KOMENTARZE | OSW

Ośrodek Studiów Wschodnich im. Marka Karpia NUMER 313 | 4.12.2019 www.osw.waw.pl

Zakneblować Runet, uciszyć społeczeństwo
Kremlowskie ambicje „suwerenizacji" Internetu

Maria Domańska

Władze Rosji postrzegają Internet przede wszystkim jako pole wojny informacyjnej – alternatywy dla działań militarnych w kontekście utrzymującej się konfrontacji z Zachodem. Elementem tej wojny ma być w percepcji Kremla rozpowszechnianie przez rodzimych internautów treści krytycznych wobec rosyjskich władz. Z tego powodu od lat nasila się dążenie do objęcia Internetu ścisłą kontrolą służb specjalnych i organów ścigania. Przejawia się to zarówno w mnożeniu prewencyjno-represyjnych mechanizmów prawnych, jak i w nielegalnych praktykach, wymierzonych w swobodę wypowiedzi, tajemnicę korespondencji i pluralizm informacyjny.

Strategia władz przynosi jak dotąd ograniczone efekty. W dużej mierze wynika to z istnienia technicznych barier dla poważnego ingerowania w funkcjonowanie rosyjskiego Internetu, dobrze zintegrowanego z globalną siecią. Obieg informacji w sieciach społecznościowych jest wciąż dość swobodny, maleje też podatność internautów na przekaz propagandowy tradycyjnych mediów. Kontynuacja walki z Internetem może w tych warunkach stwarzać polityczne ryzyko dla Kremla, podsycając narastające w Rosji nastroje protestacyjne.

Internet w rosyjskiej sferze społeczno-medialnej

Narodziny rosyjskiego segmentu Internetu (Runetu) datuje się na przełom lat osiemdziesiątych i dziewięćdziesiątych. W przeciwieństwie do Chin, gdzie Internet od początku powstawał pod kontrolą państwa, w Rosji przez pierwszą dekadę rozwijał się on w dużej mierze oddolnie i żywiołowo, z wykorzystaniem coraz nowocześniejszych technologii komunikacyjnych.

Według agencji badań rynku medialnego Mediascope w połowie 2019 r. liczba użytkowników Internetu w Rosji wynosiła prawie 96 mln (78% ludności powyżej 12. roku życia). W ostatnich latach odnotowywany jest jej stały wzrost we wszystkich grupach wiekowych; szczególnie szybko rośnie liczba użytkowników Internetu mobilnego. W listopadzie 2019 r. w systemie e-administracji „Gosusługi" zarejestrowanych było 100 mln osób. Według badań niezależnego Centrum Lewady około 70% ankietowanych korzysta z Internetu co najmniej kilka razy w tygodniu (57% – codziennie)[1].

Rozwój Internetu w Rosji idzie w parze ze wzrostem jego roli jako źródła informacji alternatywnego wobec tradycyjnych mediów (przede wszystkim telewizji – głównego kanału propagandy państwowej). Według danych Centrum Lewady w latach 2009–2019 z 94 do 72% spadł odsetek Rosjan czerpiących informacje

[1] *Mediascope расширила измерения мобильного интернета до всей России*, Mediascope, 16.09.2019, mediascope.net (dane dotyczą użytkowników powyżej 12. roku życia korzystających z Internetu co najmniej raz w miesiącu); *На «Госуслугах» зарегистрировался стомиллионный пользователь*, Радио Эхо Москвы, 26.11.2019, www.echo.msk.ru; *Пользование интернетом*, Левада-Центр, 13.11.2018, www.levada.ru.

z telewizji (jeszcze mniej im ufa: około 55% w porównaniu do 80 przed dekadą), natomiast odsetek osób czerpiących informacje z Internetu i sieci społecznościowych wzrósł z 9 do ponad 30% (zaufanie do takich informacji wzrosło kilkukrotnie i obecnie wynosi około 20%, przy czym występują wyraźne różnice w zależności od grupy wiekowej). Konkurencją dla telewizora stają się przede wszystkim sieci społecznościowe, komunikatory i blogi (popularne zwłaszcza wśród respondentów do 25. roku życia), wciąż w najmniejszym stopniu dotknięte cenzurą i stanowiące popularny i efektywny kanał rozpowszechniania informacji krytycznych wobec władz i przydatnych dla oddolnej mobilizacji potencjału protestacyjnego. W przedziale wiekowym 18–34 lata telewizja ustąpiła już sieciom społecznościowym jako źródło informacji, a wśród młodzieży codziennymi użytkownikami tych sieci jest aż 85% respondentów (najbardziej popularne sieci w Rosji to Vkontakte, Odnoklassniki, YouTube i Instagram)[2]. Rozwój Internetu w FR przyczynia się do coraz częstszego nagłaśniania przypadków korupcji, nadużyć władzy i łamania praw obywatelskich[3].

Logika myślenia władz o cyberprzestrzeni

Ambicją Kremla pozostaje objęcie Internetu podobną kontrolą, jaką na początku lat dwutysięcznych objęto sferę mediów tradycyjnych (wskutek przejmowania aktywów i wprowadzenia nieformalnej cenzury politycznej). Działania te w wielu aspektach stanowią kontynuację sowieckiej tradycji myślenia o sferze telekomunikacji. Podejście to ujawnia bariery mentalnościowe w rozumieniu zasad rządzących rozproszoną, horyzontalną strukturą Internetu. Rosyjskie służby dość dobrze pojmują naturę i skalę związanych z Internetem wyzwań i zagrożeń, zmagają się jednak z technicznymi barierami przeciwdziałania im.

W przeciwieństwie do Chin, gdzie Internet od początku powstawał pod kontrolą państwa, w Rosji rozwijał się on w dużej mierze oddolnie i żywiołowo.

Stosunek władz FR do Internetu jako sfery informacyjnej i przestrzeni komunikacji społecznej wynika z dwóch czynników. Pierwszym jest logika reżimu autorytarnego, traktująca jako bezwzględny priorytet bezpieczeństwo władzy i stabilność społeczną. Drugim – logika działania i postrzegania otaczającego świata przez służby specjalne, z których wywodzą się kluczowi rosyjscy decydenci. Symptomatyczny jest w tym kontekście fragment *Strategii rozwoju społeczeństwa informacyjnego na lata 2017–2030* (przyjętej w 2017 r.), w którym mowa o „priorytecie tradycyjnych rosyjskich wartości duchowo-moralnych i przestrzeganiu wynikających z nich reguł zachowania podczas korzystania z technologii informacyjnych i komunikacyjnych". Strategia zawiera też postulat likwidacji anonimowości w sieci i podkreśla „suwerenne prawo" państwa do określania polityki informacyjnej, technologicznej i ekonomicznej w narodowym segmencie Internetu[4].
Optyka czekistowska, właściwa współczesnym rosyjskim służbom i mająca wiele wspólnego z dziedzictwem sowieckiego KGB, skutkuje m.in. sekurytyzacją sfery wirtualnej. Kluczowe jest tu nie tyle obiektywne zagrożenie, ile kreowanie go bądź wyolbrzymianie w celu realizacji interesów politycznych i finansowych skrzydła „siłowego" we władzach. W logice tej nie ma miejsca na uznanie podmiotowości

[2] *Четверть Россиян потеряли доверие к телевидению за десять лет*, Левада-Центр, 1.08.2019, www.levada.ru.

[3] Д. Гайнутдинов, П. Чиков, *Свобода интернета 2017: ползучая криминализация*, Международная правозащитная группа Агора, 5.02.2018, www.agora.legal.

[4] *Указ Президента РФ от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы"*, Гарант, 11.05.2017, www.garant.ru.

społeczeństwa oraz prawa obywateli do pozyskiwania informacji i swobodnego komunikowania się. Internet postrzegany jest przede wszystkim w kategoriach twardego bezpieczeństwa i obrony państwa przed obcą ingerencją[5]. Przedstawiciele władz wprost definiują globalną sieć jako pole wojny informacyjnej czy wojny psychologicznej, stanowiącej przedłużenie bądź alternatywę dla działań militarnych[6]. Według słów Władimira Putina „Internet pojawił się jako projekt CIA i wciąż jako taki jest rozwijany"[7]. Ze względu na propagandowe założenie o zasadniczej zgodności interesów władzy i społeczeństwa wszelka niezależna działalność, w tym wymiana informacji i krytyka różnych aspektów polityki państwowej, traktowana jest jako skutek inspiracji i manipulacji obcych służb, działalności agenturalnej zmierzającej do wywołania w Rosji „kolorowej rewolucji". Jest ona wskazywana m.in. jako rzeczywista przyczyna narastającego od 2018 r. protestu społecznego wobec polityki Kremla – na tle zarówno socjalnym, jak i politycznym.

Dotychczasowe starania o kontrolę nad Internetem

Choć od początku swego istnienia Runet pozostawał obiektem żywego zainteresowania służb specjalnych (m.in. poprzez inwigilację użytkowników poczty elektronicznej przez Federalną Służbę Bezpieczeństwa dzięki systemom SORM-2 i SORM-3[8]), to przez wiele lat nie podejmowano na większą skalę zinstytucjonalizowanych prób jego cenzurowania. Zaczęły się one na początku pierwszej dekady XXI wieku, a systemową ofensywę przeciwko wolności słowa w Internecie, prawu dostępu do informacji i prawu do tajemnicy korespondencji uruchomiono w roku 2012 – jako odpowiedź na falę moskiewskich protestów politycznych towarzyszących powrotowi Władimira Putina na urząd prezydenta. Protesty te po raz pierwszy na tak znaczną skalę były koordynowane i nagłaśniane dzięki sieciom społecznościowym. Odegrały one istotną rolę również podczas arabskiej wiosny, potraktowanej przez Kreml jednoznacznie jako seria przewrotów państwowych inspirowanych przez Zachód, zorganizowanych przy użyciu technologii opracowanych w USA. Strategia władz rosyjskich oparta jest na logice przeciwdziałania „agresji informacyjnej" ze strony Zachodu i rzekomym próbom destabilizacji Rosji wskutek podsycania nastrojów krytycznych i opozycyjnych wśród obywateli. Logika ta często przysłania toczoną na dalszym planie, uzasadnioną walkę z terroryzmem czy ekstremizmem w sieci. Ta ostatnia, stanowiąca rutynowy przedmiot aktywności służb specjalnych, jest zresztą instrumentalnie wykorzystywana jako argument usprawiedliwiający ograniczanie swobód obywatelskich w Internecie[9].

[5] Rosyjscy decydenci posługują się terminem „bezpieczeństwo informacyjne", pojmowanym odmiennie od pojęcia „cyberbezpieczeństwo" używanego na Zachodzie, gdzie oznacza ono bezpieczeństwo komputerów i systemów komputerowych. Zob. *Kompromaty, a nie cyberwojna*, rozmowa z Iriną Borogan i Andriejem Sołdatowem, 05.2017, dwutygodnik.com.

[6] Logika ta jest widoczna m.in. w Doktrynie bezpieczeństwa informacyjnego Federacji Rosyjskiej przyjętej w 2016 r. – za: Российская Газета, 6.12.2016, www.rg.ru.

[7] *Путин: Интернет возник как проект ЦРУ, так и развивается*, Вести.Ру, 24.04.2014, www.vesti.ru.

[8] SORM – Система технических средств для обеспечения функций оперативно-розыскных мероприятий (System środków technicznych wspomagających czynności operacyjno-śledcze). Kolejne jego generacje wdrażane od połowy lat dziewięćdziesiątych służyły początkowo podsłuchiwaniu rozmów telefonicznych, a następnie śledzeniu przepływu informacji w Internecie. Operatorzy łączności mają ustawowy obowiązek instalowania systemu SORM na łączach, a także przekazywania danych FSB, pod groźbą anulowania licencji.

[9] Instrumentalne wykorzystywanie walki z terroryzmem do poszerzania kompetencji służb specjalnych plasuje Rosję w szerszym trendzie globalnym, widocznym również w zachodnich demokracjach. Należy jednak pamiętać o braku w FR jakichkolwiek bezpieczników – instytucji broniących obywateli przed bezprawnymi działaniami państwa, jak niezawisłe sądy, silne niezależne media czy wyspecjalizowane organy sprawujące kontrolę publiczną nad działaniami decydentów.

Od 2012 r. przyjęto szereg ustaw ograniczających wolność słowa w sieci (zob. Aneks). Zwraca uwagę, że upowszechnianie określonych treści w sferze wirtualnej jest traktowane jako okoliczność obciążająca – nie tylko z uwagi na możliwość dotarcia do dużej i niemożliwej do przewidzenia liczby odbiorców, lecz także ze względu na praktyczny brak możliwości skutecznego zapobiegania rozpowszechnianiu takich publikacji. Kluczowi operatorzy Runetu bez większego oporu podporządkowali się nowym regułom gry i najczęściej blokują treści wskazane przez organy cenzorskie, nawet wbrew obowiązującym procedurom[10]. Dzięki temu do najważniejszych instrumentów polityki państwowej w sferze Internetu należą filtrowanie treści przez serwisy internetowe i blokowanie adresów sieciowych przez operatorów łączności[11].

Formalnie za wdrażanie ustaw odpowiadają instytucje, które często wykorzystują powierzone im w tym zakresie zadania do wzmocnienia swojej pozycji w systemie władzy. Wiodącymi organami pilnującymi „prawomyślności" w sieci są: wśród siłowych – Federalna Służba Bezpieczeństwa (ponadto Ministerstwo Spraw Wewnętrznych, Komitet Śledczy i Prokuratura Generalna), a wśród cywilnych – Federalna Służba ds. Nadzoru w Sferze Łączności, Technologii Informacyjnych i Komunikacji Masowej (Roskomnadzor). Poza instytucjami państwowymi w walce o bezpieczny dla władzy Runet wykorzystywane są cenzorskie pseudo-NGO, tworzone i finansowane przez władze, „oddolnie" walczące z nieprawomyślnymi treściami. Zaliczają się do nich m.in.: Liga Bezpiecznego Internetu, utworzona w 2011 r., uczestnicząca w opracowywaniu pierwszej represyjnej ustawy o jednolitym rejestrze zakazanych stron, oraz tzw. cyberdrużyny, obecne w wielu regionach Rosji. Ich członkowie śledzą posty i dyskusje w sieciach społecznościowych i zgłaszają Lidze przypadki publikowania treści ustawowo zakazanych[12].

Działania Kremla wobec Internetu odzwierciedlają sowiecką tradycję myślenia o sferze telekomunikacji: priorytetem jest bezpieczeństwo autorytarnej władzy.

Wymienione podmioty prowadzą inwigilację użytkowników sieci na szeroką skalę (metodami legalnymi i nielegalnymi)[13]. W 2018 r. tylko na mocy oficjalnych decyzji Roskomnadzoru zablokowanych zostało ponad 160 tys. stron internetowych[14]. Coraz częstsza jest też, sankcjonowana przez ustawy, praktyka blokowania stron bez wyroku sądu. Wymóg sankcji sądu nie stanowi zresztą realnej przeszkody dla działań inwigilacyjnych. Rosyjski wymiar sprawiedliwości pozostaje bowiem całkowicie na usługach organów ścigania i służb specjalnych – w ponad 99% przypadków automatycznie wydaje zgodę na podsłuchiwanie obywateli i dostęp do ich prywatnej korespondencji elektronicznej. Szacuje się, że w latach 2007–2016 inwigilacją na mocy decyzji sądu mogło zostać objętych co najmniej 9 mln obywateli (ok. 6% populacji kraju)[15]. Nie wiadomo natomiast, ilu inwigiluje się bez niej.

[10] Rosyjski rynek usług internetowych, pozornie zdecentralizowany (ogółem kilka tysięcy dostawców usług), jest *de facto* opanowany przez pięć największych firm. Są one bezpośrednio lub pośrednio – dzięki lojalnym biznesmenom – kontrolowane przez państwo. Ich ogólny udział w rynku internetu szerokopasmowego wynosi 70% (w tym państwowy Rostelekom posiada 36% rynku). *Рынок ШПД B2C – 2018*, TMT Консалтинг, 02.2019, www.tmt-consulting.ru.

[11] Д. Гайнутдинов, П. Чиков, *Россия под наблюдением*, Международная правозащитная группа Агора, 16.05.2016, www.agora.legal.

[12] *Регионы заводят себе кибердружины*, Роскомсвобода, 9.10.2019, www.roskomsvoboda.org.

[13] Ciekawych szczegółów na temat systemu inwigilacji dostarczyły dane ujawnione w lipcu 2019 r. przez hakerów, którym udało się włamać do bazy jednego z największych podwykonawców pracujących dla FSB. Zob. А. Сошников, С. Рейтер, *Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ*, Русская служба BBC, 19.07.2019, www.bbc.com/russian.

[14] Д. Гайнутдинов, П. Чиков, *Россия под наблюдением*, *op. cit*.

[15] *Ibidem*.

Efekty działań władz

Choć przyjęte dotychczas ustawy są stosowane na ograniczoną skalę, a część z nich jest bardzo trudna do konsekwentnego egzekwowania, to jednak pełnią one funkcje co najmniej wygodnego „straszaka" i mechanizmu prewencyjnego, mającego zniechęcać obywateli do aktywności w określonych sferach i skłaniać do autocenzury. Jej poziom w Internecie istotnie rośnie, tym bardziej że odpowiedzialnością za upowszechnianie zabronionej informacji objęte są nawet podmioty pośredniczące, przekazujące cudze treści (dotyczy to m.in. agregatorów newsów)[16]. Wyraźnie wzrosła liczba regionów Rosji, w których użytkownicy Internetu zderzają się z poważnym ograniczaniem ich praw. Według organizacji Agora w 2018 r. było ich 41 (w 2017 r. – 26), co stanowi około połowę ogólnej liczby podmiotów Federacji Rosyjskiej. Do tej grupy należy również okupowany Krym, gdzie sytuacja systematycznie się pogarsza[17].

Efektem ofensywy przeciwko wolności Runetu było m.in. zablokowanie kilku serwisów, które odmówiły przeniesienia danych rosyjskich użytkowników na rosyjskie serwery i udostępniania ich korespondencji służbom (jako pierwszą zablokowano w 2016 r. sieć LinkedIn, następnie serwis Zello oraz komunikatory Line i BlackBerry). Jednocześnie dużo łagodniejszą politykę, opartą głównie na perswazji i niewielkich karach finansowych, stosuje się wobec wielkich międzynarodowych graczy: Google'a, Facebooka czy Twittera. Niejasne jest, czy i jakie dane podmioty te przechowują na rosyjskich serwerach, jednak oficjalne statystyki wskazują, że informacje przez nie udostępniane są wykorzystywane w sprawach karnych i administracyjnych sporadycznie (w przeciwieństwie do np. chętnie współpracującej w tym zakresie sieci społecznościowej VKontakte, należącej do okołokremlowskiego oligarchy Aliszera Usmanowa[18]). Gorzej wypadają statystyki dotyczące blokowania treści w Internecie. Według Google Transparency Report z połowy 2018 r. Google spełniał średnio 79% żądań rosyjskich władz dotyczących usuwania treści (w porównaniu z 62% podobnych żądań ze strony władz USA)[19].

Internet postrzegany jest w kategoriach twardego bezpieczeństwa i obrony państwa przed obcą ingerencją: według słów Władimira Putina Internet to projekt CIA.

Efektem represji jest też m.in. stały wzrost liczby osób osądzonych zarówno w trybie administracyjnym, jak i karnym. Prym wiedzie tu art. 282 kodeksu karnego, karzący za propagowanie treści „ekstremistycznych" (często po prostu krytycznych wobec władzy), w tym za pośrednictwem Internetu. W ostatnich latach za aktywność w Internecie procesy karne wytaczano kilkuset osobom rocznie (z czego po kilkadziesiąt skazywano na kary pozbawienia wolności), a kary administracyjne nakładano na kilka–kilkadziesiąt tysięcy[20].

Zacieśnianie kontroli nad Runetem jest odnotowywane przez międzynarodowe organizacje monitorujące przestrzeganie praw człowieka. Według raportu Freedom House (*Freedom on the Net 2018*) na tle utrzymujących się globalnych trendów ograniczania wolności w Internecie (wzrost „cyfrowego autorytaryzmu") Rosja pozostaje krajem „niewolnym". W rankingu

[16] *«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»*, Интервью с руководителем «Роскомсвободы», Информационное агентство "Znak", 21.03.2019, www.znak.com.

[17] Д. Гайнутдинов, П. Чиков, *Свобода интернета 2018: делегирование репрессий*, Международная правозащитная группа Агора, 5.02.2019, www.agora.legal.

[18] *Ibidem*. W ostatnich latach największą liczbę spraw karnych wszczynano wobec użytkowników VKontakte. W 2018 r. co najmniej 19 osób korzystających z tej sieci skazano na kary więzienia, co stanowiło 76% wszystkich tego rodzaju wyroków (w przypadku YouTube'a i Telegramu dotyczyło to łącznie czterech osób, a Facebooka – jednej).

[19] *Ibidem*.

[20] *Ibidem*.

zajęła ona 53. miejsce na 65 badanych krajów, w których ogółem zamieszkuje 87% wszystkich użytkowników Internetu[21].

Mimo przyjęcia szeregu ustaw ograniczających wolność słowa w sieci represyjna strategia władz przynosi ograniczone efekty.

Efektywność strategii władz pozostaje jednak ograniczona. Opór właścicieli serwisów internetowych oraz korzystanie przez użytkowników z technologii umożliwiających obchodzenie zakazów (programy anonimizujące, VPN-y, TOR) mogą skutecznie uniemożliwić władzom osiągnięcie ich celów. Mimo wpisania w 2016 r. na „czarną listę" Roskomnadzoru rekordowej liczby stron internetowych z nielegalną zawartością w lutym 2017 r. 65% z nich wciąż funkcjonowało[22]. Również autocenzura jak dotąd w najmniejszym stopniu dotyczy sieci społecznościowych – stąd próby FSB zdobycia tzw. kluczy szyfrowania, umożliwiających pełny, niekontrolowany dostęp do korespondencji między ich użytkownikami. Powyższe mechanizmy świetnie ilustruje przykład nieudanej blokady komunikatora Telegram[23] – próby zdobycia kluczy, a następnie zablokowania serwisu zakończyły się spektakularną porażką po stanowczej odmowie współpracy ze strony właściciela. Po półtora roku takich zabiegów Telegram nadal działa, natomiast blokadą objęto przejściowo około 20 mln adresów IP, co spowodowało problemy w funkcjonowaniu wielu stron i serwisów internetowych[24].

Rosnąca wiedza Rosjan na temat wykorzystywania technologii anonimizujących i oprogramowania umożliwiającego obchodzenie blokad[25], a także gotowość do korzystania z płatnych VPN-ów i anonimizerów stanowią nieprzewidziany przez władze skutek zacieśniania kontroli nad sferą pozostającą do niedawna jedynym stosunkowo swobodnym segmentem aktywności społeczno-politycznej w Rosji.

Jakościowy przełom? Ustawa o „suwerennym Internecie"

Problemy z kontrolowaniem treści zamieszczanych w sieci zaowocowały ustawą o „suwerennym Internecie"[26], zainicjowaną najpewniej przez szefa pionu polityki wewnętrznej Administracji Prezydenta Siergieja Kirijenkę. Jej deklarowanymi celami są stworzenie infrastruktury i procedur pozwalających na scentralizowane (bez pośrednictwa operatorów) zarządzanie Runetem w sytuacji odcięcia go od zagranicznych serwerów (np. wskutek „agresji cybernetycznej" USA), a także zminimalizowanie komponentu transgranicznego w komunikacji między rosyjskimi użytkownikami. Operatorzy zostaną zobowiązani m.in. do zainstalowania na łączach „technicznych środków przeciwdziałania zagrożeniom" (chodzi o technikę sieciową DPI – Deep Packet Inspection – pozwalającą na analizowanie treści pakietów danych), jak również do współdziałania z organami ścigania

[21] W skali od 0 do 100, gdzie 0 oznacza całkowitą wolność, a 100 całkowity brak wolności. *Freedom on the Net 2018*, Freedom House, 10.2018, www.freedomhouse.org.

[22] Д. Линделл, А. Балашова, И. Ли, *В России продолжили работать 65% заблокированных сайтов*, РБК, 16.02.2017, www.rbc.ru.

[23] K. Chawryło, *Rosja: blokada komunikatora internetowego Telegram*, 18.04.2018, www.osw.waw.pl.

[24] Szczegóły zob. Д. Гайнутдинов, П. Чиков, *Свобода интернета 2018: делегирование репрессий*, *op. cit.*

[25] Po tym, jak w 2015 r. zablokowano stronę z pirackimi treściami Rutracker.ru, Rosja zajęła drugie po USA miejsce na świecie, jeśli chodzi o liczbę użytkowników sieci TOR. Zob. *Kompromaty, a nie cyberwojna*, *op. cit.*

[26] Więcej na temat ustawy zob. M. Domańska, *Twierdza Runet: walka Kremla z „wrogim" Internetem*, 19.04.2019, www.osw.waw.pl. Podobne inicjatywy były zgłaszane już w latach 2006–2007 w kontekście pogarszających się relacji z Zachodem. О. Бешлей, Е. Нестерова, Д. Трещанин, *Кто и как придумал «суверенный рунет». Рассказы инсайдеров*, Настоящее Время, 22.04.2019, www.currenttime.tv.

w zakresie testowania bezpieczeństwa Internetu. Ponadto do końca 2020 r. ma zostać utworzony „narodowy system nazw domenowych", autonomiczny wobec globalnego systemu DNS zarządzanego przez znajdującą się w USA organizację ICANN. Większość przepisów ustawy weszła w życie 1 listopada 2019 r., pozostałe zaczną obowiązywać w styczniu 2021 r.

Formalne uzasadnienie ustawy wydaje się mieć niewiele wspólnego z jej realnymi celami. Dotychczas nie było precedensu, by jakiekolwiek państwo zostało z zewnątrz odizolowane od Internetu. Ponadto już teraz kluczowe instytucje państwowe są połączone siecią „intranetową" umożliwiającą w razie potrzeby funkcjonowanie w zamkniętym obiegu, a przez zagraniczne serwery przechodzi maksymalnie 3% wewnątrzrosyjskiego ruchu internetowego (dla porównania we Francji jest to ponad trzykrotnie więcej)[27]. Przy tym paradoksalnie centralizacja zarządzania Internetem zmniejszyłaby, a nie zwiększyła jego odporność na ataki[28].

Wszystko wskazuje zatem na dążenie Kremla do udoskonalania mechanizmów zarządzania Runetem w celu blokowania dostępu do Internetu wewnątrz kraju, np. w przypadku groźby destabilizacji sytuacji społeczno-politycznej[29]. „Suwerenizacja" oznacza tu więc nie tyle autonomię względem zagranicy, ile pełnię władzy sprawowanej na własnym terytorium. Główną ambicją rządzących wydaje się skonstruowanie „inteligentnego" systemu zarządzania łącznością internetową, tak by w razie potrzeby móc punktowo, bez szkody dla ogółu użytkowników i bez pośrednictwa operatorów, odłączać Internet na obszarach objętych protestami społecznymi bądź wybranym grupom użytkowników, blokować już nie tylko wybrane adresy IP, lecz także konkretne treści, jak również wybiórczo spowalniać przepływ określonych danych lub przepływ na określonych trasach[30].

„Suwerenizacja" Runetu ma na celu blokowanie dostępu do sieci w przypadku masowych protestów, może też doprowadzić do stopniowej centralizacji i nacjonalizacji rynku usług internetowych.

Techniczne możliwości realizacji ustawy stoją jednak pod znakiem zapytania. Jak dotąd liczne opublikowane akty wykonawcze nie rozwiały większości wątpliwości zgłaszanych przez ekspertów. Niejasne jest, w jaki sposób władze chcą zarządzać trasami przesyłu danych czy stworzyć „narodowy system nazw domenowych". Według dostępnych informacji dotychczasowe testy techniki DPI zakończyły się niepowodzeniem, a ubocznym efektem jej zastosowania było drastyczne spowolnienie Internetu. Na uwagę zasługuje fakt, że wybrano DPI produkowane przez firmę RDP.RU, kontrolowaną przez państwowy Rostelekom, w którym znaczne wpływy ma inicjator ustawy Siergiej Kirijenko[31]. Pomijając fakt, że wbrew stanowisku rządu do momentu wejścia w życie ustawy nie uregulowano kryteriów certyfikacji DPI, specjaliści spierają się co do technicznych możliwości skutecznego funkcjonowania tego narzędzia na tak dużą skalę (jak dotąd jest ono wykorzystywane jedynie na poziomie firm). Skutki uboczne w wymiarze makro zagrażałyby płynnemu funkcjonowaniu całej sfery

[27] Е. Баленко, *Эксперты оценили уровень «суверенности» Рунета*, РБК, 9.04.2019, www.rbc.ru.

[28] *«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»*, Интервью с руководителем «Роскомсвободы», *op. cit.*

[29] Precedensy miały już miejsce, dotyczyły m.in. blokowania na poziomie całego regionu dostępu do sieci w Inguszetii podczas protestów politycznych w latach 2018–2019. Zob. А. Корня, В. Кодачигов, *Житель Ингушетии пожаловался в суд на отключение мобильного интернета*, Ведомости, 24.03.2019, www.vedomosti.ru.

[30] W kwietniu 2019 r. szef Roskomnadzoru Aleksandr Żarow wprost zapowiedział, że realizacja ustawy umożliwi blokowanie zasobów internetowych zakazanych w Rosji, w tym pomoże zablokować Telegram.

[31] Е. Серьгина, *Сын Сергея Кириенко внезапно стал вторым топ-менеджером «Ростелекома»*, Ведомости, 28.09.2016, www.vedomosti.ru.

finansowo-gospodarczej Rosji. W tym kontekście na paradoks zakrawa, że koszty zakupu systemów DPI mają być pokrywane ze środków budżetowych zarezerwowanych na rozwój gospodarki cyfrowej[32].

Prognoza

W warunkach stagnacji gospodarczej, zachodnich sankcji ekonomicznych oraz pogarszającej się sytuacji materialnej obywateli i spadającego poparcia społecznego dla władz Kreml – w obawie przed wybuchem protestów społecznych na znacznie większą niż dotąd skalę – będzie próbował udoskonalać mechanizmy prewencji i represji. Podobnie jak wiele innych ustaw przepisy o „suwerennym Runecie" mogą długo pozostać „uśpione", zwłaszcza jeśli sytuacja polityczna pozostanie stabilna. Należy jednak zakładać, że testy z zakresu udoskonalania mechanizmów blokad oraz filtrowania zawartości stron internetowych i korespondencji elektronicznej będą w najbliższych latach kontynuowane. Pojawiły się też pomysły przejścia na wykorzystywanie w Runecie wyłącznie rosyjskiego oprogramowania szyfrującego[33], co dawałoby FSB swobodny dostęp np. do dotychczas niedostępnych treści przesyłanych komunikatorami. Niejasne jest jednak, w jaki sposób zmusić do używania go ogół rosyjskich internautów. Wszystkie te kwestie będą stanowiły kolejne negatywne sygnały dla inwestorów zagranicznych.

„Suwerenizacja" Runetu stwarza ponadto pole do ogromnych nadużyć finansowych i wyprowadzania znacznych sum z budżetu państwa przez producentów sprzętu i oprogramowania. Wraz z wymogami proceduralnymi, wynikającymi m.in. z realizacji poleceń stawianych przez służby specjalne, może to doprowadzić do wypierania z rynku mniejszych operatorów rosyjskich i podmiotów zagranicznych, a tym samym do stopniowej centralizacji i nacjonalizacji rynku usług internetowych. Kontynuacja walki z Runetem może też stanowić kolejny poważny punkt zapalny w relacjach władzy ze społeczeństwem. W niezależnym sondażu z początku 2019 r. około 70% ankietowanych skrytykowało projekt ustawy o „suwerennym Internecie"; większość wskazała, że osobiście odczuje jej negatywne skutki[34]. W marcu 2019 r. kilkanaście tysięcy osób wyszło na ulice Moskwy w proteście przeciwko projektowi (mniejsze wiece odbyły się też w kilku innych miastach).

[32] Z budżetu państwa wydzielono na ten cel około 21 mld rubli (prawie 330 mln USD). Według ocen rządowych ekspertów w związku z wdrażaniem ustawy operatorzy łączności internetowej poniosą ogółem koszty rzędu 130 mld rubli (ponad 2 mld USD). Zob. *«Если будем молчать, на наших кухнях появятся видеокамеры ФСБ»*, Интервью с руководителем «Роскомсвободы», *op. cit.*

[33] М. Коломыченко, *ФСБ предложила шифровать данные в Рунете «Кузнечиком»*, РБК, 24.06.2019, www.rbc.ru.

[34] *Независимый соцопрос: «Изолированный Рунет нам не нужен!»*, Роскомсвобода, 21.03.2019, www.roskomsvoboda.org.

ANEKS

Ustawy ograniczające swobodę korzystania z Internetu w Rosji

Ustawa	Data przyjęcia	Założenia
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji"	28.07.2012	Ustawa dała Roskomnadzorowi prawo do blokowania bez sankcji sądu stron internetowych, na których pojawiają się szkodliwe treści (pornografia dziecięca, promowanie narkotyków i samobójstw). Powstała wówczas „czarna lista" zakazanych stron, które operatorzy mieli obowiązek blokować. Miały na nią również trafiać strony zawierające treści ekstremistyczne – jednak niezbędny był do tego prawomocny wyrok sądu.
Nowelizacja ustawy „O ochronie dzieci przed szkodliwymi informacjami"	29.06.2013	Ustawa zakazała „propagandy homoseksualizmu wśród nieletnich" oraz zaostrzyła kary za obrazę uczuć religijnych. Wpisywała się w nurt piętnowania przez państwową propagandę przejawów „zachodniej" dekadencji i demoralizacji oraz krzewienia „tradycyjnych" rosyjskich wartości.
Nowelizacja kodeksu karnego	30.06.2013	Nowelizacja zaostrzała kary za publiczną obrazę uczuć religijnych (do trzech lat pozbawienia wolności) i stanowiła reakcję na anty-Putinowski happening grupy Pussy Riot w moskiewskim soborze katedralnym.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji" (tzw. ustawa Ługowoja)	30.12.2013	Ustawa znosiła wymóg sankcji sądu dla wnoszenia przez Roskomnadzor na „czarną listę" i blokowania stron internetowych zawierających „wezwania do działalności ekstremistycznej i masowych rozruchów". W myśl ustawy Roskomnadzor podejmuje czynności na wniosek Prokuratury Generalnej. Definicja ekstremizmu jest w praktyce bardzo szeroka – tym samym ustawa umożliwia blokowanie treści wyłącznie ze względu na ich krytyczny wobec władz charakter. W przypadku prowokacji (np. umieszczenia szkodliwych treści w komentarzach internautów) daje to pretekst do zamykania niewygodnych dla władz stron internetowych. Często też, podobnie jak w ustawie z 29.07.2012, nie jest uwzględniany kontekst, w jakim dane treści się pojawiają. W połowie 2017 r. Roskomnadzor poinformował, że w ciągu pięciu lat obowiązywania nowelizacji dotyczących „czarnej listy" wpisano na nią 275 tys. stron internetowych.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji" (tzw. ustawa o blogerach)	5.05.2014	Ustawa utrudniała publikowanie treści w Internecie, m.in. poprzez nałożenie na popularnych blogerów ograniczeń typowych dla mediów (m.in. nakazała blogerom czytanym przez ponad trzy tysiące osób dziennie obowiązek rejestracji i ujawnienia danych osobowych oraz nałożyła odpowiedzialność za rozpowszechnianie nieprawdziwych i ekstremistycznych informacji). Ustawa pozostawała przez kilka lat martwą literą; w lipcu 2017 r. przepisy dotyczące blogerów utraciły moc w wyniku kolejnej nowelizacji.
Nowelizacja kodeksu karnego	30.06.2014	Ustawa wprowadziła odpowiedzialność karną za wezwania do działalności ekstremistycznej z wykorzystaniem Internetu (do pięciu lat pozbawienia wolności).

Ustawa	Data przyjęcia	Założenia
Nowelizacja przepisów o danych osobowych (ustawa o „lokalizacji danych osobowych")	21.07.2014	Ustawa nałożyła na osoby prawne obowiązek przechowywania danych osobowych obywateli FR wyłącznie na terytorium Rosji. Jej celem było ułatwienie dostępu służb specjalnych do danych osobowych obywateli, poważnie ograniczyła też ona możliwości używania serwerów zagranicznych na potrzeby działalności niezależnej od władz.
Nowelizacja ustawy „O mediach"	15.10.2014 (weszła w życie 1.01.2016)	Ustawa ograniczyła dopuszczalny udział kapitału zagranicznego w rosyjskich mediach do 20%, zakazała też obywatelom obcych państw zakładać w Rosji środki masowego przekazu. Miała na celu likwidację lub przejęcie kontroli politycznej nad popularnymi mediami krytycznymi wobec polityki Kremla. Media miały czas do lutego 2017 r., żeby dostosować swoją strukturę właścicielską do wymogów ustawy.
Nowelizacja przepisów o terroryzmie i nowelizacja kodeksu karnego (tzw. pakiet Jarowej)	6.07.2016	Ustawa zawierała kontrowersyjny nakaz przechowywania przez operatorów łączności oraz właścicieli zasobów internetowych i komunikatorów przesyłanych w Internecie treści tekstowych i audiowizualnych, a także nagrań rozmów telefonicznych i SMS-ów przez okres sześciu miesięcy oraz udostępniania ich służbom specjalnym bez nakazu sądu. Inną kontrowersyjną kwestią był obowiązek udostępniania kluczy szyfrujących do komunikatorów internetowych na żądanie FSB.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji" (tzw. ustawa o anonimizerach)	29.07.2017	Ustawa zakazała operatorom serwisów anonimizujących, sieci VPN, serwerów proxy i sieci TOR (narzędzi służących do obchodzenia blokad treści lub ukrywania tożsamości) umożliwiania internautom dostępu do stron internetowych zablokowanych przez Roskomnadzor.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji"	31.07.2017	Ustawa znosiła anonimowość użytkowników komunikatorów internetowych, uzależniając (od stycznia 2018 r.) możliwość korzystania z komunikatorów od uprzedniej rejestracji przy użyciu numeru abonenckiego.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji" oraz ustawy „O mediach"	25.11.2017	Ustawa umożliwiła nadawanie mediom zagranicznym działającym na terenie Rosji statusu „agenta zagranicznego" (wprowadzonego nowelizacją przepisów o organizacjach pozarządowych z 2012 r.). Wprowadziła też możliwość blokowania bez wyroku sądu stron internetowych „organizacji niepożądanych" (ustawa o „organizacjach niepożądanych" z maja 2015 r. dotycząca zagranicznych i międzynarodowych NGO działających w Rosji zakazuje działalności podmiotów „zagrażających podstawom ustroju konstytucyjnego lub obronności i bezpieczeństwu państwa").

Ustawa	Data przyjęcia	Założenia
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji"	18.03.2019	Pakiet nowelizacyjny wprowadził do rosyjskiego prawa dwie istotne zmiany zaostrzające cenzurę w Internecie. Pierwszą jest zakaz rozpowszechniania nieprawdziwych informacji (fake newsów), m.in. stwarzających zagrożenie dla „zdrowia lub życia obywateli lub ryzyko masowego zakłócenia porządku lub bezpieczeństwa publicznego". Drugą są kary za rozpowszechnianie informacji, które w formie „obrażającej moralność publiczną i godność ludzką wyrażają brak szacunku wobec społeczeństwa, państwa, symboli państwowych, konstytucji lub organów sprawujących władzę państwową w Federacji Rosyjskiej". Z uwagi na szerokie, dające możliwość niemal dowolnych interpretacji definicje użyte w przyjętych przez parlament ustawach, a także dyspozycyjność rosyjskich sądów oba projekty *de facto* pozwalają karać obywateli za jakąkolwiek formę krytyki władzy i za zamieszczanie w mediach wszelkich informacji kompromitujących przedstawicieli władz, a niepotwierdzonych przez oficjalne źródła.
Nowelizacja ustawy „O informacji, technologiach informacyjnych i ochronie informacji" oraz ustawy „O łączności" (tzw. ustawa o „suwerennym Internecie")	1.05.2019 (większość przepisów działa od 1.11.2019, pozostałe wejdą w życie 1.01.2021)	Deklarowanym celem ustawy jest stworzenie infrastruktury pozwalającej na funkcjonowanie Runetu w sytuacji odcięcia go od zagranicznych serwerów. Na wypadek wystąpienia zagrożeń dla bezpieczeństwa Runetu ma zostać stworzony system scentralizowanego zarządzania przez państwo łącznością internetową na terytorium Federacji Rosyjskiej, w tym punktami wymiany ruchu sieciowego i transgranicznym przesyłem danych.

REDAKCJA MERYTORYCZNA: Adam Eberhardt,
Marek Menkiszak
REDAKCJA: Szymon Sztyk, Tomasz Strzelczyk
SKŁAD: Urszula Gumińska-Kurek, Wojciech Mańkowski

Ośrodek Studiów Wschodnich im. Marka Karpia
ul. Koszykowa 6a, 00-564 Warszawa
tel.: | +48 | 22 525 80 00

Opinie wyrażone przez autorów analiz nie przedstawiają oficjalnego stanowiska władz RP.

Zapraszamy na naszą stronę: **www.osw.waw.pl**