Geopolitica.info

RUSSIA

Ru-Splinternet. La sovranita´digitale in Russia

A cura di *Alessia Sposini*

20 OTTOBRE 2020

Il tentativo della Russia di estendere la propria sovranità esclusiva sulla Rete si inserisce all'interno di un più ampio sforzo di alcuni Stati di regolamentare Internet in maniera sempre più stringente. L'analisi dei provvedimenti adottati da Mosca nell'ultimo anno mostra, però, anche dei tratti peculiari. Il fenomeno della frammentazione, ovvero la progressiva perdita del carattere globale della rete Internet in favore dell'esercizio della Sovranità nazionale degli Stati, trova infatti nel caso russo un'interessante conferma.

DOMINO – Geopolitical Brief n. 8 / ottobre 2020 | Aut. Trib. Roma n. 88 - 6 marzo 2008
Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info
Direttore responsabile: Lorenzo Termine

Dal momento in cui nasce e si sviluppa sulla linea guida di un linguaggio comune, come quello degli indirizzi IP e di un'unica radice DNS, Internet è stato rappresentato come tendente all'unità *by design.* Al contrario, la frammentazione consiste nell'interruzione di tale unità della rete Internet globale, allo scopo di creare delle reti nazionali sovrane e isolate dal resto del mondo. Tale processo, fino ad ora mai portato a termine in maniera radicale da alcuno stato, ma anticipato dal "Great Firewall" cinese dalla fine degli anni '90, presenta dei problemi strutturali. L'utilizzo del termine frammentazione fa riferimento a un distacco tecnico intenzionale[1], parte di una politica più ampia attuata da un determinato Stato. In questo solco, si inserisce il caso specifico della Federazione Russa che, con l'ultimo pacchetto di leggi di emendamento **90-FZ**[2] riguardante la "sfera dell'informazione", ha predisposto le basi per una separazione della rete Internet russa da quella globale, aumentando il rischio della "balcanizzazione di Internet".

La creazione di una **RuNet sovrana** fa d'altronde parte di un progetto politico ben preciso, con a capo una visione di Sicurezza Nazionale delineatasi già a partire dai primi anni 2000. La particolarità dell'approccio russo alla Sovranità Digitale risiede nella sinergia tra attori e approcci differenti che hanno portato alla creazione di un substrato culturale unico. L'esistenza di una "cultura hacker" di derivazione comunista, di un approccio quasi onnicomprensivo alla "sfera delle informazioni" della Federazione e di una compenetrazione profonda tra Sicurezza nazionale, strategia militare e vita civile, ha permesso la nascita di un approccio olistico alla sfera digitale.

Dottrina della Federazione Russa in materia di Sicurezza delle Informazioni

La **Dottrina sulla Sicurezza delle Informazioni della Federazione Russa**[3], approvata con decreto del Presidente della Federazione Russa Vladimir Putin No.646 del 5 dicembre 2016, è andata a sostituire la precedente Dottrina, risalente all'anno 2000. Il

1 Mueller, M. (2017). *Will the Internet Fragment?* Cambridge: Polity Press.
2 Federal Law 90-FZ (2019) "On Amendments to the Federal Law On Communications and the Federal Law On Information, Information Technologies and the Protection of Information" (http://publication.pravo.gov.ru/Document/View/0001201905010025?index=28&rangeSize=1 ultimo accesso: 19/10/2020)
3 Doctrine of Information Security of the Russian Federation (2016) (https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB ultimo accesso: 19/10/2020)

documento, composto di soli 38 articoli è più "snello" rispetto al suo predecessore, integra quanto già previsto dalla Strategia di Sicurezza della Federazione Russa (2015 No.683). Il testo del 2016 stabilisce le priorità della sicurezza nazionale della Federazione nell'ambito della "**sfera delle informazioni**". Una delle novità introdotte dal testo è racchiusa proprio nella definizione della suddetta sfera. In quest'ultima, infatti, ricadono una combinazione di elementi, tra i quali tutta l'"informazione" e tutti i "sistemi informativi e siti web all'interno della rete di informazione e telecomunicazioni di Internet", nonché le "entità coinvolte nella generazione e nell'elaborazione delle informazioni" e "nello sviluppo e nell'utilizzo delle suddette tecnologie". La terminologia "sfera delle informazioni" allude dunque ad un campo estremamente ampio, quasi onnicomprensivo. Tra gli interessi nazionali riconosciuti da tale dottrina rientrano anche l'utilizzo delle tecnologie dell'informazione al fine di preservare i valori della cultura, della storia, della spiritualità e della morale della Federazione Russa.

Le aree chiave della strategia sono cinque: primo, deterrenza strategica e prevenzione dei conflitti cibernetici; secondo, miglioramento del sistema di sicurezza informatica della Federazione; terzo, previsione, identificazione e valutazione delle minacce informative; quarto, promozione degli interessi degli alleati della Federazione; quinto, controbilanciamento delle azioni informative e psicologiche. Come evince dall'ultimo punto, la "difesa della patria" e dei suoi valori non è solo uno dei principi guida della sicurezza nazionale, ma si costituisce anche come un elemento chiave degli obiettivi strategici. La sovranità digitale in senso forte[4], cioè intesa come la coincidenza perfetta tra confini territoriali dello stato e confini ideali della rete, deriva da tale postura strategica ed è fortemente radicato in tutta la macchina statale.

Subcultura Hacker: una strana normalità

Un altro degli elementi chiave nell'approccio russo alla sfera del digitale è da ricercare nel substrato culturale "hacker". La figura dell'hacker – non solamente in Russia, ma anche nel resto del mondo – ha apportato un contributo sociale intrinseco allo sviluppo di Internet. Confidando nel principio di reciprocità, la libertà con cui gli hacker accedono ad informazioni – piuttosto che a pro-

4 Per un approfondimento circa la distinzione tra "sovranità debole" e "sovranità forte" si veda Couture, S., Toupin, S. (2019). "What does the notion of "sovereignty" mean when referring to the digital?", *New Media & Society*, Vol. 21, No. 10, pp. 2305-2322 (https://doi.org/10.1177%2F1461444819865984)

grammi – e li divulgano, talvolta modificandoli *in melius*, è uno dei motori dietro la crescita di Internet. Pur non esistendo una "comunità hacker" *tout court*, si possono identificare alcuni elementi ricorrenti quando ci si riferisce a tali figure: la liberalizzazione dell'accesso alle informazioni, il rigetto della cultura consumista e il credo nell'abilità del computer di fare la differenza in un ipotetico scontro con la "cultura di massa".

Quello che è accaduto in Russia a partire dagli anni '90 è stato un progressivo adattamento delle sopra menzionate caratteristiche della **subcultura hacker** agli usi e costumi di una porzione di popolazione russa. Ad esempio, la "liberalizzazione delle informazioni" trova terreno fertile nella società di derivazione comunista, vista l'assenza di un "istituto di proprietà intellettuale come nell'Europa occidentale e negli Stati Uniti"[5]. Questo vuole dire che l'*open source* era la norma ancora prima di essere concepito come tale. Vien da sé che il rigetto della cultura consumista, altro caposaldo della sottocultura hacker, era già presente nella sfera ideologica dell'Unione Sovietica. La figura dell'hacker in Russia, dunque, si pone nel duplice ruolo sia dell'essere sostanzialmente un "criminale", ma anche – e soprattutto – di essere una figura con un grande supporto pubblico e statale.

La legge sull'Internet Sovrano, verso una frammentazione reale della Rete?

Legge Federale 90-FZ

La Legge Federale 90-FZ è stata firmata dal Presidente della Federazione Russa Vladimir Putin il 1° maggio 2019 ed è entrata in vigore nella sua quasi totalità il 1° Novembre dello stesso anno, mentre alcune implementazioni seguiranno entro gennaio del 2021. L'insieme di emendamenti che compongono il testo risulta essere, come già anticipato, uno degli step più recenti all'interno di un quadro normativo estremamente stratificato in materia di "sfera dell'informazione". I punti salienti tale riforma sono tre, di seguito illustrati.

1) Implementazione di un DNS, Domain Name System

L'implementazione di un **DNS**, Domain Name System, russo al fine di "garantire sicurezza e stabilità". Come evidenziato nel te-

5 Si veda Dremliuga, R. (2014). "Subculture of Hackers in Russia", *Asian Social Science*,Vol. 10, No. 18, pp. 10-18. (https://doi.org/10.5539/ass.v10n18p158)

sto, il nuovo DNS nazionale sarà progettato per "memorizzare e ottenere informazioni su indirizzi di rete e nomi di dominio"[6]. Le modalità attraverso le quali sarà consentito l'accesso alle suddette informazioni verranno definite dall'organo preposto, il *Roskomnadzor*, investito – non per la prima volta – di un potere non indifferente. Il *Roskomnadzor*, o ***Роскомнадзор***, è il "**Servizio federale per la supervisione nella sfera della connessione e comunicazione di massa**". Re-istituito nel 2008, tale organismo si occupa del controllo, della supervisione e della censura, o oscuramento, dei media e delle telecomunicazioni. Il Servizio è altresì l'organo federale autorizzato alla protezione dei dati personali dei cittadini russi.

La frammentazione di Internet per essere effettiva deve avere radici tecniche che portino ad una sistematica incompatibilità dei mezzi nazionali con l'intero sistema internazionale e la creazione di un DNS russo non sfugge a tale logica. La funzione dell'unità tecnica Internet, infatti, è presieduta dal sistema DNS, il quale assicura un'attribuzione univoca e inequivocabile tra un dato nome/dominio e un utente. Esiste quindi una gerarchia che regola l'interoperabilità in Internet, con una singola radice DNS al vertice, quella gestita da ICANN, *Internet Corporation for Assigned Names and Numbers*, che stabilisce le politiche in cui opera la IANA, *Internet Assigned Numbers Authority*. L'interoperabilità non è connaturata solamente alla singola istituzione, ma è anche tra le istituzioni: gli indirizzi IP e il sistema DNS sono abbinati tra loro per il singolo utente "risolvendo" un nome di dominio, una configurazione tecnica.

2) Gestione centralizzata della rete delle telecomunicazioni in caso di minaccia e meccanismo di controllo per le linee di connessione che attraversano i confini della Russia

In caso di minaccia alla rete delle telecomunicazioni, il *Roskomnadzor* è autorizzato ad assumere il controllo della rete. Stabilire una possibilità di un controllo centralizzato della rete porta con sé un rischio strutturale: quello di portare, in caso di "pericolo", all'adozione di pratiche quali lo *shutdown* arbitrario della rete Internet[7]. Le **minacce** che attivano l'intervento diretto del *Roskomnadzor* sono: di integrità, di stabilità o di sicurezza della rete. La

6 Vedi nota 2: Federal Law 90-FZ (2019)

7 Si veda Epifanova, A. (2020). "Deciphering Russia's "Sovereign Internet Law". Tightening Control and Accelerating the Splinternet", *DGAP Analysis*, No. 2 (https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law ultimo accesso: 19/10/2020)

definizione della tipologia di minacce rimane – forse volutamente – evanescente circa la singola fattispecie.

Uno dei punti di ulteriore interesse della Legge Federale 90-FZ è quello inerente le linee di comunicazione che oltrepassano i confini nazionali. L'emendamento punta a stabilire dei punti di snodo del traffico nazionale/internazionale in coincidenza con i confini territoriali della Federazione, col fine di poter controllare fisicamente il passaggio del traffico Internet.

Legge Federale 242-FZ

La definizione dei confini nell'immaterialità teorica del cyberspazio era già giunta ad un punto di svolta nel 2014, mediante l'adozione della Legge Federale **242-FZ**[8]. Tale emendamento ha reso obbligatoria la localizzazione dei dati personali riguardanti i cittadini russi su server basati all'interno dei confini nazionali. Il non soddisfacimento di tali requisiti da parte degli operatori esteri avrebbe dovuto portare alla soppressione del servizio del suddetto operatore in Russia. Tuttavia, più che bloccare e oscurare le piattaforme di compagnie estere come – ad esempio – Facebook e Twitter per non aver aderito agli standard, sono state erogate salate sanzioni pecuniarie[9]. Un'altra difficoltà per l'applicazione di tale legge è stata rappresentata dalla giurisdizione della stessa, come è possibile definire i "cittadini russi" su Internet? L'operatore responsabile della raccolta dati, in breve, si trova di fronte alla problematica di definire di quali utenti deve trattenere le informazioni localmente e di quali no. Come identificare la cittadinanza del soggetto dei dati personali è questione dell'operatore. Risulta, tuttavia, preferibile seguire le indicazioni del *Roskomnadzor* che suggerisce di sostituire al criterio di nazionalità quello di residenza, nel senso che i dati da ritenere oggetto della legge sono tutti quei dati raccolti nei territori della Russia, aggiungendo un secondo elemento fisico e territoriale nella definizione di tale legge.

3) Installazione obbligatoria di equipaggiamento tecnico per contrastare le minacce alla rete Internet

La legge 90-FZ ha altresì introdotto l'obbligo per gli operatori che forniscono servizi di accesso alla rete Internet, di installare un equipaggiamento tecnico per contrastare "le minacce alla stabili-

8 Federal Law 242-FZ (2014) "On Amending Certain Legislative Acts of the Russian Federation Regarding Specification of the Procedure for Processing personal Data in Information and Telecommunication Networks" (https://rg.ru/2014/07/23/persdannye-dok.html ultimo accesso: 19/10/2020)

9 Come da decisioni della Corte magistrale del distretto giudiziario di Tagansky di Mosca del 13 febbraio 2020, Facebook e Twitter sono state multate per una somma di 4 milioni di Rubli ciascuna (https://www.dataguidance.com/notes/russia-data-protection-overview ultimo accesso: 19/10/2020)

tà, alla sicurezza e all'integrità funzionale di Internet e della rete pubblica di comunicazione"[10] nel territorio della Federazione Russa. Tali operatori sono gli **ISP**, *Internet Service Provider*, ovvero un fornitore di servizi Internet, la cui categoria viene identificata però in base alla tipologia del servizio offerto. Un ISP può, dunque, essere un fornitore di accesso alla rete Internet, o di servizi quali contenuti propri o messi in rete dagli utenti, di posta elettronica, e via discorrendo.

Al di là dell'ovvia compromissione di una qualsiasi neutralità della rete, tra le preoccupazioni che tale punto ha sollevato, vi è che l'installazione di tali mezzi tecnici possa dare la capacità al *Roskomnadzor* di dare priorità a taluni fornitori di servizi rispetto ad altri. In prospettiva, l'organizzazione potrebbe garantire *performances* migliori a determinati fornitori di rete. Ne risulterebbe la creazione di fornitori di "serie A" e fornitori di "serie B", di fatto discriminando arbitrariamente tra gli operatori.

Conclusioni

La mobilitazione russa nel ciberspazio continua a rappresentare un *case study* estremamente particolare. L'aspetto stato-centrico della narrazione sulla sovranità, così come perseguita dalla Federazione, si posiziona come diametralmente opposto a quello *multi-stakeholder* portato avanti negli ultimi quindici anni dalla comunità internazionale in forum di discussione orientati all'eguale accesso alla *governance* di Internet. Tali spazi sono, ad esempio, l'*Internet Governance Forum* delle Nazioni Unite, piuttosto che il WSIS, *World Summit on Internet Society*, o organizzazioni come ITU, *International Telecommunication Union*, o la stessa ICANN. Le istituzioni sopra elencate sono portatrici di un approccio *bottom-up* che tenga conto delle istanze di tutti i membri della comunità di Internet: governi, settore tecnico e scientifico, accademia, ONG, società civile ecc... L'armonizzazione di questi *stakeholders* si contrappone alla deriva assolutistica che la Russia sta attuando nella *governance* di Internet, riconoscendo quest'ultimo come territorio oggetto della sovranità esclusiva dello Stato. Al di là del pericolo imminente di un distaccamento della Federazione dalla rete globale, quello che desta maggiore preoccupazione è che la Russia rappresenti in

10 Vedi nota 2: Federal Law 90-FZ (2019)

questo senso un esempio pratico e reale di un processo ritenuto impossibile fino a poco tempo fa. Molti sono ancora gli scettici dell'effettivo *splinternet,* ma la minaccia all'unità della rete è rappresentata anche dalla sola aspettativa che l'attuazione della Legge Federale 90-FZ possa realmente essere raggiunta così come descritta.

Quali alternative rispetto alla progressiva caduta della rete Internet sotto le sovranità forti degli Stati? Sarà possibile l'attuazione di un progetto di "sovranità popolare" su Internet, per una *governance* globale inclusiva e che scongiuri i processi di frammentazione in atto? Riuscirà la comunità *multi-stakeholder* a costituirsi come unità politica di rilevanza e influenza globale? Oppure sarà la forza centripeta dell'economia a garantire l'unità della rete? Questi, e molti altri, i quesiti che rimangono aperti circa il futuro della rete Internet e della Sovranità Digitale.

Geopolitica.info

Alessia Sposini

Co-coordinatrice di Youth IGF Italy, iniziativa giovanile riconosciuta dalle Nazioni Unite nell'ambito dell'Internet Governance Forum e volta al coinvolgimento dei giovani nel dibattito e nel processo di policy making sulle tematiche del digitale. Junior Fellow del Centro Studi Geopolitica.info per il quale si concentra sui temi della Sovranità Digitale e dei Diritti Digitali. Attualmente è studentessa di Laurea Magistrale presso Sapienza Università di Roma in Comunicazione, Valutazione e Ricerca Sociale per le Organizzazioni.

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale; la formazione attraverso i corsi in presenza e online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info