INFORME LARI

CONJUNTURA INTERNACIONAL
SOBRE

DEMOCRACIA E INFORMAÇÃO

,

14ª Edição – Agosto de 2021

pet-rel

O Informe LARI é produzido pelo Programa de Educação Tutorial de Relações Internacionais da Universidade de Brasília

Tutor:

Juliano da Silva Cortinhas

Membros:

Ana Beatriz Zanuni
Ana Luísa Vitali de Araújo
Bruna Affonso Ferreira Maciel
Celso Antônio Coelho Júnior
Ester Deise Costa Santos
Henrique Oliveira da Motta
Jales Caur S.
João Pires Mattar
Julia de Souza Sales
Luiza Batista Ferreira
Nathalia Rezende Mamede
Yara Resende Marangoni Martinelli

Edição:

Ana Beatriz Zanuni
Celso Antônio Coelho Júnior
Jales Caur S.
Juliano da Silva Cortinhas
Nathalia Rezende Mamede
Yara Resende Marangoni Martinelli

O Laboratório de Análise das Relações Internacionais

O LARI, como chamamos o Laboratório de Análise das Relações Internacionais, é um evento que acontece semestralmente e tem como objetivo observar em grupo a conjuntura internacional e discutir sobre possíveis cenários futuros, como uma forma de desenvolver a capacidade de interpretar os fatos e elaborar uma sequência lógica de possibilidades sobre eles.

Os membros do PET-REL discutem previamente temas relevantes no cenário internacional e escolhem qual será o mais interessante e produtivo. Após a pesquisa extensa sobre o assunto, divulgamos um breve resumo dos fatos e interpretações para os interessados, o que objetiva contribuir para sua participação nos debates.

Após o LARI, todos são convidados a elaborarem sua análise de conjuntura, um documento em que cada interessado desenvolve uma breve introdução do assunto e desenvolve suas visões sobre os vários cenários que entende possíveis. Nessa fase, os membros do PET se dispõem a colaborar com qualquer assunto ou dúvida, incentivando os participantes do LARI que se interessem a elaborarem sua própria análise, que pode ser publicada no nosso boletim.

Informação e o Sistema Político

A humanidade passou por diversas revoluções de caráter estrutural que alteraram a forma como nos comportamos enquanto seres individuais e coletivos. Entre as mais recentes, a primeira pode ser considerada a promovida pelo advento do motor a vapor, que substituiu o modelo agrícola e artesanal por grandes indústrias. A segunda, baseada na energia elétrica e no petróleo, deu início à produção em massa e ao uso do aço. A terceira, e última consolidada entre os debates acadêmicos, ficou conhecida justamente como a revolução da informação, baseada nos computadores e no processo de globalização da economia e dos meios de comunicação, contando, também, com o advento da internet, com o que ficou conhecido como revolução informacional. A partir daqui, temos uma sociedade em que a informação se torna uma variável fixa e de caráter extremamente volátil na equação de poder junto às demais esferas de atuação, partindo para o que o geógrafo Milton Santos definiu teoricamente como meio técnico-científico-informacional (SANTOS, 1996).

A importância da informação deixou a área dos estudos estratégicos e nos processos decisórios e passou a ter um papel fundamental nos mais diversos níveis da vida das pessoas. Com o advento das redes sociais,

a informação tornou-se a melhor arma para fortalecer as narrativas pessoais e derrubar adversários e ideologias. Exemplos disso podem ser vistos por toda a década de 2010, vindos da Europa com a crise dos refugiados e culminando na eleição de Donald Trump como presidente dos Estados Unidos. A popularização do termo *fake news* foi o legado dessa grande odisseia informacional que tomou a sociedade contemporânea.

No entanto, é válido mencionar que essa dinâmica informacional não é nova ou exclusiva da era das redes sociais. A dinâmica de propaganda da Guerra Fria, na qual os dois blocos conflitantes, o capitalista e o socialista, usavam da propaganda para reafirmar suas ideologias. O governo nazista, que tinha um ministério focado integralmente para a propaganda e a propagação de informação, também demonstra que a informação se encontra intrínseca ao processo político desde antes do advento da internet, revelando-se como a mais eficaz estratégia para a boa funcionalidade do poder em qualquer regime — incluindo a democracia (ZANUNI; CAUR; COSTA, 2021).

Considerando esse histórico, vemos como os sistemas políticos ao redor do mundo se moldaram a partir do uso da informação. As estruturas são retroalimentadas por informações que entram na forma de buscar vantagens a nível doméstico e internacional, e que saem na forma de instrumentos de operação a favor de quem está no governo. Acadêmicos como Yaacov Y. I. Vertzberger (1990) debatem acerca dessas informações e o processamento delas por parte de quem a recebe, tornando esse processo não somente uma resposta passiva ao recebimento dessas informações, mas um processo de construção de realidade.

A partir da construção da realidade, quem domina esse processo automaticamente detém o poder e tece a realidade da maneira que mais lhe agrada. E, em cima disso, vale lembrar também que a relatividade da verdade torna esse processo ainda mais complexo. A considerar que, com as diversas variáveis — principalmente a informação — que influenciam e mudam a percepção de sociedades diferentes, o que é tido como certo em uma sociedade, pode ser tido como errado em outra.

Partindo disso, o PET-REL dedicará a sexta edição da Revista Petrel para entender um pouco mais desses processos e das suas influências na democracia ao redor do mundo. Este briefing tem como propósito servir como preparatório para os debates do Laboratório de Análises de Relações Internacionais, oferecendo, como base, temas como a democracia e a segurança no processo eleitoral, o papel das mídias sociais, fake news e todo esse debate atrelado à realidade brasileira.

Democracia e Segurança Eleitoral

As últimas eleições democráticas ao redor do mundo trouxeram novas perspectivas sobre a influência da informação e da tecnologia, tanto com relação ao próprio sistema, quanto em relação à segurança. Em 2017, a inteligência estadunidense informou que a Federação Russa havia realizado operações virtuais com o objetivo de manipular as eleições de 2016, que elegeram o ex-presidente Donald Trump (HARRIS,

2019). Ademais, o uso de redes sociais foi suspenso durante as eleições sob justificativa de segurança cibernética em países como Uganda, Gana e Congo (MATFESS, 2016).

Apesar de não terem sido comprovadas fraudulentas, as eleições dos Estados Unidos colocaram no centro da discussão a segurança eleitoral e os perigos à democracia que crimes de cibersegurança podem apresentar. O vazamento de dados se tornou tema ainda mais importante, uma vez que poderia influenciar na questão do registro dos eleitores (ROBINSON, 2016). Mais recentemente, a questão se ampliou em países como o Brasil, a partir dos questionamentos do presidente da República e sua base aliada da segurança eleitoral promovida pelas urnas eletrônicas.

Nas eleições de 2016, Gana, que utiliza o conhecido modelo democrático africano, resolveu suspender a conexão de internet no país. A justificativa foi construída em cima da preocupação com a cibersegurança, com a proteção do sistema eleitoral e com a possibilidade de desestabilização do país (MATFESS, 2016). Outros países da região também realizaram o mesmo procedimento, como Etiópia, Congo, Chade e Uganda. Em 2021, a nova eleição de Uganda contou novamente com o precedente aberto 5 anos antes: um novo corte de internet e de alguns aparelhos celulares foi realizado pelo governo em exercício (KAFEERO, 2021).

Essas ações de corte no principal meio de comunicação podem ser entendidas a partir de dois pontos de vista distintos, sendo o primeiro a questão de garantir que a democracia seja cumprida em uma eleição sem influências externas ou ataques ao sistema eleitoral e a segunda como uma forma de a cercear, uma vez que restringe a capacidade de comunicação dos eleitores e da expressão de sua opinião política.

Já nas Américas, segundo relatório da Organização dos Estados Americanos (OEA) feito com dados de 34 Estados membros, cerca de 93% dos processos eleitorais são digitalizados em algum grau. Esse movimento permitiu maior participação e contribuiu para criar consciência e transparência nos processos. Porém, as Américas são uma das regiões que possuem mais ataques cibernéticos, apesar de 55% dos países não terem ciência de nenhum incidente eleitoral relacionado (OEA, 2019).

Em consonância, uma publicação da Harvard Kennedy School (HARVARD, 2020 apud OEA, 2019), apontou três categorias de acidentes eleitorais cibernéticos, sendo elas a 1) criação de contas falsas para desacreditar o sistema eleitoral; 2) exposição de informações confidenciais e 3) criação de temas irrelevantes e midiáticos, a fim de desconcentrar os eleitores.

A partir disso, é possível perceber que o debate de democracia e segurança eleitoral está no cerne da questão política, especialmente a partir da polarização nos Estados Unidos, em 2016. No Brasil, é possível perceber um esforço dos órgãos reguladores, políticos e judiciários na luta contra as *fake news* e contra o descrédito do sistema eleitoral brasileiro. Devido às declarações do presidente Jair Bolsonaro, as eleições de 2022 poderão enfrentar desafios no Brasil. Dúvidas sobre a segurança da digitalização dos processos podem elevar a polarização da sociedade, com repercussões imprevisíveis para o processo eleitoral.

Mídias Sociais, Fake News e o paradoxo da decisão democrática

Quando falamos sobre tecnologias digitais e mídias sociais, o debate sobre *Fake News* (anglicanismo que representa o fenômeno das notícias falsas que se espalham rapidamente nos meios de comunicação digitais) já é notório. Vivemos, atualmente, duas crises com relação à informação: a falsidade e o excesso de conteúdos pelos quais somos bombardeados diariamente. Somados, esses fenômenos nos levam a uma verdadeira crise de desinformação. O fenômeno poderia causar espanto, se pensarmos nas expectativas de democratização do conhecimento que a internet evocou durante seu surgimento.

A problemática não consiste na disponibilidade do conteúdo em si, mas na lógica de ganhos políticos a partir da propagação de notícias falsas de cunho político-eleitoral, ou de lucro, quando relacionadas com a competição constante das informações disponíveis pela nossa atenção. Em ambos os casos, porém, há a geração de lucro para as empresas que fornecem os meios para a divulgação de fake news. Jaron Lanier, especialista em mídias do Vale do Silício, questiona: por qual serviço as empresas multimilionárias, como Facebook, Twitter, Google e Instagram, estão sendo pagas, se os usuários não gastam um centavo para usufruir de seus produtos? Para o especialista, a resposta é clara: o produto vendido nessa troca comercial é, na verdade, representado pelos próprios usuários, seus dados e a transformação paulatina do seu comportamento (LANIER, 2020).

Segundo Tristan Harris, ex-funcionário da Google e de outras grandes empresas do Vale do Silício, a transformação de comportamento é um objetivo declarado das mídias e tecnologias em questão. Pela realização de estudos sobre psicologia e comportamento, são criados algoritmos inteligentes, como o *Growth Hacking*, capazes de traçar "perfis" de usuários e, a partir daí, direcionar a utilização da mídia para gerar o máximo possível de engajamento, mesmo que isso signifique o vício e outras consequências negativas (HARRIS, 2020).

Há dois problemas centrais nessa forma de utilização dos usuários: a venda dos dados, que são fornecidos no credenciamento e adquiridos durante o uso das mídias; e a transformação dos padrões de comportamento, sem que os alvos dessa mudança sejam alertados ou sequer tomem conhecimento (HARRIS, 2020). Na lógica do "capitalismo de vigilância", tudo que se faz, especialmente em aparelhos eletrônicos, está sendo cuidadosamente observado e internalizado – pelos algoritmos que regem o funcionamento das redes. Cada movimento é utilizado para traçar um perfil único de usuário, com dados diversos (o que o usuário gosta, quer, faz, frequenta, pensa, etc.). De posse desses dados, e sem legislações fortes que controlem a utilização indiscriminada de informações sobre bilhões de pessoas ao redor do globo, as empresas se tornam máquinas poderosas de publicidade dos mais diversos tipos (HARRIS, 2020).

E é aí que está o cerne do paradoxo entre a democracia e as tecnologias digitais: ao traçar um perfil específico para cada usuário, a ponto de produzir um *feed* de notícias

direcionado especialmente para você (cada pessoa tem acesso a uma experiência personalizada, com notificações e respostas de busca diferentes – tudo é direcionado ao seu perfil, ao seu modelo), os algoritmos passam a influenciar sistematicamente pensamentos e comportamentos (HARRIS, 2020). Isso já seria problemático se pensássemos na venda de roupas, sapatos ou outros bens e serviços, mas quando pensamos na possibilidade de influenciar opiniões políticas, escolhas eleitorais e decisões cotidianas com impacto social, o problema alcança outro nível. Qual é o sentido de uma participação democrática manifestada pelo voto, se somos manipulados pelos algoritmos das redes sociais antes de chegar à urna, e sem que sequer tomemos consciência disso?

Como se não bastasse essa incompatibilidade estrutural com o sistema político mais aceito no mundo – a democracia –, as mídias sociais nos apresentam uma questão ainda mais grave: as *Fake News*. Os algoritmos, apesar de configurarem um tipo de inteligência artificial, não são capazes de diferenciar um conteúdo verdadeiro ou falso. Ao contrário, o estímulo aceito pelo algoritmo para definir o próximo vídeo recomendado ou a próxima postagem do *feed* é, entre outras coisas, o engajamento que recebe a publicação em questão. E a mentira, segundo o programador Tristan Harris (2020) recebe mais engajamento e se espalha seis vezes mais rápido que a verdade nas mídias sociais.

Esse não é um funcionamento programado por seres humanos. É um processo que acontece durante o uso, pelo fato de que os usuários se interessam e se engajam mais em publicações com conteúdos impressionantes, chocantes, terríveis, mesmo que sejam mentirosos. E assim, são essas as publicações impulsionadas pelo algoritmo. Dentro da lógica de uma empresa que busca o lucro, e que, para isso, precisa manter o maior tempo de engajamento possível por usuário, cria-se um modelo de negócio que, intencionalmente ou não, lucra com a desinformação.

Dessa forma, o que antes pareciam inofensivos algoritmos capazes de revolucionar o mundo publicitário, se tornaram armas letais de polarização, que nos levam a passos rápidos à era da desconfiança, da desinformação sem questionamentos, da desestabilização das dinâmicas políticas e sociais. Essa realidade se manifesta em casos concretos, como a campanha pelo Brexit, os conflitos em Hong Kong e na Ucrânia, a eleição de Bolsonaro no Brasil e Donald Trump nos Estados Unidos, e teorias conspiratórias como o *Q Anon* e o *Pizza Gate*.

Nesse contexto de polarização cada vez mais acirrada, as redes sociais têm papel central no aprofundamento dos radicalismos. Por meio dos algoritmos, as informações que aparecem para usuários em *feeds* e páginas de busca se tornam cada vez mais extremas. Ao construir seu "perfil" como usuário, as redes selecionam o conteúdo que mais se assemelha à sua maneira de pensar, e acabam formando-se bolhas que reforçam a intolerância e minam a capacidade de argumentação. Além disso, a venda de dados dos usuários para empresas é um limite ético que já foi ultrapassado, como apresentado no documentário Privacidade Hackeada (2019).

Um caso que ganhou notoriedade, levando a empresa Facebook à julgamento em corte, aconteceu no Myanmar em 2018. No país, a perseguição étnica às minorias

muçulmanas já era uma realidade desde os anos 70, por dinâmicas sociais e históricas que não nos cabe discutir, mas que estavam arrefecidas. O Facebook, rede social mais utilizada no país, por meio do algoritmo de engajamento, passou a impulsionar publicações com discurso de ódio ferrenho contra essa minoria. Em agosto, as publicações amplamente compartilhadas por militares e turbas budistas, chegaram a um triste apogeu. Posts de convocação da ira popular geraram grandes manifestações direcionadas ao assassinato em massa de muçulmanos. Tristemente, tais manifestações atingiram seu objetivo – vilas foram queimadas, pessoas foram assassinadas e mulheres foram estupradas (FACEBOOK..., 2018). Yanghee Lee, investigadora da ONU para Myanmar, afirmou: "Temo que o Facebook tenha se transformado numa fera", junto a outros especialistas que concordam ter sido essa mídia a grande correia de transmissão do ódio, o impulsionador final do triste morticínio (FACEBOOK..., 2018).

Hoje, seguimos suscetíveis à influência de uma manipulação que parece não ter culpados – o algoritmo se transforma tão rapidamente, que nem seus próprios criadores são capazes de definir seu funcionamento em totalidade. O fato é que, o *attention extracting model*, vinculado ao modelo de *feed Positive Intermitent Stimulous* (que sempre se atualiza) e a testes como *massive scale contagious experiments*, entre outros, já demonstram sua capacidade de desestabilizar dinâmicas políticas e sociais e de manipular resultados reais (como eleições), sem que as pessoas sequer tenham consciência disso (ZUBOFF, 2020). A eficácia dos conteúdos extremos e mentirosos, que provocam a polarização e a desinformação, em manter as pessoas online é estratégica para essas grandes empresas. Enquanto não houver mudanças profundas em sua estrutura, a tendência é que o impulsionamento de conspirações como a terra plana (que foi recomendada milhares de vezes pelo algoritmo do Youtube, por exemplo) (CHASLOT, 2020), continuem ocorrendo. Esse debate evoca a importância da formulação de leis e regulações para controle do espalhamento de *Fake News*, para limitação dos impactos da manipulação dos algoritmos e para utilização dos dados.

Perigo à brasileira

Com os avanços tecnológicos e maior relação entre qualidade de informação e democracia, com ênfase nos riscos da propagação de *fake news* e a participação definidora de empresas como a Cambridge Analytica[1] em eleições chave do mundo todo, urge a necessidade dos Estados possuírem maior preparo ao lidar com cibersegurança e com dados e propagação de desinformação por meio de redes sociais. Entretanto, o Brasil apresenta problemas em fatores básicos na proteção e manutenção de dados, por exemplo, demonstrando a fragilidade e despreparo do país na gestão da segurança cibernética. Um exemplo disso é o apagão de dados sofrido pelo Ministério da Saúde (MS) em plena pandemia da Covid-19, em novembro de

[1] Empresa de análise de dados que faz a coleta e uso político de dados pessoais sem consentimento. Seu trabalho mais repercutido foi o de propaganda política para a campanha presidencial de Donald Trump para as eleições estadunidenses de 2016 (ENTENDA..., 2018).

2020. A rede de computadores do órgão foi comprometida por um vírus que afetou por dias a atualização dos dados de casos e mortes por Covid-19. Segundo o diretor-presidente da Agência Nacional de Vigilância Sanitária (Anvisa), Antônio Barra Torres, houve um ataque cibernético ao sistema do MS, que também afetou a agência. O então secretário-executivo do Ministério da Saúde, Élcio Franco, confirmou indícios nesse sentido (APÓS..., 2020).

Além disso, mesmo com a iniciativa de melhoria na regulamentação e preservação por meio da Lei Geral de Proteção de Dados (LGPD) — que entrou em vigência em agosto de 2020 e que promete maior segurança jurídica e proteção aos dados pessoais dos cidadãos (SERPRO, [2018?]) —, o sistema brasileiro não conseguiu impedir dois megavazamentos no início de 2021. Em janeiro, 223 milhões de CPFs de pessoas vivas e falecidas foram expostos na internet, junto ao vazamento de quase 103 milhões de registros de celulares, em fevereiro (MUNDO..., 2021).

Segundo Marco DeMello, CEO da PSafe, empresa de segurança cibernética que descobriu os dois casos de megavazamento, o mundo vive uma "pandemia" de ciberataques, com as tecnologias de defesa ainda não adaptadas às novas inteligências artificiais que colocam em posição de vulnerabilidade empresas e indivíduos. E, no caso do Brasil, estamos ainda mais despreparados que a maioria dos países. De acordo com DeMello, "o Brasil tem uma defasagem muito grande entre a sua posição econômica e a sua posição em termos de cibersegurança" (MUNDO..., 2021), pois o país é uma das maiores economia do mundo, mas o 46º de 47 países monitorados em relação a velocidade de detecção de vazamento de dados.

Além da cibersegurança, outro fator importante a ser considerado para o enfrentamento aos impactos negativos da informação na democracia — principalmente em 2022, com o contexto de eleições presidenciais — é a preparação da sociedade para lidar com as notícias falsas. O país ainda não conseguiu estruturar uma campanha efetiva contra as *fake news* — nem mesmo em relação à segurança e à confiabilidade das urnas eletrônicas (CARVALHO, 2021) —, sendo a efetividade na comunicação um ponto chave para a realização de eleições justas em 2022 (COMBATE..., 2021).

Em debates entre parlamentares brasileiros — principalmente no âmbito da Comissão Parlamentar Mista de Inquérito (CPMI) das *Fake News* —, já foram mencionados a educação e o fortalecimento da democracia como formas de combater a desinformação, pois amenizam as chances de informações falsas confundirem a formação da opinião pública e desestabilizarem, assim, o estado democrático de direito (DEBATEDORES..., 2019). Entretanto, medidas eficazes ainda devem ser tomadas por parte do governo, e certamente não ocorrerão de maneira determinante antes do período eleitoral, considerando também que o desprezo pela mídia e o uso de inverdades fazem parte da agenda do Presidente da República, que não tem interesse em alterar esse cenário.

Desse modo, o país se mostra despreparado para lidar com as problemáticas que enfrentaremos ao longo de 2022, principalmente considerando metodologias que analisam a vulnerabilidade e preparo de

países para lidar com informações, como a do europeu *Media Literacy Index* 2021 — que classifica os países do continente de acordo com o maior potencial para suportar o impacto negativo de notícias falsas e desinformação devido à qualidade da educação, mídia livre e alta confiança entre as pessoas (OSIS, 2021).

Na Europa, por exemplo, países mais afetados por tecnologias propagadoras de *fake news*, como a Bulgária, apresentavam índices muito baixos na medida citada e realmente não conseguiram enfrentar tais problemas com sucesso (FAKE..., 2017). Por outro lado, outros países já se preparam mais efetivamente depois de lidar com desinformação em suas últimas eleições, com, por exemplo, a intervenção de tecnologias russas. Entre as medidas tomadas por governos europeus visando solucionar a questão está um sistema educativo da Finlândia, que, desde 2014, disponibiliza um curso, parte iniciativa anti-*fake news* lançada pelo governo finlandês, com o objetivo de ensinar estudantes, jornalistas e políticos a combater informações falsas (MACKINTOSH, 2019). Outro exemplo é o da Espanha, cujo governo preparou protocolos para proteger as eleições gerais espanholas contra ataques cibernéticos (SPAIN..., 2019).

Além disso, a União Europeia (UE) disponibiliza o website *EU v Disinformation*, que desde 2015 foca especificamente nas campanhas de desinformação da Rússia que afetam a UE. O objetivo é aumentar a conscientização e a compreensão do público sobre as operações de desinformação do Kremlin, sendo parte da força tarefa *East StratCom*, que trata do tema na prática (QUESTIONS..., 2021).

Conclusão

Com o avanço exponencial do uso de tecnologias de informação, questões de proteção e segurança de dados estão cada vez mais presentes. Ainda, em âmbito internacional, as discussões sobre normativas para proteção de dados são fortemente regionalizadas, com tendência de produção de regulamentações surgindo apenas a partir dos anos 2000 (GONZÁLEZ, 2020). Nesse contexto, o *General Data Protection Regulation* da União Europeia foi o principal marco internacional surgido nos últimos anos, demarcando a necessidade de atuação para regulamentar o uso de dados e informações por governos e entidades privadas.

Como se pode perceber pela discussão acima, o debate sobre informação e democracia tem sido extremamente relevante para dimensões distintas das relações internacionais, inclusive com possíveis desdobramentos para a própria concepção de democracia no mundo. Nesse sentido, o debate que será realizado pelo PET-REL procurará, mesmo que de modo geral, abordar essas repercussões, de modo a fomentar a construção de ideias sobre a relação entre a informação e a qualidade das democracias . Abaixo, são mencionadas algumas perguntas com o intuito de provocar o debate:

- Quais são os principais perigos à democracia proporcionados a partir das redes sociais?
- Em âmbito internacional, qual o papel de organismos internacionais como

OCDE, G20 e ONU em regular o uso do espaço digital?
- Qual o efeito conjuntural que as notícias falsas têm proporcionado nos processos eleitorais pelo mundo?
- Quais instrumentos institucionais devem ser criados para fortalecer a democracia em espaço digital?
- Quanto às eleições brasileiras de 2022, quais são os principais perigos ao qual a nossa democracia estará submetida?

Referências

APÓS apagão de dados, secretário diz que há indícios de ataque aos sistemas do Ministério da Saúde. **G1**, 13 nov. 2020. Disponível em: https://glo.bo/3lotR6y. Acesso em: 31 jul. 2021.

CARVALHO, M. C. Justiça eleitoral faz campanha pré-histórica contra fake news da urna eletrônica. **Poder 360**, 19 mai. 2021. Disponível em: https://bit.ly/3fh35cj. Acesso em: 31 jul. 2021.

CHASLOT, G. Entrevista concedida ao documentário Dilema das Redes. Direção: Jeff Orlowski, Larissa Rhodes. Produção de Exposure Labs. Estados Unidos: Netflix, 26 de janeiro de 2020.

COMBATE à desinformação ainda será desafio nas eleições em 2022. **CNJ**, 21 jan. 2021. Disponível em: https://www.cnj.jus.br/combate-a-desinformacao-ainda-sera-desafio-nas-eleicoes-em-2022/. Acesso em: 31 jul. 2021.

DEBATEDORES apontam democracia e educação para combater fake news. **Agência Senado**, 3 dez. 2019. Disponível em: https://bit.ly/3ljJs7r. Acesso em: 31 jul. 2021.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC**, 20 mar. 2018. Disponível em: https://glo.bo/2TREUKi. Acesso em: 1 ago. 2021.

FACEBOOK foi crucial para a limpeza étnica do século XXI em Myanmar. **El País**, 13 abr 2018. Disponível em: https://brasil.elpais.com/brasil/2018/04/12/internacional/1523553344_423934.html. Acesso em 02 ago. 2021.

FAKE News and Elections in Bulgaria. **EU vs DisInfo**, 28 mar. 2017. Disponível em: https://euvsdisinfo.eu/fake-news-and-elections/. Acesso em: 31 jul. 2021.

GONZÁLEZ, M. Conheça o cenário das leis de proteção de dados ao redor do mundo. **IDBlog**, 2020. Disponível em: https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/. Acesso em: 02 ago. 2021.

HARRIS, K. Smart on Security. Penguin Books, United States of America, 2019. Capítulo 9. In: HARRIS, Kamala. **The truths we hold: An American Journey**. Penguin Books, United States of America, 2019.

HARRIS, T. Entrevista concedida ao documentário Dilema das Redes. Direção: Jeff Orlowski, Larissa Rhodes. Produção de Exposure Labs. Estados Unidos: Netflix, 26 de janeiro de 2020.

KAFEERO, S. Uganda has cut off its entire internet hours to its election polls opening. **Quartz Africa**, 2021. Disponível em: https://qz.com/africa/1957137/uganda-cuts-off-internet-ahead-of-election-polls-opening/. Acesso em: 02 ago. 2021.

LANIER, J. Entrevista concedida ao documentário Dilema das Redes. Direção: Jeff Orlowski, Larissa Rhodes. Produção de

Exposure Labs. Estados Unidos: Netflix, 26 de janeiro de 2020.

MACKINTOSH, E. Finland is winning the war on fake news. What it's learned may be crucial to Western democracy. **CNN**, 2019. Disponível em: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/. Acesso em: 31 jul. 2021.

MATFESS, H. More African countries are blocking internet access during elections. **Quartz Africa**, jun. 2016. Disponível em: https://www.wathi.org/more-african-countries-are-blocking-internet-access-during-elections-quartz-africa-june-2016/. Acesso em: 02 ago. 2021.

MUNDO vive pandemia de ciberataques e Brasil está despreparado, diz CEO de empresa que descobriu megavazamento. **BCC**, 12 fev. 2021. Disponível em: https://glo.bo/3rUS8m8. Acesso em: 31 jul. 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS [OEA]. **Consideraciones de ciberseguridad del Proceso Democrático para América Latina y el Caribe**. 2019. Disponível em: https://www.oas.org/es/sms/cicte/docs/ESP-Cybersecurity-Democratic-Process-LAC.pdf. Acesso em: 02 ago. 2021.

OSIS. **Media Literacy Index 2021**. 14 mar. 2021. Disponível em: https://osis.bg/?p=3750&lang=en. Acesso em: 1 ago. 2021.

PRIVACIDADE HACKEADA. Jehane Noujaim Karim Amer. Estados Unidos: 26 de Janeiro de 2019, Karim Amer Geralyn, White Dreyfous, Judy Korin, Pedro Kos.

QUESTIONS and Answers about the East StratCom Task Force. **EEAS**, 28 abr. 2021. Disponível em: https://bit.ly/2TNBPuB. Acesso em: 1 ago. 2021.

ROBINSON, R. Cybersecurity Lesson from the 2016 Presidential Election. **Security Intelligence**, 2016. Disponível em: https://securityintelligence.com/cybersecurity-lessons-from-the-2016-presidential-election/. Acesso em: 02 ago. 2021.

SANTOS, M. **A natureza do espaço:** técnica e tempo, razão e emoção. São Paulo: Ed. Hucitec, 1996.

SERPRO. **O que muda com a LGPD?**. [2018?]. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 31 jul. 2021.

SPAIN fights cyberattacks, fake news ahead of key elections. **Fox News**, 15 mar. 2019. Disponível em: https://www.foxnews.com/world/spain-fights-cyberattacks-fake-news-ahead-of-key-elections. Acesso em: 31 jul. 2021.

VERTZBERGER, Y. **The World in Their Minds:** Information Processing, Cognition, and Perception in Foreign Policy Decisionmaking. 1. ed. California: Stanford University Press, 1990.

ZANUNI, A.; CAUR, J., COSTA, M. Uso da Informação e Perpetuação de Poder: O Desempoderamento de Grupos Sociais Através da Criação de Um Inimigo. *In:* MEIRA, G. et al (Org.). **Power The Change:** the concept of empowerment in international relations. 1. ed. Brasília: Americas Model United Nations, 2021. p. 69-102.

ZUBOFF, Shoshana. Entrevista concedida ao documentário Dilema das Redes. Direção: Jeff Orlowski, Larissa Rhodes. Produção de

Exposure Labs. Estados Unidos: Netflix, 26 de janeiro de 2020.