozó megfelelő anyagi és eljárási  
jogszabályok.

A CLOUD-törvény rámutat az amerikai vállalatok aggodalmaira az amerikai kormányzat extraterritoriális joghatóságának érvényesítése által a transznacionális üzleti kapcsolataikra gyakorolt hatásokkal kapcsolatban.<sup>128</sup> Úgy tűnik, hogy a CLOUD-törvény nem oszlatta el teljesen ezeket az aggodalmakat, mivel a vállalatoknak a GDPR alapján egymással versengő követelményekkel kell szembenézniük.<sup>129</sup>

A Kínai Népköztársaság adatkezelési rendszere nem rendelkezik hasonló eszközökkel más országok adatkezelési kereteinek jogi követelményekkel történő befolyásolására. Úgy tűnik azonban, hogy az adatáramlás feletti kormányzati ellenőrzés és a digitális technológiák gyors fejlődése és elterjedése összeegyeztetésére tett kísérlete vonzónak tűnik a feltörekvő gazdaságok egyes kormányai számára. Ez a vonzás a pekingi hatás fő mozgatórugója. Ezt egészíti ki a kínai nyomás egyes globális adatkezelési intézményeken keresztül, amelyekre most rátérünk.

### C. Kína fejlődő szerepe a globális adatkezelési intézményekben

A hazai adatkezelési kereteket nemzetközi megállapodások és intézmények is befolyásolják. Kína fokozatosan alkalmazkodott az internet-irányítás bonyolult intézményi környezetéhez, amelyet nagyrészt az amerikai érdekeltek hoztak létre és alakítottak, és amely emiatt történelmileg konprobbált.<sup>130</sup> Miközben Kína továbbra is részt vesz a létrehozott intézményekben, saját helyszínt hozott létre, hogy ad-

---

a jogállamiság és a megkülönböztetésmentesség elveinek tiszteletben tartása; az alkalmazandó nemzetközi emberi jogi kötelezettségek betartása; az elektronikus adatok gyűjtésére, megőrzésére, felhasználására és megosztására vonatkozó egyértelmű jogi felhatalmazások és eljárások; az elektronikus adatok gyűjtésével és felhasználásával kapcsolatos elszámoltathatóság és átláthatóság mechanizmusai; valamint az információ szabad áramlása és a globális internet iránti bizonyított elkötelezettség.

128. *In re. Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2nd Cir. 2016), *vacated and remanded sub nom. United States v. Microsoft Corp.*, S 138. Ct. (11862018).

129. *Lásd* EUR. DATA PROT. SUPERVISOR & EUR. DATA PROT. BD., INITIAL LEGAL ASSESSMENT OF THE IMPACT OF THE US CLOUD ACT ON THE EU LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA AND THE NEGOTIATIONS OF A EU-US AGREEMENT ON CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE. (201910., júli.), <https://perma.cc/TV3N-SQT2>.

130. *Lásd általában* ANDY RUSSELL, *Nyílt szabványok és a digitális korszak: HISTORY, IDEOLOGY, AND NETWORKS* (2014) (az internet irányítására gyakorolt amerikai befolyást tárgyalja); LAURA DENARDIS, *THE GLOBAL WAR FOR INTERNET GOVERNANCE* (2014) (megjegyzí Kína növekvő befolyását az internetpolitikában).

vance internet-politika. Kína következetesen megfogalmazta az internet globális irányítására vonatkozó olyan elképzelését, amely a kiber- és újabban az adatszuverenitás címszó alatt az adatáramlás feletti kormányzati ellenőrzést hangsúlyozza. Kína a BRI fogadó országaival tartott többoldalú fórumai is erősítik ezeket a megközelítéseket, különösen a fejlődő országokban. Ez a szelektív alkalmazkodásról a szelektív átformálás felé való fokozatos elmozdulást tükrözi, ahogy Kína egyre határozottabb és aktívabb szerepet kezd vállalni a globális gazdasági kormányzásban.<sup>131</sup> Bár Kína elvben elfogadta a nemzetközi gazdasági jog eszközeit (például a szabadkereskedelmi megállapodásokat és a kétoldalú beruházási szerződéseket), amelyek kereskedelmi és beruházási kapcsolatainak alapját képezik, többnyire tartózkodott attól, hogy kereskedelmi megállapodásokon keresztül fejlessze adat- kormányzási rendszerét.<sup>132</sup> Ez szöges ellentétben áll az Egyesült Államokkal és - kisebb mértékben - az Európai Unióval, amelyek a nemzetközi jog formális eszközeivel igyekeznek nemzetek feletti adatkezelési kereteiket transznacionálisan előmozdítani.

Az Obama-kormányzat alatt az Egyesült Államok a digitális gazdaságra vonatkozó szabályok új sablonját dolgozta ki, hangsúlyt fektetve azokra a rendelkezésekre, amelyek az információ szabad áramlását korlátozó vagy a hazai számítástechnikai eszközök használatát megkövetelő intézkedésekhez legitim közpolitikai célt követelnek meg. Az ilyen intézkedésekre a diszkriminációmentesség/kényszeresség, a kereskedelemkorlátozó jelleg és - ami a legfontosabb - a szükségesség hármasteszte vonatkozik. Annak ellenére, hogy az Egyesült Államok végül kilépett a Csendes-óceáni Partnerségből (TPP), a megmaradt tizenegy c s e n d e s - ó c e á n i ország, köztük Kína szomszédja, Vietnam, jóváhagyta ezeket a rendelkezéseket az újraélesztett TPP-ben (amely ma már a Csendes-óceáni Partnerség átfogó és progresszív megállapodásaként (CPTPP) ismert), ami korlátozza ezen államok lehetőségét, hogy kövessék Kína adatkezelési modelljét.<sup>133</sup> A CPTPP egyes tagjai is

---

131. Pitman B. Potter, *Globalizáció és gazdasági szabályozás Kínában*: WASH2. U. GLOBAL STUD. REV. 119, 120 (2003); Heng Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, J23. INT'L ECON. L. (2020)583,584

132. Lásd az alábbi megjegyzést 139.

133. Thomas Streinz, *Digitális megareguláció vitathatatlan? A TPP modellje a globális digitális gazdaság számára*, in MEGAREGULÁCIÓ VERSENYEZETT: GLOBAL ECONOMIC ORDERING AFTER TPP 312-42 (Benedict Kingsbury et al. szerk., 2019); lásd még: Átfogó és progresszív megállapodás a Csendes-óceáni Partnerségről.

BRI-országok.<sup>134</sup> A "megaregionális" megrendelés két különböző formájában vesznek részt.<sup>135</sup> Egyrészt a CPTPP-tagok számára lehetséges lehet, hogy a CPTPP keretében a határokon átnyúló adattovábbítás mellett és a területi adatlokalizáció ellen tett kötelezettségvállalásaikat összeegyeztetik a BRI keretében a Kínával fennálló gazdasági kapcsolataikkal, mivel ez utóbbi nem ír elő a fogadó országok egy adott adatkezelési modellt. Másrészt a pekingi hatásnak kedvező országok, amelyek a KNK adatszuverenitási megközelítését akarják utánozni, tartózkodni fognak a CPTPP-típusú kötelezettségvállalásoktól. Ez az egyik fő oka annak, hogy Kína CPTPP-hez való szeptemberi csatlakozási kérelme 2021 valószínűleg nem lesz sikeres. Ez azonban jól mutatja, hogy Kína az ázsiai-csendes-óceáni térségben a kereskedelempolitika pragmatikus megközelítését alkalmazza, amelyhez az amerikai kormánnyal és szövetségeseivel szembeni reálpolitikai elem párosul.

Az Európai Unió és az Egyesült Államok között is feszültségek vannak a nemzetközi gazdasági adatok irányítása terén. Mivel az Európai Unió attól tartott, hogy a kereskedelmi megállapodásokban a szabad adatáramlásra és az adatok lokalizálására vonatkozó követelmények ellen tett kötelezettségvállalásokat az adatvédelmi rendszerével szemben mozgósítanak, az Egyesült Államokkal folytatott, sikertelen kereskedelmi tárgyalásokon a transzatlanti kereskedelmi és beruházási partnerségről (TTIP) és a megrekedt szolgáltatáskereskedelmi megállapodásokról (TISA) folytatott tárgyalásokon ellenezte az ilyen megfogalmazásokat. Végül az Európai Unió új sablont dolgozott ki, hogy a szabad adatáramláshoz fűződő érdekeit összeegyeztethesse az adatvédelemmel és a magánélet védelmével kapcsolatos aggályaival. Ezek a szabályok csak de jure tiltják az adatok lokalizálását (nem pedig a határokon átnyúló adatáramlás korlátozását, mint a GDPR szerint), és csak a

---

(CPTPP) csatlakozási folyamat, CPTPP/COM/2019/D002 melléklet, <https://perma.cc/8TX7-UXDF> (utolsó látogatás 202017., aug.).

134. A CPTPP-t ratifikáló államok közül Új-Zéland, Szingapúr és Vietnam mind aláírták a BRI keretében kötött nemzetközi megállapodásokat. *Lásd Profiles*, BELT & ROAD PORTAL, [https://eng.yidaiyilu.gov.cn/info/iList.jsp?cat\\_id=10076](https://eng.yidaiyilu.gov.cn/info/iList.jsp?cat_id=10076) (utolsó látogatás 202017., aug.). Szingapúr emellett elektronikus származási adatszere-rendszert hozott létre Kínával. *Elektronikus származási adatszere-rendszer (EODES) Kínával*, SING. CUSTOMS, <https://perma.cc/Y7EU-7B89> (utolsó látogatás 2021. október1.).

135. *Lásd* Jing Tao, *TPP és Kína: A TPP: A Tale of Two Economic Orderings?*, in MEGAREGULÁCIÓ VERSENYEZETT: GLOBAL ECONOMIC ORDERING AFTER TPP 79-99 (Benedict Kingsbury et al. eds., 2019) (a "megaregionális ordering" vizsgálata).

az adatvédelem és a magánélet védelme az állami vitarendezési vagy beruházási választottbíróóságok által végzett vizsgálat alól.<sup>136</sup> A sablon célja, hogy az Európai Unió kereskedelmi partnereit arra kényszerítse, hogy aláírják az Európai Uniónak az adatvédelemről és a magánélet védelméről mint alapvető jogokról alkotott elképzelését.<sup>137</sup> Emellett az Európai Unió testvérszervezete, az Európa Tanács is hasonló, emberi jogi alapú adatvédelmi megközelítést hirdetett a "Személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény" révén, amelyhez nem európai országok is csatlakozhatnak.<sup>138</sup>

Ezzel szemben a közelmúltig Kína szabadkereskedelmi megállapodásai vagy egyáltalán nem foglalkoztak az adatkezelés kérdéseivel (mint a 2006-os Kína-Pakisztán szabadkereskedelmi megállapodás esetében), vagy nagyon gyenge és végül következmények nélküli megfogalmazást használtak (mint a Kína-Ausztrália 2012 szabadkereskedelmi megállapodás esetében).<sup>139</sup> 2020 novemberében azonban Kína aláírta a regionális és átfogó gazdasági partnerségi megállapodást (RCEP).<sup>140</sup> Az RCEP e-kereskedelmi fejezete a CPTPP-ét követi, de al-

136. Lásd Streinz, *Supra* note 133.

137. *A határokon átnyúló adatáramlásra és a személyes adatok védelmére vonatkozó horizontális rendelkezések az EU kereskedelmi és beruházási megállapodásaiban*, EUR. COMM'N, (2018. február), <https://perma.cc/A8ET-QM38>. Az EU-UK kereskedelmi és együttműködési megállapodásban az Egyesült Királyság csak azt volt hajlandó megerősíteni, hogy az egyéneknek "joguk van" az adatvédelemhez és a magánélet védelméhez. Kereskedelmi és együttműködési megállapodás, 2021 HL (L 149.) art. 202.

138. Egyezmény az egyéneknek a személyes adatok gépi feldolgozása során történő védelméről, 1981. január 28., E.T.S. 108. sz., Argentína, Burkina Faso, Cabo Verde, Mauritius, Mexikó, Marokkó, Szenegál, Tunézia, Uruguay és Uruguay csatlakozott az Európa Tanács 47 tagjaihoz, és ratifikálta az egyezményt. A 108. számú szerződés aláírásának és ratifikálásának táblázata, EURÓ TANÁCS, <https://perma.cc/LBY4-SF78>.

139. *Szabadkereskedelmi megállapodás Ausztrália kormánya és a Kínai Népköztársaság kormánya között*, 2015. június 17., [2015] ATS 15 (hatályba lépett 201520., december) art (12.8.1 "A felek területén a személyes adatok védelmére szolgáló meglévő rendszerek közötti különbségek ellenére mindkét fél meghozza az általa megfelelőnek és szükségesnek ítélt intézkedéseket az elektronikus kereskedelem felhasználói személyes adatainak védelme érdekében."); lásd még Gao, 85. lábjegyzet (megjegyezve, hogy Kína szabadkereskedelmi megállapodásai közül csak a Koreával és Ausztráliával kötött szabadkereskedelmi megállapodás tartalmaz önálló fejezeteket az e-kereskedelemtől).

140. Az RCEP-t a tíz ASEAN-tag és legfontosabb kereskedelmi partnereik, Kína, Japán, Dél-Korea, Ausztrália és Új-Zéland írták alá, miután India kilépett a tárgyalásokból. Lásd Pasha L. Hsieh, *Against Populist Isolationism: New Asian Regionalism and Global South Powers in International Economic Law*, CORNELL INT'L L.J. (6832018).

lehetővé teszi az országok számára, hogy saját maguk értékeljék, milyen adatátviteli korlátozásokra és adatlokalizációs követelményekre van szükség.<sup>141</sup> A Kereskedelmi Világszervezetben (WTO) Kína az elektronikus kereskedelem olyan felfogását terjesztette elő, amely hangsúlyozza a digitális technológiák szerepét az áruk és szolgáltatások kereskedelmének megkönnyítésében az Alibabához hasonló online platformokon keresztül. Miközben Kína elismeri az adatáramlás jelentőségét a kereskedelem és a fejlődés szempontjából, és részt vesz a WTO-nak az elektronikus kereskedelemre vonatkozó új plurilaterális szabályok létrehozására irányuló erőfeszítéseiben, fenntartja, hogy "az adatáramlásnak a biztonság előfeltételének kell lennie", ami Kína véleménye szerint megköveteli, hogy "az adatáramlás rendezett legyen, a [WTO] tagok vonatkozó törvényeinek és rendeleteinek megfelelően".<sup>142</sup>

Miközben a kereskedelmi tárgyalásokon védekező álláspontot képvisel, a Kínai Népköztársaság egyre aktívabban támogatja az adatkezeléssel kapcsolatos elképzeléseit a különböző internetirányítási intézményekben. Ezek közé tartoznak az olyan, korábban főként nyugati részvétellel működő szervezetek, mint az Internet Corporation for Assigned Names and Numbers (ICANN) és az Internet Engineering Task Force (IETF), valamint az ENSZ olyan szervezetei, mint a Nemzetközi Távközlési Unió (ITU).<sup>143</sup> Kína tagsága és növekvő részvétele az ilyen fórumokban része annak a szélesebb körű menetrendnek, amelynek célja, hogy normáit integrálja a globális kormányzás fő intézményeibe.<sup>144</sup> A Kínai Népköztársaság ad-

---

141. *Hasonlítsa össze az RCEP cikkeit és a* h12,14, <https://perma.cc/6TNG-W2YH> 12.14,12.15 megjegyzést a CPTPP cikkével. h14.11, <https://perma.cc/4MYN-AYSF>. *Lásd még* Thomas Streinz, *RCEP's Contribution to Global Data Governance*, *AFRONOMICSLAW* (2021)9., február), <https://perma.cc/2ZDN-BSVA>.

142. Közös nyilatkozat az elektronikus kereskedelemről: Kína közleménye, WTO Doc. INF/ECOM/19 § 4.3 (2019. április 24.); *lásd általában* Henry Gao, *Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China*, in *ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW* (Shin-yi295 Peng, Ching-Fu Lin & Thomas Streinz eds., 2021) (Kína kezdeti vonakodását vizsgálva az e-kereskedelmi tárgyalásokon való részvételt illetően).

143. *Lásd* Jonathan E. Hillman, "A 'Kína-modell'? Beijing's Promotion of Alternative Global Norms and Standards," *Testimony before the U.S.-China Economic and Security Review Commission* (2020)13., március), <https://perma.cc/QZL3-GJ8U> (azzal érvelve, hogy Kína az ITU-ban a kormányok szerepét erősítő szabványokat szorgalmazott).

144. *Lásd* Ann Kent, *China's Participation in International Organizations*, in *POWER AND RESPONSIBILITY IN CHINESE FOREIGN POLICY* 132, 133 (Yongjin Zhang & Greg Austin szerk., 2013) (megfigyelve Kína folyamatos részvételét a nemzetközi szervezetekben, beleértve néhányat 502000-ig); CONGYAN CAI, THE

a több érdekelt fél részvételével történő irányítással kapcsolatos helyzetét az idők során.<sup>145</sup> Ami azonban állandó maradt, az az, hogy Kína az internetpolitika meghatározásában az állam erős szerepét támogatja, hangsúlyozva a kiber- és most már az adatszuverenitást is.<sup>146</sup>

Kína a globális kormányzás terén is támogatta értékeit azáltal, hogy párhuzamos intézményeket hozott létre a főként az Egyesült Államok által létrehozott intézményekkel. Ezek közé tartozik a Sanghaji Együttműködési Szervezet,<sup>147</sup> az Ázsiai Infrastrukturális Beruházási Bank, a Selyemút Alap, valamint saját fejlesztési finanszírozási és tengerentúli segélyezési rendszere.<sup>148</sup> Az adatkezelés sem kivétel ebben a tekintetben. Miközben Kína különösen aktívan képviselte a kiber-szuverenitással kapcsolatos nézeteit az ENSZ rendszerében a Kormányzati Szakértők Csoportján (GGE) keresztül, az Egyesült Államok ellenállásába is ütközött. Ezért Kína Oroszországgal és más hasonlóan gondolkodó országokkal együtt 2018-ban megalapította a GGE alternatív platformját, a Nyílt Végű Munkacsoportot (OEWG).

---

KÍNA FELEMELKEDÉSE ÉS A NEMZETKÖZI JOG: A KÍNAI KIVÉTELESSÉG FELVÁLLALÁSA... RIOUSLY 162 (2017) (tipológia Kína nemzetek közötti szervezetekkel való kapcsolatáról); Kristine Lee, *It's Not Just the WHO: How China is Moving on the Whole U.N.*, POLITICO (2020. április 15.), <https://perma.cc/QU45-E48G> ("Peking szisztematikusan kínai állampolgárokat helyezett az ENSZ-ügynökségek széles körének élére.").

145. Lásd Gianluigi Negro, *A History of Chinese Global Internet Governance and its Relations with ITU and ICANN*, CHINESE 13 J. COMM. 104 (2020) (a többszereplős perspektívák növekvő támogatását, de az ITU folyamatos preferenciáját állapítja meg); lásd még Thomas Streinz, *Global Hybrid Internet Governance: The Internet Corporation for Assigned Names and Numbers (ICANN)*, in GLOBAL HYBRID AND PRIVATE GOVERNANCE (Benedict Kingsbury & Richard B. Stewart eds., megjelenés: 2022) (Kína ideiglenes távolmaradását az ICANN kormányzati tanácsadó bizottságától).

146. Lásd Milton Mueller, *Kína és a globális internetirányítás: A Tiger by the Tail*, in ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 177 (Ronald Deibert et al. eds., 2011) (leírja Kína erőfeszítéseit a hazai és a globális internetes működés közötti "Nagy Tűzfal" fenntartására).

147. DAVID SUTER, THE SHANGHAI COOPERATION ORGANISATION: A CHINESE PRACTICE OF INTERNATIONAL LAW 158 (2015) ("Még arra is van kényszerítő reason, hogy Kína ügynöksége *conditio sine qua non* volt a szervezethez vezető út és végső soron annak megalapítása szempontjából. Joggal mondhatjuk, hogy Kína megteremtheti vagy megtörheti az SCO-t").

148. Lásd Erie, *Supra* note 1, 74-76. o. (leírja, hogy Kína hogyan hozta létre saját politikai bankjait a BRI-ügyletek többségének finanszírozására).

Továbbá 2014 óta a CAC és Zhejiang tartomány népi kormánya közösen rendezi meg a "World Internet Conference" (*Shijie hulianwang dahui*), más néven a "Wuzhen Summit" elnevezésű konferenciát Wuzhenben, Zhejiang tartományban, amely az Alibaba szülőhelye.<sup>149</sup> A külföldi újságírók neveltségessé tették a wuzheni csúcstalálkozót, mivel a kínai hatóságoknak lazítaniuk kell a Nagy Tűzfalon, hogy a külföldi vendégek hozzáférhessenek a Kínában általában blokkolt weboldalakhoz, köztük a nagy hírügynökségekhez.<sup>150</sup> A hivatalos kínai információk alapján a Wuzhen Summit az évek során a 2014-es 100 résztvevőről 2019-re 1500-ra nőtt, köztük internet-szakértők, kormányzati tisztviselők és technológiai vállalkozók, fejlődő és fejlett országokból egyaránt.<sup>151</sup> Vitatott, hogy más internet-irányítási intézmények képviselőinek jelenléte milyen mértékben adhat legitimitást az eseménynek.<sup>152</sup> A wuzheni csúcstalálkozó Kína számára eszköz volt arra, hogy népszerűsítse az internettel kapcsolatos elképzeléseit, beleértve a kiber-szuverenitást is.<sup>153</sup> Kína diszkurzív puha hatalma nem csak az ilyen Kína-központú platformokon keresztül szűrődik ki, hanem más két- és többoldalú találkozókra is, beleértve a Kína-USA Internet Fórumot, a Kína-UK Internet Kerekasztalt, a Kína-ASEAN Információs Kikötő Fórumot, a Kína-Arabországek Online Selyemút Fórumot és a Kína-Szingapúr Internet Fórumot.<sup>154</sup> Ezek a fórumok együttesen elősegítik az adatkezelés szelektív átalakítását Kínában.<sup>155</sup>

149. *Wuzhen Summit*, WORLD INTERNET CONF., <https://perma.cc/65P9-NJQT> (utolsó látogatás 2020. aug.); *History and Milestones*, ALIBABA GRP., <https://perma.cc/N76Y-E35L> (utolsó látogatás 2021. aug.).

150. Yuan Yang, *Vegyes üzenetek a kínai technológiai csúcstalálkozón*, FIN. TIMES (2019. nov.), <https://perma.cc/WKA9-GLUQ>.

151. *Lásd a Wuzhen csúcstalálkozót, lásd a fenti lábjegyzetet.* 149.

152. *Lásd Milton Mueller, The Wuzhen Compradors*, INTERNET GOVERNANCE PROJECT (2015. dec.), <https://perma.cc/5QG2-YTY8> (az internetirányítási témákban Kínával való együttműködés mellett érvel, de a KKP által támogatott rendezvény támogatása ellen).

153. *Lásd pl. Zhou Lanxu & Wang Ying, Sovereignty in Cyberspace Paper Unveiled*, CHINA DAILY (2019. október 22.), <https://perma.cc/S85B-34A3> (a kiberfelségjogot úgy határozzák meg, mint "a nemzeti szuverenitáson alapuló igazságos és méltányos nemzetközi kibertér- rend elősegítése").

154. *Lásd a fenti megjegyzést.* 89.

155. *Lásd Sarah McKune & Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, INT'L J. COMM. 3835 (2018) (azzal érvelve, hogy Peking nemzetközi fórumokat használ fel az internetes szuverenitás modelljének előmozdítására, amely az "internetes szabadság" szöges ellentéte).

Kína diszkurzív átformálása további normatív formát ölthet, például a 2017-es "Kibertérrel kapcsolatos nemzetközi együttműködési stratégiában", amely a "szuverenitást" (*zhuquan*) a kiberügyek nemzetközi koordinációjának sarokköveként határozza meg.<sup>156</sup> Kína 2020 szeptemberében javaslatot tett egy globális adat- szuverenitási kezdeményezésre, amely az országok szuverenitásának, joghatóságának és adatkezelési jogainak tiszteletben tartását sürgeti.<sup>157</sup>

Összefoglalva, bár Kína tartózkodott attól, hogy a nemzeti jog segítségével más országokba exportálja a hazai adatkezelésre vonatkozó megközelítését, ellentétben az Egyesült Államokkal és kisebb mértékben az Európai Unióval, egyre határozottabb szerepet játszik a meglévő és az újonnan létrehozott globális adatkezelési intézményekben. Ezek az intézmények széleskörűen diszkurzívek lehetnek; azt mutatják, hogy Kína hogyan operacionalizálja a meglévő ~~intézmény~~ csatornákat, és néha sajátokat hoz létre, hogy a külföldi szereplőket a saját megközelítéséhez szocializálja. Továbbá, ezen intézmények némelyike döntő szerepet játszik a digitális infrastruktúra szabványainak meghatározásában, ami az egyik oka Kína növekvő jelentőségének az infrastrukturális adatkezelésben.

#### D. *Kína növekvő jelentősége az infrastrukturális adatkezelésben*

Az infrastrukturális adatkezelés rávilágít arra, hogy az adatáramlás szabályozása milyen mértékben függ a fizikai, digitális és platform-infrastruktúrától, amelyek a digitális főtevékenységet alakítják. Megjegyzendő, hogy minden digitális infrastruktúra nem digitális infrastruktúrára támaszkodik. Az adatokat nem egy efemer "felhőben", hanem adatközpontokban lévő merevlemezekben tárolják. Ahogy Tung-Hui Hu kifejti: "A digitális felhőt hely nélküli, néma, éteri és közvetíten felhőként képzelhetjük el. A felhő valósága azonban több ezer hatalmas adatközpontban testesül meg, amelyek bármelyike annyi áramot használhat, mint egy közepes méretű város".<sup>158</sup> Amikor az adatok "áramlanak" az interneten keresztül, a nullákból és egyesekből álló csomagokat réz- vagy üvegszál kábelén keresztül szállítják, vagy pedig

156. Wangluo kongjian guoji hezuo zhanlu'e (网络空间国际合作战略) [International Strategy of Cooperation on Cyberspace] (2017. március 7.), 2.2. fejezet, <https://perma.cc/JCZ3-R6WB>.

157. *Quanguo shuju anquan changyi* (全球数据安全倡议) [Globális ~~adatok~~ kezdeményezés], ZHONGHUA RENMIN GONGHEGUO WAJIAOBU (中华人民共和国外交部) [PRC MINISTRY OF FOREIGN AFFS.] (2020. szeptember 8.), <https://perma.cc/8SXX-9TWT>.

158. TUNG-HUI HU, A CLOUD ELŐTÖRTÉNETE (kivonat) (2015).

elektromágneses sugárzás útján továbbítják a helyi hálózatokat létrehozó routerek (pl. WiFi) vagy a mobiltelefon-hálózatokat létrehozó antennák.<sup>159</sup> Ezen anyagi összetevők és a kapcsolódó infrastruktúrák (pl. elektromosság) nélkül az adatokat nem lehet tárolni, feldolgozni vagy továbbítani. Ez alapvetőnek tűnhet, de az embrionális digitális infrastruktúrával rendelkező fejlődő országok számára alapvető fontosságú. Amint azt bemutatjuk, Kína növekvő befolyásának egyik központi oka a transznacionális adatkezelésben az, hogy a kínai technológiai vállalatok egyre nagyobb mértékben fejlesztik, szállítják és karbantartják azokat a fizikai elemeket, amelyekre a digitális infrastruktúrák épülnek.<sup>160</sup>

A fizikai összetevők mellett az adatátvitel szabványosított protokollokra támaszkodik. Az internetes hálózatépítést az internetes protokollcsomag teszi lehetővé, amely az alapvető TCP/IP protokoll körül forog. Még az olyan országok, mint például Kína, amelyek a határokon átnyúló adatforgalmat külön adatellenőrzési infrastruktúrákon keresztül korlátozzák, is ezekre a protokollokra támaszkodnak. Általában megfelelnek az ICANN által működtetett tartománynévrendszernek (DNS) is, amely biztosítja, hogy az internet minden egyes csomópontja egyértelműen azonosítható legyen egy számmal (az IP-címmel), amely egy ugyancsak egyértelműen azonosítható névvel (a domainnévvel) korrelál.<sup>161</sup> Más szóval, Kína adatkezelési infrastruktúrája kompatibilis az internet központi infrastruktúrájával.

Nincs szükség arra, hogy Kína vagy bármely más ország beavatkozzon az internet alapvető protokolljaiba, hogy a belföldi vagy transznacionális adatforgalom felett ellenőrzést gyakoroljon. Ez azonban nem jelenti azt, hogy az ilyen ellenőrzés gyakorlása egyszerű. A köznyelvben a kínai "Nagy Tűzfal" (GFW) néven ismert jelenség valójában egy összetett adatellenőrzési infrastruktúra, amely különböző jogi és technikai eszközöket kombinál a kívánt mértékű ellenőrzés érvényesítéséhez, amely még a KNK esetében sem abszolút.<sup>162</sup> A GFW ellenőrzi a globális internetről Kínába irányuló forgalmat.

---

159. James Grimmelmann, *INTERNETJOG*: (11. kiadás, 2021).

160. *Lásd az alábbi III. szakaszt.*

161. *Lásd Streinz, Supra note 145.*

162. *Lásd Richard Clayton, Steven J. Murdoch & Robert N.M. Watson, Ignoring the Great Firewall of China, in PRIVACY ENHANCING TECHNOLOGIES (2016), George Danezis & Philippe Golle szerk., 2006) (a "Nagy Tűzfal" mechanizmusának részletes bemutatása).*

és figyelemmel kíséri a kínai internetszolgáltatók közötti adatforgalmat.<sup>163</sup> Ahol a kínai hálózat összekapcsolódik más hálózatokkal, a GFW olyan szoftverekből áll, amelyek minden adatcsomagot kiszűrnek a tiltott tartalom szempontjából.<sup>164</sup> Belsőleg, amikor egy felhasználó megpróbál betölteni egy weboldalt, az internetszolgáltatója megpingeli a tiltott URL-ek listáját; amennyiben a felhasználó kérése nem tiltott, a kérést egy internet-hozzáférési ponthoz (IAP) továbbítják, amely a kínai szerverekre irányuló forgalmat kezeli.<sup>165</sup> Az IAP-okat a fizikai infrastruktúra korlátozza, ebben az esetben egy üvegszál hálózat, amely három olyan fojtóponttal rendelkezik, ahol az adatforgalom blokkolható.<sup>166</sup> Ezt az infrastruktúrát tekintik mintának más államok számára, amelyek osztják Peking kettős prioritását: a nemzeti biztonságot és a digitális kereskedelmet.<sup>167</sup>

A külföldi vállalatok termékeik szegmentálásával reagálnak a kínai adatáramlás-ellenőrzési infrastruktúrára. Alkalmanként a "geofencing" - az adatlokalizáció következménye - próbálkozásai kudarcot vallanak, és az adatok véletlenül átkerülnek a kínai szárazföldre, és ki vannak téve a kínai megfigyelésnek. Amikor 2020 tavaszán a koronavírus-járvány miatt a nyugati országok zárlat alá kerültek, és a videokonferencia iránti kereslet az egekbe szökött, a Zoom növelte felhőinfrastruktúráját, és tartalékként kínai adatközpontokkal bővítette. Ez azt eredményezte, hogy a Kínán kívüli felhasználókat érintő Zoom-értekezletek adatforgalmát a kínai szárazföldön keresztül irányították.<sup>168</sup> A megnövekedett sáv szélesség és a csökkentett késleltetés miatt a Hongkongon keresztül történő adatáramlással kapcsolatos aggodalmak arra késztették az amerikai kormányt, hogy kényszerítse a Google-t és a Facebookot, hogy hagyjanak fel a Hongkongnak a Pacific Light Cable Net-hez való csatlakoztatására vonatkozó terveikkel.

---

163. JAMES GRIFFITH, A NAGY TŰZFAL KÍNÁBAN: HOGYAN ÉPÍTSÜNK ÉS AZ INTERNET ALTERNATÍV JÖVŐKÉPÉNEK ELLENŐRZÉSE 23-33 (2019).

164. *Id.*

165. *Id.*

166. *Id.*

167. Lásd Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet*, DGAP ANALYSIS, Jan. 2020, 9. o., <https://perma.cc/52VH-G7WQ> (kiemelve, hogy Oroszország régóta partneri kapcsolatban áll Kínával az internet irányításával kapcsolatos kérdésekben).

168. Bill Marczak & John Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, CITIZEN LAB (Apr. 20203.), <https://perma.cc/5B2W-3KG6>. Eric S. Yuan, *Response to Research From University of Toronto's Citizen Lab*, ZOOM BLOG (Apr. 20203.), <https://perma.cc/U7Q5-7HNN>.

amely összeköti Los Angelesst a Fülöp-szigetekkel és Taiwanal.<sup>169</sup>

Az adatáramlás-szabályozási infrastruktúrákon túlmenően az új átviteli protokollok szabványosítása is nagy figyelmet kapott, és ennek következtében jelentős geopolitikai feszültségeket generált. Az ötödik generációs (5G) szabvány a mobilhálózatokon keresztüli adatátvitelre vitathatatlanul az első olyan alkalom az internet korszakában, amikor a kínai vállalatok műszaki és kereskedelmi szempontból is vezető szerepet töltenek be.<sup>170</sup> Ez a szakértelem és kereskedelmi hatalom természetesen jelentős és növekvő befolyást jelent a nemzetközi műszaki szabványalkotó testületben, ami globálisan erősítheti a szabványokat.<sup>171</sup> Míg korábban számos hivatalos szabványfejlesztő szervezetben nyugati állampolgárok töltötték be a vezető pozíciókat, a kínai cégek, különösen a Huawei, gyorsan felzárkóznak.<sup>172</sup> A kínai technológiai vállalatok növekvő tervezői ereje azonban a műszaki szabványok globális közösségének jóváhagyása nélkül is egyre jelentősebb. Ha a kínai technológiai vállalatok egy bizonyos szabványnak megfelelő berendezéseket gyártanak, és ezeket a berendezéseket más országokba exportálják, akkor a termékekbe beágyazott szabványok is exportra kerülnek. Ez az alapvető felismerés nem csak a mobilhálózatokra és azok műszaki szabványaira igaz; más digitális infrastruktúrákra is érvényes, például az összekapcsolt "intelligens" városokban alkalmazott megfigyelési technológiára.<sup>173</sup>

---

169. Lásd Todd Shields, *Google, Facebook Dump Plans for U.S.-Hong Kong Undersea Cable*, BLOOMBERG (Aug. 202028), <https://perma.cc/A4GW-87VZ> (kiemelve a Trump-kormányzat nemzetbiztonsági aggályait).

170. Lásd Paul Triolo et al., *Eurasia Group White Paper: The Geopolitics of 5G*, EURASIA GRP. (Nov. 201815.), <https://perma.cc/72BS-54W4> (Kína technológiai fejlesztéseinek leírása és az 5G terén betöltött vezető szerepének előrejelzése).

171. Lásd: Olia Kanevskaia, *Az IKT-szabványosítás irányítása*: N45.C. J. INT'L L. (5492020) (annak vizsgálata, hogy a szabványalkotó szervezetek figyelembe vehetik-e a kínai székhelyű vállalatok részvételéből eredő adatvédelmi és biztonsági aggályokat); Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards*, 22 BERKELEY TECH. L.J. 1403 (2007) (elemzi, hogy a szabványok hogyan szolgálhatnak a kereskedelem elősegítésére vagy akadályozására, kiemelve Kína azon kísérletét, hogy a WAPI-t a vezeték nélküli kommunikáció titkosítási szabványaként írja elő).

172. Justus Baron & Olia Kanevskaia, *Global Competition for Leadership Positions in Standards Development Organizations* (202129., április), <https://perma.cc/429N-849A>.

173. Lásd az alábbi IV.B. szakaszt.

Amikor az infrastruktúrák szabályoznak, az nem csak fizikai összetevőik vagy szabványaik és protokolljaik miatt történik.<sup>174</sup> Az infrastruktúrák többről szólnak, mint alkotóelemeik. A digitális infrastruktúrákat többnyire az emberek fejlesztik, építik, konfigurálják, karbantartják, megszakítják vagy akár el is pusztítják a megfelelő szervezeti környezetben, legyen szó akár kormányzati vagy kereskedelmi infrastruktúrákról. Más szóval, a politika nem választható el az infrastruktúrától. A digitális infrastruktúra fizikai összetevői feletti területi ellenőrzés önmagában nem elegendő a belföldi vagy határokon átnyúló adatáramlás ellenőrzéséhez. Az adatszuverenitásra törekvő kormányzatnak az ezeket az infrastrukturális funkciókat ellátó szervezetek feletti ellenőrzésre van szüksége. Ezért az a tény, hogy a digitális infrastruktúrát egyre inkább kínai technológiai vállalatok biztosítják, a KKP-vel való bonyolult kapcsolatuk miatt külön kihívást jelent.<sup>175</sup> Következésképpen a külföldi joghatóságok, különösen a fejlődő országok számára nehéz lehet hatékony joghatósági ellenőrzést gyakorolni a kínai technológiai vállalatok felett, legyenek azok állami tulajdonban vagy (hivatalosan) magántulajdonban.<sup>176</sup>

Az infrastrukturális jellemzőkkel rendelkező platformok a vállalatok által végzett globális adatkezelés fontos helyszínei.<sup>177</sup> A kínai vállalatok növekvő befolyása a Kínán kívüli távközlési és e-kereskedelmi platformok felett tehát a pekingi hatás egyik fő mozgatórugója. A platformok a beszéd cenzúrázására vagy az adatokhoz való hozzáférés biztosítására irányuló kormányzati igények célpontjai, de szabályozási körük túlmutat a nyilvános adatkezelésben betöltött közvetítői szerepükön. Különösen a közösségi médiaplatformok váltak világszerte a beszéd és az adatok új szabályozójává.<sup>178</sup> Jelentős szabadságot élveznek, a felhasználók szerződéses hozzájárulása alapján a

---

174. Lásd a 37-38. megjegyzéseket kísérő szöveget.

175. Lásd a 210-219. lábjegyzeteket.

176. Lásd a 203-205. megjegyzéseket kísérő *infra* szöveget.

177. Lásd Jean-Christophe Plantin et al., *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook*, *NEW MEDIA & SOC'Y* 1 (2016) (magyarázza el, hogy a platformok hogyan teszik lehetővé és korlátozzák az új digitális szolgáltatásokat, amelyek az infrastruktúra jellemzőit nyerik el).

178. Kate Klonick, *Az új kormányzók: The People, Rules, and Processes Governing Online Speech*, HARV131. L. REV. 1598,1603 (2017) (az "új kormányzókat" az állam és a beszélők-kiadók között ülésező új beszédtriász modell részeként azonosítja); Rebecca Hamilton, *Governing the Global Public Square*, HARV62. INT'L L.J. (117,2021119) (annak leírása, hogy a közösségi médiaplatform-vállalatok hogyan hozzák létre és ezáltal hogyan szabályozzák a globális nyilvánosságot).

szolgáltatási feltételek, amelyek mögött számos joghatóságban felelősségbiztosítás áll, és amelyeket csak tökéletlenül korlátoznak az adatvédelmi és magánélet védelmére vonatkozó jogszabályok annak eldöntésében, hogy milyen tartalmat engedélyezzenek és milyen adatokat gyűjtsenek. Az olyan amerikai platformok, mint a Facebook, az amerikai szólásszabadság értékeihez és a nemzetközi emberi jogi normákhoz igyekeztek igazodni a tartalommoderálási gyakorlatukban, és sok kritikát kaptak a félretájékoztatás és a káros, de nem illegális tartalmak kezelése miatt.<sup>179</sup> Az olyan kínai platformok, mint a TikTok, hasonló döntésekkel szembesülnek a világméretű működésük során.<sup>180</sup> A TikTok fenntartja, hogy amerikai platformján nem távolít el tartalmakat Kínával kapcsolatos érzékenység alapján,<sup>181</sup> de moderálási irányelvei úgy tűnik, hogy tiltják a "rendkívül ellentmondásos témákat, mint például a szeparatizmus, vallási szekták közötti konfliktusok, etnikai csoportok közötti konfliktusok, például az iszlám szekták közötti konfliktusok eltűlése", ami összhangban van a KNK Hszincsiangban élő ujjurok elleni kampányával.<sup>182</sup> Az infrastrukturális adatkezelést a hazai és a nemzetközi jognak való megfelelés alakítja, de a platformok által a jogi igények és az etikai, politikai vagy piaci nyomás hatására hozott döntések is meghatározzák.

Összefoglalva, Kína egyre nagyobb befolyással bír az infrastrukturális adatok irányításában, mivel a kínai technológiai vállalatok egyre nagyobb mértékben szállítják a digitális infrastruktúrák releváns fizikai összetevőit, meghatározzák a vonatkozó hazai és nemzetközi szabványokat, és Kínán kívül működtetik és ellenőrzik a digitális platform-infrastruktúrákat. Mindezek az elemek jelen vannak a DSR-ben, és hozzájárulnak a pekingi hatáshoz.

---

179. *Id.*; lásd még David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right of Freedom of Opinion and Expression*, A/HRC/38/35 (2018. április 6.) (az online véleménynyilvánítás szabadságának előmozdításáról és védelméről szóló különmegbízott jelentése, A/HRC/38/35 (2018. április 6.) (az online véleménynyilvánítás szabadságát és az ennek felelősségteljes megvalósításához szükséges eszközöket ajánlja).

180. Például a TikTok tartalommoderálási gyakorlatát kritika érte, amiért az új felhasználók bevonása érdekében elnyomja a "csúnya" és szegény emberek posztjait. Sam Biddle, Paul Victor Ribeiro & Tatiana Dias, *Láthatatlan cenzúra: TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users*, INTERCEPT (Mar. 202016.), <https://perma.cc/35KU-EW6P>.

181. *Nyilatkozat a TikTok tartalommoderációs és adatbiztonsági gyakorlatáról*, TIKTOK (201924., okt.), <https://perma.cc/UAX7-BNXT>.

182. Lily Kuo, *TikTok 'Makeup Tutorial' Goes Viral with Call to Action on China's Treatment of Uighurs*, GUARDIAN (Nov. 201927.), <https://perma.cc/9XVW-XGQR> (idézi a kiszivárgott moderációs irányelveket).

### III. KÍNA DIGITÁLIS SELYEMÚTJA

Amikor a legtöbb ember azt hallja, hogy "Övezet és Út Kezdeményezés" (BRI), autópályákra, gátakra és gazdasági folyosókra gondol. A Digitális Selyemút (DSR) a nagyobb BRI egy nagyrészt figyelmen kívül hagyott, de nem kevésbé szórakoztató része, amely még nagyobb jelentőségre tehet szert a Covid utáni jövőben. A DSR-t a kínai távközlési és e-kereskedelmi vállalatok globalizációja hajtja. A globalizációnak ez a formája Kínát egy új globális digitális gazdaság epicentrumaként képzelel el, és digitális infrastruktúrák kiépítésére törekszik a fejlődés érdekében. A DSR előmozdítja a nemzetgazdaságok közötti digitális összekapcsolhatóságot a transznacionális gazdasági kapcsolatok megkönnyítése érdekében. A kínai vállalatok digitális globalizációja erős támogatást kapott a központi kormánytól. A DSR illeszkedik az olyan kezdeményezésekhez, mint a "Made in China 2025" terv, amelynek célja, hogy Kína az "intelligens" gyártás révén feljebb lépjen a globális értékláncban, és amely 2020-ban 1,4 billió dollárral támogatott.<sup>183</sup>

A DSR a BRI alkotó része, és számos közös jellemzője van vele. A BRI retorikájához hasonlóan a DSR fogalmi és definíciói is változóban vannak. A politikai dokumentumok az évek során felváltva használták az "információs selyemutat" (*xinxi sichouzhilu*), az "online selyemutat" (*wangshang sichouzhilu* vagy *hulian hutong zhi sichou zhilou*) és a "digitális selyemutat", és a konszenzusos használat az utóbbit preferálta nagyjából 2017-től, az első pekingi BRI-fórum évétől. A DSR, a BRI-hez hasonlóan, a diskurzusgyártás pezsgését mutatja, amely gyakran elhomályosítja a tényleges operatív mechanizmusokat és a valóságot a helyszínen.<sup>184</sup>

A DSR-ről szóló hivatalos nyilatkozatok gyakran hivatkoznak az "összekapcsolhatóságra", amely talán az egyik meghatározó fogalom a globalizáció kínai felfogásában. Ennek a diskurzusnak az egyik hivatkozási pontja Xi Jinpingnek az első világkonferencián elhangzott beszéde.

---

183. Jost Wu'bbecke et al., *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*, MERICS (2016. dec.), <https://perma.cc/26K7-B6H4> (részletezve Kína erőfeszítéseit, hogy katalizálja csúcstechnológiai iparágait a külföldi függőség csökkentése érdekében); Joe Devanesan, *Inside China's New \$1.4 Trillion-Dollar Digital Transformation Master Plan*, TECHWIRE ASIA (2020. május), <https://perma.cc/EXC5-CR9X> (kifejtve, hogy a tőkeinjekció válasz volt arra, hogy az amerikai kormány blokkolja a kínai befektetéseket a technológiai szektorban).

184. Lásd az alábbi IV. szakaszt.

BRI Fórumon, amikor bemutatta a DSR-t. Xi felszólította a résztvevőket, hogy "folytassák az innovációvezérelt fejlődést és fokozzák az együttműködést az olyan határterületeken, mint a digitális gazdaság, a mesterséges intelligencia, a nanotechnológia és a kvantumszámítástechnika, és mozdítsák elő a nagy adatmennyiség, a felhőalapú számítástechnika és az intelligens városok fejlesztését, hogy a XXI. század digitális selyemútjává váljanak."<sup>185</sup> A beszédben gyakran szerepel az angolul "connectivity"-nek fordított kifejezés. Ez azonban az eredeti kínai fogalom leegyszerűsítése, amely többértékű. Az eredeti kínai például olyan kifejezéseket használ, mint "politikai kommunikáció" (*zhengce goutong*), "infrastrukturális összekapcsoltság" (*sheshi liantong*), "kereskedelem feloldása" (*maoyi chantong*), "pénzügyi forgalom" (*zijin rongtong*) és "népi érzelmek összekapcsolása" (*minxin xiangtong*).<sup>186</sup> Mindezeket akár a beszédek hivatalos angol nyelvű változataiban, akár a szakirodalomban "összekapcsolhatóság"-ként fordítják. A 2017-es beszéd ezen egyéb intézkedések mellett megemlíti továbbá a *hulian hutongot*, egy olyan kifejezést, amelyet "kibertér-összekapcsolhatóság"-ként fordítanak, de amely pontosabban "kibertér-összekapcsolhatóságot" jelent.<sup>187</sup> A kifejezések pontosabb helyesbítése feltárja, hogy Xi globalizációs diskurzusa az egymásra épülő egységek összeszerelését idézi fel, ahol a kibertér-interoperabilitás az összekapcsolhatóság mellett az integráció fő mecha- nizmusa a közös szabványok és a különböző rendszerek közötti adatmegosztásra szolgáló digitális infrastruktúrák alapján. Bár a DSR egyedi jellemzőkkel rendelkezik, nem összeegyeztethetetlen a meglévő digitális infrastruktúrákkal, és építhet rájuk.

A diskurzustól a működés felé haladva a DSR két kulcsfontosságú eleme, amely a pekingi hatást generálja, a digitális infrastruktúra fizikai elemeibe - például földi és tenger alatti kábelekre - történő beruházás, valamint a kínai technológiai vállalatok erős szerepe az infrastrukturális szolgáltatások nyújtójaként. A DSR ezen elemei - néhány kivételtől eltekintve, mint például az 5G-szabványok - nem feltétlenül jelentik azt, hogy Kína saját digitális ökoszisztémát hoz létre a fogadó államokban, mivel a legtöbb fogadó állam már rendelkezik nem kínai szolgáltatók által létrehozott digitális infrastruktúrával. Ehelyett a fogadó gazdaságok egy szedi-

---

185. Xi Jinping elnök, Work Together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road, Keynote Speech at the Opening Ceremony of the Belt and Road Forum for International Cooperation (2017. május), <https://perma.cc/3AH3-NLZX>.

186. *Id.*

187. *Id.*

a kínai és a nem kínai digitális infrastruktúrákat, bár az előbbiek bizonyos esetekben dominánsak lehetnek. A kínai cégek által biztosított digitális infrastruktúrák esetében a pekingi hatás előfeltétele a cégek és a kínai pártállam közötti kapcsolat jellege. Mint általában a BRI esetében, a nemzetközi jog értelmében nincs hivatalos szerződés, amely a partnerországokat a DSR iránti elkötelezettségükben kötelezné. Ehelyett a DSR nem kötelező erejű nem kötelező erejű jogi eszközök, például egyetértési megállapodások és politikai dokumentumok bonyolult szövevénye alapján működik. A következőkben sorra vesszük ezeket a jellemzőket.

A. *A DIGITÁLIS INFRASTRUKTÚRA FIZIKAI ÖSSZETEVŐINEK ELLÁTÁSA*

A DSR első fő eleme a digitális infrastruktúrákhoz szükséges fizikai komponensek szállítása. Ahogy a kínai Nemzeti Fejlesztési és Reformbizottság, a Külügyminisztérium és a Kereskedelmi Minisztérium 2015-ös fehér könyvében állítja: "[Kínának] közösen kell előmozdítania a határokon átnyúló optikai kábelek és más kommunikációs törzshálózatok kiépítését, javítania kell a nemzetközi kommunikációs összeköttetéseket, és létre kell hoznia egy információs selyemutat".<sup>188</sup> Az Államtanács ezt követő, 2016-os ötéves nemzeti gazdasági és társadalmi fejlődési terve egy egész szakaszt szentel a digitális infrastruktúráknak.<sup>189</sup> Célként fogalmazza meg a zökkenőmentes nemzetközi kommunikációs létesítmények létrehozását, a nemzetközi kommunikációs hálózatok elrendezésének optimalizálását és a határokon átnyúló szárazföldi és tengeri kábel-infrastruktúra javítását, megemlítve a kínai-arab "online selyemutat" a "Kína-ASEAN információs kikötő" mellett, amelyet nagy hévvel jelentettek be a bár2015, úgy tűnik, hogy nem haladt előre.<sup>190</sup> A

188. Keshav Kelkar, *A selyemszáltól a száloptikáig: The Rise of China's Digital Silk Road* OBSERVER RES. FOUND. ONLINE (2018., aug.), <https://perma.cc/NS85-HVJP>.

189. Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisan ge wunian guihua gangyao (中华人民共和国国民经济和社会发展第十三个五年规划纲要) [National Economic and Social Development Thirteenth Five-Year Plan Outline] (kiadta a KNK központi kormánya), 2017. március 17., 7. oldal, <https://perma.cc/US4X-WTCG>.

190. *China-ASEAN Information Harbor Forum (2015. szeptember 13-14.)*, CHINADAILY, <https://perma.cc/SUK4-EFZ6> (utolsó látogatás: 202017., aug.).

a DSR keretében megvalósuló egyes projektek egyenlőtlen végrehajtása nagyjából reprezentatív a BRI egészére nézve, tekintettel a projektek széleskörűségére és hatókörére, amelyek közül sok a kihívásokkal teli szabályozási környezetben és azokon belül helyezkedik el.

A DSR egyik jellemzője, hogy kínai technológiai vállalatok nem kínai partnerekkel konzorciumi projekteken vesznek részt, hogy tenger alatti kábeleken keresztül fizikai internetkapcsolati infrastruktúrát építsenek ki. Ilyen projektek többek között: Az Afrika Európa-1 (AAE-1) tenger alatti kábel a China Unicom részvételével; a Bengáli-öböl átjáró (BBG) és a Délkelet-Ázsia-Közel-Kelet-Nyugat-Európa tenger alatti kábel (SEA-ME-WE 5) a Bengáli-öbölön keresztül, mindkettő a China Mobile részvételével; és a tenger alatti Pakisztán-Kelet-Afrika kábel expressz, amelyet a Huawei Marine vásárol, és amelyhez a kínai Hengtong csoport szállítja az optikai kábelt és két földkábel, mindkettő a China Telecom részvételével: Az egyik Kína (Kashgar) és Afganisztán (Faizabad) között a Wakhan régióban, a másik Kína (Jilongzhen) és Nepál (Rasuwagadi) között Katmandun kívül.<sup>191</sup> A China Mobile a "2Afrika" projekt egyik szereplője, amely egy 37 000 kilométeres kábelt, a világ egyik legnagyobb tenger alatti kábelét foglalja magában, amely 2024-re készül el, és Afrikát, Európát és a Közel-Keletet köti össze.<sup>192</sup> Az Arctic Connect projekt Európa és Ázsia összekapcsolására törekedett egy új, részben a Huawei által épített, az északi tengeri útvonalon húzódó tenger alatti kommunikációs kábelen keresztül.<sup>193</sup> Míg az üvegszál kábelek továbbra is a világ legfontosabb fizikai infrastruktúrája a transznacionális adatforgalom számára,<sup>194</sup> Kína érdeklődést mutatott az internetkapcsolat világúron keresztüli biztosítása iránt is.

---

191. Lásd CAVE ET AL., *fenti* lábjegyzet15, (az ASPI adatbázisát 3tárgyalva, amely a kínai vállalatok által lefektetett tenger alatti kábeleket térképezi fel).

192. Alex Alley, *China Mobile and Facebook in Joint Project to Build 2Africa Submarine Cable*, DATA CTR. DYNAMICS (202018., május), <https://perma.cc/RZR5-NMMQ>.

193. Frank Juris, *Az infrastruktúra átadása Kína stratégiai céljai érdekében: SINOPSIS* (2020. július 7.), <https://perma.cc/PF7X-43FZ>. A projektet azóta felfüggesztették. Natalie Bannerman, *Arctic Connect Cable is Put on Ice*, CAPACITY MEDIA (20213., június), <https://perma.cc/C2KT-92V2>.

194. Lásd: *SUBMARINE CABLES: THE HANDBOOK OF LAW & POLICY* (3Douglas R. Burnett et al. szerk., 2014) (becslések szerint 2014-ben a nemzetközi kommunikáció mintegy 97%-a tenger alatti kábeleken keresztül zajlott).

alacsony pályán keringő műholdak.<sup>195</sup> Ezek a fejlemények összhangban vannak azzal az általános tendenciával, amely szerint az internet anyagi alpinfrastruktúrája feletti ellenőrzés az amerikai vállalatoktól a vállalatok szélesebb és földrajzilag változatosabb körére, köztük kínai cégekre száll át.<sup>196</sup>

A DSR részeként különböző kínai vállalatok adatközpontokat építenek a fogadó államokban. Az Alibaba Cloud 2017-ben a világ tizenhét régiójában, köztük Malajziában, Indonéziában és Szingapúrban "Flying Apsaras Data Centers" (*feitian shuju zhongxin*) néven felhőalapú számítástechnikai nagy adatközpontokat hozott létre, létrehozva Ázsia legnagyobb felhőalapú számítástechnikai platformját.<sup>197</sup> A China Telecom Global adatközpontokat épít a BRI-országokban, amelyekben nagy kapacitású szervereket és adattároló rendszereket helyeznek el a felhőalapú számítástechnikai szolgáltatásokhoz.<sup>198</sup> 2020 novemberében a Huawei bejelentette, hogy tervezi harmadik adatközpontjának megépítését Thaiföldön, hogy az országot az ASEAN digitális központjává tegye.<sup>199</sup>

A DSR tehát az adatok kezeléséhez, továbbításához és tárolásához szükséges fizikai komponensekből áll. Bár a költségversenyképesség csak az egyik, és nem feltétlenül a döntő tényező, amely a kínai technológia iránti keresletet megteremti, lehetővé teszi, hogy

---

195. Lásd AJEY LELE & KRITIKA ROY, INST. FOR DEF. STUD. & ANALYSIS, ANALYS-ING CHINA'S DIGITAL SPACE BELT AND ROAD INITIATIVE (2019), <https://perma.cc/Z7J8-JD6L> (kiemelve Kína 2018-as 320 műholdas konstellációjának indítását). A COVID-19 világjárvány a jelek szerint hatással volt a kínai műholdgyártási kapacitásra Wuhanban. Xinmei Shen, *Why the Coronavirus Slowed China's Plan to Take on Elon Musk's Internet Satellites*, ABACUS (2020. április 15.), <https://perma.cc/86SZ-8ME5>.

196. Lásd: Dwayne Winseck, *Internet Infrastructure and the Persistent Myth of U.S. Hegemony*, in INFORMATION, TECHNOLOGY AND CONTROL IN A CHANGING WORLD 93, 111-12 (Blayne Haggart et al. eds., 2019) (leírja, hogy az elmúlt két évtized során hogyan változott az anyagi internetes infrastruktúra feletti ellenőrzés; azt is megállapítja, hogy az amerikai internetes vállalatok gyakran "fontos, de alárendelt szereplők a konzorciumokban").

197. Zhongguo IDC Quan (中国IDC圈), *Shiqi daqushu shige feitian shuju zhongxin, Aliyun cheng Yazhou guimo zuida yun pingtai* (17个大区数十个飞天数据中心, 阿里云成亚洲规模最大云平台) [Több tucatnyi of Feitian Data Centers in 17 Regions, Alibaba Cloud Has Become the Largest Cloud Platform in Asia], IDC XINWEN (新闻) [IDC NEWS] (201716., június), <https://perma.cc/D7EG-ZJSS>.

198. Zen Soo, *China Telecom Global Sets Sights on Data Centres for Belt and Road Region*, S. CHINA MORNING POST (201725., ápr.), <https://perma.cc/BX99-3SNZ>.

199. Komsan Tortermvasana, *Huawei investing B700m in new data center in Thailand*, BANGKOK POST (202011., november), <https://perma.cc/E3S8-QE4>.

DSR fogadóállamok, hogy korlátozott erőforrásokkal elégtérjen ki az infrastrukturális igényeket.<sup>200</sup> Fontos azonban, hogy az optikai kábelek, adatközpontok és műholdak nem működhetnek önmagukban. Számos, kínai fejlesztési bankok által finanszírozott BRI-ügylet megköveteli, hogy kínai vállalkozók építsék és tartsák fenn a megfelelő infrastruktúrát, és ez alól a digitális infrastruktúrák sem képeznek kivételt.<sup>201</sup> Ily módon a kínai technológiai vállalatok fontos infrastruktúra-szolgáltatókká válnak.

B. *A kínai technológiai vállalatok mint infrastrukturális szereplők*

A kínai vállalatok központi szerepet játszanak a DSR-ben, nemcsak a hardver és a szoftver telepítésében, hanem karbantartásukban is.<sup>202</sup> A DSR bizonyos mértékig egyenértékű a kínai vállalatok globális terjeszkedési stratégiáival olyan ágazatokban, mint az e-kereskedelem, a távközlés, valamint a kutatás és fejlesztés (K+F). Fontos, hogy ezek a szolgáltatási ágazatok maguk is infrastrukturális jellegűek, mivel lehetővé teszik más vállalatok számára, mind a külföldiek, mind a hazaiak számára, hogy hasznot húzzanak az áruk és szolgáltatások e-kereskedelmi és mobilfizetési platformokon keresztül történő értékesítéséből, a helyi és határokon átnyúló ellátási láncok mentén történő kommunikáció megkönnyítésével, valamint az innováció és a növekedés környezetének megteremtésével. Az e digitális szolgáltatásokat nyújtó vállalatok közelebbi vizsgálata feltárja, hogy a pártállammal való kapcsolatuk hogyan teszi lehetővé a pekingi hatást.

A DSR-t mind a kínai állami vállalatok, mind a nagy multinacionális magánvállalatok építik.

---

200. A szélessávú infrastruktúra tekintetében a kínai cégek a svéd Ericsson és a finn Nokia versenyében állnak, amelyek szintén aktívak a feltörekvő piacokon, bár úgy tűnik, hogy mindkettő egyre inkább veszít a Huawei és a ZTE pozíciójából. Juan Pedro Tomá's, *Ericsson Targets Emerging Markets with New Suite of Solutions*, RCR WIRELESS NEWS (Sept. 201614,), <https://perma.cc/4ADY-RVQ3>; *Nokia Named Winning Emerging Market Player*, ARTHUR D. LITTLE, <https://perma.cc/WH2C-GDK2>.

201. *Lásd* Erie, *Supra* note 1, 87. o. (leírja, hogy a tipikus BRI-ügyletek hogyan használják a "kötött kölcsönöket" a kínai vállalatok hatékony előnyben részesítésére és a helyi közbeszerzési szabályok elkerülésére).

202. A hagyományos infrastruktúra fenntartása, bár háttérbe szorult az új építési projektek elindítására irányuló médiafigyelem mellett, újabban a tanulmányok tárgyává vált. *Lásd például* „Agnieszka Joniak-Lu”thi, *A Road, A Disappearing River and Fragile Connectivity in Sino-Inner Asian Borderlands*, 78 POL. GEOGRAPHY 102 (2020) (a Hszincsiangban található utak fenntartásának nehézségeit elemezve).

(MNC-k), amelyek különböző mértékben állnak ügynök-főnök viszonyban a pártállammal, és ez a szervezeti tény hatással van az adatkezelésre. Míg a BRI-t általában Kína nagy állami vállalatai vezették az építőipar, az olaj- és gázipar és az acélipar területén, addig a DSR-t nagyrészt a kínai "magán" technológiai vállalatok vezették, mint például az Alibaba Group Holding Limited ("Alibaba"), a Tencent Holding Limited ("Tencent"), a Huawei Technologies Company Limited ("Huawei"), a ZTE Corporation ("ZTE") és a J.D.com Incorporated ("Jingdong"). Kína távközlési állami vállalatai, a China Mobile, a China Unicom és a China Telecom szintén erős szerepet játszanak. A kínai állami vállalatok nemcsak kereskedelmi szereplők, hanem politikai szereplők is, amelyek a pártállam geopolitikai céljait szolgálják.<sup>203</sup> Az MNC-k és a pártállam közötti kapcsolat kevésbé egyértelmű, és az amerikai-kínai kereskedelmi konfliktus egyik legvitatottabb kérdésévé vált.<sup>204</sup>

A kínai vállalatok, legyenek állami vagy magántulajdonban, a kormányt, a KKP-t, a gazdaságot és esetenként a hadsereget összekötő ökoszisztéma részét képezik. Elemzők "államtőkeizmusnak" nevezik Kína megközelítését, ahogyan ezeket a szektorokat összeolvasztja.<sup>205</sup> Különböző érvek szólnak amellett, hogy a Kínai Népköztársaság

---

203. Li-Wen Lin & Curtis J. Milhaupt, *Mi vagyunk a (nemzeti) bajnokok: Understanding the Mechanisms of State Capitalism in China*, 65 STAN. L. REV. 697, 699-700 (2013); CHING KWAN LEE, THE SPECTER OF GLOBAL CHINA: POLITICS, LABOR, AND FOREIGN INVESTMENT IN AFRICA (332018) (megállapítva, hogy a központi állami vállalatokat nemcsak a profit motiválja, hanem a "nemzet stratégiai, létfontosságú, biztonsági érdekei" is).

204. *Lásd pl.* Press Release, U.S. Dep't of Justice, Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets (Feb. 13, 2020), <https://perma.cc/9BAN-DYAK> (részletezve, hogy a New York állambeli Brooklyn szövetségi bíróságán a Huawei-t a Racketeer Influenced and Corrupt Organizations Act megsértésével vádolják); Press Release, U.S. Dep't of Commerce, Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies (2020. május 15.), <https://perma.cc/F9NH-VEU6> (a Huawei azon képességének korlátozása, hogy amerikai technológiát és szoftvert használjon félvezetőinek külföldi tervezéséhez és gyártásához, mivel "a Huawei olyan tevékenységeket folytat, amelyek ellentétesek az Egyesült Államok nemzetbiztonsági vagy külpolitikai érdekeivel").

205. *Pl.* Lin & Milhaupt, *supra* note 203, 706-07; BARRY NAUGHTON & KELLE S. TSAI, STATE CAPITALISM, INSTITUTIONAL ADAPTATION, AND THE CHINESE MIRACLE (2015); BENJAMIN L. LIEBMAN & CURTIS J. MILHAUPT, REGULATING THE VISIBLE HAND? THE INSTITUTIONAL IMPLICATIONS OF CHINESE STATE CAPITALISM (2016). *Contra* BRANKO MILANOVIC, CAPITALISM, ALONE: THE FUTURE OF THE SYSTEM THAT RULES THE WORLD 87-96 (2019) (a világot uraló rendszer FUTURE-jának leírása).

Az államkapitalizmus problémás a feltörekvő gazdaságok és a liberális demokráciák szempontjából.<sup>206</sup> Nem feltételezzük a pártállam és az összes kínai technológiai vállalat közötti elválaszthatatlanságot, és elismerjük, hogy még az állami vállalatok és az állami szabályozó hatóságok között is vannak ügynöki problémák.<sup>207</sup> Az elmúlt években a pártállam mégis arra törekedett, hogy a kínai vállalatok érdekeit a saját érdekeihez igazítsa, amint <sup>208</sup>azt a technológiai vállalatok elleni közelmúltbeli kemény fellépés is mutatja.<sup>209</sup> Bár a kínai vállalatok nem eredendően a kínai állam eszközei, mégis beágyazódnak a pártállam ellenőrzési rendszerébe, amelynek különböző módszereit érdemes felülvizsgálni.

Az első a vállalatok tulajdonosi struktúrája. Sok vita folyt a kínai vállalatok tulajdonosi hátteréről, hogy a kínai állami érdekek hogyan befolyásolják vagy befolyásolják-e a vállalatok berendezéseinek tervezését és működtetését az állami irányítású hírszerzés és a titkos kiberműveletek megkönnyítése érdekében.<sup>210</sup> Az MNC-k, amelyek közül a Huawei és a ZTE a legjelentősebbek, névlegesen teljes egészében az alkalmazottaik tulajdonában vannak, de tulajdonosi struktúrájuk bonyolultabb, mint azt az önreprezentációjuk sugallná. A Huawei például egy holdingvállalat tulajdonában van, amely viszont körülbelül egy százalékban az alapító Ren Zhengfei, kilencvenkilenc százalékban pedig

---

Kína rendszere "politikai kapitalizmus", hatékony bürokráciával, a jogállamiság hiányával és az állam autonómiájával).

206. *Lásd pl.*, Mark Wu, *The "China, Inc." Challenge to Global Trade Governance*, 57 HARV. INT'L L.J. 261, 264 (2016) (elemezve, hogy Kína felemelkedése miért jelent kihívást a WTO többoldalú kereskedelmi rendszere számára).

207. *Lásd* Angela Huyue Zhang, *Közvetlen külföldi befektetések Kínából*: NW. J. INT'L L. & BUS. 395, 446-48 (2014) (azzal érvelve, hogy a kínai nemzeti olajtársaságok nem az állam "bábjai").

208. *Lásd általában* Tamar Groswald Ozery, *The Politicization of Corporate Governance-A Viable Alternative?*, AM. J. COMP. L. 14-15 (megjelenés előtt) (magyarázza a "vállalatirányítás politizálását" Kínában, amelynek során a vállalatirányítási funkciókkal rendelkező intézményeket a vállalatokon belül intézményesítették).

209. *Lásd* Charlie Campbell, *How China is Cracking Down on Its Once Untouchable Tech Titans*, TIME (2021. május), <https://time.com/6048539/china-tech-giants-regulations/> (kifejtve, hogy a korábban szabadabban működő technológiai cégeket ma egyre inkább szabályozói ellenőrzésnek vetik alá).

210. *Lásd pl.*, *Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE: Hearing before the U.S. H.R. Permanent Select Comm. on Intelligence*, 112th Cong. (2012) (a vállalat tulajdonlásának kérdését és annak az USA nemzetbiztonsági érdekeire gyakorolt hatását tárgyalja).

százalékban egy "szakszervezeti bizottság" tulajdonában van.<sup>211</sup> A szakszervezeti bizottság tagjai nem rendelkeznek a Huawei vagy annak holdingvállalatának részvényeivel, hanem egyfajta virtuális részvényekkel rendelkeznek egy szerződés révén, amely lehetővé teszi számukra, hogy részesedjenek a nyereségből.<sup>212</sup> Szerződéses jogként a virtuális részvények nem biztosítanak alapot a szavazati joghoz, és így a vállalat feletti ellenőrzéshez sem. A Huawei virtuális részvényei talán nem különböznek túlságosan a Szilícium-völgyi startupoknál megszokott tulajdonosi modellektől.<sup>213</sup> A különbség az, hogy Kínában a szakszervezetek a KKP ellenőrzése alatt működnek.<sup>214</sup>

A második érv az állami elfogásra vonatkozik.<sup>215</sup> A nemzetbiztonsági célú információgyűjtés különösen hangsúlyos ebben a vitában. A leggyakoribb példa, amelyet újrahasznosítanak

Az amerikai közbeszédben az a jogi követelmény, hogy a kínai vállalatok kérésre adatokat szolgáltatassanak a kínai kormányoknak. Ennek a követelménynek az alapja a 2018. évi nemzeti hírszerzési törvény és a 2014. évi kémelhárítási törvény.<sup>216</sup> Az állami foglyul ejtés azonban a jogi követelményeken kívül is működhet, olyan mechanizmusokon keresztül, amelyek közé tartoznak például a politikai kapcsolatokkal rendelkező vállalkozók, a kormányzati támogatások és a kereskedelmi kamarákon keresztül történő extralegális ellenőrzés.<sup>217</sup> Az előírt

211. Christopher Balding & Donald C. Clarke, *Kié a Huawei?*, 2 (2019), ápr.), <https://perma.cc/MRJ8-BWRL>.

212. *Id.* 5.

213. *Lásd pl.* „Alex Lazarow, *Beyond Silicon Valley*, HARV. BUS. REV. „Mar.-Apr. <https://perma.c2020,c/S358-KJVY> (a Fenix International példájának ismertetése, ahol a vezérigazgató "Fenix Flames" fantomrészvényeket hozott létre, amelyek a közvetlen részvénytulajdonláshoz hasonlítottak, hogy részvényjuttatásokat biztosítson az alkalmazottak számára).

214. *Lásd általában* CYNTHIA ESTLUND, A NEW DEAL FOR CHINA'S WORKERS? 190 (2017) (összehasonlítva az állam által a kínai szakszervezetek felett gyakorolt ellenőrzést a függetlenebb német rendszerrel).

215. *Lásd általában* Curtis J. Milhaupt & Wentong Zheng, *Beyond Ownership: Állami kapitalizmus és a kínai cég*, 103 GEO. L.J. 665 (2015) (a kínai cégek állami fogságra való fogékonyságának és lehetséges következményeinek tárgyalása).

216. Zhonghua Renmin Gongheguo Guojia Qingbaofa (中华人民共和国国家情报法) [A KNK nemzeti hírszerzési törvénye] (kihirdetve a Nat'l People's Cong. által, 2018.27. ápr. hatályos 2018.), art. 7 (előírja, hogy minden szervezetnek vagy állampolgárnak támogatnia kell a nemzeti hírszerzési munkát); Zhonghua Renmin Gongheguo Fanjiandiefu (中华人民共和国反间谍法) [Counterespionage Law of PRC] (kihirdette a Nat'l People's Cong., Nov. effective 1,2014, Nov. 2014.), art. 22 (amely előírja, hogy a szervezeteknek információt vagy bizonyítékot kell szolgáltatniuk a nemzetbiztonsági hatóságnak, ha erre felkérik őket).

217. Milhaupt & Zheng, *fenti* 215,683-86. o.

A Kínai Népköztársaság törvényeiben szerepel, hogy minden kínai vállalatnak - hazai és külföldi - pártcellával kell rendelkeznie.<sup>218</sup> A KKP különösen a technológiai cégekbe való beágyazódásra összpontosított. A Huawei például rendelkezik 300pártággal, az Alibaba kétszázal, a Tencent pedig nyolcvankilencvennel.<sup>219</sup> Emiatt lehetetlen elválasztani a kínai technológiai vállalatok működését a pártállami érdekektől.

A kínai technológiai vállalatok a DSR keretében szintén részt vesznek az intézményépítésben. Az Alibaba és a hangcsoui kormány közösen létrehozott egy elektronikus világkereskedelmi platformot (eWTP) Hangcsouban, 2017-ben pedig Malajzia és az Alibaba közösen elindította az első eWTP "kísérleti zónát", a Malajziai Digitális Szabadkereskedelmi Zónát Kínán kívül.<sup>220</sup> A két csomópont összekapcsolják, hogy elősegítsék az együttműködést a vámkezelés, az ellenőrzés és az engedélyezés terén, valamint az adatvezérelt kereskedelemkönnyítést és a szakpolitikai innovációt.<sup>221</sup> A WTO és a Világgazdasági Fórum (WEF) támogatta az eWTP-t, mint a gazdasági globalizációt elősegítő intézményi infrastruktúrájuk kiegészítését, és ez az egyik példa arra, hogy Kína nyitott a ~~menek~~ nemzetközi szervezetekkel való együttműködésre.<sup>222</sup> Hangzhou készpénzmentes társadalomra vonatkozó megközelítése alapján az Ant Financial, az Alibaba leányvállalata, amely a világ legnagyobb online fizetési platformját, az Alipayt üzemelteti, kiterjesztette az ilyen digitális pénzügyi tranzakciós infrastruktúrát Szingapúrra, Thaiföldre, a Fülöp-szigetekre, Vietnamra,

218. *Lásd* Zhonghua Renmin Gongheguo Gongsifa (中华人民共和国公司法) [Kínai Népköztársaság társasági törvénye] (kihirdetve a Nat'l People's Cong. által, 201826. októberi hatállyal26,2018.), art. 19 (előírja a vállalatok számára, hogy biztosítsák a "szükséges feltételeket" a pártszervezetek tevékenységének megkönnyítéséhez).

219. CAVE ET AL., *supra* note at 15,7.

220. *Alibaba eWTP shouge haiwai 3-hub zai Malaixiya zhengshi qudong* (阿里巴巴eWTP首个海外e-hub在马来西亚正式启动) [*Alibaba eWTP első eWTP-je Overseas E-Hub Officially Launched in Malaysia*], ALIBABA JITUAN (阿里巴巴集团) [ALIBABA GRP.], (Nov. 20173.), <https://perma.cc/VZ32-3T3L>.

221. *Alibaba datong zhongma "shuzi zhongshu" jiakuai tuijin eWTP* (阿里巴巴打通中马"数字中枢"加快推进eWTP) [*Az Alibaba megnyitja a Kína-Malaysia "Digital Hub" and Accelerates eWTP*], SOHU (2017. május 12.), <https://perma.cc/W5RD-DQ8H>.

222. *Lásd* Roberto Azevedo, a Kereskedelmi Világszervezet főigazgatója, Remarks at WTO-eWTP-WEF Enabling E-Commerce Launch Event (2017. december 11.), <https://perma.cc/64NL-ERVK> (az Alibaba alapítójával, Jack Ma-val való együttműködésről).

és legutóbb Malajziába. Malajziában két központi malajziai bank együttműködési megállapodás keretében elfogadta az Alipayt, így a malajziai kereskedők akár nyolcvan százaléka is használhatja a platformot.<sup>223</sup>

Eközben a kínai távközlési vállalatok a DSR révén kiterjesztették globális elérésüket. Kínában a távközlési ágazatot három állami vállalat irányítja: China Mobile, China Unicom és China Telecom. Ezek az állami vállalatok mindegyike globális jelenlétet alakított ki a BRI-pályáknak megfelelően azáltal, hogy a feltörekvő piacokra a hazai vállalatokban<sup>224</sup> való részesedés szerzés vagy konzorciumok létrehozása révén léptek be.<sup>225</sup> Ennek eredményeként a China Unicom International Ethernet Private Line ötven nagyobb országban és régióban érhető el.<sup>226</sup> A China Unicom egy összekapcsolt felhőplatformot is kiépített, amely lehetővé teszi a felhasználók számára, hogy bármelyik China Unicom felhőcsomópont segítségével hozzáférjenek a globálisan elosztott nyilvános felhőkhöz.<sup>227</sup> A China Unicom továbbá 112 országot és régiót lefedő nemzetközi 4G roaming-szolgáltatásokat nyitott, és tíz tengerentúli, teljes tulajdonú leányvállalatot, valamint huszonegy tengerentúli irodát hozott létre.<sup>228</sup> A China2017, Unicom létrehozta a

223. *Mayi jinfu qianzhou Malaixiya yinhang 8cheng shangdianhu dou neng shiyong Zhifubao* (蚂蚁金服牵手马来西亚银行 8成商户都能使用支付宝) [Ant Pénzügyi partnerségek a malajziai bankkal, a kereskedők 80%-a használhatja az Alipayt], JINRONGJIE WANGZHAN (金融界网站) [FIN. WORLD NET] (201723., március), <https://perma.cc/4BPJ-PT6R>.

224. *Lásd pl. , China Mobile Acquires Paktel*, DAWN (2007. május 19.), <https://perma.cc/S3NP-5RQT> (amely szerint a China Mobile 460 millió dollárért 88,86 százalékos részesedést szerzett a Paktel Ltd.-ben, Pakisztán első mobilszolgáltatójában); *lásd még Zhongguo yidong quanqiu buju? Bushi mai lege jingwai qiye, jiu jiao "quanqiu buju"* (中国移动全球布局? 不是买了个境外企业, 就叫"全球布局") [A China Mobile globális terjesztése? Instead of Buying an Overseas Company, it's Calved "Global Distribution"], SOHU (2017. április 28.), <https://perma.cc/8BV5-QQ34> (leírja, hogyan szerzett a China Mobile kisebbségi részesedést a thaiföldi True távközlési szolgáltatóban és az Axiata-ban, Malajzia legnagyobb vezeték nélküli szolgáltatójában).

225. *Lásd pl. , Ma Si, China Telecom Enters Philippine Market*, CHINA DAILY (2018. november 21.), <https://perma.cc/RWT2-XLFF> (leírja azt a módszert, amellyel a China Telecom konzorciumot kötött két helyi vállalattal a mobil távközlési szolgáltatások működtetésére a Fülöp-szigeteken).

226. *IEPL*, CHINA UNICOM, <https://www.chinaunicomglobal.com/au/iepl> (utolsó látogatás 202017., augusztus).

227. *China Unicom Global UniCloudWAN*, CHINA UNICOM, <https://www.chinaunicomglobal.com/us/UniCloudWAN> (utolsó látogatás 20203., október).

228. Wu Weiqun (吴卫群), *Zhongguo liantong jinnian ni touzi jingwai xi-angmu, "yidaiyilu" quyue zhan bida 82%* (中国联通今年拟投资的境外项目, "一带一路"区域占比达82%) [In the Over-tengerek Projektek, amelyekbe a China Unicom idén kíván befektetni, az "Övezet és út" kezdeményezés...]

a BRI mentén tizenegy országban, köztük Oroszországban, Indonéziában, Malajziában, Vietnamban, Thaiföldön, Mianmarban, Indiában, Kazahsztánban, az Egyesült Arab Emírségekben, a Fülöp-szigeteken és Dél-Afrikában.<sup>229</sup> Összességében a BRI-államokba történő befektetések a China Unicom külföldi befektetéseinek nyolcvankét százalékát tették ki a következő években 2017.<sup>230</sup>

Az olyan multinacionális vállalatok, mint a Huawei és a ZTE nagy támogatói a DSR-nek. Ezek a vállalatok a fő mozgatórugói a kínai megfigyelési technológia exportjának.<sup>231</sup> 2019-ben Kína hatvanhárom országba szállított megfigyelési technológiát, amelyek közül harminchat BRI-tagország.<sup>232</sup> A Huawei az ilyen technológia vezető szállítója a világon, és világszerte több mint ötven országnak szállít felügyeleti berendezéseket.<sup>233</sup> A ZTE ötvenhárom BRI-államban van jelen, vezeték nélküli hálózata negyven országot, vezetékes hálózata pedig ötvenkét országot fed le.<sup>234</sup> A ZTE három módon segítette a DSR kommunikációs hálózatának kiépítését: a határokon átnyúló hálózati összeköttetések kiépítésével, a nemzeti hálózatok felgyorsításával és a szolgáltatások átjárhatóságának elősegítésével.<sup>235</sup> A ZTE többféle módon éri el ezeket a célokat. Először is, a ZTE együttműködik a három távközlési állami vállalattal a határokon átnyúló átjárhatóság felgyorsítása érdekében.<sup>236</sup> Másodsor, a ZTE vezeték nélküli és vezetékes kommunikációs hálózatokat épített ki a BRI tagállamai, köztük Pakisztán, Indonézia, Vietnam, Thaiföld és Törökország számára.<sup>237</sup> Harmadszor, a ZTE segít adatközpontok és egyéb szolgáltatások kiépítésében a BRI-államok és az ott működő multinacionális vállalatok számára.

82%-os arányt képvisel], SHANGGUAN (上观) [SHANGHAI OBSERVER] (május 12, 2017), <https://perma.cc/L78Q-GP7S>.

229. *Id.*

230. *Id.*

231. Lásd általában Steven Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INT'L PEACE (16Sept. 2019), <https://perma.cc/222R-FHUX> (tisztázva, hogy az "AI surveillance" technológia exportja közös a liberális és az autoriter országokban).

232. *Id.* 1.

233. *Id.* 1,13.

234. *Zhongxing Tongxun Zhao Xianming: jianzhe "yidaiyilu" guojia xinxi gaosu gonglu* (中兴通讯赵先明: 建设“一带一路”国家信息高速公路) [ZTE Zhao Xianming: SINA (201722., május), <https://perma.cc/CU9H-MVZ3>.

235. *Id.*

236. *Id.*

237. *Id.*

tások. A ZTE például több mint 100 millió dollárt fektetett be a bangladesi nemzeti adatközpontba.<sup>238</sup> Ilyen módon a magánszektor kiegészíti az állam által irányított tevékenységet a DSR kiépítésében.

Az alapvető távközlési infrastruktúrákon kívül a kínai technológiai vállalatok egyre gyakrabban nyújtanak személyes távközlési szolgáltatásokat közösségi médiaplatformok formájában. Kínában a Tencent Weixinje lett a domináns közösségi hálózat, napi mintegy egymilliárd felhasználóval.<sup>239</sup> Kínán kívüli változatát, a WeChatet havonta mintegy 100-200 millió aktív felhasználó használja.<sup>240</sup> A kínai diaspora Délkelet-Ázsiában olyan helyeken segítette elő a hálózat használatát, mint Malajzia, ahol mintegy húszmillió felhasználó van, vagy Thaiföld, ahol a lakosság mintegy tizenhét százaléka használja az alkalmazást.<sup>241</sup> A TikTok Kínán kívül még szélesebb felhasználói bázist gyűjtött össze, mint a WeChat. A TikTok 2018 augusztusában egyesült az amerikai Musical.ly alkalmazással, és 2019-ben az amerikai Szövetségi Kereskedelmi Bizottság megbírságolta, mert jogellenesen gyűjtött adatokat tizenhárom év alatti felhasználókról.<sup>242</sup> Indonéziában a Tik Tokot ideiglenesen betiltották "pornográfia, nem megfelelő tartalom és istenkáromlás" megjelenítése miatt.<sup>243</sup> Nyugati társaikhoz hasonlóan a kínai közösségi médiaplatformok is egyre bonyolultabbá váló, kormányzati megrendelésű tartalommoderációval szembesülnek, ami megnehezíti törekvéseiket arra, hogy a kínai változat mellett, amelynek meg kell felelnie a Kínai Népköztársaság összetett cenzúra-rendszerének, Kínán kívül is globálisan egységes termékkel rendelkezzenek.

A kínai technológiai vállalatok nagymértékben fektetnek be a kutatás-fejlesztésbe, ami a digitális infrastruktúrák jövőbeli kialakítása és konfigurálása szempontjából is fontos lehet. Ilyen például a Huawei,

---

238. *Id.*

239. Mansoor Iqbal, *WeChat bevételi és használati statisztikák (2021)*, BUS. OF APPS (202121., június), <https://perma.cc/BQ6E-B9E3>.

240. CAVE ET AL., *supra* note at 15,14.

241. *Id.*

242. *Video Social Networking App Musical.ly megegyezik, hogy rendezi FTC állítások, hogy megsértette a gyermekek adatvédelmi törvény, FED. TRADE COMM'N* (Feb. 201927.), <https://perma.cc/6JNC-58DZ>.

243. *Indonesia Bans Chinese Video App Tik Tok for 'Inappropriate Content'*, REUTERS (20184., július), <https://perma.cc/KDH5-E7QW>.

évente értékesítési bevételeinek tíz százalékát fordítja K+F-re.<sup>244</sup> A BRI-országok alapvető fontosságúak voltak a Huawei növekedése szempontjából, ahol a vállalat alapító éveiben a piacainak mintegy hetven százaléka Kínán kívül, a szomszédos ázsiai országokban és Afrikában volt, a mai BRI-nek megfelelően.<sup>245</sup> A Huawei K+F beruházásai ezekben az országokban tükrözik a vállalat portfóliójában elfoglalt arányukat, mivel a Huawei a BRI-országok felé tekint saját szellemi tulajdonjogainak, márkájának és piaci csatornáinak megteremtése érdekében.<sup>246</sup> Összefoglalva, a pártállamot érdekelt félként megjelenítő vállalatirányítási struktúrájuknak köszönhetően a kínai technológiai és távközlési vállalatok vállalati szinten lehetővé teszik a pekingi hatást, amikor digitális infrastruktúrákat, intézményeket, platformokat és technológiákat szállítanak, amelyek a DSR-t alkotják a fogadó országokban.

### C. A DSR jogi és intézményi irányítási infrastruktúrája

Sok szó esett arról, hogy Kína megközelítése a transznacionális rendezéssel kapcsolatban különbözik-e az angol-amerikai demokratikus államokétól.<sup>247</sup> A DSR mint transznacionális adatkezelés szempontjából olyan jellemzőket látunk, amelyek megkülönböztetik a kínai kormányzati és vállalati szereplők stratégiáit amerikai társaikétól. Míg Kína a WTO-t a globális gazdasági rend alapvető infrastruktúrájaként értékeli, és a BRI-országokkal kötött további szabadkereskedelmi és kétoldalú beruházási megállapodásokra támaszkodik, addig a DSR számára nincs meg a megfelelő jogi infrastruktúra. Ennek oka az, hogy Kína nem kereskedelmi megállapodásokon keresztül népszerűsíti az adatkezelésre vonatkozó megközelítését, és tartózkodik attól, hogy aláírja az Európai Unió és az Egyesült Államok által alkalmazott modelleket.

---

244. "Yidaiyilu" yanxian diaoyan - Huawei zai e ershinian: Zhongguo qiye ruhe zhagen haiwai ( "Belt and Road" 沿线调研 | 华为在俄二十年: 中国企业如何扎根海外) ["Belt and Road" kutatás és fejlesztés: Huawei húsz éve Oroszországban: How do Chinese Companies Take Root Overseas], SOHU (Aug. 201830), <https://perma.cc/TL9Y-PMA9>.

245. Zhang Yansheng: Huawei you jintian quan kao "yidaiyilu" ( 张燕生: 华为有今天全靠"一带一路") [Zhang Yansheng: Huawei Today Entirely Depends on the "Belt and Road"], XINLANG CAIJING (新浪财经) [SINA FINANCE], (Nov. 201730), <https://perma.cc/EYB6-4535>.

246. *Id.*

247. *Lásd a fenti megjegyzést 1.*

támogatják.<sup>248</sup> A nemzetközi jog szerinti szerződések helyett a Kínai Népköztársaság nem kötelező erejű két- és többoldalú eszközöket hozott létre a saját maga és a DSR-nek otthont adó államok közötti nemzetközi koordináció érdekében. 2019-től Kína mintegy tizenhat országgal írt alá együttműködési megállapodásokat a DSR előmozdítása érdekében.<sup>249</sup> Ezért ahelyett, hogy a kereskedelmi és beruházási megállapodások megszokott formáinak kiépítésén keresztül működne, a pekingi hatás előnyben részesíti a puha jog különböző típusait, mind a kétoldalú, mind a többoldalú jogokat.

A DSR egyik programnyilatkozata a "Belt and Road Digital Economy International Cooperation Initiative" (*Yidaiyilu shuzi jingji guoji hezuo changyi*, a továbbiakban: "a Digi- tal Initiative"), amelyet Kína és hat másik BRI-ország indított el 2017 decemberében.<sup>250</sup> A Digitális Kezdeményezés öt- tizenöt általános elvből áll, amelyek célja "a politikai kommunikáció, az összekapcsolhatóság, a kereskedelem, a finanszírozás és a közhangulat erősítése".<sup>251</sup> Egyes elvek közvetlenül a digitális infrastruktúra fizikai összetevőire vonatkoznak, például "a szélessávú hozzáférés bővítésére és a szélessávú minőség javítására".<sup>252</sup> Mások a digitális gazdaság fejlesztésével foglalkoznak általánosságban ("a digitális átalakulás előmozdítása", "a kis-, közép- és mikrovállalkozások fejlődésének előmozdítása"), ágazati ("az e-kereskedelmi együttműködés előmozdítása", "az információs és kommunikációs technológia területén történő beruházások előmozdítása"), de társadalmi szinten is ("a digitális készségek képzésének erősítése", "a digitális integráció javítása", "a bizalom és a bizalom erősítése").<sup>253</sup>

248. *Lásd fentebb a II.C. szakaszt.*

249. Tuijin "yidaiyilu" jianshe gongzuo lingdao xiaozu bangongshi (推进"一带一路"建设工作领导小组办公室) [Vezető kisvállalkozói hivatal]. Group for Promoting the Construction of the "Belt and Road Initiative", *Gongjian "yidaiyilu" changyi: jinzhan, gongxian yu zhanwang* (共建"一带一路"倡议: 进展、贡献与展望) [Az "Övezet és Út Kezdeményezés" építése].

*tíve*": WANG (新华网) [XINHUANET] (Apr. 201922), <https://perma.cc/8VU6-HLZU>.

250. A többi ország Laosz, Szaúd-Arábia, Szerbia, Thaiföld, Törökország és az Egyesült Arab Emírségek. "Yidai yilu" shuzi jingji guoji hezuo changyi ("一带一路"数字经济国际合作倡议发布) [Az "Övezet és Út" Digi- és Közlekedési hálózat elindítása].

*tal Economy International Cooperation Initiative*], CYBERSPACE ADMIN. OF CHINA (201811., május), <https://perma.cc/M7KB-N744> [a továbbiakban *Digital Initia- tive*].

251. *Id.*

252. *Id.*

253. *Id.*

A tizenégyes elv kifejezetten említi a kiberszuverenitás "teljes körű tiszteletben tartását", amely a "békés, biztonságos, nyitott, együttműködő és rendezett kibertér" kiépítésére ösztönöz.<sup>254</sup> Az elv hallgatólagosan elismeri a fokozott digitális összeköttetés által elősegített "nyitottság" és az adatáramlás feletti kormányzati ellenőrzés közötti feszültséget. Ugyanez az elv "egy többoldalú, demokratikus és átlátható nemzetközi internetirányítási rendszer létrehozására" szólít fel, visszhangozva az Egyesült Államok által dominált, több érdekelt fél részvételével működő internetirányítási intézményekről - például az ICANN-ről - régóta folyó vitát, amellyel szemben Kína következetesen az internet feletti nagyobb kormányzati ellenőrzés mellett érvelt az ENSZ keretein belül, nem pedig azokon kívül.<sup>255</sup> Hasonlóképpen, a tizenharmadik alapelv - "az együttműködés ösztönzése és a független fejlődés tiszteletben tartása" - arra törekszik, hogy összehangolja a digitális szuperhatalommal való, rendkívül egyenlőtlen viszonyban való "együttműködés" elkerülhetetlen dinamikáját a DSR-nek otthont adó államoknak a digitális jövő felé vezető saját útjuk megtervezésében való érdekelttségével. Ez a nyelvezet jelentősen különbözik attól, ahogyan az Egyesült Államok és az Európai Unió a digitális fejlődésre vonatkozó sajátos modelljeiket népszerűsítik.<sup>256</sup>

A digitális kezdeményezés három alapelve kifejezetten kormányzati kérdésekkel foglalkozik. Először is, a dokumentum "átlátható digitális gazdaságpolitikák kidolgozására" ösztönöz.<sup>257</sup> Ha közelebbről megvizsgáljuk ezt az átláthatósági elvet, kiderül, hogy a követelt átláthatóság típusa kapcsolódik ahhoz az e-kormányzati stratégiához, amelyet Kína az elmúlt évtizedekben támogatott (és Szingapore tökéletesített), és amely a nyílt pályáztatásra és a pro-curementre összpontosít.<sup>258</sup> Az átláthatóságnak ebben a felfogásában a politikai beszéd cenzúrázása nem ellenkezik a kereskedelmi átláthatósággal. Másodszor, a digitális kezdeményezés a nemzetek közötti szabványok előmozdítására szólít fel. Azzal az általános feltételezéssel szemben, hogy a BRI megpróbálja kiszorítani a meglévő nemzetközi szervezeteket, a gyakorlatban a BRI, beleértve a DSR-t is, sok esetben a következő módon működik: "A BRI a nemzetközi szervezetek helyébe lép".

---

254. *Id.*

255. *Lásd fentebb a II.C. szakaszt.*

256. *Lásd fentebb a II.C. szakaszt.*

257. *Lásd a fenti megjegyzést 250.*

258. *Lásd általában Ian Holliday, Building E-Government in East and Southeast Asia: Regionális retorika és nemzeti (nem)cselekvés, 22 PUB. ADMIN. & DEV. 323 (2002) (az e-kormányzati gyakorlat és fejlődés leírása különböző kelet- és délkelet-ázsiai országokban, köztük Szingapúrban és Kínában).*

esetekben a nemzetközi együttműködés meglévő platformjain keresztül.<sup>259</sup> Ahol alkalmazható és hasznos volt, a kínai kormány arra törekedett, hogy a DSR-t beépítse a meglévő nemzetközi szabályozási keretekbe.<sup>260</sup> A 2017, Kínai Népköztársaság Ipari és Informatikai Minisztériuma (MIIT) például szándéknyilatkozatot írt alá az ITU-val az információs és kommunikációs technológiák (IKT) koordinálására a BRI keretében.<sup>261</sup> A Kínai 2019, Export-Import Bank az ITU-val egyetértési nyilatkozatot írt alá a BRI-n keresztül a fenntartható fejlődés menetrendjének 2030 előmozdításáról.<sup>262</sup> Mivel a legtöbb BRI-állam tagja a WTO-nak, a technológiai termékeknek és szolgáltatásoknak "összhangban kell lenniük a nemzetközi szabályokkal, beleértve a WTO szabályait és elveit".<sup>263</sup> Harmadszor, a Digitális Kezdeményezés többszintű kommunikációs mechanizmusok létrehozására ösztönöz a kormányok, a vállalkozások, a tudományos kutatóintézetek és az ipari szervezetek között. Az elv kifejezetten felszólít a "szakpolitika-formálás és a jogi tapasztalatok" cseréjére, valamint a "legjobb gyakorlatok megosztására" a BRI mentén fekvő országok között. Ezek a cserék hozzájárulhatnak a "pekingi hatáshoz".<sup>264</sup>

A digitális kezdeményezésen kívül, és a BRI csomóponti jellegét tükrözve, Kína a MIIT-en keresztül szándéknyilatkozatokat írt alá kambodzsai kormányzati ügynökségekkel is,

---

259. *Lásd a fenti szöveg kísérő megjegyzését 143.*

260. *Lásd pl. , Ershi guo jituan shuzi jingji fazhan yu hezuo changyi ( 二十国集团数字经济发展与合作倡议 ) [The G20 Digital Economy Development and Cooperation Initiative], CYBERSPACE ADMIN. OF CHINA (2016, szeptember), <https://perma.cc/2Z8F-2D3W> (amely azt állítja, hogy az internet irányításának továbbra is az információs társadalomról szóló világszúcstalálkozóval összhangban kell működnie, és továbbra is elkötelezettnek kell lennie az internet irányításának folyamatban lévő modelljei mellett). Kína vezető szerepéről a G20-ak nemzetközi beruházási sztemderdek kialakításában, lásd Karl P. Sauvant, *China Moves the G20 towards in International Investment Framework and Investment Facilitation, in CHINA'S INTERNATIONAL INVESTMENT STRATEGY: BILATERAL, REGIONAL, AND GLOBAL LAW AND POLICY 318-19311*, (Julien Chaisse szerk., 2019).*

261. GONG ET AL., *supra* note at 15,5.

262. Ministry of Foreign Affs. of China, *List of Deliverables of the Second Belt and Road Forum for International Cooperation*, Global Times (2019. április 27.), <https://perma.cc/4XPR-XNLA> [a továbbiakban: *List of Deliverables*]. *Lásd még: List of Deliverables of the Second Belt and Road Forum for International Cooperation, The Second Belt and Road Forum for International Cooperation (2019,27., ápr.)*, <https://perma.cc/26M3-ZFTN>.

263. *Digitális kezdeményezés, supra* note 250.

264. *Lásd fentebb a II.C. szakaszt.*

Irán, Banglades és Afganisztán.<sup>265</sup> Megállapodást írt alá továbbá a Kelet-afrikai Közösség öt tagállamával, Etiópiával és az ITU-val, hogy Kelet-Afrikában "információs autópályákat" építsenek, amelyek nem tévesztendőek össze az Al Gore által harminc évvel ezelőtt hirdettekkel.<sup>266</sup> Regionális szinten cselekvési tervet adott ki az ASEAN-nal való partnerségre az IKT-k fejlesztése érdekében.<sup>267</sup> Hasonlóképpen, a kínai multinacionális vállalatok is kötöttek nem kötelező erejű megállapodásokat külföldi kormányokkal a DSR támogatására. A legtöbb fent tárgyalt kezdeményezés, nevezetesen az adatközpontok és a felhőhálózatok, ilyen megállapodások eredménye. Az Alibaba például 2018 áprilisában szándéknyilatkozatot írt alá a thaiföldi kormánnyal egy AI-adatközpont létrehozásáról a keleti gazdasági folyosón, hogy segítse az ott található kkv-k digitalizációját és fokozza az e-kereskedelmet.<sup>268</sup>

Mindezek a megállapodások általános keretet biztosítanak a DSR mentén történő koordinációhoz anélkül, hogy az adatkezelés bizonyos megközelítését előírják. A fentiek szerint azonban a BRI- vagy DSR-államok lemásolhatják Kína adatkezelésre vonatkozó megközelítésének bizonyos elemeit, mivel az megfelel a politikai preferenciáiknak. Például a Kína és Magyarország közötti szándéknyilatkozat egyidejűleg jött létre a magyarországi Digitális Kormányzati Ügynökséggel, amely az informatikai beszerzésekért felelős és a Fidesz, a kormánypárt ellenőrzése alatt áll.<sup>269</sup> Bár látszólag a DSR a kínai állami vállalatokon és magánvállalatokon keresztül biztosítja a transznacionális összeköttetést, a DSR belföldi adatbezáráshoz vezethet, ha a fogadó államok úgy döntenek, hogy utánozzák Kína belföldi adatkezelési rendszerét, és a kínaihoz hasonló adatellenőrzési infrastruktúrákat hoznak létre. Ily módon a kínai pártállam befolyásolhatja mind a jogi, mind az infrastrukturális adatkezelést a BRI-államokban.

---

265. GONG ET AL., *supra* note at 15,5.

266. *Id.*

267. *Id.*

268. *Id.*

269. Kétoldalú cselekvési terv a digitális selyemútról szóló együttműködésről, amelyet 27,2019.a kínai Nemzeti Fejlesztési és Reformbizottság és a magyar Innovációs és Technológiai Minisztérium írt alá a pekingi második Övezet és Út Nemzetközi Együttműködési Fórumon, áprilisban. A Digitális Kezdeményezés "átláthatósági elvével" ellentétben ezt a dokumentumot nem hozták nyilvánosságra.

## IV. DIGITÁLIS SELYEMÚT ESETTANULMÁNY: PAKISZTÁN

Ebben a szakaszban Pakisztánra összpontosítunk, hogy bemutassuk a DSR által kiváltott pekingi hatás példáját egy fejlődő országban. Pakisztánra azért esett a választásunk, mert Pakisztán közel áll Kínához.<sup>270</sup> Míg a kínai-pakisztáni kapcsolat nem feltétlenül reprezentálja Kína más alacsony és alacsony közepes jövedelmű gazdaságokkal való kapcsolatát, egy készséges partnerrel megmutatja a lehetőségeket, amelyek más államokban is megismételhetők. A Kína-Pakisztán gazdasági folyosó (CPEC) kiemelkedő szerepet kapott a BRI-ben, és Pakisztán fedezeti stratégiája sok olyan fejlődő gazdaságra jellemző, amelyek kereskedelmi és politikai szempontból mind Kína, mind az Egyesült Államok és szövetségesei felé helyezkednek el.<sup>271</sup> A "Kína-Pakisztán gazdasági folyosó hosszú távú terve (2017- 2030)" (a továbbiakban: "hosszú távú terv") a CPEC-et a Kínát és Pakisztánt összekötő "növekedési tengelyként és fejlesztési övként" határozza meg, amely "átfogó közlekedési folyosót és ipari együttműködést ... konkrét gazdasági és kereskedelmi együttműködéssel, valamint az emberek közötti cserét és kulturális kommunikációt" foglal magában, amelynek célja "az infrastruktúra építésére, az iparfejlesztésre és a megélhetés javítására irányuló nagy együttműködési projektek".<sup>272</sup> A DSR szintén a CPEC alapvető részét képezi; a hosszú távú terv meghatározza az "információs hálót".

---

270. Lásd GHULAM ALI, KÍNA-PAKISZTÁN KAPCSOLATOK: A HISTORICAL ANALYSIS ch. 4 (2017) (a kínai-pakisztáni kapcsolatok jelentőségének bemutatása a hidegháború óta); ANDREW SMALL, THE CHINA-PAKISTAN AXIS: ASIA'S NEW GEOPOLITICS (2015) ("Pakistan is a central part of China's transition from a regional power to a global power.").

271. Lásd Trang (Mae) Nguyen, *Nemzetközi jog mint fedezeti ügylet*: AM144. J. INT'L L. UNBOUND 237-38237, (2020) (kifejtve, hogy a kis államok hogyan használják a nemzetközi jogot a nagyhatalmak "fedezésére").

272. PAKISZTÁN KORMÁNYA, TERVEZÉSI, FEJLESZTÉSI ÉS REFORMMINISZTERIUM ÉS A KÍNAI PAKUSZTÁN KÖZTÁRSASÁG, NEMZETI FEJLESZTÉSI ÉS REFORMKÖZMŰVELŐI BIZOTTSÁG, HOSSZÚ TÁVÚ TERV A KÍNA-PAKISZTÁN GAZDASÁGI KAPCSOLATRA (2017-2030) (42017), <https://perma.cc/8YEX-B9LU> [a továbbiakban HOSSZÚ TÁVÚ TERV]. E dokumentummal kapcsolatban némi vita van. Az újságírók egy sokkal hosszabb "hosszú távú terv" (2015. decemberi keltezésű) másolatát kapták meg, de a tisztviselők 2017 februárjában egy rövidebb változatot hoztak nyilvánosságra. Vita folyik arról, hogy ezek ugyanannak a dokumentumnak a különböző tervezetei-e, vagy különböző dokumentumok, az egyik "belső", a másik pedig a nyilvánosság számára készült szánált változat. A hosszabb változat értékelését lásd Khurram Husain, *Exclusive: CPEC Master Plan Revealed*, DAWN (2017.21. jún.), <https://perma.cc/T4BS-WQJ2>.

munkainfrastruktúra", mint az együttműködés egyik kulcsfontosságú területe.<sup>273</sup> A következőkben a DSR Pakisztánra gyakorolt hatását elemezzük a digitális összekapcsolhatóság, a biztonságos városok felügyeleti infrastruktúrája és a fejlődő hazai adatkezelési rendszer tekintetében.

#### A. *Digitális összeköttetés Pakisztánban és azon túl*

Míg a pakisztáni, kínai és máshol a sajtó nagy része a CPEC nagy energiaprojektjeire és tömegközlekedési rendszereire összpontosított, a CPEC az adatáramlás elsőbbségét is mutatja Kína határokon átnyúló fejlesztésében. A hosszú távú terv az információs hálózati infrastruktúrával kapcsolatban a következő konkrét elemeket határozza meg:

- A Kína és Pakisztán közötti határokon átnyúló optikai szálak kábelek építésének és a pakisztáni optikai szálak gerinchálózat kiépítésének előmozdítása.
- Pakisztán hálózati létesítményeinek korszerűsítése, beleértve a nemzeti adatközpontot és a második tengeralatti kábel leszállóállomást.
- A kínai digitális földfelszíni multimédiás műsorszórási szabvány (DTMB) pakisztáni átvételének felgyorsítása.
- Pakisztán IKT-alapú fejlesztésének előmozdítása, beleértve az e-kormányzatot, az elektronikus határellenőrzést és a biztonságos városépítést; az e-kereskedelem fejlesztésének előmozdítása Pakisztánban.
- Az információs ipar fejlesztésének fokozása Pakisztánban; IT ipari parkok és IT ipari klaszterek létrehozása Pakisztánban a pakisztáni információs technológia és szolgáltatások beszerzésének javítása érdekében.
- A pakisztáni személyzet számának növelése a kínai csereprogramokban, technikai képzési központok létrehozása Pakisztánban, és az IKT humánerőforrás kiépítésének megerősítése Pakisztánban.<sup>274</sup>

Ezek a célok nagyjából tükrözik Kína fentebb vázolt, a transznacionális adatkezelésre vonatkozó megközelítésének mintáit, beleértve az olyan digitális infrastruktúrákat, mint az optikai kábelek és a

273. HOSSZÚ TÁVÚ TERV, lásd a271, fenti megjegyzést. 15.

274. *Id.*

adatközpontok, technikai szabványok meghatározása, valamint a Kínához kapcsolódó külföldi digitális gazdaságok növekedésének előmozdítása.<sup>275</sup> Pakisztán és a tágabb dél-ázsiai régió, beleértve Indiát is, csábító piac a kínai technológiai vállalatok számára. Pakisztán lakossága 212 millió fő, többségében fiatal és gyorsan urbanizálódó. Egy jelentés szerint Pakisztán egyike annak az öt országnak, amely a milliárdnyi 1.6ú mobilinternet-felhasználó növekedésének ötven százalékát fogja kitenni az év végéig.<sup>276</sup> Ugyanakkor a Huawei globális csatlakozási indexe Pakisztánt a világ hetvenkilenc országából hetvenhétre rangsorolta az IKT tekintetében.<sup>277</sup> A pakisztáni növekedési potenciált és a meglévő gyenge digitális infrastruktúrát összevetve a kínai technológiai vállalatok különösen szívesen vetik meg a lábukat az országban, és az e-kereskedelem pakisztáni támogatói általában támogatják.<sup>278</sup>

Jelentős lépések történtek Kína és Pakisztán digitális infrastruktúráján keresztül történő összekapcsolása érdekében.<sup>279</sup> 2018-ban véglegesítették a Pakisztán-Kína optikai száloptikai projektet, amely Pakisztánt és Indiát egy új földi száloptikai kábelrel keresztül köti össze a kínai-pakisztáni határon lévő Khunjerab-hágó és Rawalpindi városa között.<sup>280</sup> A kábel összeköti Pakisztánt az Európa és Ázsia földkábeles tranzithálózzal, csökkentve ezzel Pakisztán tenger alatti kábelektől való függőségét a transznacionális összeköttetés terén. Ezen túlmenően az új pakisztáni Kelet-Afrika Kábel Expressz (PEACE), egy tenger alatti kábelrendszer építése, amely állítólag a legközvetlenebb útvonalat jelenti a nagysebességű internet számára.

275. *Lásd fentebb a II.*

276. BYTES FOR ALL, PAKISTAN'S INTERNET LANDSCAPE at2018, (112018), <https://perma.cc/8VXC-EHEB> (idézi a GSMA Intelligence jelentését).

277. *Id.*

278. *Id.* at (79idézi Syed Salman Hassan, a TCS Ecom vezérigazgatójának szavait: "A pakisztáni fogyasztókban rejlő potenciál - több mint 200 millió ember, akiknek 65 százaléka 30 év alatti - végre felismerhető. Azzal, hogy az Alibaba belépett a helyi piacra, a helyzet innentől kezdve még jobb lesz. Jack Ma és az Alibaba támogatta a kis- és középvállalkozói szektort, és Kína a bizonyíték.").

279. *De lásd* Jonathan E. Hillman & Maesea McCalpin, *The China-Pakistan Economic Corridor at Five*, CTR. FOR STRATEGIC & INT'L STUD. (2020. április 2.), <https://perma.cc/H57N-JB2J> (a CPEC nyolc IKT-projektje között "vegyes végrehajtást" állapított meg).

280. Zafar Bhutta, *Pak-China Fibre Optic Cable to Start Functioning by Year-End*, EXPRESS TRIB. (201816., szeptember), <https://tribune.com.pk/story/1804386/2-pak-china-fibre-optic-cable-start-functioning-functioning-year-end/>.

az Afrika és Ázsia közötti forgalom jelenleg Gwadar és Karacsi leszállóhelyekkel folyik.<sup>281</sup>

Pakisztán kialakulóban lévő adatkapcsolatai Kínával nem csak a föld felett vagy alatt, hanem az űrben is zajlanak. Pakisztán az egyik első alkalmazója volt a BeiDou navigációs műholdrendszernek (*Beidou weixing daohang xitong*), amelyet a GPS (a világszerte domináns amerikai rendszer), a Galileo (az Európai Unió építés alatt álló alternatívája) és a GLONASS (az orosz rendszer) vetélytársaként emlegetnek.<sup>282</sup> A BeiDou-t eredetileg a kínai hadsereg fejlesztette ki a 2000-es évek elején, hogy elkerülje a GPS-re való támaszkodást, azóta azonban kereskedelmi forgalomban is elterjedt, és a Huawei, a Xiaomi és mások által gyártott kínai telefonok mind BeiDou-kompatibilisek. A BeiDou 2020 júniusában érte el a globális lefedettséget.<sup>283</sup> Egyesek azt sugallják, hogy a pakisztáni hadsereg hozzáférhet a nagy pontosságú katonai jelhez, amely egyébként a kínai fegyveres erők számára van fenntartva.<sup>284</sup>

Míg a kínai technológiai vállalatok általában véve jelentős teret hódítottak Ázsiában, <sup>285</sup>talán sehol sem érződik jobban a jelenlétük, mint Pakisztánban. A távközlési ágazatban a China Mobile 2009-ben lépett be a pakisztáni piacra, és ez idő alatt digitális ökoszisztémát hozott létre, valamint a pakisztáni mobiltelefon-felhasználókat a 2G-ről a 4G-technológiára fejlesztette, és a tervek szerint a rendszereket 2020-ban 5G-re fejleszti. A Zong 4G, a China Mobile Pakistan helyi márkája, a piaci részesedést tekintve megelőzte versenytársait, több mint harminckétfélmillió előfizetővel, tizennyolcmillió szélessávú előfizetővel, több mint tízmillió 4G előfizetővel, és több mint tízmillió 4G előfizetőt épített ki.

---

281. Jonathan E. Hillman, *War and PEACE on China's Digital Silk Road*, CTR. FOR STRATEGIC & INT'L STUD. (May 201916, ), <https://perma.cc/74FJ-M3CR>; Winston Qiu, *Pakistan to be Linked with PEACE Cable System with up to 60Tbps Capacity*, SUBMARINE CABLE NETWORKS (Apr. 201816, ), <https://perma.cc/Q7VW-KMED>.

282. Degan Sun & Yuyou Zhang, *Egy "külső űrselyemút" építése: China's Beidou Navigation Satellite System in the Arab World*, 10 J. MIDDLE E. & ISLAMIC STUD. (IN ASIA) (2018)24.

283. *BeiDou*: BBC (2020. június 23.), <https://perma.cc/8P2V-SA6M>.

284. *Pakistan Becomes One of the First Country to Hook on to China's BeiDou Satellite Navigation System for Military Purpose: Sources*, TIMES OF ISLAMABAD (Jan. 20192, ), <https://perma.cc/9DDP-97VV>.

285. Brian Harding, *China's Digital Silk Road and Southeast Asia*, CTR. FOR STRATÉGIÁI ÉS NEMZETKÖZI TANULMÁNYOK. (Feb. 201915, ), <https://perma.cc/2MEC-TETD>.

10,550 bázisállomások 4G szolgáltatásokkal országszerte.<sup>286</sup> Míg az Egyesült Államok és egyes szövetségesei megvetik a Huawei-t, Pakisztán felkarolja a vállalatot. A Zong 4G és a Huawei 2019 elején jelentette be, hogy együttműködnek a hálózataik üzemeltetése érdekében.<sup>287</sup> A Huawei Marine, a Huawei leányvállalata, szintén részt vesz a fent említett PEACE projekt kiépítésében.<sup>288</sup>

A mobiltechnológia mellett a kínai vállalatok az adatfinanszírozás és az e-kereskedelem területén is erős jelenlétet mutattak Pakisztánban. Az államkapitalizmus logikájának megfelelően a két kormány vezetői láthatóan részt vettek a kínai e-kereskedelem és a pakisztáni e-kereskedelem összekapcsolásában. Az első pekingi BRI-fórumot követően Sharif akkori miniszterelnök meglátogatta az Alibaba csoport székhelyét Hangzhou-ban, és ugyanazon a napon a Pakisztáni Kereskedelemfejlesztési Hatóság és az Alibaba szándéknyilatkozatot írt alá a pakisztáni kkv-k e-kereskedelem révén történő globalizációjának előmozdításáról.<sup>289</sup> A megállapodás részeként a kínai vállalatoknak segíteniük kellett Pakisztán e-kereskedelmi infrastruktúrájának kiépítésében.<sup>290</sup> E megállapodást követően az Ant Financial negyvenöt százalékos részesedést szerzett a karacsi székhelyű Telenor mikrofinanszírozási bankban a Telenortól, egy norvég távközlési vállalattól.<sup>291</sup> Két hónappal később az Alibaba száz százalékos részesedést szerzett a Darazban, Pakisztán első számú online re-tailerében, amelyet a német Rocket Internet inkubált.<sup>292</sup> A fintech és az e-kereskedelem terén is jelentős akciók az Alibaba általános stratégiája Ázsiában, bár más országok, mint például India, jobban védik ezeket az iparágakat, mint Pakisztán. Míg a kínai akvizíciók nagyobb és olcsóbb hozzáférést biztosítanak

---

286. Xinhua, *Chinese Enterprise Plays Pivotal Role in Promoting Pakistan's Telecom Infrastructure: Minister*, CHINA DAILY (Jan. 201930.), <https://perma.cc/MTW6-ZTFT>.

287. Muhammad Hamza, *Zong 4G és Huawei partner a digitális átálláshoz*, TECHWIRE (20197. február), <https://perma.cc/M3GJ-GZWD>.

288. Qiu, *fenti* megjegyzés 280.

289. *Az Alibaba egyetértési nyilatkozatot ír alá a pakisztáni Kereskedelemfejlesztési Hatósággal a kkv-k és a pénzügyi szolgáltatások e-kereskedelmi fejlesztésének támogatására*, ALIBABA GRP. (201716. május), <https://perma.cc/Q6LR-5HEL>.

290. *Id.*

291. Shahbaz Rana, *CCP jóváhagyja az Alipay 45%-os részesedését a Telenor Mikrofinanszírozási Bankban*, EXPRESS TRIB. (2018. november 8.), <https://tribune.com.pk/story/1842703/2-ccp-approves-alipays-45-stake-telenor-microfinance-bank/>.

292. Sumaira Jajja, *Ahogy az Alibaba megveszi a Daraz-t, sokan kérdezik: Mi a következő lépés?*, DAWN (20189. május), <https://perma.cc/7UGJ-8V5L>.

A pakisztáni szakértők számos aggályra hivatkoztak, a vállalatirányítástól kezdve a korrupcióellenes végrehajtás hiányán át a kiberbiztonságig és a megfigyelési kockázatokig, amelyek Pakisztán születőben lévő jogszabályait tekintve a helyénvalóak.<sup>293</sup>

Egy beszélgetőpartner benyomása szerint a platformalapú szolgáltatásokat nyújtó európai és amerikai technológiai vállalatokkal ellentétben, amelyekről köztudott, hogy viszonylag szigorúan követik a helyi törvényeket, a kínai vállalatok alkalmazkodóbb megközelítést alkalmaznak.<sup>294</sup> Pakisztáni ipari bennfentesek azt állították, hogy a kínai vállalatok a kereskedelmi kamarától privilegizált információkat szereztek, és ezen információk segítségével olyan platformot építettek, amelyen keresztül a pakisztáni szállítók egymással versenyeznek. E folyamat során a kínai vállalatokról ismert, hogy illegális kifizetéseket kaptak, amit a helyi hatóságok általában tolerálnak.<sup>295</sup> Bár fennáll a veszélye annak, hogy az anekdotikus beszámolókból kiindulva általános kijelentéseket teszünk a kínai technológiai vállalatok vállalati kultúrájáról, az biztosnak tűnik, hogy a vállalatok csak olyan mértékben hangsúlyozzák a vállalati szabálykövetést, amennyire a fogadó állam ténylegesen megköveteli azt. A vonatkozó pakisztáni szabályozó ügynökségek, például a nemrég megreformált Pakisztáni Média Szabályozó Hatóság, amely most már a kiber médiára is kiterjed, az átlátható szabályokkal szemben az állami ellenőrzést helyezhetik előtérbe, és ezzel megteremtik a környezetet a határokon átnyúló félállami vállalatok növekedéséhez.<sup>296</sup>

#### B. Kínai felügyeleti infrastruktúra az intelligens és biztonságos városokban

A DSR pakisztáni elterjedésének legmarkánsabb következménye a felügyelet lehet, különösen az intelligens vagy biztonságos városok formájában, ahogyan Pakisztánban ismertebbek.<sup>297</sup> Kína világszerte az intelligens városok előmozdításában.

293. Lásd az alábbi IV.C. szakaszt.

294. Interjú Anonymusszal, Iszlámábád, Pakisztán. (20192., ápr.).

295. *Id.*

296. *De lásd a kísérő megjegyzéshez tartozó infra* szöveget. 352.

297. Az "intelligens városok" általános meghatározását az Európai Unió adja meg: "Az intelligens város olyan hely, ahol a hagyományos hálózatokat és szolgáltatásokat digitális megoldások alkalmazásával hatékonyabbá teszik a lakosok és az üzleti élet javára." *Intelligens városok*, EUR. COMM'N, <https://perma.cc/UWE5-XY94> (utolsó látogatás 2021. aug.12.). A "biztonságos városok" egy szorosan kapcsolódó koncepció, amely a modern technológiák használatát hangsúlyozza, hogy

olyan városok, amelyek nagy adatelemzéseket használnak a városirányításhoz.<sup>298</sup> Csak a Huawei közel hetvenöt intelligens városok biztonságát szolgáló projektet szállított világszerte.<sup>299</sup> A digitális technológiák elvileg megkönnyíthetik a közszolgáltatásokat, de az emberek mindennapi életére gyakorolt infrastrukturális következményekről sem feledkezhetünk meg. Az arcfelismerő technológiák különösen erősítik a kormányok megfigyelési képességeit, és sérthetik az egyenlő jogok védelmét, a magánélet védelmét és a fogyasztói jogokat.<sup>300</sup>

A biztonságos városok különösen vonzóak a pakisztáni kormány számára, tekintettel a közrenddel kapcsolatos aggodalmaira. A biztonságos városok kiépítése érdekében 2015. számos szubnacionális rendőri hatóságot hoztak létre, például a Pandzsáb Biztonságos Városok Hatóságát (PSCA).<sup>301</sup> A kínai technológia rendkívül vonzó az olyan szabályozó hatóságok számára, mint a PSCA, mivel integrált megoldásokat kínál a városirányítás problémáira.<sup>302</sup> A Huawei már korán a PSCA végrehajtó partnere lett, hogy felszereléseket szállítson számos biztonságos pandzsábi városba. A PSCA keretében megvalósuló Lahore Safe City projekt például egy több mint 76,000 négyzetméteres területre kiterjedő parancsnoki és irányító központot tartalmaz a felhő használatával.

---

a bűnüldözés fokozása, a közlekedési szabálysértésektől kezdve a terrorizmusig. Lásd: *The Lahore Safe City Project*, ARUP, <https://perma.cc/D5Y4-ZE7E> (utolsó látogatás 2021. augusztus 12.).

298. Lásd általában Alan Smart & Dean Curran, *The Prospects and Social Impact of Big Data-Driven Urban Governance in China: Provincializing Smart City Research*, in CHINA URBANIZING: IMPACTS AND TRANSITIONS (Weiping Wu & Qi Gao szerk., megjelenés előtt).

299. CAVE ET AL. „*supra*” note at 15,10; lásd még Jonathan E. Hillman & Maesea McCalpin, *Watching Huawei's "Safe Cities"*, CTR. FOR STRATEGIC & INT'L STUD. (Nov. 2019.), <https://perma.cc/PD6L-YDXP> (megállapítva, hogy a Huawei "biztonságos város" megoldásainak előnyeit nehéz ellenőrizni, és hogy a helyi kontextus kulcsfontosságú).

300. Lásd pl. Zhejiang Pufa (浙江普法) [Zhejiang Law Popularization], Yin Dongwu Shijie Qiyong Renlian Shibie, Zhejiang Yi Daxue Jiaoshou Jiang Yuanfang Qisu Zhi Fayuan (因动物世界启用人脸识别, 浙江一大学教授将园方起诉至法院) [Because the Safari Park Started Using Facial Recognition, A Professor From A University in Zhejiang Took the Park Straight to Court], BAIJIAHAO (百家号) (Nov. 3, 2019), <https://perma.cc/X9KQ-24UT> (leírja, hogyan perelt be egy férfi egy szafari parkot, mert arczkennelést követelt, hivatkozva a Kínai Népköztársaság Consumer Rights Protection Law megsértésére).

301. Punjab Safe Cities Authority Act No2016. of (12016Pak.) (a pandzsábi kormány által kihirdetett).

302. Interjú Akbar Nasir Khannal, a PSCA-Lahore operatív igazgatójával, Huawei, <https://perma.cc/4R6L-KSEU> (utolsó látogatás 2021. október 3-án).

és egyéb IKT-technológiák, valamint a Huawei által tervezett és telepített megfigyelő 10,000kamerák.<sup>303</sup> A Huawei 2016-ban nyerte el a szerződést összesen 84,7 millió dollár értékben.<sup>304</sup> Akkoriban a Huawei a projektet "a világ legnagyobb átfogó Safe City-architektúrájaként" reklámozta.<sup>305</sup> A projekt azonban ellentmondásos lett, amikor kiderült, hogy a rendszer CCTV-szekrényei nem nyilvános WiFi adóvevőket tartalmaznak, ami kérdéseket vetett fel az adatbiztonsággal kapcsolatban.<sup>306</sup> Augusztusban egy 2021,

Az amerikai szoftvercég, amely a Huawei-vel a Lahore Safe City projektben együttműködött, beperelte a Huawei-t Kaliforniában, azt állítva, hogy üzleti titkokkal való visszaélést követett el, és azt állította, hogy a Huawei "hátsó ajtót" épített érzékeny adatok Kínába történő exportálására, állítólag a pakisztáni kormány jóváhagyásával.<sup>307</sup>

A civil társadalom tagjai arról is beszámoltak, hogy a Huawei által biztosított technológia lehetővé tette a PSCA számára, hogy biztonságos városaikban eltávolítsa az általuk kifogásolhatónak ítélt anyagokat az internetről, ami meghaladja a hivatalos hatáskörüket.<sup>308</sup> Tovább bonyolítja a képet, hogy bár a biztonságos városok technológiáját eredetileg rendőri használatra és forgalomirányításra tervezték, a pakisztáni hadsereg és a hírszerzés azóta már működteti ezeket a hálózatokat. A pakisztáni rend- és biztonságvédelem és a kínai digitális infrastruktúra kombinációja megmutatja a kölcsönös akció előnyeit és buktatóit egyaránt.

---

303. Sebastian Moss, *Huawei Signs MoU with Pakistan for Cloud Data Center*, DATA CTR. DYNAMICS (201929., ápr.), <https://perma.cc/RL2T-RHUR>.

304. *Id.*

305. Huawei News Room, *Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities*, HUAWEI (2018. október 15.), <https://perma.cc/Z3CM-NDFS>.

306. *Lásd Moss, fenti megjegyzés (302a kártyák későbbi eltávolításáról).*

307. *Panasz a Bus3., Efficiency Sols., LLC kontra Huawei Techs. Co. Ltd., No. 8:21-cv-1330 (C.D. Cal. Aug. 202111),* [https://regmedia.co.uk/2021/08/12/bes\\_v\\_huawei.pdf](https://regmedia.co.uk/2021/08/12/bes_v_huawei.pdf); *lásd még Thomas Claburn, Huawei Stole Our Tech and Created a 'Backdoor' to Spy on Pakistan, Claims IT Biz*, THE REGISTER (Aug. 202113,), <https://perma.cc/MU77-6ZNN> (idézi a Huawei képviselőjét, aki tagadja a hátsó ajtóval kapcsolatos állítást, és jelzi, hogy a két vállalat szerződéses viták miatt választottbíróügyi eljárást is folytat Pakisztánban).

308. *Lásd: Interjú Anonymus közérdekű jogással, Lahore, Pakisztán. (201927., november) (megjegyezve, hogy az internetes tartalmak eltávolítására vonatkozó hatáskör a Pakisztáni Távközlési Ügynökséget illeti meg az elektronikus bűncselekmények megelőzéséről szóló 2016. évi törvény 37. szakasza alapján).*

cess. Bár a technológia megerősítheti a helyi és nemzeti hatóságok rendőri erejét, ezt olyan módon is megteheti, amely meghaladja a vonatkozó törvényeket. Miközben a rendőrség, a hadsereg és a hírszerző ügynökségek a kínai technológia segítségével igyekeznek bővíteni információgyűjtési kapacitásaikat, lehet, hogy egy még nagyobb adatgyűjtési és adatellenőrzési rendszernek rendelik alá magukat, amelyet Kína információgyűjtési képességei irányítanak.

Mindazonáltal a CPEC keretében további biztonságos városokkal kapcsolatos projektek vannak folyamatban Iszlámábádban, Pesavarban, Karacsiban, Gwadarban és Quettában.<sup>309</sup> Ezeket a biztonságos városokat összekapcsolják az ország adatkezelését szolgáló, a "hosszú távú terv" által "információs hálózati infrastruktúrának" nevezett rendszer részeként.<sup>310</sup> Az ilyen összekapcsolás a Digitális Kezdeményezés nyolcadik elvét, nevezetesen a "városok közötti digitális gazdasági együttműködés" (*tuidong chengshi jian de shuzi jingji hezuo*) előmozdítását példázza.<sup>311</sup> A dél-pakisztáni Gwadart a nyugat-kínai Kash- garral biztonságos és intelligens városokon keresztül összekötő folyosó az egyik módja annak, hogy a CPEC integrálja a két gazdaságot.<sup>312</sup>

A DSR biztonságos és intelligens városaiban alkalmazott technológiák egy részét először Hszincsiangban fejlesztették ki a muszlim kisebbségek elnyomására.<sup>313</sup> Ez a helyben kifejlesztett, majd transznacionálisan exportált felügyeleti infrastruktúra gyakran globális forrásból származik. Amikor a kínai felügyeleti infrastruktúra-szolgáltatók Kínán belül telepítik technológiájukat, vagy harmadik országokba exportálják azt, bizonyos termékeket és szolgáltatásokat a következő országokból származó termékekre és szolgáltatásokra támaszkodhatnak

---

309. Talal Raza, *exkluzív: DIGIT: The CPEC Plan for Pakistan's Digital Future*, DIGIT. RTS. MONITOR (2017.13., okt.), <https://perma.cc/9NGE-SBJN>.

310. *Lásd a fenti szöveg kísérő megjegyzését 272.*

311. *Lásd a fenti szöveg kísérő megjegyzését 250.*

312. *Lásd Husain, 271. lábjegyzet (megjegyezve, hogy a CPEC "messze túlmutat a Kashgart és Gwadart összekötő egyszerű optikai szálak kiépítésén").*

313. *Lásd James Millward & Dahlia Peterson, China's System of Oppression in Xinjiang: How it Developed and How to Curb It*, CTR. FOR SEC. & EMERGING TECH. 5 (Sept., 2020), <https://perma.cc/9KKF-3NAH> (az ujugurok biológiai adatainak gyűjtésére szolgáló rendszerek leírása, valamint az, hogy ezeket az adatokat hogyan használják fel a "szélsőséges" prediktálására); Yves Morea, *Crack Down on Genomic Surveillance*, NATURE (Dec. 2019.), <https://www.nature.com/articles/d41586-019-03687-x?sf225143202=1> (utalva arra, hogy 2017-ben Hszincsiangban 19 millió embertől gyűjtöttek biometrikus adatokat társadalmi ellenőrzés céljából).

Amerikai technológiai vállalatok.<sup>314</sup> Az Egyesült Államok kormánya szankciókkal sújtotta az emberi jogok hszincsiangi megsértésében érintett kínai vállalatokat, ami megakadályozza őket abban, hogy amerikai cégekkel üzletet kössenek, de nem akadályozza meg őket abban, hogy máshonnan szerezzenek finanszírozást vagy alkatrészeket.<sup>315</sup> A megfigyelési technológia virágzó exportja egy kulcsfontosságú különbséget is szemléltet a pekingi hatás megvalósulásának két mechanizmusa között.<sup>316</sup> Bizonyos digitális infrastruktúrák exportja, különösen azoké, amelyek gépi tanulással képzett algoritmusokat tartalmaznak, olyan élő környezetet hoz létre, amelyet a számítógépes kódok közvetlen átültetése alakít.<sup>317</sup> Ezzel szemben a jogi kódoknak nincs ilyen közvetlen exportja. A fogadó államok az adatkezelésre vonatkozó kínai megközelítések bizonyos aspektusait vagy a mögöttük meghúzódó ideológiákat átvehetik, de a kínai modellt nem ültetik át teljes egészében, ahogyan azt a pakisztáni példa is mutatja.

### C. Pakisztán kialakulóban lévő adatkezelési rendszere

A Pakisztánban vagy máshol működő kínai technológiai vállalatoknak be kell tartaniuk a helyi törvényeket. Mivel azonban a pakisztáni adatvédelmi törvény viszonylag új keletű, a mai napig kevés védelmet nyújt a külföldi behatolással és ellenőrzéssel szemben. A meglévő szabályok inkább a rendőrségi hatáskörök és a hírszerző szolgálatok hatókörének növelését szolgálják, mintsem a polgárok adatainak védelmét. A

---

314. Lásd Lin & Chin, *fenti* megjegyzés (többek között az Intel és a Hewlett Packard kínai megfigyelést segítő vállalatokat 75azonosít); Paul Mozur & Don Clark, *China's Surveillance State Sucks Up Data. U.S. Tech is Key to Sorting It.*, N.Y. TIMES (2021. január 20.), <https://perma.cc/27XK-5WRZ>; lásd még Marco Rubio & Chris Smith, *Letter to Commerce Secretary About Sale of Surveillance Technology to Chinese Police*, CONG.-EXEC. COMM'N ON CHINA (20189., május), <https://perma.cc/6QVJ-5RGJ> (kérdőjelezi, hogy az amerikai technológia lehetővé tette-e az etnikai kisebbségek emberi jogi visszaéléseit Hszincsiangban).

315. Lásd egyes szervezetek felvétele a szervezetek listájára, 15 C.F.R. § 744 (2021) ("[E]zek a szervezetek érintettek az emberi jogok megsértésében és visszaélésekben a kínai elnyomási kampány, a tömeges fogva tartás és a csúcstechnológias megfigyelés végrehajtása során az ujjurok, kazahok és a Hszincsiang-Ujgur Autonóm Területen (Xinjiang Uyghur Autonomous Region, XUAR) élő muszlim kisebbségi csoportok más tagjai ellen."); lásd még Dave Gershgorn, *US Sanctions a Chinese Facial Recognition Company with Silicon Valley Funding*, THE VERGE (2021. július 9.), <https://perma.cc/BD7B-NMUK> (kiemelve a megfigyelési iparban működő transznacionális pénzügyi kapcsolatokat).

316. Lásd *fentebb* a II.A. szakaszt.

317. Lásd *fentebb* a II.D. szakaszt.

a CPEC által katalizált pakisztáni és kínai adatkezelési megközelítések közötti látens konvergencia. Pakisztánnak nagy igénye van a kifinomult digitális infrastruktúrára egy olyan politikai rendszerben, amely a társadalmi stabilitást helyezi előtérbe. Ennek a kombinációnak az egyik következménye, hogy Pakisztán digitális infrastruktúrájának fejlődése gyorsabban felgyorsulhat, mint az adatokkal kapcsolatos jogi infrastruktúrája. Ezek a tényezők Pakisztánt a pekingi hatás elsődleges helyszínévé teszik.

Az elmúlt években jelentős viták folytak Pakisztánban a kiberbiztonságról és a magánélet védelméről. Egyrészt az ország évtizedek óta a terrorizmus elleni harcban áll, és ezért a nemzetbiztonságnak, beleértve az adatokhoz való kormányzati hozzáférést is, erős előjogai vannak.<sup>318</sup> Másrészt Pakisztánban aktív igazságszolgáltatás működik, amely kiterjedt joggyakorlatot hozott létre az alapvető jogokról, beleértve a magánéletet is.<sup>319</sup> Ez a dinamika magában a pakisztáni alkotmányban is érzékelhető, mivel az védi a magánéletet, de az ilyen alapvető jogokat a fegyveres erők és a rendőrség közrend fenntartására vonatkozó előjogai alá sorolja.<sup>320</sup> Ezek a debátumok alakítják a pakisztáni adatkezelés szabályozási környezetét.

A kínai szétválasztott szabályozási rendszerrel párhuzamosan az országban is<sup>321</sup> számos internetes szabályozó hatóság működik: a Pakisztáni Távközlési Hatóság (PTA), a Szövetségi Nyomozó Ügynökség, a Pakisztáni Legfelsőbb Bíróság, az Informatikai Minisztérium, valamint a Vallási Ügyek és Vallásközi Harmónia Minisztériuma által létrehozott Web Evaluation Cell (WEC). Ezek a szervek felelősek a pakisztáni kibertér irányításáért, különös tekintettel a potenciálisan felforgató jellegű anyagok blokkolására.

---

318. *Lásd általában* AYESHA SIDDIQA, *MILITARY INC.: INSIDE PAKISTAN'S MILITARY ECONOMY* (2d ed. 2017) (elemzi, hogyan ellenőrzi a hadsereg az országot).

319. *Lásd* MUHAMMAD AZEEM, *LAW, STATE, AND INEQUALITY IN PAKISTAN: EXPLAINING THE RISE OF THE JUDICIARY* (92,2017127,203) (az "alapvető jogokkal" kapcsolatos vitatott joggyakorlat krónikája, amely az alkotmányban és 1956, 1962, az alkotmányban 1973 való elismerésükből ered).

320. *Lásd a* PAKISZTÁNI SZÖVETSÉG 14. cikk, 1. § ("Az emberi méltóság és - a törvényre is figyelemmel - a magánélet sérthetetlen."). *Lásd azonban a* PAKISZTÁN SZÖVETSÉGES ÁLLAMSZERZŐDÉST. art. 8. cikke (amely előírja, hogy "a fegyveres erők, a rendőrség vagy a közrend fenntartásával megbízott más erők tagjaira vonatkozó törvények" nem semmisek, ha nem állnak összhangban az alapvető jogokkal).

321. *Lásd a fenti* szöveg kísérelő megjegyzését 90.

ema a nemzetbiztonságra és az iszlámra. Ezek közül a legfontosabb a PTA, amely az ország összes távközlési rendszerét és szolgáltatását szabályozza, és kapuórként szolgál. A WEC ajánlására például a PTA 2017-ben 6149 weboldalt blokkolt.<sup>322</sup> 2019-ben a PTA 900 000 URL-t blokkolt "olyan okok miatt, mint az istenkáromló és pornográf tartalmak és/vagy az állam, a dzsidás vagy a fegyveres erők elleni érzelmek hordozása".<sup>323</sup> Az internetszűrésen túl a PTA a titkosító szoftverek és a virtuális magánhálózatok (VPN) használatát is igyekezett szabályozni.<sup>324</sup> A PTA ellenőrzése kiterjed minden, az országba behozott mobiltelefonra egy új adórendszer révén, amely előírja, hogy az országba belépő személyeknek regisztrálniuk kell a telefonjukat, ha nem külföldi SIM-kártyát használnak.<sup>325</sup> Emellett a Nemzeti Adatbázis- és Regisztrációs Hatóság (NADRA) ellenőrzi a polgárok adatainak központosított tárolását.<sup>326</sup> Az adatszivárgások széles körű személyazonosság-lopást okoztak, mivel a szerver a sérülékeny e-kormányzati mo- bile alkalmazásokra támaszkodik.<sup>327</sup> A NADRA adatbázisa összekapcsolódik a biztonságos városok projektjeivel, például a PSCA által vezetett projektekkel, ami lehetővé teszi a hatóságok számára a polgárok megfigyelését.<sup>328</sup> Összefoglalva, Pakisztán igénye a kormány ellenőrzése alatt álló, csúcstechnológiát képviselő digitális infrastruktúra iránt egy olyan jogi infrastruktúra háttérében jelentkezik, amely, ahol ez

---

322. 6,149 weboldal blokkolása a Vallásügyi Minisztérium Web Evaluation Cell (WEC) ajánlására, URDUPOINT (20181., június), <https://perma.cc/8477-CWVX>.

323. Kalbe Ali, *900,000 Websites Blocked over Content, Says PTA*, DAWN (Sept. 201927.), <https://perma.cc/Y7XD-NVKL>.

324. Hija Kamran, *PTA Restricts Access to Proxy11,000 Servers; Aims to Regulate VPN Use in Pakistan 'Through a New Model'*, DIGIT. RTS. MONITOR (2019. július 19.), <https://perma.cc/TJ5B-EMYB>.

325. Ashfaq Ahmed, *Pakisztánba utazik? Akkor regisztrálnia kell a Mobil Phone telefonját*, GULF NEWS (201923., január), <https://perma.cc/8TZQ-4G5P>.

326. *Lásd a 2000. évi VIII. számú, a Nemzeti Adatbázis- és Regisztrációs Hatóságról szóló rendeletet*, THE GAZETTE OF PAKISTAN EXTRAORDINARY, 2000. március 10. (a NADRA-t felhatalmazza arra, hogy országos szintű regisztrációs rendszert hozzon létre valamennyi polgár számára).

327. Jannat Ali Kalyar, *Cyber Insecurity*, THE NEWS ON SUNDAY (2019. december 22.), <https://perma.cc/8SWY-3D2M>.

328. *Lásd, Id.* (leírja, hogy a kormány hogyan azonosított egy párt, akik intim aktusokat folytattak egy autóban).

létezik, kiegészíti az állam stabilitási imperatívuszát, hogy a kínai jogi tanulmányok egyik kifejezésével éljek.<sup>329</sup>

Pakisztánban hiányoznak az érintettek, az adatkezelők és az adatfeldolgozók - többek között a távközlési és internetszolgáltatók, az elektronikus vállalkozások, a pénzügyi intézetek és a kormányzati szolgáltatási portálok - közötti kapcsolatot szabályozó szabályok.<sup>330</sup> A hatályos jogszabályok széleskörű jogköröket biztosítanak a felhatalmazott tisztviselőknek az adatok<sup>331</sup> átkutatására és lefoglalására, és előírják, hogy az internetszolgáltatóknak a felhasználók adatait legalább egy évig meg kell őrizniük.<sup>332</sup> Az 1996-os pakisztáni távközlési (újjászervezési) törvény,<sup>333</sup> amelyet a mobilszolgáltatások és az internet pakisztáni bevezetését követően hirdettek ki, felhatalmazza a kormányt a digitális kommunikáció ellenőrzésére, és korlátozza a titkosítási technológia használatát.<sup>334</sup>

Az elektronikus bűnözés megelőzéséről 2016 sz. törvény (PECA) a számítástechnikai bűnözéssel kapcsolatos legfontosabb jogszabály. A PECA a bűncselekmények széles és hosszú listáját tartalmazza, beleértve többek között a kiberterrorizmust, a gyűlöletbeszédet, a személyazonosító adatok jogosulatlan felhasználását, a SIM-kártyák jogosulatlan használatát, a gyermekpornográfiát, a rosszindulatú kódot, a cyberstalkingot, a spamküldést és a hamisítást. A PECA szigorú szankciókat ír elő, például aki bűnösnek találják spoofingban, három évig terjedő szabadságvesztéssel, ötszázezer rúpia (kb. 6600 dollár) pénzbírsággal vagy mindkettővel büntethető.<sup>335</sup> A felsorolt bűncselekmények közül számos jóval túlmutat a nemzetközi normákon, például az Európa Tanács számítógépes bűnözésről szóló egyezményében (Budapesti Egyezmény) foglaltakon, amelynek sem Pakisztán, sem Kína nem részese.<sup>336</sup> A végrehajtást illetően a PECA szilárd...

329. Lásd SARAH BIDDULPH, THE STABILITY IMPERATIVE: HUMAN RIGHTS AND LAW IN CHINA 10 (2015) (azzal érvelve, hogy Kínában a jog a "társadalmi stabilitás" (*weiben*) védelmét szolgálja).

330. UMER GILANI ET AL., BYTES FOR ALL, ELECTRONIC DATA PROTECTION IN PAKISTAN: WHAT NEEDS TO BE DONE? 5 (2017), <https://perma.cc/2GL7-AJJB>.

331. Az elektronikus bűncselekmények megelőzéséről szóló 2016. évi XL. törvény, 32. §, THE GA-ZETTE OF PAKISTAN EXTRAORDINARY, aug. 19, 2016.

332. *Id.* at § 29.

333. A pakisztáni távközlési (átszervezési) törvény, XVII.17. sz. a PAKISZTÁNI KÜLÖNLEGES 1996, GAZETTE, okt. 1996.

334. GILANI, *Supra* note at 329, 8.

335. Az elektronikus bűncselekmények megelőzéséről szóló 2016. évi XL. törvény 23. §-a, THE GA-ZETTE OF PAKISTAN EXTRAORDINARY, aug. 19, 2016.

336. *Lásd:* Egyezmény a számítógépes bűnözésről, 2001. november 23., E.T.S. No. 185 (példák a számítógépes bűncselekményekre).

a PTA a digitális média szabályozásának legfőbb tárcaközi szerve. A PECA harmincnégyes szakasza széleskörű jogköröket biztosít a PTA számára a "jogellenes online közvetítések" blokkolására, ha a PTA úgy ítéli meg, hogy ez "az iszlám dicsőségének, illetve Pakisztán integritásának, biztonságának vagy védelmének" érdekében áll.<sup>337</sup> Ezekben az esetekben a PTA jogosult az adatok átkutatására és lefoglalására is, bírósági felügyelet nélkül.<sup>338</sup> Végezetül, a pakisztáni harci cselekmények nyomon követésének eredményeképp pénzmosás és a terrorizmus finanszírozásának a Financial Action Task Force (FATF) által történő megakadályozása érdekében Pakisztán kihirdette a 2019. évi keresési és lefoglalási szabályokat ("SECP-szabályok").<sup>339</sup> A SECP-szabályok a SECP által a vállalati szektorban folytatott családgyakorlatok azonosítása érdekében bármely vagyontárgy átkutatására és lefoglalására vonatkozó hatáskörök használatára vonatkozó eljárást állapítanak meg. A SECP-szabályok lehetővé teszik a nyomozó tisztviselő számára az elektronikus eszközökhöz való hozzáférést, azok lefoglalását és biztosítását, és hozzáférést biztosítanak az elektronikus eszközök működtetéséhez szükséges jelszavakhoz.<sup>340</sup> Így még az olyan nemzetközi szabványok, mint például a FATF által kihirdetett szabványok végrehajtását célzó jogszabályok is növelhetik a szabályozó hatóságok diszkréciós jogkörét, ami a magánszemélyek adatainak védelme rovására megy.

Az adatokhoz való állami hozzáférést lehetővé tevő digitális infrastruktúra iránti növekvő igényt és a vékony jogi infrastruktúrát jól mutatja, hogy Pakisztánban nincs adatvédelmi törvény. A "személyes adatok védelméről szóló törvénytervezet" a parlamentben lappangott, és súlyos hiányosságokat tartalmazott. Egy pakisztáni civil társadalmi csoport egyik tagjának szavaival élve:

Az adatvédelmi törvénytervezet 2018. júliusi első tervezete kifejezetten kivételt tett a kormányzati szervek és a kormányzati szervek által tárolt személyes adatok tekintetében. Más országokban a legnagyobb problémát az adatokkal rendelkező magáncégek jelentik, de Pakisztánban az állampolgárok adatait az állam (pl. biometrikus adatok) és [a] NADRA adatbázisában tárolja. A kormány tehát nem hajlandó

337. Az elektronikus bűncselekmények megelőzéséről szóló 2016. évi XL. törvény 34. §, THE GAZETTE OF PAKISTAN EXTRAORDINARY, Aug. 19, 2016.

338. *Id.* a 32. §-ban (messzemenő hatásköröket biztosít a felhatalmazott tisztviselők számára az adatok átkutatására és lefoglalására).

339. A pakisztáni értékpapír- és tőzsdebizottság (kutatás és lefoglalás) szabályai (2019), S.R.O. (713I)/2019, <https://khilji.net.pk/wp-content/uploads/2019/07/Search-and-Seizure-Rules-2019.pdf>.

340. *Id.* at § 7.

elszámoltathatóvá teszi magát. Ezt a kivételt egy későbbi tervezetből törölték, de [még mindig] láthatunk hatalmas kivételeket.<sup>341</sup>

A személyes adatok védelméről szóló törvénytervezet 2020 kötelezővé teszi az érintett hozzájárulását az adatai kezeléséhez,<sup>342</sup> de felsorolja az e szabály alóli széleskörű kivételeket, többek között "bármely törvény által vagy annak alapján bármely személyre ruházott feladat gyakorlása céljából",<sup>343</sup>

A digitális infrastruktúra iránti nagymértékű kereslet és a szilárd jogi keret nélküli digitális infrastruktúra iránti nagymértékű kereslet kombinációjából nem az a kép rajzolódik ki, hogy Kína ráerőlteti a saját modelljét Pakisztánra. Ehelyett Pakisztán és Kína az adatkezelésre vonatkozó megközelítésekben egyezőséget mutat, amit elősegít, hogy Pakisztán a kínaiak által épített és üzemeltetett infrastruktúrára támaszkodik. Ez a konvergencia azonban korántsem elkerülhetetlen. A digitális tekintélyelvűség tézise hajlamos azt feltételezni, hogy a tekintélyelvűek felcserélhetők, és hogy Kína adatkezelési megközelítése exportálható. Pakisztán esetében egyik feltételezés sem állja meg a helyét, ahol erős a hadsereg, de többpárti demokratikus rendszer, intervencionista igazságszolgáltatás, hangos sajtó, liberális civil társadalom, aktivista szakszervezetek és kozmopolita muszlim lakosság is van, ami legalábbis megnehezítheti a kínai adatkezelési megközelítések átvételét.

Márciusban például a 2012. pakisztáni kormány pályázatot írt ki egy olyan projektre, amely "egy nemzeti szintű URL-szűrő és blokkoló rendszer kifejlesztését és működtetését" célozza.<sup>344</sup> Az akkori ítélezési gyakorlatból kiderült, hogy az igazságszolgáltatás a kínai jogszabályokat tekintette mintának az internetes istenkáromló tartalmak blokkolására.<sup>345</sup> Az aktivisták azonban megghiúsították az országos szűrőrendszer tervét. A pakisztáni aktivistáknak a megszegyenítés stratégiáját alkalmazva sikerült elérni, hogy

---

341. Interjú Anonymusszal, Lahore, Pakisztán. (2019. november).

342. Személyes adatok védelméről szóló 2020. évi törvényjavaslat, konzultációs tervezet, 2020. április 9., cikk. [https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%205.1.Protection%20Bill%202020%20Updated\(2\).pdf](https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%205.1.Protection%20Bill%202020%20Updated(2).pdf).

343. *Id.* 5.2(g).

344. PAKISZTÁNI NEMZETI I C T K+F ALAP, AJÁNLATTÉTELI FELHÍVÁS: NA-TIONAL URL FILTERING AND BLOCKING SYSTEM (2012), <https://perma.cc/4ZCJ-NXSC>.

345. *Lásd* Islamic Lawyers Movement v. Federation of Pakistan, (2012) CLC (Lahore) (1300Pak.) ("[A]z államnak törekednie kell arra, hogy a Kínán kívül más iszlám országok által már elfogadott irányvonalaknak megfelelő jogszabályokat hozzon.").

a világ öt vezető technológiai vállalata nem biztosítaná a szűrőrendszer digitális infrastruktúráját.<sup>346</sup> A három hallgatott technológiai vállalat közül kettő kínai, egy pedig kanadai volt. Végül egy módosított szűrőrendszert hoztak létre a kanadai cégen keresztül;<sup>347</sup> a civil társadalom ellenállása pedig a kínai modellről alkotott közfelfogást Pakisztán számára nem vonzónak minősítette.

Míg a kínai adatkezelés teljes körű exportálása az olyan országokba, mint Pakisztán, nem megvalósítható, a kínai digitális infrastruktúrára való fokozatos és növekvő támaszkodás valószínűsíthető. Pakisztán szívesen építene és támaszkodna a Kínában gyártott digitális infrastruktúrára, például optikai kábelekre, adatközpontokra, e-kereskedelmi platformokra és műholdas rendszerekre.<sup>348</sup> Kritikus, hogy ezeket az infrastruktúrákat kínai vállalatok biztosítják. A 2017. PTA például felavatta a Pakistan Internet Exchange Pointot (ismert nevén PKIX), biztosítva, hogy minden, akár Pakisztánban keletkező, akár az országon áthaladó adatot egyetlen, Iszlámábádban található, az internetszolgáltatók és tartalomszolgáltatók közötti interfészen keresztül kelljen továbbítani. Az internetes cserepontosítók alapvető internetes infrastruktúrát jelentenek, amely a globális délen történelmileg hiányzott, de a megfigyelés vektoraként is funkcionálhatnak.<sup>349</sup> A PKIX-et, akár csak a PEACE tenger alatti kábelrendszert, a Huawei működteti.<sup>350</sup> A kínai IKT-óriás Pakisztán internetes infrastruktúrájának középpontjában működik.

Az olyan országok, mint Pakisztán, igyekeznek utánozni Kína megközelítését az adatszuverenitás köré összpontosító adatkezeléssel kapcsolatban. Mivel azonban a digitális infrastruktúrát építő és működtető kínai vállalatok elválaszthatatlanul összefonódnak a digitális infrastruktúrával.

---

346. Michael Newman, *Say No to Government Censorship of the Internet in Pakistan*, BUS. & HUM. RTS. RES. CTR. (2012. március 2.), <https://perma.cc/4PCA-V4XK>.

347. Jakub Dalek et al., *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-Based Netsweeper's Role in Pakistan's Censorship Regime*, THE CITIZEN LAB (Jun. 201320.), <https://citizenlab.ca/2013/06/o-pakistan/#8>.

348. *Lásd fentebb a IV.A-B. szakaszt.*

349. *Lásd* Fernanda R. Rosa, *Global Internet Interconnection Infrastructure: Materiality, Concealment, and Surveillance in Contemporary Communication* (2019) (doktori disszertáció, American University), <https://perma.cc/24F2-BNJU> (az internetes cserepontosítók általi kormányzásról és a társadalmi, politikai és közértékekről, amelyek a tét).

350. Egy második PKIX-helyszín, amelyet az Internet Society (ISOC) üzemeltet, februárban nyílt meg Karacsiban. *IXP2019. Locations*, PKIX, <https://perma.cc/HV93-NVVJ> (utolsó látogatás 202017., augusztus).

a pártállammal, és kérésre adatokat oszthatnak meg Pekinggel, az ilyen adatszuverenitás végső soron illuzórikus. A pakisztáni szakértők több szinten is azt gyanítják, hogy Pakisztán átengedi szuverenitását Kínának. Az aggodalmak a kínaiak által épített infrastruktúrától kezdve a kiszivárgást lehetővé tevő és a dezinformáció Iszlámábádba való eljuttatásáig terjednek, amely Peking kiberkérdésekkel kapcsolatos politikájához kötődik, akár az ENSZ-ben, akár az ITU-ban, akár a Sanghaji Együttműködési Szervezetben.<sup>351</sup> Noha a behatolásra számos bizonyíték van, az adatok kínai ellenőrzése nem egyértelmű. Például a PTA és a TikTok közötti kapcsolat a "beszéd kormányzójaként" egyre nagyobb szabályozási diszkoordinációról, ha nem is versengésről tanúskodik.<sup>352</sup> A TikTok cenzora a pakisztáni hatóságok számára úgy tűnik, hogy potenciálisan egyszerre túlságosan is és alul is befogadó.<sup>353</sup> Ami az utóbbit illeti, a TikTok Pakisztánból való kitiltása érdekében pereket indítottak.<sup>354</sup> Októberben a 2020,PTA betiltotta a TikTOKot, majd tizenegy nappal később feloldotta a tiltást.<sup>355</sup> Az esetet jól ismerő ügyvédek szerint az epizód nem kínai szándékról tanúskodik, hanem inkább a belpolitikai küzdelmeket mutatja, különösen, hogy a PTA a katonai vezetés kívánalmaival összhangban igyekszik ellenőrizni a közszférát.<sup>356</sup> Összefoglalva, a TikTok és a PTA közötti feszült kapcsolat jól mutatja a kínai szabályozási bizonytalanság magas fokát.

---

351. Telefonos interjú névtelen, iszlámábádi ügyvéddel (2019., március).

352. *Lásd* Klonick, *Supra* note 178.

353. *Compare* Zaheer Ali Khan, *TikTok Blocks Accounts 93,000 with "Objectionable Content" in Pakistan*, SAMAA (Sept. 202016, ), <https://perma.cc/LC4B-TKDV> (megállapítva, hogy míg a PTA kérte a TikTok-ot, hogy blokkolja a fiókokat 93,000, a TikTok saját kezdeményezésére millió 5.6 videót és linket blokkolt, ami a vállalat által gyakorolt jelentős végrehajtási hatásköröket jelzi), *with Lahore High Court Moved for Ban on TikTok App*, DAWN (Aug. 4, 2019), <https://perma.cc/GY77-77F3> (a Lahore-i Legfelsőbb Bíróságon a TikTok betiltására irányuló kereset ismertetése, azzal az indokkal, hogy az alkalmazás por- nográfiai és illegális anyagokat tesz közzé).

354. *Lásd pl.* „,DAWN, 352. lábjegyzet; Sajjad Haider, *Petition to Ban Tiktok Filed in the Peshawar High Court*, SAMAA (Sept. 20208, ), <https://perma.cc/NEE8-7BC8> (jelezve, hogy a Tiktok ellen "erkölcstelen és kifogásolható" tartalma miatt indítottak pert).

355. Manish Singh, *Pakistan Lifts Ban on TikTok*, TECHCRUNCH (2020. október 19.), <https://perma.cc/SR7W-XVCJ>.

356. Telefoninterjú névtelen pakisztáni ügyvéddel (202028., október); telefoninterjú névtelen pakisztáni ügyvéddel (20202., november).

amelyekkel a befektetők szembesülnek az olyan országokban, mint Pakisztán. Ez azt is szemlélteti, hogy Kína milyen korlátok közé szorítja a határain túli adatkezelés ellenőrzését.

#### V. A PEKINGI HATÁS ÉRTÉKELÉSE: AZ ADATSZUVERENITÁS ÉS DIGITÁLIS FEJLESZTÉS

A COVID által sújtott nyáron a kínai vállalatok által végzett adatgyűjtéssel kapcsolatos aggodalmak<sup>2020</sup>, a BRI-n kívüli kormányzat erőteljes válaszlépéseihez vezettek. India egyenesen betiltott bizonyos kínai alkalmazásokat, szuverenitási és biztonsági aggályokra hivatkozva.<sup>357</sup> Az Egyesült Államok kormánya követte a példát, és bejelentette a TikTok és a WeChat várható korlátozását.<sup>358</sup> Ezek a lépések a pekingi hatásra adott válaszoknak tekinthetők: ha Kína növekvő befolyása a transznacionális adatkezelésre aggodalomra ad okot, akkor a kínai vállalatok működésének korlátozása a főbb piacokon hatékony ellenstratégiának tűnhet. Míg India döntése összhangban van azzal a szélesebb körű programmal, amely az indiai adatok stratégiai erőforrásként való megőrzésére törekszik, addig<sup>359</sup> az Egyesült Államok ellentmondott a szabad adatáramlás és az internet szabadsága iránti régóta fennálló, de egyre inkább vitatott kötelezettségvállalásoknak.<sup>360</sup> A kínai vállalatok kiszorítása a főbb piacokról azonban csak megerősítheti a harmadik országoktól való függőségüket, amelyek továbbra is szívesen fogadják tevékenységüket, ezáltal akaratlanul is erősítve a pekingi hatást. Ráadásul a kínai adatgyűjtéssel kapcsolatos aggodalmak az Egyesült Államokban üresnek tűnnek, ha figyelembe vesszük, hogy

357. Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat*, N.Y. TIMES (2020. június), <https://perma.cc/M9ER-K4VA>.

358. Végrehajtás. 13,942. sz. rendelet, 85 Fed. Reg. 48,637 (Aug. 6, 2020), <https://perma.cc/7XQS-JYHX> (a TikTok által jelentett fenyegetéssel foglalkozik); Exec. Order No. Fed13,943,85. Reg. 48,641 (Aug. 2020.), <https://perma.cc/K276-6N9N> (a WeChat által jelentett fenyegetéssel foglalkozik). A Biden-kormányzat 2021 júniusában mindkét rendeletet visszavonta, és egy olyan jelentést rendelt meg, amely ~~árta~~ tartalmazott az amerikai személyek érzékeny adatainak korlátlan eladásából, továbbításából vagy az azokhoz való hozzáférésekből eredő károk elleni védelemre. Exec. Order No. 14,034, 86 Fed. Reg. 31423 (2021. június 9.), <https://perma.cc/X4LD-NPDN> ("Protecting Americans' Sensitive Data from Foreign Adversaries").

359. GOV'T OF INDIA, DEP'T FOR PROMOTION OF INDUS. & INTERNAL TRADE, DRAFT NATIONAL E-COMMERCE POLICY (2019), [https://dpiit.gov.in/sites/default/files/DraftNational\\_e-commerce\\_Policy\\_23February2019.pdf](https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf).

360. Lásd Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (2018. június), <https://perma.cc/T8YZ-9JJ5> (az adatszabadság történetének ismertetése a USA és a közelmúltbeli korlátozások ellen).

Az amerikai vállalatok adatgyűjtési gyakorlata átfogó szövetségi adatvédelmi és kiberbiztonsági jogszabályok hiányában. A következőkben két kulcsfontosságú szempontra összpontosítunk, amelyek megmagyarázzák a fejlődő országok növekvő keresletét a kínai digitális infrastruktúra és az adatkezelés kínai megközelítése iránt - az adatszuverenitás és a digitális fejlődés kettős ígérete -, miközben feltárjuk a benne rejlő ellentmondásokat is. Mindezek alapján óva intünk a digitális infrastruktúrák megfelelő jogi infrastruktúrák nélküli kiépítésétől.

#### A. Az adatszuverenitás vonzereje és korlátai

Az adatszuverenitás különböző változataira hivatkoztak az Egyesült Államokban élő indián törzsek, az innovatív városi adatkezelési projektek <sup>361</sup>támogatói az Európai Unióban, India fejlődő digitális ipari vállalkozásainak <sup>362</sup>képviselői <sup>363</sup>és mások. A kifejezés ilyen sokszínű mobilizálása nem meglepő, mivel az adatszuverenitás az alul-specifikált fogalmak elemeit ötvözi. A fogalomnak nincs általánosan elfogadott definíciója. Ennek eredményeképpen a fogalom használatát, vonzerejét és korlátait gondosan meg kell vizsgálni abban a kontextusban, amelyben alkalmazzák.

Kína az adatszuverenitás egy sajátos változatának bajnokaként lépett fel, folytatva a kiberszuverenitásnak az internetirányítási intézményekben való hangoztatását. Ez nem jelenti azt, hogy lineáris fejlődésről lenne szó, mivel a kifejezés kínai használata változóban van, és összefonódik Kína "szuverenitáshoz" fűződő, ellentmondásos történelmi viszonyával.<sup>364</sup> "Kiberszuverenitás".

361. *Lásd pl. Rebecca Tsosie, Tribal Data Governance and Informational Privacy: Constructing "Indigenous Data Sovereignty"*, 80 MONT. L. REV. 229 (2019) (az amerikai őslakos törzsek által az adatszuverenitásnak tulajdonított különböző jelentések és azok következményeinek tárgyalása).

362. *Lásd* DECODE, <https://perma.cc/XTV5-CM5G> (utolsó látogatás: 2020. augusztus 17.) ("A DECODE olyan eszközöket kínál, amelyek segítségével az egyének maguk dönthetnek arról, hogy személyes adataikat magánügyben tartják-e meg, vagy a közjó érdekében osztják meg.")

363. *Lásd*: INDIA KORMÁNYA, MINISZTERIUM AZ ÉPÍTÉSÉRT ÉS AZ INFORMÁCIÓÉRT. TECH., REPORT BY THE COMMITTEE BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK (2020, július), <https://perma.cc/A8EJ-JMN5> (az indiai adatszuverenitásra való hivatkozással kapcsolatos kutatásokat és terveket tárgyalja a fejlődő adattrendek fényében).

364. *Lásd* Rogier Creemers, *China's Conception of Cyber Sovereignty: GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY* 107 (Dennis Broeders & Bibi van den Berg eds., 2020) (megjegyezve Kína szuverenitáskonceptiójának többdimenziós jellegét); MARIA ADELE CARRAL, SOVEREIGNTY IN CHINA, A GENEALOGY OF A CONCEPT SINCE at (1840,72019).

eignty" célja az volt, hogy megkérdőjelezze az Egyesült Államok hegemóniáját az internet irányításában, és visszavágjon a "kiberanarchia" és a "kiberlibertarianizmus" fogalmainak, amelyek azt sugallták, hogy az internet alapvetően nem szabályozható a kormányok által. Az adat-önrendelkezés összhangban van ezekkel az elképzelésekkel, mivel szembeszáll az amerikai szereplők globális dominanciájával az adatgyűjtési kapacitás tekintetében, valamint a határokon átnyúló és országon belüli adatáramlások feletti kormányzati hatalom érvényesítésével. A hangsúly "kiber"-ről "adat"-ra való áthelyezése jelentős, mivel jelzi az adatok kiemelkedő jelentőségének felismerését a huszonegyedik század elején.<sup>365</sup> Az adatok egyszerre jelentenek erőforrást a gazdasági fejlődéshez, különösen a gépi tanulási algoritmusok bemeneti tényezőjeként, és a digitalizált társadalomban a kormányzás eszközeként. Az adatok szuverenitásának kínai számonkérése ezeket az érzéseket tükrözi, és a pártállam társadalmi ellenőrzésre irányuló célkitűzésével ruházza fel őket.<sup>366</sup>

Az adatszuverenitás alapelvei, azaz a kormányzati ellenőrzés, az önrendelkezésen alapuló gazdasági fejlődés és a társadalmi rend jelentős vonzeróval bírnak a világ országai számára, és nem feltétlenül korlátozódnak a nem demokratikus kormányokra. Amennyiben ezek a törekvések korlátozzák a határokon átnyúló adatáramlást, feszültségbe kerülnek az internetnek a globális összekapcsoltságot elősegítő potenciáljával. Ha az adatszuverenitásra hivatkozva ellenőrzik és cenzúrázzák az országokon belüli és országok közötti adatáramlást, akkor az internet egykori felszabadító erejének ígérete szertefoszlik. Az adatszuverenitás ezen kompromisszumai és hátrányai jól ismertek.<sup>367</sup> Ezek azonban valószínűleg nem fogják befolyásolni azokat az országokat, amelyek Kína adatszuverenista politikáját követik, mivel a cél az adatforgalom kormányzati ellenőrzése ökológiai, társadalmi vagy politikai célokból, az adatszuverenitást pedig az adatszuverenitás és az adatbiztonság rovására.

---

(a "Kína által a [szuverenitás] kifejezés kisajátításában és módosításában való közreműködésének magyarázata").

365. Lásd Lizhi Liu, *Az adatpolitika felemelkedése: Digital China and the World*, 56 *STUD. IN COMPAR. INT'L DEV.* 45 (2021) (az adatok összehasonlítása más stratégiai eszközökkel).

366. Lásd a fenti szöveg kíséző megjegyzését 89.

367. Lásd Andrew Keen Woods, *Litigating Data Sovereignty*, 128 *YALE L.J.* 328, 360-66 (2018) (az adatszuverenitás leíró jellegű bemutatása, amely egy terület feletti legfelsőbb ellenőrzés más uralkodóktól független ellenőrzését foglalja magában).

a globális összekapcsolódásra és bizonyos egyéni jogokra gyakorolt negatív externáliákat.<sup>368</sup>

Az is jól érthető, hogy a kiber-felsőjog és ezen keresztül az adatszuverenitás koncepciói, amelyek az adatokat qua adatlokalizáció (újra)territorializálására törekszenek, ahogy Kína teszi, nem illeszkednek jól az internet egymással összekapcsolt autonóm rendszerek architektúrájába.<sup>369</sup> Még Kína kifinomult, határokon átnyúló adatáramlás-ellenőrzési infrastruktúrája sem vezet a fizikai (területek közötti) és a virtuális (hálózatok közötti) határok tökéletes átrendeződéséhez. Azonban sem a kiber-szuverenitás, sem az adatszuverenitás nem igényel ilyen összhangot céljaik eléréséhez.

Valójában a szuverenitás soha nem volt abszolút, és csak különböző mértékben érhető el és gyakorolható, így az államok szuverén egyenlőségét pusztán elvnek, nem a valóság leírásának, ha nem is "szervezett képmutatásnak", de leleplezi.<sup>370</sup> Az adatszuverenitás sem kivétel, és az egyenlőtlen hatalomnak erre a dimenziójára szeretnénk felhívni a figyelmet. Ha igaz az az állításunk, hogy a pekingi hatást a fogadó államok "adatszuverenitásra" irányuló törekvései vezérlik, akkor számolniuk kell az adatszuverenitás eredendő korlátaival egy még mindig összekapcsolt világban. Ahogy Henry Farrell és Abe Newman kimutatta, az összekapcsolt hálózatok olyan kölcsönös függőségi struktúrákat hoznak létre, amelyeket a megfelelő infrastruktúrát irányító fegyverként használhatnak fel.<sup>371</sup> Meghatározzák a "panoptikum-hatást", amely lehetővé teszi a kiterjedt információgyűjtést, és a "fojtópont-hatást", amelynek révén a hálózati hozzáférés megtagadható. Mivel Kína egyre inkább a DSR-en keresztül látja el a digitális infrastruktúrákat, egyre nagyobb mértékben képes kihasználni ezt a fajta infrastrukturális hatalmat. Ez különösen aggasztó az Egyesült Államok szempontjából,<sup>372</sup> mivel

---

368. Lásd Eyal Benvenisti, *Sovereigns as Trustees of Humanity*, AM107. J. INT'L L. 295 (2013) (a szuverenitás olyan felfogása mellett érvelve, amely megköveteli a külső hatások nemzetek felismerését és lehetőség szerint elkerülését).

369. Lásd Milton Mueller, *Against Sovereignty in Cyberspace*, INT'L STUD. REV. (2019) (azzal érvelve, hogy a szuverenitás alkalmazása a kibertérre "nem illik a területhez").

370. STEPHEN D. KRASNER, SZUVERENITÁS: (1999).

371. Henry Farrell & Abe Newman, *Fegyveres kölcsönös függőség*: INT44'L SEC. 42 (2019).

372. Lásd Stephanie Kirchgaessner, *Revealed*: GUARDIAN (2020. december 15.), <https://perma.cc/6S4H-DGWX> (kiemelve a távközlési hálózatok kínai ex-ploitatációjából származó, az Egyesült Államokat fenyegető kockázatokat).

az Egyesült Államok a második világháború óta hegemóniát élvez a globális hálózatok felett. Ez megmagyarázza, hogy az Egyesült Államok miért olyan hajthatatlan az ellenállás megszervezésében a Huawei 5G-bővítésben való részvétele ellen.

A fejlődő országok, például Pakisztán szempontjából azonban a helyzet kevésbé egyértelmű. A fegyveres kölcsönös függőség a digitális infrastruktúrák feletti egyenlőtlen ellenőrzés függvénye. Az alternatív infrastruktúrák létrehozása meghaladja a legtöbb állam kapacitását; még az Európai Unió kilátásai is legfeljebb bizonytalannak tűnnek egy alternatív felhőinfrastruktúra létrehozásában.<sup>373</sup> Ugyanakkor a digitális izolacionizmus aligha vonzó lehetőség, tekintve a digitális átalakulás vélt öko- nomikus, társadalmi és politikai vonzerejét. Ebből következik, hogy a fejlődő országok számára elérhető adatszuverenitás mértékét olyan tényezők határozzák meg, mint technológiai kapacitásuk, gazdasági erejük, valamint jogrendszerük fejlettsége és hatékonysága.

Az adatáramlás feletti kormányzati ellenőrzés nemcsak az adatok feletti területi ellenőrzéstől függ, ami az adatok területi lokalizálásával érhető el, hanem a vonatkozó infrastruktúrát kiépítő, működtető és fenntartó vállalatok feletti hatékony ellenőrzést is igényel. Ez általánosságban igaz az adott vállalat származási országától függetlenül - sőt, a hazai vállalatokra is vonatkozik. Amennyiben a kínai vállalatok a KKP ellenőrzése alatt működnek, amikor külföldön digitális infrastruktúrát biztosítanak, aláássák az adatszuverenitást, amelyre a DSR fogadó államai törekszenek. A kínai állami vállalatok a kínai állam kiterjesztései, még akkor is, ha egyesek saját birodalomként működnek, és így Pekingtől talán autonómabbak, mint mások. Az a kérdés, hogy a névlegesen magánvállalatok követik-e vagy milyen mértékben követik a párt diktátumát, egy élő kérdés, amelyről nem tudunk végleges bizonyítékokkal szolgálni. Egy-egy adat arra utal, hogy egyes cégek bizonyos körülmények között megtagadhatják az adatkérésekhez való hozzáférést.<sup>374</sup> Mindazonáltal a kínai vállalatok jogi szolgáltatóival végzett kezdeti terepmunka során a kínai vállalatoknak nyújtott

---

373. Lásd GAIA-X, <https://perma.cc/2DBB-9B8J> (utolsó látogatás: 2020. augusztus 17.) (egy európai adatinfrastruktúra-projekt bemutatása).

374. Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE (Apr. 20202.), <https://perma.cc/YQ4W-8UW5> (példák a Didi, Tencent és Alibaba kínai vállalatokra, amelyek visszautasították a kormányzati adatkéréseket).

A feltörekvő gazdaságokban tapasztalható fejlődés azt sugallja, hogy még a magáncégeknek is gyakorolniuk kell az úgynevezett "utánzási tudatosságot" (*kanqi yishi*), vagy ahogy egy beszélgetőpartner fogalmazott: "igazodjatok a vezérekhez, a Legfelsőbbhöz, Xi elnökhöz".<sup>375</sup> A kínai technológiai vállalatok, akárcsak más iparágak kínai vállalatai, folyamatosan tárgyalásokat és kompromisszumokat kötnek a szabályozó hatóságokkal és a párt tisztviselőivel, akik újrarajzolhatják a megengedett vállalati magatartást meghatározó vörös vonalakat.

A fejlődő országok valószínűleg tisztában vannak ezekkel a tényezőkkel, mégis egyre nagyobb az igényük a kínai digitális infrastruktúra iránt. A pekingi hatás ebben a tekintetben az Egyesült Államok által biztosított digitális infrastruktúra csökkenő vonzerejének függvénye. A Snowden-nyilatkozatok megingatták az Egyesült Államokba, mint a szabad adatáramlás globális intézőjébe vetett bizalmat. Az amerikai technológiai vállalatok (legalábbis eddig) viszonylag nagyfokú szabadságot élveztek globális működésük során; egyesek még arra is törekedtek, hogy semleges "digitális svájci országgént" pozicionálják magukat.<sup>376</sup> Mégsem menekülhetnek meg a hazai joghatóságuk követelése elől, akár a CLOUD-törvény szerinti transznacionális adatkérésekhez való hozzáférés formájában, akár az amerikai nemzetbiztonsági ügynökségek rendelkezésére álló egyéb eszközökkel. Ráadásul globális dominanciájuk - amellyel csak a kínai vállalatok vetekednek - és szemérmetlen adatéhségük aggodalomra ad okot a kapitalizmus gyarmatosító mintáinak folytatásaként történő adatszerzéssel kapcsolatban.<sup>377</sup> A pekingi hatás elleni legjobb stratégia vitathatatlanul az, hogy a kínai digitális infrastruktúra relatív vonzerejét olyan alternatívák biztosításával csökkentjük, amelyek megfelelnek a fogadó államok igényeinek, miközben a bizalom helyreállítása érdekében hiteles jogi és technológiai biztosítékokat hozunk létre a panoptikum és a fojtópont hatásaival, valamint a felügyeleti kapitalizmus túlkapásaival szemben. Ilyen ellenstratégiák hiányában az adatszuverenitás és a digitális fejlődésben érdekelt fogadó államok az amerikai digitális infrastruktúrával szemben a kínaiakat részesíthetik előnyben.

---

375. Kínai vállalatok külföldi ügyleteiben segítő ügyvéd e-mailje a szerzőnek (20207., ápr.).

376. Kirsten Eichensehr, *Digital Switzerlands*, 167 U. PENN. L. REV. 665 (2019).

377. *Hasonlítsuk össze NICK COULDRY & ULISES ALI MEJIAS, THE COSTS OF CONNECTION: HOW DATA IS COLONIZING HUMAN LIFE AND APPROPRIATING IT FOR CAPITALISM* (2019) (a folytonosságot hangsúlyozva), és SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* (2020) (kiemelve a surveillance capitalism és a kapitalizmus korábbi formái közötti különbségeket).

### B. *A digitális selyemút és a digitális fejlődés*

A pekingi hatás második fő hajtóereje a digitális fejlődés ígérete. A Világbank és más fejlesztési szervezetek kulcsfontosságú támogatói voltak a gazdaságok technológiai innováción, hozzáférhető digitális infrastruktúrán, valamint nyílt és egyetemes kormányzati kereteken keresztül történő átalakításának.<sup>378</sup> A BRI-n keresztül, amely alapvetően egy fejlesztési projekt és különösen a DSR révén a kínai pártállam és a kínai vállalatok a digitális fejlődés saját verzióját kínálják. Ez az út a digitális infrastruktúra hozzáférhetővé tételétől függ, miközben az adatok feletti ellenőrzés névlegesen a fogadó kormányzatnál összpontosul. Az adatáramlás feletti kormányzati ellenőrzés megmaradása feszültségben áll az adatok "szabad áramlását" hangsúlyozó fejlesztési modellekkel,<sup>379</sup> de a Kínai Népköztársaság digitális gazdaságának sikeres fejlesztése hitelt ad a DSR gazdasági növekedést lehetővé tevő ígéretének. Különösen a kínai e-kereskedelmi platformokat emlegetik a kkv-k számára fontos infrastruktúrákként.<sup>380</sup>

Nem tudjuk felmérni a DSR gazdasági hatását általánosságban vagy különösen az olyan országokra, mint Pakisztán, de a jog és a fejlődés szempontjából óvatosságra intünk. Általános megfigyelésként elmondható, hogy a pekingi hatás eltérő hatással lehet a fogadó állam jogfejlődésére. Egyfelől elképzelhető, hogy a jobb digitális infrastruktúra katalizálhatja a jogi infrastruktúrákhoz való hozzáférést, ahogyan a digitális fejlődés a piacokhoz való hozzáférést is.<sup>381</sup> Például az e-kereskedelemben a költségghatékony online vitarendezés jobban védheti a fogyasztók jogait, mint az offline analógok. Az egyre automatizáltabbá váló

378. *Lásd: Digital Development*, WORLD BANK, <https://perma.cc/C8NX-BCBL> (utolsó megtekintés: 2020. augusztus 17.) (a "globális digitális szakadék megszüntetésére" irányuló erőfeszítések leírása).

379. *Lásd James Manyika et al., Digitális globalizáció: A globális áramlások új korszaka*, MCKINSEY DIGIT. (2016. február 24.), <https://perma.cc/2CK8-DSRT> (az adatok szabad áramlásának gazdasági előnyeit ismertetve); Martina Ferracane & Erik van der Marel, *Do Data Policy Restrictions Inhibit Trade in Services?* (Eur. Ctr. for Int'l Pol. Econ, DTE Working Paper No. 2, 2018) ("A szigorú adatpolitikák negatívan és jelentősen befolyásolják az adatintenzív szolgáltatások importját.").

380. *Lásd WORLD BANK & ALIBABA GRP., E-COMMERCE DEVELOPMENT: EXPERIENCE FROM CHINA* (2019), <https://perma.cc/RQS7-KXR4> (a Taobao Villages jótékony hatásainak méltatása).

381. *Lásd GILLIAN HADFIELD, RULES FOR A FLAT WORLD 9* (2016) (amely szerint az elavult jogi infrastruktúrákat a digitális technológiák felhasználásával kellene felváltani).

a jogi szolgáltatások iránti igényt megváltoztathatják. Összességében a digitális ellátási láncok magánirányítási rendszerei összekapcsolhatják a gazdaságokat és csökkenthetik a belépési korlátokat.<sup>382</sup> A jog és a technológia integrációja a digitális infrastruktúrára építve az egyik olyan "alternatív fejlesztési stratégiát" jelentheti, amelyet David Trubek, a jog és a fejlődés tanulmányozásának egyik alapítója már régóta keres.<sup>383</sup>

A fentiek ellenére megkérdőjelezzük Kína adatvezérelt fejlesztési stratégiájának megvalósíthatóságát, és óva intünk a megfelelő biztosítékok nélküli digitális átalakulástól. Úgy tűnik, hogy a pekingi hatást jelentős mértékben az a vágy ösztönzi, hogy Kína erősen digitalizált gazdaságra való átállását utánozzák. Ebben az összefüggésben fontos szem előtt tartani a Kínai Népköztársaság egyedi jellemzőit, különösen a hatalmas fogyasztói bázist, amely lehetővé teszi egy olyan digitális ökoszisztéma kialakítását, amely a külföldi vállalatoktól viszonylag nagyfokú függetlenségre törekszik, és a Kínán belül működni engedett vállalatokat szabályozási kényszerzubbony alá helyezi. Egyesek a kínai digitális gazdaság viszonylag gyors növekedését a jog hiányának tulajdonítják, különösen a szellemi tulajdonjogok érvényesítésének tekintetében, ami állítólag lehetővé tette a gyilkos versenyt, az innovációt és a növekedést.<sup>384</sup> Bár ez hitelt adhat azoknak, akik bírálták az erős szellemi tulajdonvédelem gazdasági fejlődésre gyakorolt hatását, téves lenne Kína gazdasági sikerét elszigetelten ennek az elemnek tulajdonítani. Az öko- nomikus fejlődés mindig összefonódik a különböző jogi struktúrákkal.<sup>385</sup> A Kínai Népköztársaságon belül a kínai vállalatok olykor "kínai stílusú" törvényhozáshoz folyamodtak azáltal, hogy a jogszabálysértő jogszabályok érvényesítésével

---

382. ENSZ-KONFERENCIA. ON TRADE & DEV., DIGITAL ECONOMY REPORT 2019, 130. o. (2019) (példaként említve, hogy a digitális gazdaság hogyan tette képessé a haitiai nők mikrovállalkozásait).

383. David M. Trubek, *A "jogállamiság" a fejlesztési támogatásban: Múlt, előzmények és jövő*, in: AZ ÚJ JOG ÉS A GAZDASÁGI FEJLŐDÉS (74, David 93 M. Trubek & Alvaro Santos szerk., 2006).

384. Lásd Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563, 1564 (2018) (azzal érvelve, hogy a Taobaóhoz hasonló pri- vátnak szereplők alkotják a saját jogukat Kínában).

385. Lásd általában Jedediah Britton-Purdy et al., *Building a Law-and-Political- Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784 (2019) (a jogi tudományosság új jog- és politikai gazdaságtani megközelítését javasolja).

a szerződések megkötése, a viták rendezése és a csalások megelőzése a szilárd állami jogrendszer hiányában.<sup>386</sup> De nem tudják egyszerűen lemásolni az önkormányzatiság ezen jellemzőit külföldön. A pakisztáni példával élve, bár az adatkezelésre vonatkozó pakisztáni törvények még kialakulóban vannak, a pakisztáni piac nem a normák sivataga. Vannak állami és nem állami szereplők, akik aktívan alakítják a szabályokat, legyenek azok jogilag kötelezőek vagy informálisak. A fogadó országok politikai-gazdasági ökoszisztémája - néha jelentősen - eltér a kínai szereplők által megszokottól, és ez hatással van a kínai növekedési történet megismételhetőségére.

Sok tinta folyt már a múltbeli gazdaságfejlesztési erőfeszítések általános hibáiról, valamint a kialakult fejlesztési intézmények által létrehozott és jogi eszközökben, például kétoldalú beruházási szerződésekben vagy hitelfeltételekben rögzített függőségekről.<sup>387</sup> A pekingi hatás azonban aggodalomra ad okot egy másfajta függőséggel kapcsolatban, amelyet a digitális infrastruktúrák viszonylag gyors létrehozása okoz a megfelelő jogi keretek hiányában. Miközben nagy figyelmet kell fordítani azokra a jelentős társadalmi és politikai költségekre, amelyeket a digitális infrastruktúrák okozhatnak, például amikor lehetővé teszik a kormányzati ellenőrzési keretek megszűnését, a gazdasági fejlődés szempontját is figyelembe kell venni. Ha a fejlődő országok olyan digitális gazdaságra térnek át, amely a kínai digitális infrastruktúrára támaszkodik anélkül, hogy megfelelő jogi keretek (például az adózás tekintetében) biztosítanák a társadalmi előnyök kiaknázását, a digitális fejlődés inkább súlyosbíthatja, mint enyhítheti az országokon belüli egyenlőtlenségeket, mivel a digitális átalakulás nyerteseket és veszteseket hoz létre. Az a tény, hogy a nyugati társadalmak éppen ezzel a problémával küzdenek, nem bizakodásra ad okot, hanem még sürgetőbbé teszi a kérdést.

## VI. KÖVETKEZTETÉS

A koronavírus világvilágjárvány fordulópontot jelent a

---

386. Liu & Weingast, *supra* note at 384,1565.

387. *Lásd pl.* WILLIAM EASTERLY, *THE WHITE MAN'S BURDEN: WHY THE WEST'S EFFORTS TO AID THE REST HAVE DONE SO MUCH ILL AND SO LITTLE GOOD* (2006); DAMBISA MOYO, *DEAD AID: MIÉRT NEM MŰKÖDIK A SEGÉLYEZÉS, ÉS HOGYAN VAN JOBB ÚT AFRIKA SZÁMÁRA* (2010); GILBERT RIST, *A FEJLESZTÉS TÖRTÉNETE: A NYUGATI EREDETEKTŐL A GLOBÁLIS HITIG* (2006); SARA LORENZINI, *GLOBAL DEVELOPMENT: A HIDEGHÁBORÚ TÖRTÉNETE* (2019).

az adatok globális irányítása.<sup>388</sup> A világ alkalmazkodik, egyre inkább függ a digitális technológiáktól, hogy virtuális környezetben folytathassa üzleti tevékenységét. Következésképpen az adatáramlás a globális gazdaság létfontosságúvá válik, és egyre nagyobb az igény a digitális infrastruktúrák iránt, valamint a digitális infrastruktúrákra való támaszkodás. Ezen okok miatt az, amit mi pekingi hatásként próbáltunk megfogalmazni, valószínűleg növekedni fog, legalábbis a közeljövőben. Amint azt ebben a cikkben megállapítottuk, Kína jelentős hatást gyakorol a nemzetek közötti adatkezelésre. Ez a hatás nem annak a következménye, hogy Kína egy bizonyos modellt exportál, és nem is a brüsszeli hatáshoz hasonló dinamika, amely szerint a vállalatok az európai jog felé vonzódnak. Inkább a digitális infrastruktúra iránti kormányzati igény és annak következményei, nevezetesen az adatszuverenitás, de általában véve a gazdasági fejlődés és a társadalmi rend iránti igény az, ami Kína felemelkedését a globális adatkezelésben hajtja.

Mégis korai lenne megjósolni, hogy Kína adatkezeléssel kapcsolatos megközelítése, más országok által történő utánzása és az ilyen fejleményekre adott nyugati válaszok az In- ternet különböző "adatbirodalmakra" "törrik".<sup>389</sup> A globális kommunikációs infrastruktúrákért folytatott geopolitikai harcok nem új keletűek, és az összekapcsolhatóság fenntartása mellett szóló gazdasági érvek túlsúlyosak. A különbségek ellenére Kína, az Európai Unió és az Egyesült Államok megközelítései fontos közös vonásokat mutatnak, és így nem zárják ki egymást. A fejlődő országok nehéz döntések előtt állnak. Bár nem tudnak megmenekülni a pekingi hatástól, és nem érhetik el az adatfelügyeletet anélkül, hogy lemondanának a digitális fejlődésben rejlő lehetőségekről, képesek lehetnek fedezni, azaz háromszögbe rendezni a digitális nagyhatalmakkal való kapcsolatukat. Amint azzal érveltünk, a digitális fejlesztési stratégia olyan jogi keretek megfelelő fejlesztését igényli, amelyek a digitális átalakulást a társadalom számára előnyös irányba terelik.

---

388. Lásd Kathleen R. McNamara & Abraham L. Newman, *The Big Reveal: COVID-19 and Globalization's Great Transformations*, 74 INT'L ORGS. 1, 13-15 (2020) (azt állítva, hogy a világjárvány aláhúzta a digitális technológiák fontosságát).

389. Lásd Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: J. INT'L ECON: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT'L ECON. L. 245 (2018) (azt állítva, hogy az Egyesült Államok, az EU és Kína három elkülönült adatbirodalmat hozott létre, eltérő adatkezelési megközelítésekkel).