DEMOCRACIA E TECNOLOGIA DIGITAL

Ted Piccone

• *Os desafios singulares que a tecnologia digital representa para os governos democráticos e como estes governos, junto com a sociedade civil, precisam reagir* •

RESUMO

Os governos democráticos estão enfrentando desafios singulares para maximizar o lado positivo da tecnologia digital ao mesmo tempo em que minimizam suas ameaças às sociedades mais abertas. Proteger eleições justas, direitos fundamentais on-line e enfoque da governança da internet que envolva múltiplos atores são três prioridades inter-relacionadas essenciais para defender democracias fortes em uma era de insegurança crescente, aumento de restrições e competição geopolítica.

Os desafios crescentes que as democracias enfrentam ao administrar as dimensões complexas da tecnologia digital tornaram-se uma questão definidora para as políticas externas e internas, com implicações diretas para os direitos humanos e a saúde democrática das nações. A digitalização progressiva de quase todas as facetas da sociedade e a natureza transnacional inerente da internet suscitam uma série de problemas difíceis quando as informações públicas e privadas on-line são submetidas a manipulação, invasão e roubo.

Este artigo aborda a tecnologia digital em sua relação com três subtemas distintos, mas inter-relacionados: eleições livres e justas, direitos humanos e governança da internet. Nessas três áreas, os governos e o setor privado estão batalhando para acompanhar os aspectos positivos e negativos da difusão rápida da tecnologia digital. Para enfrentar esses desafios, os governos e legisladores democráticos, em parceria com a sociedade civil e as empresas de mídia e de tecnologia, deveriam urgentemente abrir o caminho para criar e instaurar regras e melhores práticas a fim de proteger processos eleitorais justos e livres da manipulação externa, defender os direitos humanos on-line e proteger a governança da internet de abordagens restritivas e de mínimo denominador comum. O artigo conclui com a exposição de como deveriam ser algumas dessas regras e melhores práticas.

PALAVRAS-CHAVE

Democracia | Internet | Direitos humanos | Segurança cibernética | Eleições | Governança

1 • O que a evidência nos diz

a - Eleições livres e justas

Os ataques cibernéticos promovidos por governos autoritários e atores não estatais representam uma ameaça clara e crescente às democracias em todo o mundo devido à interferência que promovem em eleições livres e justas. Esses ataques assumem muitas formas e podem minar e desestabilizar de várias maneiras os processos democráticos e a governança.

Há pelo menos quatro maneiras pelas quais os ataques cibernéticos podem influenciar as eleições: (1) manipular fatos e opiniões que instruem o voto dos cidadãos, por exemplo, através de relatos falsos da mídia social, *bots* e propaganda; (2) interferir no ato de votar (por exemplo, adulterar listas de registro eleitoral); (3) alterar os resultados da votação; e (4) minar a confiança na integridade da votação.[1] Essas ameaças partiram de países como a Rússia e a China e, nos últimos anos, tiveram por alvo nações do Ocidente democrático. Por exemplo, o Serviço Geral de Inteligência e Segurança da Holanda apontou especificamente a Rússia, a China e o Irã como ameaças à segurança nacional devido a ataques cibernéticos.[2] O Birô Federal de Investigação (FBI, na sigla em inglês) e o Departamento de Segurança Interna (DHS, na sigla em inglês) dos Estados Unidos divulgaram várias declarações em 2016 que detalhavam as conexões da Rússia a recentes ataques e vazamentos com a intenção de influenciar as eleições dos EUA.[3] Em maio de 2017, o presidente francês Emmanuel Macron acusou a mídia oficial russa de disseminar propaganda enganosa e notícias falsas com a intenção de influenciar os resultados eleitorais em favor de seu oponente.[4]

Ataques semelhantes estão se tornando cada vez mais frequentes, com mais *hackings* de instituições públicas e empresas privadas, como a interrupção das comunicações pela internet na câmara baixa do parlamento alemão e a disseminação de campanhas de desinformação e notícias falsas antes do referendo constitucional italiano e da eleição presidencial dos EUA.[5] Os ataques cibernéticos constituem ameaças tanto diretas quanto indiretas à integridade do processo democrático, pois são frequentemente motivados pela intenção de minar o apoio popular às democracias, sua legitimidade e seu poder brando.[6]

A manipulação de fontes de informação para o discurso político e a tomada de decisões é particularmente insidiosa e difícil de combater. As características próprias das formas contemporâneas de propaganda russa, que podem apresentar conteúdos polarizadores transmitidos rapidamente através da mídia tanto social como tradicional, de modo contínuo e repetido, com pouco compromisso com a realidade objetiva ou consistência, são difíceis de serem contestadas pela mídia independente e pelos governos, para não falar dos cidadãos.[7] Atores não estatais da direita e da esquerda radicais e aqueles envolvidos no terrorismo também estão explorando a natureza aberta da internet para múltiplos propósitos, inclusive influenciar a opinião pública antes e durante eleições.[8]

b - Direitos humanos on-line

A internet pode servir de ferramenta tanto para proteger como para violar os direitos humanos, com implicações diretas na segurança física e cibernética dos indivíduos. A difusão da tecnologia digital expandiu enormemente as oportunidades dos cidadãos de exercer seus direitos à liberdade de expressão e associação, de participar da vida cívica e de responsabilizar as autoridades públicas, ingredientes essenciais para a realização de eleições livres e justas. Os recentes avanços tecnológicos também ajudaram a lançar luz sobre as violações dos direitos humanos cometidas em todo o mundo. Grupos de vítimas utilizam agora diversos meios (postagens, transmissões ao vivo, financiamento coletivo) para divulgar vídeos e fotos de violações no YouTube e em outras plataformas, na esperança de que possam ser usados como prova em processos de responsabilização. Investigadores de direitos humanos usaram imagens de satélite para denunciar abusos nas prisões políticas norte-coreanas, limpeza étnica em Mianmar e potenciais valas comuns no Burundi que, de outra forma, talvez não fossem descobertas.[9]

Em anos recentes, no entanto, tem havido também uma deterioração contínua dos direitos humanos on-line, apesar das declarações inequívocas da Assembleia Geral das Nações Unidas e do Conselho de Direitos Humanos de que os direitos off-line definidos pela lei internacional de direitos humanos também são protegidos on-line.[10] O direito internacional garante essencialmente os mesmos direitos à privacidade e segurança dos dados on-line de uma pessoa de que gozam os arquivos na casa dela. Por exemplo, a vigilância em massa na internet, praticada até mesmo em democracias estabelecidas, é uma violação direta da segurança dos dados pessoais de um indivíduo, e o mesmo se pode dizer de uma legislação vaga com significativa autoridade discricionária para monitorar a vida digital de uma pessoa.[11] Provedores de serviços de internet e companhias de telecomunicações estão ficando drasticamente atrasadas na oferta aos consumidores de produtos de *hardware* e *software* que os protejam adequadamente contra uma infinidade de ataques cibernéticos.[12] O aumento da disponibilidade no comércio lícito e ilícito de sofisticadas armas cibernéticas e ferramentas de vigilância está facilitando esses tipos de ataques, como se viu nos ataques mundiais de pedidos de resgate "WannaCry" de *hacker*s em 2017.[13]

A exploração maliciosa da tecnologia também pode afetar a segurança física de indivíduos e Estados. Para começar, o aumento da digitalização das duas últimas décadas criou um "efeito inibidor" sobre a liberdade de expressão: cidadãos de certos países sentem-se menos seguros para afirmar suas opiniões, sabendo que seus dados pessoais são monitorados ou arquivados.[14] Através do rastreamento de localização, da mídia social e paralisações da internet, os problemas de segurança on-line também se tornam físicos, permitindo que oponentes da democracia e dos direitos humanos ameacem a segurança física de seus supostos alvos.

As paralisações e outras restrições da internet efetuadas por governos para suas populações são generalizadas, com mais de sessenta desligamentos documentados nos primeiros nove meses de 2017,[15] justificados por "segurança nacional" ou "ordem pública".[16] Esses

apagões digitais são particularmente perigosos para os direitos humanos. Em 2016, por exemplo, após o bombardeio do aeroporto de Istambul e a detenção de onze legisladores pró-curdos, o governo turco cortou o acesso a sites de mídia social e serviços de mensagens como Facebook, WhatsApp e Twitter para bloquear a circulação de notícias ou fotografias relacionadas a esses eventos.[17] Essas paralisações não restauraram a ordem, mas violaram os direitos básicos e provocaram medo e confusão entre os cidadãos.

As paralisações da internet não só prejudicam a governança democrática através da supressão da liberdade de expressão e das funções normais do governo, como também podem causar pânico e elevar as preocupações de saúde pública.[18] Essas violações também prejudicam o sistema internacional baseado em regras para a governança da internet e estimulam a competição estatal para instaurar códigos legais intrusivos e capacidades cibernéticas ofensivas. Por fim, é importante ressaltar que a deterioração dos direitos on-line não é apenas uma tática de regimes autoritários, mas também de governos democráticos. A falta de mecanismos efetivos de regulamentação ou supervisão do papel das empresas privadas na proteção dos dados dos cidadãos é outro elemento do dilema.

Apesar dessas ameaças cibernéticas aos direitos humanos, alguns países estão na vanguarda da adoção de leis e códigos de conduta para proteger os direitos on-line de seus cidadãos. No Brasil, o Marco Civil da Internet (lei 12.965 de 2014) "garante o direito à liberdade de expressão, protege a privacidade dos usuários, exclui a responsabilidade pelo conteúdo da web gerado por terceiros e preserva a neutralidade da Internet".[19] Também em 2014 foi estabelecida a Agenda para a Liberdade On-line de Tallinn, na qual os membros da Freedom Online Coalition, que inclui países como Canadá, Gana e Holanda, prometeram promover os direitos humanos on-line e se comprometeram com a transparência do uso pelo governo dos dados do cidadão, bem como protegê-los. O respeito por esses princípios, inclusive de Estados signatários como o México e o Quênia, é, no entanto, um desafio permanente. O Conselho da Europa aprovou uma promissora Estratégia de Governança da Internet para 2016-19 que destaca a construção da democracia on-line, a proteção dos direitos humanos e a garantia de segurança e proteção on-line.[20] Essas leis, estratégias e coalizões representam avanços promissores para os direitos humanos e, embora não sejam isentas de problemas, são passos na direção certa.

c - Governança da internet

A governança da internet desempenha um papel crucial na proteção dos direitos humanos e na manutenção de democracias saudáveis em todo o mundo. A internet foi fundada com base nos princípios de auto-organização descentralizada e fluxo de informações transnacional e é dirigida principalmente por atores privados na forma de uma rede de redes. No entanto, a crescente regulamentação da internet por parte de Estados-nação e a fragmentação causada por fronteiras jurisdicionais e territoriais ameaçam cada vez mais esses princípios. Se o acesso à internet de um país é restringido, por exemplo, isso interfere no acesso do resto do mundo. Mais de quarenta governos, entre eles, os da China e da Rússia,

promulgaram restrições a informação, dados e conhecimento na internet.[21] De acordo com o estudo Freedom on the Net, realizado em 2017 pela Freedom House, menos de 25% dos usuários da internet residem em países "livres", onde não há grandes obstáculos ao acesso ou restrições sobre o conteúdo.[22]

A expressão "governança da internet" refere-se também aos protocolos internacionais que governam a interoperabilidade global da internet. O debate em andamento sobre os modelos de governança da internet está centrado no desejo dos EUA de continuar com o enfoque que leva em conta os múltiplos atores da internet, no qual os setores privado, social e governamental estão incluídos no modelo de governança.[23] Como o local de grande parte do crescimento e da inovação da internet foram os Estados Unidos, este país teve uma influência significativa sobre sua autoridade governante, a Corporação Internet para Atribuição de Nomes e Números (ICANN); isso levou outros países a questionar se o enfoque de múltiplos atores é excessivamente tendencioso, dando vantagem ao governo e ao setor privado americanos.[24]

Em setembro de 2016, com o objetivo de responder a essas preocupações e no espírito de preservar uma internet aberta, o governo Obama decidiu não renovar o contrato dos EUA com a ICANN, abrindo mão de sua influência predominante e tornando a ICANN independente.[25] Não obstante, países como Rússia, Índia e China ainda criticam o modelo de múltiplos atores e defendem um enfoque multilateral centrado no Estado, o que lhes daria maior influência porque instituições internacionais, como as Nações Unidas, governariam a internet.[26]

Os proponentes do enfoque de múltiplos atores, particularmente dos setores privado e sem fins lucrativos, temem que se for promulgado um modelo de governança multilateral conduzido pelo Estado, ocorrerão sérias perdas de liberdade e inovação na internet. O enfoque multilateral dá aos países que não compartilham dos mesmos valores democráticos uma participação maior na governança da internet, permitindo assim que as ferramentas não democráticas de censura e a soberania nacional da internet sejam introduzidas mais amplamente. China e Rússia já censuram a internet que podem controlar dentro de suas fronteiras; dar-lhes poderes de decisão na governança global da internet poderia levar a violações dos princípios fundamentais sobre os quais a internet foi fundada.

O Brasil introduziu outra abordagem que incorpora tanto princípios de múltiplos atores quanto multilaterais na qual os componentes privado, social e governamental estão incluídos, juntamente com outras partes interessadas, como a academia e a representação não governamental eleita; esse processo seria, por sua vez, governado por um órgão que permitiria aos países participação igual no processo de tomada de decisão.[27] Embora esse enfoque combine ambos os modelos de governança, é improvável que seja adotado sem amplo apoio internacional. Desse modo, a governança da internet tornou-se cada vez mais uma questão em que as democracias e as autocracias assumem lados opostos, e que, argumentam os estudiosos, é de importância vital para o futuro da segurança, abertura e resiliência da própria internet.

2 • Implicações políticas e recomendações

À luz das atuais e futuras ameaças à democracia e aos direitos humanos decorrentes de usos irresponsáveis e disruptivos das comunicações digitais, o momento para os defensores de direitos humanos se mobilizarem em relação às questões de tecnologia digital é *agora*. É imperativo que as ações governamentais não adotem uma visão estreita de segurança em que segurança nacional, contraterrorismo e soberania sejam consideradas acima de todo o resto. Estratégias desse tipo, embora potencialmente poderosas no curto prazo, têm maior probabilidade de contribuir para a deterioração da segurança global e nacional em longo prazo.

Proteger os processos democráticos. O ambiente para eleições livres e justas e formação da opinião pública deveria tornar-se mais seguro contra influências estrangeiras e hackers. Propostas, como a feita nos EUA, de "designar o sistema eleitoral como 'infraestrutura crítica', uma medida que exigiria que as proteções de segurança cibernética fossem reforçadas", seria um bom começo.[28]

- Para garantir a integridade de suas eleições, as democracias deveriam atualizar seus sistemas eleitorais e usar dispositivos que não estivessem conectados a uma rede digital,[29] ou que tivessem *backups* manuais para sistemas digitais. A segurança cibernética deveria ser continuamente atualizada nas tecnologias sensíveis de votação relacionadas a listas de registro de eleitores, votação e tabulação de resultados.

- Os países deveriam considerar a adoção de princípios de dados eleitorais abertos que permitissem aos candidatos e ao público verificar a integridade desses processos como uma salvaguarda adicional e como meio de estabelecer confiança pública neles.[30]

- Os governos democráticos deveriam trabalhar com urgência para detectar e punir os *hackings* patrocinados pelo Estado e os assim chamados "patrióticos", a fim de deter e impedir futuras interferências nos sistemas democráticos.[31]

- Deveriam também desenvolver protocolos para facilitar a cooperação transnacional para processar os *hackers* da infraestrutura eleitoral e elaborar um código de conduta com promessas de não interferência nas eleições uns dos outros. É também cada vez mais urgente proteger o papel da mídia independente de ataques infundados.

- As democracias deveriam trabalhar para criar um consenso nos fóruns internacionais de que um ataque cibernético deliberado a infraestruturas críticas de sistemas eleitorais equivale a um ataque físico ao seu território, viola as leis internacionais de soberania e não ingerência nos assuntos internos e justifica reações de autodefesa.

Proteger os direitos humanos on-line. A comunidade internacional deveria implementar e promover as leis e os mecanismos existentes de direitos humanos e ser implacável ao defender on-line os direitos off-line.

- Acima de tudo, as democracias deveriam dar um exemplo positivo, respeitando elas mesmas esses direitos.[32] Legislações como o Marco Civil de Internet do Brasil, ou o novo Regulamento Geral de Proteção de Dados da União Europeia, e iniciativas de múltiplos atores que privilegiam segurança e abertura, como a Freedom On-line Coalition, são exemplos de leis e iniciativas concretas que deveriam ser expandidas e apoiadas.[33]

- Os Estados, em parceria com a sociedade civil e o setor privado, deveriam coordenar posições para fortalecer resoluções e mecanismos da ONU voltados à instituição de normas e monitoramentos adequados, como as resoluções da Assembleia Geral da ONU e do Conselho de Direitos Humanos sobre internet e privacidade patrocinadas pela Alemanha (A/C.3/71/L.39/Rev. 1º. de novembro de 2016) e Brasil (A/HRC/32/13 de julho de 2016).

- É fundamental que as empresas do setor privado no ecossistema da internet estabeleçam sistemas, produtos e protocolos muito mais rigorosos para proteger os cidadãos de intrusões por parte de atores estatais e não estatais.

- As políticas que regem as restrições de conteúdo na web e nas comunicações digitais devem ser cuidadosamente elaboradas com a participação de todas as partes interessadas relevantes e de acordo com as leis internacionais de direitos humanos, como liberdade de expressão e direito à privacidade e ao devido processo legal.

Pressionar em favor de uma governança da internet aberta. As nações democráticas deveriam adotar uma postura mais ativa e unificada nos debates sobre governança da internet, uma vez que a abordagem histórica do tipo *laissez-faire* não mais se sustenta.[34] Elas deveriam defender que a governança da internet se baseasse em valores de uma internet aberta, diversa, neutra e universal. Ela deveria incorporar quatro princípios fundamentais: (1) liderança compartilhada; (2) fluxo livre de informações e dados e, ao mesmo tempo, proteção da propriedade intelectual e a privacidade individual; (3) enfoques de múltiplos atores envolvendo poderes emergentes e estabelecidos da internet e uma sociedade civil e um setor privado ativos; e (4) enfoques liderados pela indústria do setor para combater ataques cibernéticos.[35]

Instituir um código de governança da internet. Uma coalizão de Estados com ideias afins deveria criar um grupo de trabalho de segurança cibernética composto por especialistas do governo, da indústria e da sociedade civil para elaborar e propor um código voluntário de governança da internet. Esse código deveria refletir os valores compartilhados de fortalecimento da governança democrática e da transparência, promoção dos direitos humanos, proteção dos dados dos cidadãos e defesa do modelo de múltiplos atores.

- As estratégias a serem consideradas na adoção deste código deveriam ser a Estratégia de Governança da Internet 2016-2019 do Conselho da Europa e a Agenda de Tallinn de 2014 para a Liberdade On-line, bem como outros modelos atuais.

• O grupo de trabalho poderia ajudar a coordenar a educação especializada e a capacitação de formuladores de políticas sobre a complexa relação entre direitos humanos e tecnologia digital e buscar formas de ajudar os membros a desenvolver uma capacidade de segurança cibernética mais forte para proteger os processos democráticos.

• Ao estabelecer esses padrões, o grupo de trabalho deveria considerar as consequências para os criminosos flagrantes, inclusive o condicionamento da cooperação bilateral à conformidade com a segurança cibernética. É preciso colocar a questão: como as democracias devem tratar as nações que tentam ataques cibernéticos aos seus processos democráticos fundamentais?

NOTAS

1 • Jakob Bund, *Cybersecurity and Democracy – Hacking, Leaking and Voting* (Paris: European Union Institute for Security Studies, 2016): 3.

2 • Kingdom of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service, *Annual Report 2015: A Range of Threats to the Netherlands* (Zoetmeer: General Intelligence and Security Service, 2016).

3 • "GRIZZLY STEPPE - Russian Malicious Cyber Activity," U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), 2016, acesso em 4 de junho de 2018, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf. Mais recentemente, o Comitê de Inteligência do Senado concluiu que os ataques cibernéticos de fontes do governo russo obtiveram acesso a elementos restritos da infraestrutura eleitoral. "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," Richard Burr, 8 de maio de 2018, acesso em 4 de junho de 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

4 • Michel Rose e Denis Dyomkin, "After Talks, France's Macron Hits out at Russian Media, Putin Denies Hacking." Reuters, 28 de maio de 2017, acesso em 4 de junho de 2018, https://www.reuters.com/article/us-france-russia-idUSKBN18P030.

5 • Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, 8 de dezembro de 2016, acesso em 4 de junho de 2018, https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html; Anne Applebaum, "The Dutch Just Showed the World How Russia Influences Western European Elections." The Washington Post, 8 de abril de 2016, acesso em 4 de junho de 2018, https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/b427602a-fcf1-11e5-886f-a037dba38301_story.html?utm_term=.79384727c9c9; Jason Horowitz, "Spread of Fake News Provokes Anxiety in Italy." The New York Times, 2 de dezembro de 2016, acesso em 4 de junho de 2018, https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html.

6 • Jakob Bund, "Cybersecurity and Democracy – Hacking, leaking and voting." EUISS, novembro de 2016, acesso em 4 de junho de 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_30_Cyber.pdf; Melissa Eddy, "After a Cyberattack, Germany Fears Election Disruption." The New York Times, 8 de dezembro de 2016, acesso em 4 de junho de 2018, https://www.

nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html.

7 • Christopher Paul e Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model* (Arlington: Rand Corporation, 2016): 4, acesso em 4 de junho de 2018, http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

8 • Alice Marwick e Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, 2017): 19, acesso em 4 de junho de 2018, https://datasociety.net/output/media-manipulation-and-disinfo-online/.

9 • Christoph Koettl, "These Images Don't Lie: Exposing North Korea's Dirty Little Secret." Amnesty International, 5 de dezembro de 2013, acesso em 4 de junho de 2018, http://blog.amnestyusa.org/asia/these-images-dont-lie-exposing-north-koreas-dirty-little-secret/; "Burundi: Satellite Evidence Supports Witness Accounts of Mass Graves," Amnesty International, 28 de janeiro de 2016, acesso em 4 de junho de 2018, https://www.amnesty.org/en/latest/news/2016/01/burundi-satellite-evidence-supports-witness-accounts-of-mass-graves/; "Burma: 40 Rohingya Villages Burned Since October," Human Rights Watch, 17 de dezembro de 2017, acesso em 4 de junho de 2018, https://www.hrw.org/news/2017/12/17/burma-40-rohingya-villages-burned-october.

10 • David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." Assembleia Geral das Nações Unidas, A/71/373, 6 de setembro de 2016, acesso em 4 de junho de 2018, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc; "Silencing the Messenger: Communication Apps Under Pressure. Freedom on the Net Report 2016," Freedom House, novembro de 2016, acesso em 4 de junho de 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2016; Antonio Segura-Serrano, "Internet Regulation and the Role of International Law," *Max Planck Yearbook of United Nations Law* 10 (2006): 191-272.

11 • David Kaye, "Report of the Special Rapporteur," 2016.

12 • Toomas Hendrik Ilves, "A Plan for Making the Cyber World Safe." World Economic Forum, p. 2, 20 de setembro de 2016, acesso em 4 de junho de 2018, https://www.weforum.org/agenda/2016/09/making-the-cyber-world-safe-will-require-more-collaboration-than-ever-before/.

13 • WannaCry é o nome de um prolífico ataque de hackers conhecido como "ransomware" que mantém reféns os dados de um computador até que se pague um resgate. Ian Sherr, "WannaCry Ransomware: Everything You Need to Know." C|net, 19 de maio de 2017, acesso em 4 de junho de 2018, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

14 • Eileen Donahoe, "Human Rights in the Digital Age." Just Security, p. 1, 23 de dezembro de 2014, acesso em 4 de junho de 2018, https://www.justsecurity.org/18651/human-rights-digital-age/.

15 • Entre os países que fizeram isso estão Bangladesh, Brasil, Burundi, Tajiquistão, Índia, Etiópia, Argélia, Congo, Paquistão, Síria e Iraque. "#KeepItOn," Access Now, 2017, acesso em 4 de junho de 2018, https://www.accessnow.org/keepiton/.

16 • David Kaye, "Report of the Special Rapporteur," 2016; Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year." Center for Technology Innovation at Brookings, outubro de 2016, acesso em 4 de junho de 2018, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

17 • Yasmeen Abutaleb e Can Sezer, "Turkey Appears to Be in Vanguard of 'Throttling' Social Media after Attacks." Reuters, 6 de julho de 2016, acesso em 4 de junho de 2018, http://www.reuters.com/article/us-mideast-crisis-socialmedia-idUSKCN0ZM2O3; Can Sezer e Humeyra Pamuk, "Turkey Blocks Access to Twitter, WhatsApp: Internet Monitoring Group." Reuters, 2016, acesso em 4 de junho de 2018, http://www.reuters.com/article/us-turkey-security-internet-idUSKBN12Z0H4.

18 • "POLICY BRIEF: Internet Governance and the Future of the NetMundial Initiative," Access Now, 2015, acesso em 4 de junho de 2018, https://www.accessnow.org/cms/assets/uploads/archive/docs/POLICYBRIEFInternetGovernanceandtheFutureoftheNetMundialInitiative.pdf David Kaye, "Report of the Special Rapporteur," 2016.

19 • Carl Meacham, "Is Brazil a Global Leader in Internet Governance?" Center for Strategic and International Studies, 15 de maio de 2014, acesso em 4 de junho de 2018, https://www.csis.org/analysis/brazil-global-leader-internet-governance. Porém, é preciso mais trabalho para fortalecer as leis de proteção de dados no Brasil conforme os novos regulamentos adotados pela União Europeia.

20 • "Internet Governance – Council of Europe Strategy 2016-2019," Council of Europe, 2016, acesso em 4 de junho de 2018, https://edoc.coe.int/en/internet/7128-internet-governance-council-of-europe-strategy-2016-2019.html.

21 • John D. Negroponte, Samuel J. Palmisano, e Adam Segal, *Defending an Open, Global, Secure, and Resilient Internet* (New York: Council on Foreign Relations, 2013): 13, acesso em 4 de junho de 2018, https://www.cfr.org/report/defending-open-global-secure-and-resilient-internet.

22 • "Manipulating Social Media to Undermine Democracy," Freedom House, 2017, acesso em 4 de junho de 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

23 • Harold Trinkunas e Ian Wallace, "Converging on the Future of Global Internet Governance: The United States and Brazil." Foreign Policy at Brookings, julho de 2015, acesso em 4 de junho de 2018, p. 26, https://www.brookings.edu/research/converging-on-the-future-of-global-internet-governance-the-united-states-and-brazil/.

24 • *Ibid.*

25 • Megan Stifel, "Maintaining U.S. Leadership on Internet Governance." Council on Foreign Relations, 21 de fevereiro de 2017, acesso em 4 de junho de 2018, https://www.cfr.org/report/maintaining-us-leadership-internet-governance.

26 • Harold Trinkunas e Ian Wallace, "Converging on the Future," 2015, p. 19.

27 • *Ibid.*

28 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy." MIT Technology Review, 4 de agosto de 2016, acesso em 4 de junho de 2018, https://www.technologyreview.com/s/602108/what-the-dnc-hack-says-about-cyber-based-threats-to-democracy/.

29 • Sergio Hernandez, "How to Stop Election Cyberthreats." CNN, 5 de novembro de 2016, acesso em 4 de junho de 2018, http://www.cnn.com/2016/11/05/politics/voting-vulnerabilities-cyberattacks/index.html.

30 • Open Election Data Initiative, Homepage, 2018, acesso em 4 de junho de 2018, http://www.openelectiondata.net/en/.

31 • Mike Orcutt, "What the DNC Hack Says about Cyber-Based Threats to Democracy," 4 de agosto de 2016.

32 • David Kaye, "Report of the Special Rapporteur," 2016.

33 • *Ibid.*; "POLICY BRIEF," 2015.

34 • Robert K. Knake, "Internet Governance in an Age of Cyber Insecurity." Council on Foreign Relations, 2010, acesso em 4 de junho de 2018, p. 7, https://www.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.

35 • John D. Negroponte *et* al., "Defending an Open, Global, Secure, and Resilient Internet," 2013; Harold Trinkunas e Ian Wallace, "Converging on the Future," 2015, p. 5.

TED PICCONE – *Estados Unidos*
Ted Piccone é *Senior Fellow* e Charles Robinson *Chair* em Política Externa na Brookings Institution. Ele tem escrito extensamente sobre as dimensões de política externa da democracia e dos direitos humanos, inclusive em seu livro mais recente, *Five Rising Democracies and the Fate of the International Liberal Order*. Este artigo baseia-se em um *briefing* que ele fez para a *Community of Democracies* em setembro de 2017, com a valiosa ajuda de Hannah Bagdasar, Carlos Castillo, Jesse Kornbluth e Matthew Koo.

contato: *TPiccone@brookings.edu*

Recebido em abril de 2018.
Original em inglês. Traduzido por Pedro Maia Soares.