Tölgyesi Beatrix

Az orosz „szuverén internet” törvényről[1]

A tanulmány a 2019 novemberében hatályba lépett orosz szuverén internetről szóló törvényt elemezve ismerteti a törvény előzményeit, a törvénnyel kapcsolatos, az ellenzék, az államapparátus, a szakértők és az üzleti szereplők soraiból érkező kritikákat, a megvalósíthatóság gyakorlati korlátait, illetve a szabályozás lehetséges következményeit. Ezen túlmenően bemutatja orosz médiatörvénynek az online tartalmak cenzúrázása felé mutató módosítását is. Ezek alapján arra a következtetésre jut, hogy a jogi szabályok változása – bár az indoklás szerint a külső fenyegetések elhárítására irányul – lehetővé teszi a társadalmi elégedetlenség hatékonyabb kontrollálását, és ezáltal a jelenlegi vezetés hatalombirtoklásának biztosítását.

Kulcsszavak: *Oroszország, internet, kiberbiztonság, információs hadviselés, online cenzúra*

Tölgyesi Beatrix: About the Russian “Sovereign Internet” Law

By analysing the Russian sovereign Internet law, which came into force in November 2019, the study presents the history of the law, criticisms from the opposition, the state apparatus, experts and business, the practical limitations of feasibility and the possible consequences of the regulation. It also presents an amendment to Russian media law to censor online content. On this basis, the study concludes that the change in legal regulations, while arguably aimed at countering external threats, allows for more effective control of social dissatisfaction and thus secures the grip on power of the current establishment.

Keywords: *Russia, Internet, cybersecurity, information warfare, online censorship*

Bevezetés

A 2019. november 1-jén hatályba lépett, az orosz „szuverén internetről” szóló törvény[2] számos kommentárt és kritikát generált, amiben ellentmondásos céljai és felhasználási lehetőségei mellett szerepe lehetett annak is, hogy a „Kínai Nagy Tűzfal” mellett az egyik első olyan próbálkozásról van szó, amely az internet állami felügyelet alá vonására irányul. A jogszabály lényege az internetforgalom nemzeti útválasztási rendszerének és egy központi felügyeleti rendszernek a létrehozása abból a célból, hogy megvédje az oroszországi internet épségét abban az esetben, ha az Amerikai Egyesült Államok (a továbbiakban: Egyesült

[1] Ez a cikk a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal 129243-as számú, „*Hagyomány és rugalmasság Oroszország biztonság- és védelempolitikájában*” című kutatási pályázatának támogatásával valósult meg.

[2] Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи” и Федеральный закон „Об информации, информационных технологиях и о защите информации”, [online], 2019. 05. 01. Forrás: Pravo [2020. 03.25.]

Államok, USA) megkísérelné azt „lekapcsolni" a nemzetközi hálózatról.[3] Ebbéli aggodalmukat az USA 2018-ban elfogadott Nemzeti Kiberbiztonsági Stratégiájára *(National Cyber Strategy)*[4] alapozzák, amely kilátásba helyezi a kibertér felhasználását támadóműveletekhez. (Eközben az amerikai stratégia mindössze a kibertérben fellelhető fenyegetések felderítéséről, megakadályozásáról és legyőzéséről beszél.[5])

Az alábbiakban a jogszabály tartalmának bemutatásán túlmenően ismertetem a törvény előzményeit, a törvénnyel kapcsolatos, az ellenzék, az államapparátus, a szakértők és az üzleti szereplők soraiból érkező kritikákat, a megvalósíthatóság gyakorlati korlátait, illetve a szabályozás lehetséges következményeit.

Előzmények

Az a törvény, amelynek módosításai képezik az úgynevezett „szuverén internet" törvényt, 2003-ban született, így értelemszerűen az internetforgalom szabályozásával kapcsolatos passzusok későbbi módosítások révén kerültek bele. Az internet oroszországi szabályozásának a 2011–2013 során folyó kormányellenes tüntetések adtak ösztönzést, ahol – a „színes forradalmakhoz" hasonlóan – az internetes aktivizmus és a közösségi oldalak fontos szerepet játszottak.

Az internet orosz cenzúrája 2012 óta elsősorban a Roszkomnadzor (Szövetségi Kommunikációs, Információs Technológiai és Tömegkommunikációs Felügyeleti Szolgálat) által fenntartott központosított „feketelista", az úgynevezett Tiltott Honlapok Egységes Nyilvántartása által valósult meg. Ezen a feketelistán főként olyan honlapok, domainnevek és IP-címek szerepelnek, amelyek a kábítószerrel való visszaélést és a kábítószer-előállítást propagáló anyagokat, az öngyilkossági módszerek leírását és gyermekpornográfiát tartalmaznak. Később módosították annak érdekében, hogy lehetővé tegyék a szélsőséges kategóriába sorolt anyagok blokkolását azáltal, hogy felveszik azokat a szélsőséges anyagok szövetségi listájára.[6] Az úgynevezett „Lugovoj-törvény" pedig lehetővé teszi a közrendet veszélyeztető, tömeges rendbontásra és extremista tevékenységre buzdító anyagokat tartalmazó weboldalak blokkolását a főügyész kezdeményezésére, bírósági döntés nélkül, az internetszolgáltatók Roszkomnadzor általi megkeresésén keresztül. Egyes

---

[3] A „lekapcsolásra" elrettentő példaként a szíriai internet 2012. november 29-ei lekapcsolását hozták fel, amellyel azonban a szír hatóságok a terroristákat gyanúsították. Andrew Quinn – Cynthia Osterman: U.S. says Syrian opposition can skirt Internet shutdown, [online], 2012. 11. 29. Forrás: Reuters [2020. 03. 25]. Edward Snowden verziója szerint viszont az NSA hackerei megkíséreltek beavatkozni az egyik fő szíriai internetes szolgáltató útválasztójába azzal a céllal, hogy hozzáférjenek az ország nagy részén folyó e-mailes és egyéb internetes forgalomhoz. De valami baj történt, és az útválasztót működésképtelenné tették. James Bamford: Edward Snowden: The Untold Story, [online], 2014. 08. 13. Forrás: Wired [2020. 03. 25.]

[4] National Cyber Strategy of the United States of America, [online], 2018. Forrás: The White House [2020. 03. 25.]

[5] John Bolton: „For any nation that's taking cyber activity against the United States, they should expect […] we will respond offensively as well as defensively"; Kevin Liptak: John Bolton: US is going on the offensive against cyberattacks, [online], 2018. 09. 20. Forrás: CNN Politics [2020. 03. 25.]
„All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States." National Cyber Strategy of the United States of America: *i. m.*

[6] Paul Goble: FSB Increasingly Involved in Misuse of 'Anti-Extremism' Laws, SOVA Says, [online], 2015. 03. 29. Forrás: The Interpreter [2020. 03. 25.]

vélemények szerint[7] 2012 közepétől kezdve ezekkel a rendeletekkel gyakran visszaéltek a szövetségi kormány vagy a helyi közigazgatás kritikájának megakadályozása érdekében. A tömegtájékoztatás szabadságával való visszaélést tiltó törvény alapján online médiumokat zártak be.[8] 2019 márciusában elfogadtak egy törvényjavaslatot, amely pénzbírságot vezetett be azok számára, akik (a kormány szerint) „hamis híreket" terjesztenek és „az állami hatóságokkal szemben nyilvánvaló tiszteletlenséget mutatnak".[9]

Ide tartozik továbbá a Jarovaja-törvény,[10] amely lehetővé teszi a Szövetségi Biztonsági Szolgálatnak (a továbbiakban: FSZB), hogy az internetes társaságoktól információt kérjen a felhasználói forgalom dekódolására. Ezt 2016-ban nemzetbiztonsági és terrorizmusellenes intézkedésként fogadták el.[11] A szabályozás arra kötelezi a távközlési szolgáltatókat, hogy az Orosz Föderáció kormánya által meghatározott ideig (de legfeljebb 6 hónapig) tárolják az előfizetők hívásait és üzeneteit, valamint az üzenetek és hívások fogadásának, továbbításának, kézbesítésének és feldolgozásának tényeire vonatkozó információkat pedig három évig. Az internetes cégek és szolgáltatók kötelesek tárolni és a titkosszolgálatok rendelkezésére bocsátani az alábbi adatokat: felhasználónév, születési idő, lakcím, név, köznév, személyazonossági okmány adatai, a felhasználó által beszélt nyelvek, rokonai listája, üzenetek szövege, audio- és videófelvételek, e-mail-cím, dátum, valamint a felhasználói hitelesítés és az információs szolgáltatásból való kilépés ideje, az ügyfélprogram neve. A kormány 2018. április 12-ei rendelete alapján 2018. október 1-jétől a távközlési szolgáltatóknak 30 napig kell szöveget, hangot, videót és egyéb felhasználói üzeneteket tárolniuk. Ezenkívül a szolgáltatóknak évente 15%-kal kell növelniük a tárolást.

A cikk tárgyát képező, legújabb szabályozás[12] elfogadását megelőzően több éven keresztül folyt a szakértői egyeztetés egy olyan törvénytervezettel kapcsolatban, amelynek célja az orosz internet biztonságának szavatolása. (Az orosz nyelvű szövegekben általában Runetnek nevezik az internet oroszországi, illetve a nagyrészt a szovjet utódállamokban használt, orosz nyelvű szegmensét.) 2014 szeptemberében kezdődött az egyeztetés több orosz távközlési szolgáltató, internetes társaság és nonprofit szervezet munkatársai részvételével, illetve a Szövetségi Biztonsági Tanács ülésén is tárgyalták a témát, amelynek lényege az ország leválasztásának lehetősége a globális internetről rendkívüli helyzet esetén.

---

7 Marija Kravcsenko: Неправомерное применение антиэкстремистского законодательства в России в 2014 году, [online], 2015. 03. 28. Forrás: Polit.ru [2020. 03. 25.]
Examples of forbidden content, [online], é. n. Forrás: Запрещено в России [2020. 03. 25.]

8 Freedom House: Freedom on the Net 2016 – Russia, [online], 2016. 11. 14. Forrás: Refworld [2020. 03. 25.]

9 Путин подписал законы о фейкньюс и неуважении к власти, [online], 2019. 03. 18. Forrás: Vedomosztyi [2020. 03. 25.]

10 Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», [online], 2016. Forrás: Consultant [2020. 03. 25.]
Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»,[online], 2016. Forrás: Wikisource [2020. 03. 25.]

11 Alekszandra Prokopenko: What's Behind Russia's New Offensive Against the Internet Economy?, [online], 2019. 08. 12. Forrás: Carnegie Moscow Center [2020. 03. 25.]

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

Előtte júliusban a Biztonsági Tanács a Távközlési Minisztériummal és az FSZB-vel együtt gyakorlatokat hajtott végre, amelyek célja az oroszországi internet stabilitásának tesztelése volt, illetve a jogsértések megakadályozása barátságtalan „célzott cselekvések" esetén.[13] Egy titkosszolgálati tisztviselő szerint a Kommunikációs és Médiaügyi Minisztérium által végzett gyakorlatok bebizonyították, hogy a Runet sebezhető, és meg fogják vitatni a kockázatok minimalizálására irányuló intézkedéseket, ideértve a Runet külvilágról való ideiglenes leválasztásának lehetőségét is.[14] Később szinte minden évben megismételték a gyakorlatokat.[15] A *Vedomosztyi*nak nyilatkozó egyik illetékes szerint vészhelyzetnek tekinthetők a katonai műveletek, de az országban zajló komoly tüntetések is. (Analogikus intézkedésként említhető meg, amikor a 2011-es egyiptomi zavargások alatt a hatóságok az ország egész területén kikapcsolták az internetet és a mobilkommunikációt, de később Oroszországban – Ingusföldön – is volt példa hasonló intézkedésre.) Egy másik ötlet volt, hogy az orosz állam átvenné az orosz domainnevek felügyeletét, amelyet az ICANN-nel *(Internet Corporation for Assigned Names and Numbers)* együttműködő Nemzeti Internetdomain Koordinációs Központ nevű nonprofit szervezet *(*Координационный центр национального домена сети *Интернет)* kezel, amelynek igazgatótanácsában a Távközlési Minisztérium képviselője is jelen van. Az ICANN nevű, elsősorban a domainnevek nyilvántartásával foglalkozó szervezet akkoriban még az Egyesült Államok Kereskedelmi Minisztériuma alá rendelt Nemzeti Telekommunikációs és Információs Igazgatóság felügyelete alá (*National Telecommunication and Information Administration* – NTIA) tartozott, azóta viszont 2016-ban megszüntette szerződését az amerikai állammal, és belépett a magánszektorba.

Az ötlet felmerülésének időpontját nem nehéz összefüggésbe hozni a 2011–2013 közötti oroszországi parlamenti választásokat követő, nagyrészt az interneten szervezett tiltakozóakciókkal.

A javaslat szerzői megjegyezték, hogy nem akarnak saját internetet létrehozni, az új szabályozás kizárólag „duplikált infrastruktúra" kialakítására vonatkozik.[16]

2016 novemberében a Távközlési Minisztérium közzétette a törvénytervezet első verzióját, amelyet nemcsak az informatikai szakértők bíráltak, hanem különböző állami hivatalok is, különösen a Pénzügyminisztérium és a Gazdaságfejlesztési Minisztérium, ezért azt nem nyújtották be az Állami Dumának. A Biztonsági Tanács azonban 2017 novemberében utasította a minisztériumot, hogy nyújtsák be újból. A törvényjavaslat kidolgozásával éveken át foglalkozott Alekszej Szokolov kommunikációsminiszter-helyettes, aki korábban az FSZB-nél szolgált.[17]

2016. december 29-én German Klimenko, Putyin elnök tanácsadója az internetes ügyekben bejelentette, hogy védelmi forgatókönyveket kell kidolgozni az Oroszország, az Egyesült Államok és az Európai Unió országai közötti külpolitikai kapcsolatok további

---

[13] Охранник суверенного Рунета, [online], 2019. 11. 27. Forrás: Meduza [2020. 03. 25.]

[14] Совет безопасности обсудит отключение России от глобального интернета, [online], 2014. 09. 19. Forrás: Vedomosztyi [2020. 03. 25.]

[15] Охранник суверенного Рунета: *i. m.*

[16] Закон об автономном Рунете не ставит задачу создать „свой интернет", [online], 2018. 12. 14. Forrás: Rosszijszkaja Gazeta [2020. 03. 25.]

[17] Охранник суверенного Рунета: *i. m.*

romlása esetén. Nagyon magasnak értékelte Oroszország leválasztásának valószínűségét a globális internetről. Felhívta a figyelmet arra, hogy „Oroszország nyugati partnerei leválasztották a Krímet a Google és a Microsoft szolgáltatásairól". (Miután az Egyesült Államok és az Európai Unió 2014-ben szankciókat vezetett be a Krím ellen, olyan nagyvállalatok, mint az Amazon, az eBay, a GoDaddy és a Paypal, beszüntették tevékenységüket a félszigeten, az AppStore alkalmazásbolt leállt, a HP és a Dell pedig felfüggesztette termékei szállítását a területre.[18]) A kritikus infrastruktúrának, beleértve a domainzóna másolatát is, orosz területen kell lennie, hogy senki se tudja leválasztani; az átlagfelhasználókat viszont nem fogja érinteni a törvény.[19] Szintén 2016 decemberében az FSZB bejelentette, hogy külföldi hírszerző ügynökségek számos kibertámadást készítenek elő Oroszország pénzügyi rendszerének destabilizálása érdekében. A Rosztelekom megerősítette ezt az információt, és hozzátette, hogy visszaverte az öt legnagyobb bank és pénzügyi szervezet elleni támadásokat. Az állítólagos akciók irányítóközpontjai Hollandiában voltak, és a BlazingFast ukrán vállalat tulajdonában álltak. (Érdekes, hogy éppen az MH17 2014-es katasztrófájában érintett két országról van szó.) Az FSZB szerint a több tucat orosz várost is érintő akciót tömeges sms-küldés és közösségi hálókon és blogokon való tömeges posztolás is kísérte volna, amelyben provokatív információkat terjesztettek volna az orosz pénzügyi rendszerről, vezető bankok fizetésképtelenségéről és a rubel árfolyamának zuhanásáról.[20] Hozzá kell azonban tenni, hogy számos országot ért már hasonló kibertámadás (a legismertebb példa talán a 2007-es észtországi, amikor a külföldi hackereknek valóban sikerült is megbénítaniuk számos intézmény holnapját), azonban ez máshol nem váltott ki az oroszországihoz hasonló, a nemzeti hálózat állami kontrollálására irányuló törekvéseket.

2017 közepén megjelent a tervezet frissített változata, amelyben javaslatot tettek arra, hogy korlátozzák a külföldiek 20%-os részvételét azon vállalatok tőkéjében, amelyek Oroszországban forgalomcsere-pontokkal rendelkeznek. A szakértők és a piaci szereplők bírálták ezt a javaslatot.[21]

2019 áprilisában Leonyid Levin képviselő, az Állami Duma illetékes bizottságának elnöke a NetBlocks civil szervezet kalkulátorára hivatkozott, amelynek segítségével kiszámolta, hogy az orosz gazdaságot naponta 20 milliárd rubel kár érné, ha lekapcsolnák az internetről, és ezzel támasztotta alá az orosz internet állami ellenőrzés alá vonásának szükségességét. A törvénytervezet végrehajtására fordított összeget 20–30 milliárd rubelre becsülte.[22]

Egy másik, a Runet irányítására irányuló kezdeményezés a Szövetségi Biztonsági Tanácstól érkezett, amely 2017 őszén utasította a Távközlési Minisztériumot és a Külügyminisztériumot, hogy a BRICS-együttműködés keretében vitassák meg egy saját rendszer létrehozásának lehetőségét, amely domainnevek gyökérszervereinek másolatait

---

[18] Клименко допустил отключение России от «мирового интернета», [online], 2016. 12. 29. Forrás: Dozsgy [2020. 03. 25.]

[19] Клименко: Россия должна быть готова к отключению от мирового интернета, [online], 2016. 12. 29. Forrás: TASS [2020. 03. 25.]

[20] ФСБ узнала о подготовке кибератак на финансовую систему России, [online], 2016. 12. 20. Forrás: RIA Novosztyi [2020. 03. 25.]

[21] Anna Balasova – Jevgenyija Kuznyecova – Alekszandra Poszipkina: РФ и точка: какие риски несет проект о суверенном Рунете, [online], 2018. 12. 15. Forrás: RBC [2020. 03. 25.]

[22] В Госдуме оценили потери российской экономики в случае отсутствия интернета, [online], 2019. 04. 11. Forrás: TASS [2020. 03. 25.]

tartalmazná, és amely – független lévén az ICANN, az IANA és VeriSign nemzetközi szervezetek irányításától – összeomlás vagy célzott behatás esetén képes kiszolgálni ezen országok felhasználóinak kéréseit. Ennek az utasításnak a végrehajtásáról azonban nem adtak tájékoztatást.[23]

A törvénymódosítás

A közbeszédben „szuverén internet" törvényként[24] elhíresült rendelkezés valójában a távközlésről szóló 2003. évi szövetségi törvény módosítása.[25] A 2019. április 16-án az Állami Duma által elfogadott, április 22-én a Szövetségi Tanács által jóváhagyott és május 1-jén az elnök által aláírt törvénymódosítás legfontosabb elemei a következők:

- a távközlési szolgáltatók kötelesek állami tulajdonban lévő berendezéseket telepíteni az országon belüli forgalom elemzése és szűrése céljából (mély csomagok ellenőrzése; DPI – Deep Pocket Inspection[26]) a forgalomcserélő pontokra és az orosz határt átlépő kommunikációs vonalakra; (a forgalomcsere-pontok működésének biztosítására vonatkozó követelményeket a Távközlési Minisztérium határozza meg az FSZB-vel egyetértésben);
- a távközlési szolgáltatóknak nyilvántartásba kell venniük ezeket a pontokat, és kizárólag ezeket szabad használniuk;
- a Roszkomnadzor végrehajtja a Runet „központosított irányítását" („az Internet valamint az Orosz Föderáció területén működő nyilvános kommunikációs hálózat stabilitását, biztonságát és integritását fenyegető veszélyek fennállása esetén"; 65. § 2. bek.);
- a Roszkomnadzor korlátozza az Oroszországban betiltott internetes oldalakhoz való hozzáférést (eddig ezt a szolgáltatók végezték);
- gyakorlatokat folytatnak az eljárások ellenőrzésére;
- nemzeti domainnév-rendszert és -nyilvántartást hoznak létre (2021. január 1-jéig).

Lényeges még kiemelni, hogy „azoknak a kommunikációs eszközöknek, amelyekkel a centralizált irányításban részt vevő személyek utasításokat hajtanak végre egy nyilvános kommunikációs hálózat központosított irányítása keretében, az Oroszországi Föderáció területén kell elhelyezkedniük" (65. § 8. bek.).

Ezek a rendelkezések egy olyan internetfelügyeleti rendszert hoznak létre, amely bár nem olyan kiterjedt, mint a kínai, de lényegesen több jogosítványt ad az államnak az internet szabályozására, mint az európai országok jogszabályai, amelyek általában csak bizonyos tartalmak cenzúrázását teszik lehetővé, mint a gyermekpornográfia, szerzői jogokat sértő tartalmak (például a német és francia szabályozás). Bár meg kell jegyezni, hogy sok európai

---

[23] Balasova–Kuznyecova–Poszipkina: *i. m.*

[24] A közbeszédben az orosz „szuverén internetet" tréfásan-gúnyosan *Cseburnet*ként emlegetik Cseburaska szovjet mesefigura után, de előfordul a *Putyinnet* megnevezés is.

[25] Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи" и Федеральный закон „Об информации, информационных технологиях и о защите информации": *i. m.*

[26] A mélycsomag-ellenőrzés (DPI) egy olyan adatfeldolgozás, amely részletesen megvizsgálja a számítógépes hálózaton keresztül elküldött adatokat, és általában megfelelő módon blokkolja, továbbirányítja vagy naplózza őket.

országban az extremista, terrorizmushoz kötődő és gyűlöletkeltő tartalmak is cenzúrázhatók, így nagyon sok függ attól, hogy ezzel a lehetőséggel az adott ország mennyire él visszsza. A törökországi szabályozással összevetve a jelenlegi orosz rendelkezések talán hasonló szintűnek nevezhetők, azzal a különbséggel, hogy magukban foglalják az országos hálózat leválasztását a globálisról.

Kínában a kormányzat nemcsak blokkolhatja honlapok tartalmát, hanem figyelemmel kísérheti az egyének internet-hozzáférését is.[27] A kínai cenzúra nemcsak egyes webhelyeket blokkol, hanem olyan technikákat használ, amelyek ellenőrzik az URL-eket és a honlapok tartalmát a feketelistán szereplő kulcsszavak azonosítása céljából (például „Tienanmen"), és blokkolja az ilyen forgalmat. Blokkolja a külföldi közösségi oldalakat, mint például a Twitter, és arra kényszeríti az állampolgárokat, hogy kínai megfelelőiket használják, mint például a Sina Weibo, így ellenőrizni és cenzúrázni tudja ezeket. A webhelyek és oldalak blokkolására szolgáló módszerek közé tartozik a DNS-hamisítás, az IP-címekhez való hozzáférés blokkolása, az URL-ek elemzése és szűrése, a mélycsomag-ellenőrzés (DPI) és a kapcsolatok alaphelyzetbe állítása (reset).[28] Az állami média szerint több mint 2 millió embert alkalmaznak a webes tevékenység, elsősorban a közösségi média és a mikroblogok nyomon követésére.[29]

Törökországban az internetet szabályozó, 2014-ben elfogadott törvény lehetővé teszi a távközlési hatóságnak (TIB), hogy négy órán belül blokkolja a weboldalakat anélkül, hogy előzetesen bírósági határozatot kellene kérnie, és megköveteli az internetszolgáltatótól, hogy két évig tárolja az összes internetes felhasználó tevékenységével kapcsolatos adatot, és kérésre hozzáférhetővé tegye a hatóságok számára. Ez azt is jelenti, hogy többek között a cégek titkos adatai is mind hozzáférhetők az állam számára.[30] A török hatóságok több alkalommal blokkolták a YouTube-ot és a Twittert, illetve demonstrációk idején több városban magát az internet-hozzáférést is.[31] A Wikipédia Törökországban 2017 áprilisától 2020 januárjáig nem volt elérhető.[32] A törvény előírja, hogy az online videó- és streamingszolgáltatóknak engedélyt kell kérniük a török internetes felhasználók számára történő sugárzáshoz.[33]

A legizgalmasabb kérdés természetesen, hogy mikor áll fenn az orosz internet fenyegetettsége, amely lehetővé teheti az orosz internet központosított irányítását: milyen kritériumok alapján és ki állapítja ezt meg. A törvény szövege szerint az Oroszországi Föderáció kormánya hagyja jóvá a nyilvános kommunikációs hálózat központi irányításának eljárását, amely magában foglalja többek között az orosz internetet fenyegető veszélyek típusait, a foganatosítandó intézkedéseket, illetve az ezekhez tartozó technikai követelményeket és módszereket (65. § 5. bek.).

---

27 Sally Croft: Internet censorship in China, [online], 2015. 07. 06. Forrás: CNN [2020. 03. 25.]

28 Chris Hoffmann: How the "Great Firewall of China" Works to Censor China's Internet, [online], 2017. 09. 10. Forrás: How-To Geek [2020. 03. 25.]

29 China employs two million microblog monitors state media say, [online], 2013. 10. 04. Forrás: BBC News [2020. 03. 25.]

30 Constanze Letsch: Turkey pushes through new raft of ‚draconian' internet restrictions, [online], 2014. 02. 06. Forrás: The Guardian [2020. 03. 25.]

31 Freedom House: Freedom of the Press – Turkey 2015, [online] 2015. Forrás: Internet Archive [2020. 03. 25.]

32 Wikipedia ban lifted after top court ruling issued, [online], 2020. 01. 15. Forrás: Hürriyet Daily News [2020. 03. 25.]

33 Letsch: *i. m.*

Szintén érdekes adalék a törvény hátteréhez, hogy miután több évig dolgozott a törvényjavaslaton Alekszej Szokolov miniszterhelyettes, akit egy meg nem nevezett forrás „Patrusev [a Szövetségi Biztonsági Tanács titkára, 1999–2008 között az FSZB igazgatója] meghosszabbított karjaként" aposztrofált, a parlamentnek adták tovább a labdát, így a törvényjavaslatot végül Andrej Klisasz és Ljudmila Bokova szenátorok, valamint Andrej Lugovoj alsóházi képviselő nyújtották be.[34] Lugovoj pedig, aki egy korábbi hasonló törvényt is jegyez, nem más, mint ugyanaz az egykori KGB- majd FSZB-tiszt, akit Nagy-Britanniában Alekszandr Litvinyenko megmérgezésével vádolnak. Kiadatását Oroszország megtagadta, majd pár hónappal később Vlagyimir Zsirinovszkij Liberális Demokrata Pártjának képviselője lett az Állami Dumában.

A törvény intézkedései alapján a Runetet központilag irányító, 2008-ban létrehozott Roszkomnadzor a Távközlési Minisztériumnak van alárendelve, feladatai közé tartozik a kommunikáció, az információs technológia és a média területének, valamint a személyes adatok védelmének felügyelete a törvényekkel összhangban és a rádiófrekvencia-szolgáltatás szervezése. A Roszkomnadzornak alárendelt rádiófrekvenciás szolgálatban egy speciális megfigyelőközpont jön létre, amelynek kritikus helyzetekben kell kezelnie a hálózatokat. A központot, amely információt kap az egész orosz kommunikációs infrastruktúráról, és 2019 végéig kellett létrehozni.[35]

Kritikák

A törvénymódosítással kapcsolatos kritikák vonatkoztak mind maga az intézkedés szükségességére, mind a kivitelezés nehézségeire és költségeire, és egyaránt érkeztek ellenzéki és civil szervezetektől, szakértőktől és állami szervektől. A kritikák több különböző szempontból bírálják a törvényt, amelyek közül a legfontosabbak: az állami szabályozás és a központosítás kockázatai, a forgalomszűrés nehézségei, a Runet izolációjának veszélyei.

A törvényjavaslat előkészítésének egész ideje alatt a képviselők csak egyszer találkoztak az ágazat képviselőivel. A parlamenti pártok közül a törvényjavaslatot az Egyesült Oroszország támogatta, míg a Liberális Demokrata Párt, az Igazságos Oroszország párt és a Kommunista Párt nem.[36]

A törvényjavaslat szerzői által hivatkozott, 2018 szeptemberében elfogadott amerikai Nemzeti Kiberbiztonsági Stratégia biztonsági kihívásként nevezi meg a kibertérben Oroszországot Kínával, Iránnal és Észak-Koreával együtt, mivel a dokumentum szerint kibereszközök segítségével aláássák az amerikai gazdaságot és demokráciát, ellopják a szellemi tulajdont, és ellenségeskedést szítanak a demokratikus folyamatokban.[37] A törvénymódosítás támogatói az amerikai stratégia egyik pillérére is hivatkoznak, amely „A béke megőrzése erő segítségével" *(Preserve Peace through Strength)*. Egy, a témával

[34] Охранник суверенного Рунета: *i. m.*

[35] Szvetlana Jasztrebova: Закон о «суверенном рунете» может вступить в силу 1 ноября, [online], 2019. 04. 09. Forrás: Vedomosztyi [2020. 03. 25.]

[36] Valerija Smirova: «Железо» для закона о суверенном Рунете обвалило сервисы «Яндекса», [online], 2019. 04. 16. Forrás: Cnews.ru [2020. 03. 25.]

[37] National Cyber Strategy of the United States of America: *i. m.*

foglalkozó cikkben idézik John Bolton nyilatkozatát a CNN-nek, amelyben azt mondta, hogy „[n]em csak védelmi intézkedéseket fogunk alkalmazni, támadó műveletekben is részt kívánunk venni, és riválisainknak ezt szem előtt kell tartaniuk".[38] A PIR-Centrum orosz elemzőközpont és civil szervezet szakértői szerint az amerikai kiberbiztonsági stratégia nem jelent fenyegetést arra nézve, hogy kibertámadásokra válaszul adott esetleges szankcióként lekapcsolhatnák Oroszországot az internetről.[39] A PIR tanácsadója, Oleg Gyemidov szerint az Egyesült Államok által foganatosítandó intézkedések közé tartozik az információcsere az állami kiberfenyegetésekről szövetségeseivel, segítségnyújtás a kibertámadások kivizsgálásában és attribúciójában (a „tettes" kilétének, illetve hovatartozásának megállapításában), a válaszintézkedések összehangolása és támogatása, beleértve a szankciókat is. Gyemidov úgy véli, bár az Egyesült Államok érvel Oroszország kibertérben való feltartóztatásának szükségessége mellett, nem világos, hogy milyen összefüggés van e között és a Roszkomnadzor speciális berendezéseinek az üzemeltetők hálózataiba való telepítésére irányuló javaslat között, amely tökéletesebb internetblokkolási lehetőséget biztosít a hivatal számára azáltal, hogy beleavatkozik az útválasztási rendszerbe. Annak érdekében, hogy a tiltott forrásokat blokkolhassa, a Roszkomnadzornak át kell néznie az üzemeltetők által továbbított forgalmat, vagyis olyan hatásköröket kell megszereznie, amellyel jelenleg csak a titkosszolgálatok rendelkeznek.[40]

Bár külön nem hivatkoztak rá, a NATO főtitkárának 2019. augusztusi nyilatkozata is releváns Oroszország szempontjából, amelyben Stoltenberg kijelentette, hogy egy esetleges kibertámadás az 5. cikkely szerinti választ von maga után, akárcsak egy konvencionális támadás.[41]

Oleg Ivanov orosz távközlésiminiszter-helyettes azt mondta, hogy nem helyes, ha idegen kézben van az a rendszer, amely nemcsak az állampolgárokra, hanem a gazdaság egészére is döntő hatással van. Az internet fejlesztését nem szabad a véletlenre bízni, mert Oroszország elvesztheti szuverenitását.[42]

A hivatalnokok amiatt aggódtak, hogy az Oroszországi Föderáció alanyai közötti belföldi orosz forgalom nyugati üzemeltetőkön halad keresztül. Dmitrij Burkov, a RIPE NCC regionális internetes nyilvántartás testületének tagja azonban felhívta rá a figyelmet, hogy az orosz internetes forgalom csak 1–2%-át cserélik ott, a többi része az országon belül zajlik. Ezenkívül a szakértő biztos abban, hogy a törvényjavaslat kidolgozói túlbecsülték a forgalomcserélő pontok fontosságát. Véleménye szerint Oroszországban a forgalom legfeljebb 20%-a halad át rajtuk, a fennmaradó részt a távközlési szolgáltatók adják át egymás között. Az oroszországi fő forgalomirányító pont a Rosztelekom által irányított MSK-IX. Egy meg nem nevezett hivatalnok szerint a Rosztelekom lobbizott a törvénymódosításért.[43]

---

[38] Jevgenyij Pudovkin: Явная виртуальная угроза, [online], 2018. 08. 22. Forrás: RBC [2020. 03. 25.]; Liptak: *i. m.*

[39] Balasova–Kuznyecova–Poszipkina: *i. m.*

[40] Balasova–Kuznyecova–Poszipkina: *i. m.*

[41] Jens Stoltenberg: NATO will defend itself, [online], 2019. 08. 27. Forrás: Prospect [2020. 03. 25.]

[42] Dmitrij Sesztoperov – Natalja Korcsenkova – Julija Tyisina: С суверенностью в завтрашнем дне, [online], 2018. 12. 25. Forrás: Kommerszant [2020. 03. 25.]

[43] Vlagyiszlav Novij: В законопроекте „О связи" появились точки, [online], 2017. 01. 12. Forrás: Kommerszant [2020. 03. 25.]

A kormány mellett dolgozó szakértők úgy vélték, hogy a törvényjavaslat célkitűzése nem tűnik átláthatónak: „Nem világos, hogy miben állnak a fenyegetések. Sem a törvényjavaslat, sem a magyarázó megjegyzés nem írja le sem a veszélyeket, sem a jelenlegi jogszabályok hibáit."[44]

A kormány mellett működő tanács szakértői a törvény végrehajtásának eredményeként előálló hálózati zavarok kockázatát „magasnak" értékelik. A kormány szakértői megjegyzik, hogy a hálózati topológia folyamatosan változik, és a törvény előírja a távközlési szolgáltató számára, hogy továbbítsa az „útválasztási sémákat".[45]

Konsztantyin Noszkov, a Távközlési Minisztérium vezetője beszélt a Roszkomnadzor túlzott hatásköreiről: megemlítette a média által a szabályozási szervhez benyújtott nagyszámú panaszt „szőrszálhasogatás", például a szerkesztők nevében elkövetett hibák vagy a helytelen életkorjelölés miatt. A minisztérium negatív véleményt adott a Runet elszigeteléséről szóló törvényjavaslatról,[46] de ezt követően támogatta azt.

Az Internet Kutatóintézet stratégiai projektigazgatója, Irina Levova megjegyezte, hogy nem világos, milyen kiegészítőberendezéseket kell az üzemeltetőknek telepíteniük a hálózatukba, de lehetségesnek tartotta, hogy ezzel jelentősen növekedhet az oroszországi internet leállásának veszélye, és akár a kapcsolat teljes elvesztéséhez is vezethet az internet külföldi szegmensével. Bírálta a Roszkomnadzor szabályainak a forgalom irányításakor történő betartására vonatkozó rendelkezést, mivel ez műszakilag tarthatatlan – az IP-protokollt úgy tervezték, hogy az adatok továbbítása az optimális útvonalon történjen, és nem úgy, ahogyan azt egy adott ügynökség kívánja. Ezenkívül attól tart, hogy a forgalomirányítás központosítása a Roszkomnadzor kezében betörés esetén teljesen megbéníthatja az internetet Oroszországban. Egy másik piaci szereplő szerint a javaslat „az egész orosz Internet topológiájának újjáépítését" javasolja, és a Roszkomnadzort túlzott hatáskörökkel ruházza fel. Azt is lehetségesnek tartja, hogy a felhasználói üzeneteket is cenzúrázzák majd, ami sérti a polgárok alkotmányos szabadságjogait.[47]

A szakértők arra is felhívták a figyelmet, hogy a dokumentum azt követeli a távközlési szolgáltatóktól és másoktól, hogy adják át a Roszkomnadzornak a hálózat teljes rendszerét és a forgalom irányítását, ami technikailag lehetetlen, mivel a hálózat egy élő, többszintű rendszer, amely folyamatosan bővül és frissül. Ezenkívül a tervezet bizonyos esetekben a távközlési szolgáltatók és a szabályozók közötti útválasztók irányításának átadásáról szól. Ez a hálózatok instabilitásához vezet, mivel a Roszkomnadzor nem rendelkezik az ilyen irányításhoz szükséges felszereléssel, szoftverrel és szakmai személyzettel. Azt is megjegyezték, hogy korrupciós kockázatokat is rejt magában a tervezet.[48]

Dmitrij Galusko, az OrderCom infokommunikációs tanácsadó cég vezérigazgatójának értékelése szerint valójában a törvényjavaslat megismétli a már elfogadott, a kritikus információs infrastruktúrák biztonságáról szóló törvényt, mivel céljaik azonosak: a külső kiber-

[44] Sesztoperov–Korcsenkova–Tyisina: *i. m.*
[45] Sesztoperov–Korcsenkova–Tyisina: *i. m.*
[46] Lilit Szarkiszjan: Роскомнадзор поиграет с «ядерной кнопкой», [online], 2019. 04. 16. Forrás: Novaja Gazeta [2020. 03. 25.]
[47] Szarkiszjan: *i. m.*
[48] Sesztoperov–Korcsenkova–Tyisina: *i. m.*

netikai támadások elleni védelem. A költségvetésben előirányzott alapok felhasználhatók lennének a meglévő törvény végrehajtására, amely eddig még nem történt meg.[49]

Az Oroszországi Iparosok és Vállalkozók Szövetsége Infokommunikációs és Távközlési Technológiai Bizottságának értékelése szerint a külföldi gyökérszerverekről való leválasztás veszélye nem releváns, mivel az Oroszországban már meglévő gyökérkiszolgálók másolatai elvégzik a megfelelő funkciókat (a 13 gyökér DNS-kiszolgáló közül a legtöbb az USA-ban, néhány Európában és Japánban található). Ezenkívül a DNS-kiszolgálók architektúrája miatt az oroszországi hálózat leválasztása az USA-ból vagy bármely más országból származó paranccsal lehetetlen, és egy ilyen kísérlet maga az USA számára járna magas költségekkel.[50] Alekszandr Sohin, a szervezet elnöke arra figyelmeztette a Duma elnökét, Vjacseszlav Vologyint, hogy a törvényjavaslat végrehajtása az Oroszországi Föderáció kommunikációs hálózatainak katasztrofális kudarcához vezethet.[51] Arra is felhívta a figyelmet, hogy a távközlési szolgáltatók ingyenesen részesülnek a feladatok elvégzéséhez szükséges pénzeszközökből az állami költségvetés terhére, de az internetes cégeknek ez nem biztosított. Ezenkívül nem világos, kinek a költségén történik a berendezések telepítése, karbantartása és áramellátása. A szövetség úgy véli, hogy ezeket a költségeket a távközlési szolgáltatók és az ORI (Információterjesztő Szervezők Nyilvántartása) viseli, és az előzetes becslések szerint öt év alatt eléri a 2 milliárd rubelt a nagyvállalatok számára. A törvényjavaslat szerzői viszont biztosították, hogy a berendezések vásárlásának költségeit belefoglalják a *Digitális gazdaság* nemzeti projektbe. Azt is javasolta a szervezet, hogy zárják ki a projektből a nemzeti domainnévrendszer létrehozását célzó intézkedéseket, jelezve, hogy Oroszországban már létezik ilyen, és a Nemzeti Domain Koordinációs Központ és az Internet Technikai Központ támogatja, amelyek teljes állami ellenőrzés alatt állnak. Elképzelésük szerint a megfelelő megoldás a forgalom irányításának kezelésére szolgáló eljárás kidolgozása lenne, amelyet csak a kritikus infrastruktúra alanyaira terjesztenének ki, de nem az előfizetői forgalomra, ideértve a filmeket, zenét, játékokat stb.[52]

Az MTS, a Tele2 és a Vimpelkom telekommunikációs cégek képviselői szerint a forgalomcserélő pontok állami nyilvántartásának létrehozása az üzemeltetők költségeinek növekedéséhez vezet.[53] A Vimpelkom képviselője szerint fontos lenne tudni, hogy pontosan milyen műszaki követelmények és normák lesznek az alsóbb szintű jogszabályokban.[54]

A Dolgok Internetje Piaci Szereplőinek Szövetsége szerint a törvény lelassíthatja a dolgok internetjének fejlődését Oroszországban, amely érzékeny az esetleges adatátviteli késésekre, és ez hátrányosan befolyásolhatja az „intelligens városok" ígéretes projektjeinek megvalósítását, valamint a közlekedési infrastruktúra és az ipari internet digitalizálását.[55]

A tervezet szerzői kezdetben azt állították, hogy megvalósítása nem igényel többletkiadásokat a szövetségi költségvetésből. De kormány a február 4-én benyújtott véleményében

---

[49] Sesztoperov–Korcsenkova–Tyisina: *i. m.*

[50] Julija Tyisina – Natalja Korcsenkova: Суверенный рунет вышел на связь, [online], 2019. 02. 08. Forrás: Kommerszant [2020. 03. 25.]
Makszim Iszhakov: Что такое корневой сервер DNS?, [online], 2019. 01. 02. Forrás: Bezopasnik [2020. 03. 25.]

[51] Tyisina–Korcsenkova: *i. m.*

[52] Tyisina–Korcsenkova: *i. m.*

[53] Novij: *i. m.*

[54] Sesztoperov–Korcsenkova–Tyisina: *i. m.*

[55] Julija Tyisina: Операторы задумались о вещном, [online], 2019. 03. 21. Forrás: Kommerszant [2020. 03. 25.]

rámutatott, hogy a projekt mégis igényel költségvetési forrásokat. Andrej Klisasz bejelentette, hogy három évre több mint 20 milliárd rubelt különítenek el a *Digitális gazdaság* nemzeti projekt Információs biztonság nevű alprogramjára az orosz internetszegmens biztonságát biztosító szoftver- és hardvereszközök beszerzésére. A 2019–2021-es költségvetés további mintegy 1,8 milliárd rubelt is tartalmaz a nyilvános kommunikációs hálózat központjának és információkezelő rendszerének létrehozására és működtetésére.[56] A kormány mellett működő szakértői tanács szerint kompenzációra lesz szükség a távközlési szolgáltatók számára hálózati zavarok esetén, amelyek kockázatát az iparági résztvevők magasnak ítélik meg.[57]

A számvevőszék nem támogatta a törvényjavaslatot, és számos észrevételt tett, többek között hogy „a törvényjavaslat végrehajtása az áruk és szolgáltatások költségeinek növekedéséhez vezet az orosz piacon".[58]

Az Internetfejlesztési Intézet igazgatója, Szergej Petrov szerint sok országban ez a folyamat már régóta elindult; a törvény pedig lendületet ad Oroszország számára az informatikai ipar fejlesztéséhez és az orosz berendezések gyártásához.[59] A javaslat egyik társszerzője, Andrej Lugovoj orosz kriptográfia használatára is kötelezné a hatóságokat.[60]

Megvalósítási nehézségek

Az internet globális hálózatát lokális hálózatok, intranetek, különböző távolsági hálózatok alkotják, amelyek az internetprotokoll (IP) segítségével kommunikálnak egymással. Az adatok a legkülönfélébb fizikai közegekben utazhatnak telefonvonalak, különféle hálózati kábelek vagy kommunikációs műholdak segítségével. Az internetnek nincs egyetlen központosított irányítása sem a technológiai megvalósításban, sem a hozzáférés és a használat szabályozásában; minden egyes alkotó hálózat saját maga határozza meg a politikáját. Az internet két fő névtérének, az Internet Protocol address (IP-cím) térnek és a Domain Name Systemnek (DNS) igazgatását az ICANN (Internet Corporation for Assigned Names and Numbers) látja el. Ebből a decentralizált szerkezetből adódik egyes országokban az internet nemzeti ellenőrzése iránti igény, de egyszersmind ennek megvalósítási nehézségei is.

Ami a törvénymódosítás gyakorlati megvalósítását illeti, elsőre kézenfekvőnek tűnhet a kínai modell lemásolása, de bár az orosz illetékesek irigykedve nézik a kínai forgalomszűrő rendszert, elismerik, hogy Oroszországban ez nem valósítható meg. Ennek két oka van: technológiai és társadalmi. A kínai internet a kezdetektől elszigetelt volt, a rendszerben csak három csomópont van a forgalom kicserélésére a külvilággal, amelyeket meglehetősen könnyű kontrollálni. Oroszországban több száz ilyen csomópont létezik, és nem mindegyikről tud a Roszkomnadzor és a titkosszolgálatok, ahogy azt az elnöki adminisztráció üléseinek egyik résztvevője elismerte; emiatt esett a választás a DPI-technológiára. A másik különbség, hogy Kínában a globális internetes szolgáltatások (fizetési rendszerek, online

[56] Tyisina: *i. m.*

[57] Sesztoperov–Korcsenkova–Tyisina: *i. m.*

[58] Счетная палата не поддержала законопроект об устойчивом Рунете, [online], 2019. 02. 07. Forrás: Interfax [2020. 03. 25.]

[59] Makszim Kolomijec: Закон о надежном Рунете принят Госдумой, [online], 2019. 04. 16. Forrás: Ridusz [2020. 03. 25.]

[60] Jasztrebova: *i. m.*

áruházak, közösségi hálók és keresőmotorok) nagy részét sikeresen helyettesítették kínai megfelelőkkel.[61]

A gyakorlatban a törvény még nem működik, azonban a szükséges felszereléseket már valós felhasználókon tesztelték az Urálban. A hálózati infrastruktúra kezelésére a törvénynek megfelelően létrehozták az Általános Használatú Kommunikációs Hálózatok Megfigyelési és Igazgatási Központját (CMU) a Roszkomnadzorban. Ez a szervezet elemzéseket gyűjt a hálózat működéséről, kezeli a tiltott webhelyek blokkolását, és képes lesz átvenni a Runet központosított irányítását a biztonságot fenyegető veszélyek esetén. A Meduza online hírportál tudomására jutott információk szerint vezetője Szergej Hutorcev[62] lett, aki több évig szolgált a Szövetségi Védelmi Szolgálatnál (FSZO), amely a magas rangú állami tisztviselők védelmét látja el.[63]

2019 március közepén a szuverén Runet-törvény végrehajtására szolgáló technológia használata megzavarta a Yandex (orosz informatikai szolgáltató, amely a legnagyobb orosz keresőmotort üzemelteti) szolgáltatásait egy hálózati támadás miatt. A támadók a Roszkomnadzor által használt webhelyblokkoló rendszer hibáit használták ki. A DNS-támadás használatával blokkolható egy teljesen legális weboldal, ha az elkövető rendelkezik egy domainnel a tiltott erőforrások nyilvántartásában. Ehhez csak rá kell kötnie a webhely IP-címét a domainre.[64] A társaság képviselője szerint „a Roszkomnadzor blokkolásával kapcsolatos okokból a forgalom a már létező DPI-operátorokon ment keresztül, ezután a legtöbb szolgáltatás összeomlott".[65] A törvény alapján a külső fenyegetések elleni küzdelem eszközei nem mások, mint a DPI-rendszerek, amelyeken keresztül tervezik az összes forgalom átvezetését. A Yandex hálózati fejlesztési igazgatója szerint a jelenlegi forgalom volumene mellett ilyen DPI-k nem léteznek a világon, sőt még nem is fejlesztik azokat, hogy támogathassanak egy ilyen rendszert a szolgáltatások jelentős vesztesége nélkül. Az egyik szolgáltató szerint csak elméletileg lehetséges a teljes forgalmat a DPI-eszközökön keresztül továbbadni: a költségek csillagászatiak, és nincs kapacitás az adatok elemzésére; a nagy piaci szereplők a DPI-vel a forgalom csak azon részét elemzik, amelyet potenciálisan veszélyesnek tartanak. Ezenkívül a jövőben hálózati támadások is lehetnek maga a DPI ellen.[66]

A hasonló korlátozások megkerülésére használt VPN-ek (*Virtual Private Network* – virtuális magánhálózat[67]) az Urálban végzett tesztüzem tapasztalatai alapján továbbra is

---

[61] Szarkiszjan: *i. m.*

[62] Hutorcev a Rosztelekom elnökének tanácsadója is. A Rosztelekom az egyetlen kommunikációs szolgáltató a szövetségi hatóságok és egészségügyi intézmények számára, egységesített állami felhőplatform és más kormányzati szolgáltatások üzemeltetője. Охранник суверенного Рунета: *i. m.*

[63] Охранник суверенного Рунета: *i. m.*

[64] Smirova: *i. m.*

[65] Технология из закона о суверенном Интернете ударила по сервисам «Яндекса», [online], 2019. 04. 16. Forrás: Fontanka [2020. 03. 25.]

[66] Marija Koromicsenko – Natalja Gyemcsenko: «Яндекс» счел технологию из закона о Рунете ухудшающей работу сервисов, [online], 2019. 04. 16. Forrás: RBC [2020. 03. 25.]

[67] A virtuális magánhálózat (VPN) kiterjeszti a magánhálózatot egy nyilvános hálózaton keresztül, és lehetővé teszi a felhasználók számára, hogy adatokat küldjenek és fogadhassanak megosztott vagy nyilvános hálózatokon, mintha számítástechnikai eszközeik közvetlenül kapcsolódnának a magánhálózathoz.

használhatók lesznek, VPN és proxy[68] segítségével egy kattintással megkerülhető a blokkolás.[69] Mihail Klimarev telekommunikációs elemző szerint Oroszországban a *Telegram* (az egyik legnépszerűbb orosz üzenetküldő alkalmazás) letiltásának egyetlen módja az internet kikapcsolása. És ez az egyetlen, amelyben a DPI valóban segíthet: néhány perc alatt lehetséges az internet kikapcsolása minden helyszínen, mert nem lesz szükség papírmunkára: a régi szabályozás szerint a Roszkomnadzornak levelet kellett írnia az internetszolgáltatónak, amelyben kéri az internet kikapcsolását, és meg is kell előbb tudnia, melyik operátor szolgálja ki az adott helyet. Ez legalább egy napig tart. Most a Roszkomnadzor azonnal képes lesz az internet kikapcsolására.[70] Ezt a módszert használták 2018 októberében is Ingusföldön: egyszerűen kikapcsolták a mobilinternetet, amikor tiltakozások bontakoztak ki a Csecsenfölddel történt területcsere miatt.[71]

A szabályozás gyakorlati megvalósításának áttekintése mellett azt a kérdést is érdemes feltenni, hogy az orosz legfelsőbb döntéshozás mennyire volt tisztában ezekkel a nehézségekkel és azzal, hogy egyáltalán hogyan működik az internet.

2011-ben az elnök szokásos év végi kérdés-válasz interjújában úgy nyilatkozott, hogy az államnak nem szabad irányítania az internetet; ha nem tetszik neki, ami ott történik, akkor meg kell jelennie az interneten, alternatívát kell kínálnia. Azt is megemlítette a témával kapcsolatban, hogy sok pedofil használja az internetet. A *Guardian* újságírója szerint Putyinnak nyilvánvalóan fogalma sem volt róla, hogy miről beszél. Arra a kérdésre, hogy használja-e az internetet, az elnök bevallotta, hogy nincs rá ideje, még televíziót sem néz.[72]

Az orosz elnök más források szerint is ritkán használja az internetet, aminek feltehetően csak az egyik oka a biztonságra való törekvés: a dolgozószobájában nincsenek képernyők, csak piros mappák papírdokumentumokkal és régimódi szovjet vezetékes telefonok.[73]

Lehetséges következmények

Az Internet Kutatóintézet stratégiai projektigazgatója, Irina Levova szkeptikus a törvény gyakorlati alkalmazásával kapcsolatban. Szerinte a hatályba lépéssel megkezdődik a berendezések tanúsítása, tesztelése és elrendezése. Ezek a folyamatok nagyon hosszú ideig meghosszabbíthatók, de valószínűleg nem lesznek képesek arra, hogy az internet orosz szegmensének biztonságát valóban szavatolják.[74]

Számos szakértő attól tart, hogy ezek a változások a kormány és az elnök stratégiájának részét képezik, amelynek célja az internet feletti ellenőrzés megerősítése és a cenzúra szigorítása az országban, és a törvény elfogadásának valódi oka a hatalmon lévők nép-

[68] A proxyszerver olyan kiszolgálóalkalmazás vagy -készülék, amely közvetítőként szolgál az ügyfelek kéréseire azon erőforrásokat kereső kiszolgálóktól, amelyek ezeket az erőforrásokat szolgáltatják. Egy proxyszerver így működik az ügyfél nevében, amikor szolgáltatást igényel, potenciálisan elfedve a kérés valódi eredetét az erőforrásszerver felé.

[69] Ivan Zsilin: Суверенный интернет не настолько суровый, [online], 2019. 09. 27. Forrás: Novaja Gazeta [2020. 03. 25.]

[70] Zsilin: *i. m.*

[71] Russia internet: Law introducing new controls comes into force, [online], 2019. 11. 01. Forrás: BBC News [2020. 03. 25.]

[72] Vladimir Putin Q & A and reaction – Thursday 15 December, [online], 2011. 12. 15. Forrás: The Guardian [2020. 03. 25.]

[73] Ben Judah: A day in the life of Vladimir Putin: The dictator in his labyrinth, [online], 2014. 07. 25. Forrás: Independent [2020. 03. 25.]

[74] Jasztrebova: *i. m.*

szerűségének csökkenése, valamint az ezzel összefüggő tiltakozóakciók visszaszorítására való törekvés.[75]

A Roszkomnadzor vezetője, Alekszandr Zsarov szerint a törvény elfogadása után „alvó" állapotban lesz, „mint egy nukleáris fegyver".[76] Hangsúlyozta, hogy jelenleg nincs kilátás Oroszország leválasztására az internetről.[77]

Zsarov 2019. április 9-én azt is mondta, hogy a „szuverén Runet" törvény elősegíti az Oroszországban tiltott információforrások elleni küzdelmet, ideértve a Telegram üzenetküldő alkalmazást is.[78] Ez egy a WhatsApphoz vagy a Viberhez hasonló, Oroszországban és a szovjet utódállamokban rendkívül népszerű és az ellenzékiek által is széles körben használt[79] üzenetküldő alkalmazás. 2018-ban egy moszkvai bíróság betiltotta a szoftvert, miután a cég elutasította az FSZB számára a felhasználói kommunikáció megtekintéséhez szükséges titkosítási kulcsokhoz való hozzáférést, ahogy azt a szövetségi terrorizmusellenes törvény előírja.[80] Márciusban ismertté vált, hogy a Zsarov vezette munkacsoport különféle mélycsomag-ellenőrző (DPI) rendszereket tesztelt, laboratóriumi körülmények között blokkolva a Telegramot.[81]

2019. március 10-én a moszkvai Szaharov sugárúton a szabad internet támogatását célzó gyűlést szerveztek az Internetvédő Társaság és a nyilvántartásba nem vett Libertárius Párt aktivistái, akik előző évben tömeges demonstrációt tartottak a Telegram blokkolása ellen. A rendőrség szerint mintegy 6500 ember vett részt a rendezvényen, más adatok 18 ezer résztvevőről szólnak.[82]

Szintén érdemes megemlíteni az Állami Duma által március 7-én elfogadott „fake news törvényt"[83] is, amely felhatalmazza a Roszkomnadzort, hogy haladéktalanul blokkolja azokat a webhelyeket, amelyeken olyan valótlan információkat tartalmazó publikációk találhatók, amelyek terjesztése veszélyt jelent a polgárok életére vagy egészségére, megzavarja a közrendet és a stratégiailag fontos infrastrukturális rendszerek működését,[84] illetve sértik a kormányt és az államot. Az ilyen cselekményekért 30 ezer és 1,5 millió rubel közötti pénzbírságot szabnak ki, de a hatóság először felszólítja az adott kiadványt a szóban forgó

---

[75] Закон об изоляции Рунета прошёл третье чтение в Госдуме, [online], 2019. 04. 16. Forrás: Radio Svoboda [2020. 03. 25.]; Alekszandra Prokopenko: Закон о суверенном рунете. Как он возник и к чему приведет, [online], 2019. 04. 18. Forrás: Carnegie Moscow Center [2020. 03. 25.]

[76] Глава Роскомнадзора сравнил закон о суверенном Рунете с ядерным оружием, [online], 2019. 04. 16. Forrás: RBC [2020. 03. 25.]

[77] Глава Роскомнадзора оценил возможность отключения России от интернета, [online], 2018. 12. 24. Forrás: Regnum [2020. 03. 25.]

[78] Жаров назвал одной из целей закона о «суверенном рунете» борьбу с Telegram », [online], 2019. 04. 09. Forrás: Kommerszant [2020. 03. 25.]

[79] Az alkalmazás egyébiránt a Közel-Keleten is kedvelt, például Iránban, illetve szigorú adatvédelmi előírásai miatt az Iszlám Állam és más terrorszervezetek is előszeretettel használják.

[80] Neil MacFarquhar: Russian Court Bans Telegram App After 18-Minute Hearing, [online], 2018. 04. 13. Forrás: The New York Times [2020. 03. 25.]

[81] Jasztrebova: *i. m.*

[82] Anasztaszija Kramer: Митинг «Против изоляции Рунета» прошел в Москве, [online], 2019. 03. 10. Forrás: Moszkovszkaja Gazeta [2020. 03. 25.]

[83] Федеральный закон от 18.03.2019 № 31-ФЗ „О внесении изменений в статью 15-3 Федерального закона „Об информации, информационных технологиях и о защите информации", [online], 2019. 03. 18. Forrás: Pravo [2020. 03. 25.]

[84] Госдума приняла закон о запрете фейковых новостей в интернете, [online], 2019. 03. 07. Forrás: Novaja Gazeta [2020. 03. 25.]

információ azonnali eltávolítására. Ennek a jogszabálynak szintén Andrej Klisasz szenátor a szerzője,[85] aki a Szövetségi Tanács alkotmányosjog-alkotással és államépítéssel foglalkozó bizottságának vezetője.

Következtetések

Hogy valójában a gyakorlatban milyen mértékben fogják az orosz hatóságok igénybe venni a forgalom ellenőrzésének és az orosz internet leválasztásának lehetőségét, és mennyire fogják ezt akadályozni a pénzügyi és a technikai nehézségek, illetve mindez milyen hatással lesz Oroszország gazdasági fejlődésére, és előidézheti-e az ország izolációját és lemaradását, azt egyelőre szinte lehetetlen megmondani. Mindenesetre a jogszabály szélesebb hatáskört biztosít az orosz államnak az internetes forgalom kontrollálására, és a technikai háttér kiépítésével lehetővé válik a rendszerkritikus üzenetek blokkolása, demonstrációk szervezésének ellehetetlenítése a közösségi hálókon vagy üzenetküldő alkalmazásokon keresztül, aminek egy esetleges társadalmi elégedetlenség és tiltakozási hullám esetén nagy használt veheti a vezetés.

Függelék: A médiatörvény módosításának következményei

Bár nem kapcsolódik szorosan a „szuverén internet" törvényhez, szintén az online tartalmak cenzúrázása felé mutat, hogy tavaly novemberben a médiatörvényt is módosították Oroszországban azzal a céllal, hogy korlátozzák a külföldi médiumok és véleményformálók befolyását. A *Kommerszant* szerint a módosítás folyományaként bármely állampolgár megkaphatja az „idegen ügynök" minősítést, bár a hatóságok kimondottan azt ígérik, hogy szelektíven fogják alkalmazni a jogszabályt.[86]

Az Állami Dumában speciálisan létrehozott bizottság, a rendvédelmi tisztviselőkkel és a Szövetségi Tanács hasonló bizottságával az év második felében aktívan vizsgálta az ország belső ügyeibe való idegen beavatkozás állítólagos tényeit. A törvénymódosítás szerint természetes személyek is minősíthetők ügynöknek.

A hangsúly elsősorban a külföldi média kiadványain van: 2020-tól az orosz állampolgárok továbbra is gond nélkül hallgathatják, nézhetik és elolvashatják őket, ám tartalmuknak a közösségi médiában való újraposztolásánál már körültekintőbbnek kell lenniük. A módosítások elfogadása után az orosz hatóságoknak joguk van külföldi ügynöknek minősíteni azokat az állampolgárokat, akik a tömegtájékoztatási eszközökön külföldi ügynökök által létrehozott üzeneteket és anyagokat terjesztenek, és ezzel egyidejűleg külföldi finanszírozást kapnak. A jogalkotók nem határozták meg, hogy az állampolgároknak hol kell terjeszteniük ezeket az információkat, hogy külföldi ügynökké váljanak, de az „internet telekommunikációs hálózatának felhasználásával" történő terjesztést figyelembe veszik. Az új törvény nem eléggé konkrét megfogalmazása aggodalmakat vet fel az emberi jogi jogvédők és az átlagos felhasználók részéről: ha a hatóságok úgy akarják, a törvény alapján bárki felelősségre vonható. Például a YouTube-on működő tartalomkészítők többsége

[85] Госдума приняла закон о запрете фейковых новостей в интернете: *i. m.*

[86] Nyikita Proksin: Привет, иностранный агент, [online], 2019. 12. 31. Forrás: Kommerszant [2020. 03. 25.]

külföldi finanszírozást kap, legalábbis díj formájában, a videóikban szereplő hirdetések automatikus megjelenítéséért. A videohosting önállóan integrálja a reklámokat a tartalomba, és amikor a közönség interakcióba lép (rájuk kattint vagy megnézi őket), a szerző pénzt kap közvetlenül a platformtól.[87] És a YouTube Oroszországban természetesen külföldi cég. A YouTube-streamerek online közvetítéseket folytatnak, amelyek során a nézők adományokat küldenek a csatorna szerzőjének/tulajdonosának. Ha a közvetítés során a streamer egy külföldi médiumot idéz, eközben pénzügyi juttatást kap külföldi forrásból, akkor ezzel automatikusan külföldi ügynök lesz. Azoknak az állampolgároknak, akik „külföldi ügynök" minősítést kaptak, tájékoztatniuk kell a közönséget erről, tartalmuk megfelelő megjelölésével. Tevékenységük folytatása érdekében orosz jogi személyt kell létrehozniuk. Mindent és mindenkit figyelemmel követni nehéz lesz, ha egyáltalán lehetséges.

A parlamenti képviselők azonban nem rejtik véka alá, hogy az új jogalkotási normát szelektív módon alkalmazzák. Az Állami Duma Információs Politikai Bizottságának elnöke, Leonyid Levin kifejtette, hogy „ezt minden esetben az Igazságügyi Minisztérium és a Külügyminisztérium együttes határozata dönti el".[88] Az eljárást azonban a törvény nem írja elő.

Az igazságügyi minisztérium listáján szereplő, a külföldi médiában dolgozó újságírók is bekerülhetnek a külföldi ügynökök bandájába, mivel a fizetésük külföldi finanszírozásnak tekinthető. Levin szerint mindez „nem azt jelenti, hogy automatikusan külföldi ügynökökké válnak".[89] De maga is azonnal hozzáteszi: ha valaki a társadalmi-politikai helyzettel kapcsolatos anyagokat ír, akkor természetesen lehetséges az idegen ügynökké válás, de ha egy újságíró kultúráról, sportról vagy zenéről ír, akkor úgy tűnik, hogy nincs kockázat. Ezzel az orosz parlament gyakorlatilag bevallja a szelektív jogalkalmazást, ami súlyos jogi kérdéseket vet fel. A törvényhozók maguk sem leplezik, hogy a normát a kellemetlen vagy kifogásolható bloggerek és újságírók ellen kívánják alkalmazni. A homályos nyelvezet megkönnyíti a helyzet manipulálását a végrehajtás szintjén. Nyikita Proksin újságíró szerint „a kezdeményezés úgy néz ki, mint egy kísérlet a cenzúra alól mentesülő tartalomkészítők tevékenységének ellenőrzésére".[90] Eddig tíz szervezet szerepelt az oroszországi külföldi médiaügynökök listáján, köztük az Amerika Hangja és a Szabad Európa Rádió *(Radio Free Europe/Radio Liberty).* Vlagyimir Putyin elnök december 2-án írta alá a törvénymódosítást, és azóta a tavalyi évben nem volt olyan eset, hogy természetes személyt külföldi ügynöknek nyilvánítottak volna.

Decemberben éves sajtótájékoztatóján Putyin elnök úgy kommentálta a módosítást, hogy ez csak azokat a polgárokat érinti, akik külföldről kapnak pénzt, és belpolitikai tevékenységet folytatnak. „A külföldi ügynökszervezetekről szóló törvény erről szól: ha külföldről kap pénzt és belpolitikai tevékenységet folytat, akkor mondja meg. Aki fizet a zenéért, az rendeli meg, hogy mit játsszanak. Csak nyilvánossá kell tenni, hogy tudjanak

---

[87] Bár meg kell jegyezni, hogy a jogszabály szövege alapján a reklámterjesztésért kapott pénzösszegre nem vonatkoznak a törvényi kötelezettségek (jelentéstétel). Закон РФ от 27.12.1991 N 2124-1 (ред. от 02.12.2019) „О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.01.2020), [online], 2019. 12. 02. Forrás: Consultant [2020. 03. 25.]

[88] Proksin: *i. m.*

[89] Proksin: *i. m.*

[90] Proksin: *i. m.*

erről az emberek"– mondta Putyin, megjegyezve, hogy kerülni kell a kiterjedt értelmezést a külföldi ügynökökre vonatkozó törvény vonatkozásában.[91]

Az Európai Parlament képviselői még decemberben elfogadtak egy állásfoglalást, amely bírálta Oroszországot a külföldi ügynökökről szóló törvénye miatt. Az EP elítélte a nemrégiben elfogadott törvénymódosításokat, amelyek „jelentősen kibővítik a törvény alkalmazási körét, és lehetővé teszik az egyének diszkriminálását és külföldi ügynökökként történő megbélyegzését, ezzel megsértve emberi jogaikat, különösen a véleménynyilvánítás és az egyesülés szabadságát, valamint polgári jogaikat". Amint azt az állásfoglalás kimondja, a törvény „megsérti Oroszországnak az EBESZ tagjaként és az Emberi Jogok Egyetemes Nyilatkozatát aláíró országként vállalt kötelezettségeit".[92]

FELHASZNÁLT IRODALOM

Balasova, Anna – Kuznyecova, Jevgenyija – Poszipkina, Alekszandra: РФ и точка: какие риски несет проект о суверенном Рунете, [online], 2018. 12. 15. Forrás: RBC [2020. 03. 25.]

Bamford, James: Edward Snowden: The Untold Story, [online], 2014. 08. 13. Forrás: Wired [2020. 03. 25.]

China employs two million microblog monitors state media say, [online], 2013. 10. 04. Forrás: BBC News [2020. 03. 25.]

Croft, Sally: Internet censorship in China, [online], 2015. 07. 06. Forrás: CNN [2020. 03. 25.]

Европейский парламент призвал Россию отменить закон об иностранных агентах, [online], 2019. 12. 19. Forrás: TASS [2020. 03. 25.]

Examples of forbidden content, [online], é. n. Forrás: Запрещено в России [2020. 03. 25.]

Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», [online], 2016. Forrás: Consultant [2020. 03. 25.]

Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», [online], 2016. Forrás: Wikisource [2020. 03. 25.]

Федеральный закон от 18.03.2019 № 31-ФЗ „О внесении изменений в статью 15-3 Федерального закона „Об информации, информационных технологиях и о защите информации", [online], 2019. 03. 18. Forrás: Pravo [2020. 03. 25.]

Федеральный закон от 01.05.2019 № 90-ФЗ „О внесении изменений в Федеральный закон „О связи" и Федеральный закон „Об информации, информационных технологиях и о защите информации", [online], 2019. 05. 01. Forrás: Pravo [2020. 03. 25.]

Freedom House: Freedom of the Press – Turkey 2015, [online] 2015. Forrás: Internet Archive [2020. 03. 25.]

Freedom House: Freedom on the Net 2016 – Russia, [online], 2016. 11. 14. Forrás: Refworld [2020. 03. 25.]

ФСБ узнала о подготовке кибератак на финансовую систему России, [online], 2016. 12. 20. Forrás: RIA Novosztyi [2020. 03. 25.]

Глава Роскомнадзора оценил возможность отключения России от интернета, [online], 2018. 12. 24. Forrás: Regnum [2020. 03. 25.]

[91] Президент разъяснил, кого касаются поправки в закон о СМИ–иноагентах, [online], 2019. 12. 19. Forrás: RAPSZI [2020. 03. 25.]

[92] Европейский парламент призвал Россию отменить закон об иностранных агентах, [online], 2019. 12. 19. Forrás: TASS [2020. 03. 25.]

Глава Роскомнадзора сравнил закон о суверенном Рунете с ядерным оружием, [online], 2019. 04. 16. Forrás: RBC [2020. 03. 25.]
Госдума приняла закон о запрете фейковых новостей в интернете, [online], 2019. 03. 07. Forrás: Novaja Gazeta [2020. 03. 25.]
Goble, Paul: FSB Increasingly Involved in Misuse of 'Anti-Extremism' Laws, SOVA Says, [online], 2015. 03. 29. Forrás: The Interpreter [2020. 03. 25.]
Hoffmann, Chris: How the "Great Firewall of China" Works to Censor China's Internet, [online], 2017. 09. 10. Forrás: How-To Geek [2020. 03. 25.]
Iszhakov, Makszim: Что такое корневой сервер DNS?, [online], 2019. 01. 02. Forrás: Bezopasnik [2020. 03. 25.]
Jasztrebova, Szvetlana: Закон о «суверенном рунете» может вступить в силу 1 ноября, [online], 2019. 04. 09. Forrás: Vedomosztyi [2020. 03. 25.]
Judah, Ben: A day in the life of Vladimir Putin: The dictator in his labyrinth, [online], 2014. 07. 25. Forrás: Independent [2020. 03. 25.]
Kolomijec, Makszim: Закон о надежном Рунете принят Госдумой, [online], 2019. 04. 16. Forrás: Ridusz [2020. 03. 25.]
Клименко допустил отключение России от «мирового интернета», [online], 2016. 12. 29. Forrás: Dozsgy [2020. 03. 25.]
Клименко: Россия должна быть готова к отключению от мирового интернета, [online], 2016. 12. 29. Forrás: TASS [2020. 03. 25.]
Koromicsenko, Marija – Gyemcsenko, Natalja: «Яндекс» счел технологию из закона о Рунете ухудшающей работу сервисов, [online], 2019. 04. 16. Forrás: RBC [2020. 03. 25.]
Kramer, Anasztaszija: Митинг «Против изоляции Рунета» прошел в Москве, [online], 2019. 03. 10. Forrás: Moszkovszkaja Gazeta [2020. 03. 25.]
Kravcsenko, Marija: Неправомерное применение антиэкстремистского законодательства в России в 2014 году, [online], 2015. 03. 28. Forrás: Polit.ru [2020. 03. 25.]
Letsch, Constanze: Turkey pushes through new raft of ‚draconian' internet restrictions, [online], 2014. 02. 06. Forrás: The Guardian [2020. 03. 25.]
Liptak, Kevin: John Bolton: US is going on the offensive against cyberattacks, [online], 2018. 09. 20. Forrás: CNN Politics [2020. 03. 25.]
MacFarquhar, Neil: Russian Court Bans Telegram App After 18-Minute Hearing, [online], 2018. 04. 13. Forrás: The New York Times [2020. 03. 25.]
National Cyber Strategy of the United States of America, [online], 2018. Forrás: The White House [2020. 03. 25.]
Novij, Vlagyiszlav: В законопроекте „О связи" появились точки, [online], 2017. 01. 12. Forrás: Kommerszant [2020. 03. 25.]
Охранник суверенного Рунета, [online], 2019. 11. 27. Forrás: Meduza [2020. 03. 25.] DOI: https://doi.org-/10.1055/s-0040-1709402
Президент разъяснил, кого касаются поправки в закон о СМИ–иноагентах, [online], 2019. 12. 19. Forrás: RAPSZI [2020. 03. 25.]
Prokopenko, Alekszandra: What's Behind Russia's New Offensive Against the Internet Economy?, [online], 2019. 08. 12. Forrás: Carnegie Moscow Center [2020. 03. 25.]
Prokopenko, Alekszandra: Закон о суверенном рунете. Как он возник и к чему приведет, [online], 2019. 04. 18. Forrás: Carnegie Moscow Center [2020. 03. 25.]
Proksin, Nyikita: Привет, иностранный агент, [online], 2019. 12. 31. Forrás: Kommerszant [2020. 03. 25.]
Pudovkin, Jevgenyij: Явная виртуальная угроза, [online], 2018. 08. 22. Forrás: RBC [2020. 03. 25.]
Путин подписал законы о фейкньюс и неуважении к власти, [online], 2019. 03. 18. Forrás: Vedomosztyi [2020. 03. 25.]
Quinn, Andrew – Osterman, Cynthia: U.S. says Syrian opposition can skirt Internet shutdown, [online], 2012. 11. 29. Forrás: Reuters [2020. 03. 25.]
Russia internet: Law introducing new controls comes into force, [online], 2019. 11. 01. Forrás: BBC News [2020. 03. 25.]

Sesztoperov, Dmitrij – Korcsenkova, Natalja – Tyisina, Julija: С суверенностью в завтрашнем дне, [online], 2018. 12. 25. Forrás: Kommerszant [2020. 03. 25.]
Smirova, Valerija: «Железо» для закона о суверенном Рунете обвалило сервисы «Яндекса», [online], 2019. 04. 16. Forrás: Cnews.ru [2020. 03. 25.]
Stoltenberg, Jens: NATO will defend itself, [online], 2019. 08. 27. Forrás: Prospect [2020. 03. 25.]
Szarkiszjan, Lilit: Роскомнадзор поиграет с «ядерной кнопкой», [online], 2019. 04. 16. Forrás: Novaja Gazeta [2020. 03. 25.]
Счетная палата не поддержала законопроект об устойчивом Рунете, [online], 2019. 02. 07. Forrás: Interfax [2020. 03. 25.]
Совет безопасности обсудит отключение России от глобального интернета, [online], 2014. 09. 19. Forrás: Vedomosztyi [2020. 03. 25.]
Технология из закона о суверенном Интернете ударила по сервисам «Яндекса», [online], 2019. 04. 16. Forrás: Fontanka [2020. 03. 25.]
Tyisina, Julija: Операторы задумались о вещном, [online], 2019. 03. 21. Forrás: Kommerszant [2020. 03. 25.]
Tyisina, Julija – Korcsenkova, Natalja: Суверенный рунет вышел на связь, [online], 2019. 02. 08. Forrás: Kommerszant [2020. 03. 25.]
В Госдуме оценили потери российской экономики в случае отсутствия интернета, [online], 2019. 04. 11. Forrás: TASS [2020. 03. 25.]
Vladimir Putin Q & A and reaction – Thursday 15 December, [online], 2011. 12. 15. Forrás: The Guardian [2020. 03. 25.]
Wikipedia ban lifted after top court ruling issued, [online], 2020. 01. 15. Forrás: Hürriyet Daily News [2020. 03. 25.]
Закон об автономном Рунете не ставит задачу создать „свой интернет", [online], 2018. 12. 14. Forrás: Rosszijszkaja Gazeta [2020. 03. 25.]
Закон об изоляции Рунета прошёл третье чтение в Госдуме, [online], 2019. 04. 16. Forrás: Radio Szvoboda [2020. 03. 25.]
Законопроект № 608767-7 О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», [online], 2019. 05. 01. Forrás: Система обеспечения законодательной деятельности [2020. 03. 25.]
Закон РФ от 27.12.1991 N 2124-1 (ред. от 02.12.2019) „О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.01.2020), [online], 2019. 12. 02. Forrás: Consultant [2020. 03. 25.] DOI: https://doi.org/10.1055/s-0040-1705696
Жаров назвал одной из целей закона о «суверенном рунете» борьбу с Telegram », [online], 2019. 04. 09. Forrás: Kommerszant [2020. 03. 25.]
Zsilin, Ivan: Суверенный интернет не настолько суровый, [online], 2019. 09. 27. Forrás: Novaja Gazeta [2020. 03. 25.]