Conjecturas

DOI: 10.53660/CONJ-1424-Z20

Democracia em alerta: a face obscura do ciberespaço e suas implicações para o direito

Democracy on war: the dark face of cyberspace and its implications for law

Alexandre Peres Teixeira[1]*, Liziane Paixão Silva Oliveira[1]

RESUMO

O ciberespaço é fruto da genialidade humana e veio para melhorar a qualidade de vida da sociedade. Seu potencial benéfico é inquestionável e tem revolucionado não apenas a ciência, mas também as relações interpessoais. As plataformas de redes sociais figuram, atualmente, como o lugar no qual grande parte do planeta vive. São milhões de interações diárias, que abandonam uma quantidade imensa de dados órfãos, para formar o que se conhece como Big Data. Com ferramentas analíticas especiais, comportamentos humanos são mapeados, com a finalidade de facilitar as relações de consumo. Entretanto, o pleito eleitoral de 2016, nos Estados Unidos da América apresentou para o mundo a face obscura do ciberespaço, que permite que operações cibernéticas maliciosas possam ser executadas, com emprego de técnicas de propaganda e largo uso de ferramentas de análise de Big Data. As operações maliciosas perpetradas pela Rússia, bem como a participação da empresa privada Cambridge Analítica, na campanha eleitoral de 2016, colocaram as democracias de todo planeta em alerta e provaram que o ciberespaço possui um lado obscuro que pode ser usado tanto contra a soberania popular, por meio da manipulação da construção da livre vontade e violação da privacidade.

Palavras-chave: Democracia; Ciberespaço; Direito; Redes sociais.

ABSTRACT

Cyberspace is the result of human genius and came in order to improve the life´s quality in society. Its beneficial potential is unquestionable and has revolutionized, not only science, but also interpersonal relationships. Social media platforms are currently the locus where much of the planet´s population lives. There are countless daily interactions, which abandon an immense amount of data, which build what is known as “Big Data”. With special analytical tools, human behaviors are mapped in order to facilitate consumer relations. However, the 2016 election in the United States of America presented the dark face of cyberspace to the world, which allows malicious cyber operations to be carried out, with the use of propaganda techniques and extensive use of Big Data analysis tools. The malicious operations perpetrated by Russia, as well as the participation of the private company Cambridge Analytica, in the 2016 election campaign, put all the democracies in the world on alert, and proved that cyberspace has a dark side that can be used both against popular sovereignty, through manipulation of the construction of free will and breach of privacy.

Keywords: Democracy; Cyberspace; Law; Social media.

[1] Centro de Ensino Unificado de Brasília 1.
*E-mail: alexandreperes@yahoo.com.br

INTRODUÇÃO

O ciberespaço[2] permite interações que variam desde simples movimentações financeiras eletrônicas, até complexas análises no campo da engenharia, da medicina, da psicologia comportamental e de diversos outros campos. Tais análises, mais recentemente, são realizadas com emprego de ferramentas de Big Data[3] e Inteligência Artificial[4]. É indiscutível que seu surgimento trouxe benefícios inestimáveis para as sociedades de todo o planeta.

Porém, o uso do ambiente informacional realizado por russos e pela empresa privada Cambridge Analítica[5], durante o pleito eleitoral norte americano, em 2016, acionou um alerta para as instituições que possuem a responsabilidade de salvaguardar o perfeito funcionamento da democracia.

Com a finalidade de nortear a presente pesquisa, cabem os questionamentos: o mau uso do ciberespaço pode representar uma ameaça real para a democracia? É possível que atores estatais e não estatais, com a utilização do ciberespaço, tenham condições de interferir ilicitamente no processo de formação do livre convencimento da sociedade, durante uma campanha eleitoral e assim violar direitos fundamentais?

Em processo realizado pelo Senado (INTELLIGENCE..., 2017) dos Estados Unidos da América (EUA) ficou comprovada a atuação da Rússia nas últimas eleições de 2016. A ação dos agentes russos foi perpetrada com a larga utilização de operações

---

[2] A expressão *cyberspace* é atribuída a William Gibson e foi cunhada na obra de ficção *Neuromancer*, publicada em 1984, em Nova Iorque, pela Editora Ace Books. Compõe uma trilogia e explora a relação entre o homem e a máquina; recebeu os principais prêmios de produção literária de ficção científica e serviu de base para o filme Matrix, no qual o ator Keanu Reaves entra no ciberespaço e conecta seu sistema nervoso central a um computador (SALDAN, 2012, p. 15).

[3] Com tantas pessoas utilizando o ciberespaço, a quantidade de dados que vai se armazenando na rede é impressionante, formando verdadeiras montanhas de dados, denominadas tecnicamente de Big Data, que muitas vezes excedem a capacidade de armazenamento e processamento da própria rede. O Big Data, atualmente, é considerado uma grande *commodity* do ciberespaço, fazendo surgir uma atividade conhecida como "mineração de dados", que basicamente se traduz a extrair, com o uso de ferramentas especiais de análise, informações que podem ser usadas em processos decisórios, principalmente para fins comerciais. Na grande parte das vezes, estes dados são utilizados sem a autorização ou até mesmo conhecimento de seus titulares (SIMONCINI, 2016, p. 2).

[4] Muito se fala em Inteligência Artificial (IA), entretanto, para efeito deste artigo, a IA se refere a uma tecnologia transversal, que tem como proposito dotar computadores, por meio da utilização de uma grande quantidade de dados (denominada na literatura como *big data*), com capacidades computacionais apropriadas e processos específicos de análise e decisão, para que possam alcançar realizações que se aproximam da capacidade humana, ou até mesmo a supere (HOFFMANN-RIEM, 2019. p. 2).

[5] A Cambridge Analítica é uma empresa privada, que se utiliza de ferramentas modernas de análise de Big Data, capazes de construir padrões de comportamento e direcionar campanhas de marketing personalizadas.

cibernéticas maliciosas, que tiveram como meta interferir, de forma velada, na livre formação de vontade do eleitorado norte-americano.

Pelo que pôde ser apurado, os *hackers* russos teriam atuado em duas principais vertentes: a invasão dos servidores do Partido Democrata, com a extração de e-mails pessoais de uma das candidatas ao pleito; e a utilização massificada de *fake News*, por meio das redes sociais.

Além desta suposta ação ilegal da Rússia, a democracia dos EUA também sofreu interferência, mas de forma supostamente legal, com a participação da empresa Cambridge Analítica, que atuou utilizando propaganda massificada e direcionada de redes sociais, em favor do candidato republicano eleito Donald Trump. As ações da Cambridge Analítica foram de cunho manipulativo e utilizadas no contexto de um pleito eleitoral, se caracterizando como a primeira participação de uma empresa privada estrangeira, de alta tecnologia, em um pleito eleitoral de tão alta significância, como o pleito eleitoral dos EUA.

Cabe ressaltar que, tanto os agentes russos, como a Cambridge Analítica se utilizaram largamente das plataformas de redes sociais e tal fato, no contexto em comento, desvelou a face mais obscura do ciberespaço, que foi a ferramenta que proporcionou a ingerência nas eleições da potência hegemônica do século XXI.

O cerne ontológico da democracia representativa é o voto livre. Por meio dele a sociedade tem a oportunidade de escolher aqueles que irão representá-la. Desta forma, o direito de participação democrática deve ser garantido ao cidadão, para que o princípio democrático seja observado. As operações cibernéticas maliciosas, perpetradas no contexto do pleito eleitoral de 2016, podem ter violado, não apenas o direito da livre participação do cidadão norte-americano, mas também o direito à privacidade, ambos consignados, internacionalmente, como direitos fundamentais.

Destarte, a hipótese de pesquisa aventada no presente artigo é a de que a utilização maléfica do ciberespaço, no sentido de interferir no livre processo de formação da convicção do eleitorado durante um pleito eleitoral, pode representar uma séria ameaça para a democracia. A relevância social da pesquisa repousa na necessidade de desvelar, para a sociedade brasileira, o perigo que a utilização maliciosa do ciberespaço pode significar para o resultado de um pleito eleitoral.

Justifica-se a pesquisa devido a necessidade de incluir este importante tema no debate acadêmico, de forma a incentivar novas pesquisas que possam estudar o assunto e

contribuir para a diminuição dos impactos negativos do mau uso do ciberespaço para a democracia. Neste caminho, acredita-se que o engajamento responsável da sociedade na utilização parcimoniosa do ciberespaço, durante o processo de escolha de candidatos, em pleitos eleitorais, terá como resultado a diminuição dos efeitos de tais interferências. Por todas essas razões, realizou-se uma pesquisa qualitativa, bibliográfica e documental baseada em procedimentos metodológicos comparativos e históricos, guiada por uma abordagem dedutiva amparada no estudo de caso.

O presente artigo propõe uma análise sobre o caso das eleições norte-americanas, em 2016, focando no perigo que a utilização de operações cibernéticas maliciosas pode representar para a democracia e para a livre escolha de representantes pela sociedade. Na primeira seção, será realizado estudo de caso, que se iniciará com uma análise sumária do uso de operações cibernéticas, no contexto de pleitos eleitorais em todo planeta; em seguida será exposto detalhadamente o caso da interferência da Rússia e da Cambridge analítica, no pleito eleitoral norte-americano, em 2016; e a seção se encerrará com uma análise detalhada do potencial de risco das plataformas de redes sociais para os pleitos eleitorais. Na segunda seção serão analisados os aspectos jurídicos do caso em estudo, inicialmente por meio de uma reflexão sobre aspectos que envolvem a reunião do direito, com a política e com a tecnologia; em um segundo tópico serão analisados os reflexos da interferência, no pleito de 2016, para o direito pátrio. Por derradeiro, será efetuada uma síntese dos assuntos tratados no artigo, em forma de conclusão.

A AMEAÇA CIBERNÉTICA CONTRA A DEMOCRACIA

O futuro do planeta é digital, isto não se pode negar. No alvorecer do séc. XXI as tecnologias inovadoras, que fazem uso do ciberespaço, chegaram ao alcance de uma considerável parcela da população global, de norte a sul. Atualmente não se concebe viver sem as facilidades presentes nos computadores, smartphones ou tablets, bem como nas redes sociais, como o Facebook, Instagram e o Twitter. Tais aspectos desempenham um papel fundamental no desenvolvimento da democracia digital e da expressão cívica da sociedade (ALOUANE, 2014, p. 1).

Entretanto, para uma parte da crítica, o ciberespaço permitiu a criação de um movimento dissimulado, supostamente não violento, mas que vem desenvolvendo estratégias alternativas para a violência. O ciberespaço fez com que o florescimento de novas formas não violentas de oposição ganhasse impulso. Isso inclui desobediência civil eletrônica e hacktivismo, principalmente quando ativistas online têm como alvo governos e corporações, agindo por meio da desfiguração de sites, publicação de informações privadas e por meio de ataques de negação de serviço (DDoS)[6] que prendem sites e redes (MINDUS, 2011, p. 19). A chamada "engenharia social", realizada por meio de extração de informações das redes sociais, também figura como uma forma de ação não violenta, voltada para um fim, normalmente, ilícito.

O uso do ciberespaço pode ser feito para o bem ou para o mal. Na esteira desta relação ambígua, os impulsos transformativos que a tecnologia da informação trouxe para a política criam desafios a serem enfrentados pela democracia representativa, principalmente em relação ao fenômeno de formação da opinião pública. O ciberespaço pode ser utilizado por atores externos, por atores de oposição interna, ou até mesmo por foras da lei para desafiar o sentimento democrático. Isto acontece não apenas devido à equalização que o meio informacional proporciona, ou seja, na rede todos os *bits* são iguais, tornando as posições extremistas não menos disponíveis do que as opiniões convencionais, mas também por conta do efeito deliberativo que o ciberespaço proporciona, pois, conforme afirma Sunstein (2009):

> Quando as pessoas falam o que acontece? Os membros do grupo se comprometem? Eles se movem para o meio (...)? A resposta agora está clara e não é o que a intuição sugere: os grupos vão a extremos. Mais precisamente, os membros de um grupo deliberativo geralmente acabam em uma posição mais extrema (...). A polarização de grupo é um fenômeno típico em grupos deliberativos (SUNSTEIN, 2009, p.3).

Além da polarização, o efeito de bolha é outra questão inquietante, ou seja, o fato de que as pessoas entram em círculos fechados, de informações políticas, onde os cidadãos podem facilmente filtrar notícias que lhes sejam mais convenientes, para as quais estejam mais inclinados, devido principalmente à preferência por evitar "dissonância cognitiva".

---

[6] Do inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet (SALDAN, 2012, p. 61).

Este fenômeno não é novo, entretanto, a tecnologia da informação ampliou seus efeitos, ao ter a liberdade de selecionar e escolher fontes mais compatíveis com a preferência do eleitor, dentro de um panorama de mídia mais fragmentada, onde a "confiança" está fadada a se tornar um valor epistêmico central e talvez a chave para a compreensão da orientação política.

Em um mundo onde mais de 50% da população mundial tem acesso a alguma combinação de tecnologia da informação (5 bilhões de usuários de telefones celulares, cerca de 2 bilhões de usuários de internet, cerca de 6,7% da população mundial com acesso privado à web) "outro problema para a opinião pública são os efeitos de longo prazo da fofoca desenfreada no sistema democrático, que tendem a tornar falsos boatos virais" (MINDUS, 2011, p. 17, tradução nossa).

Por conta deste atrativo universo de possibilidades que o mau uso do ciberespaço oferece, a interferência cibernética, em pleitos eleitorais, se traduz em uma séria ameaça global. Nos últimos anos, vários Estados ocidentais sofreram interferência eleitoral, constituindo um sério impedimento às suas capacidades de realização de eleições livres e justas. Este tipo de ataque cibernético não se trata de um fenômeno recente, mas o que a torna diferente dos ataques cibernéticos gerais é a (i) natureza do alvo, (ii) a natureza do ataque, (iii) a natureza do dano e (iv) a falta de uma solução apropriada, quer no direito internacional quer no direito interno (VELDE, 2017, p. 8).

Em relação a natureza do alvo, sabe-se que os ataques cibernéticos, perpetrados por Estados, em sua maioria, buscam infringir um dano cinético, ou até mesmo uma perda de funcionalidade, que tenha como consequência a interrupção de funcionamento da estrutura alvo. Em relação à natureza do ataque, é fato que a interferência cibernética em pleitos eleitorais não se constitui em simples operações de hackeamento, mas incorporam solidas campanhas de informação e desinformação. Em relação a natureza do dano, ao contrário de um ataque com efeitos cinéticos, como o realizado com o *Stuxnet*[7], o dano

[7] Em outubro de 2010, o vírus Stuxnet, supostamente desenvolvido pelos governos israelense e americano, foi infiltrado, possivelmente por um *pen drive*, nos sistemas do reator nuclear de Bushehr, no Irã, construído pela Rússia, com a finalidade de inutilizar centrífugas, aumentando sua rotação, enquanto sinais de normalidade eram enviados para o controle. O episódio afetou o projeto nuclear iraniano e, por isso, é amplamente noticiado como espécie de ataque de guerra cibernética. A empresa russa de segurança da computação Kaspersky Labs afirmou, em dezembro de 2011, que o Stuxnet pode ser o primeiro de um conjunto de armas cibernéticas (SALDAN, 2012, p. 72). Na ação contra o Irã foi fácil verificar o número de centrifugas que foram danificadas, mas nas eleições de 2016 não se tem evidência material para se afirmar a quantidade de eleitores que potencialmente modificou seu convencimento pela ação manipulativa da Rússia.

causado por uma operação cibernética maliciosa contra um pleito eleitoral tem um padrão de resultado que é difícil de identificar. Em relação à falta de uma solução apropriada, as operações maliciosas contra estruturas públicas e contra cidadãos, neste contexto de exercício da democracia, figuram como interferências diretas e ilícitas no exercício pleno do poder do Estado. Este tipo de ação maliciosa tem o potencial de fazer os Estados buscarem a retratação do agressor por meio do conflito armado (VELDE, 2017, p.7-9).

A operação de interferência cibernética em uma eleição é peculiar em dois aspectos, o primeiro é que a infraestrutura cibernética atacada é pública e o ataque pode ser considerado uma violação da soberania deste Estado alvo, caso o atacante seja um outro Estado. O outro aspecto diferenciado é que o objetivo do ataque é mais amplo, ele não visa danificar sistemas apenas, ou infringir dano físico, mas sim capturar as mentes e corações de cidadãos, com a finalidade de turbar o processo da livre construção da vontade. Portanto, o alvo, para este tipo de ataque, são pessoas e não sistemas lógicos de dados (VELDE, 2017, p. 8).

Desta forma, o dano a ser causado não é cinético, mas abstrato, porque busca modificar a cognição do eleitor, não existe um ativo físico visado na campanha maliciosa. Os ataques cibernéticos, em geral, não são visíveis, desta forma, se tornam difíceis de serem identificados antes da execução. Também é difícil a realização da atribuição pelo ataque, com a finalidade de se promover a devida sanção e exigir a reparação, se assim for o caso (VELDE, 2017, p. 9).

Fato é que a tentativa de interferência de governos estrangeiros nos assuntos internos dos EUA não é algo recente, remontando à época colonial, com os atos do governo inglês, passando por antigas ações da própria Rússia, realizadas desde 1919, chegando a época da corrida ideológica da Guerra Fria e finalmente atingindo à sofisticada campanha de 2016, com o uso malicioso do ciberespaço (ACEVES, 2019, p.184-189). É fato também que os EUA não são totalmente inocentes neste cenário tenebroso da interferência eleitoral. Entre os anos de 1950 até 1980 o país se engajou em campanhas secretas para desestabilizar e influenciar conjunturas políticas em Estados estrangeiros (SCHMITT, 2018, p. 37). Mas a interferência sistemática, com largo uso do ciberespaço, é produto da era da informação e se reveste de características que a tornam mais perigosa e infinitamente mais letal para a democracia. Existem diversos registros de ação de *hackers*, por meio de operação cibernética maliciosa, contra pleitos eleitorais.

A dificuldade de detecção prévia deste tipo de ataque cibernético, bem como a dificuldade de levantamento da identidade do atacante são fatores que, no caso de um pleito eleitoral, que deve acontecer em dia determinado, podem gerar consequências irreversíveis para a democracia e provocar crises políticas de dimensões constitucionais (VELDE, 2017, p. 9). Sem contar que a interferência em pleito eleitoral desacredita o pleito, afetando assim a sua legitimidade, influenciando diretamente a participação da sociedade no processo democrático e impedindo que a democracia seja, efetivamente, exercida no Estado alvo. O dano causado atinge o coração do sistema democrático, gerando uma comoção pública ainda maior e as consequências deste tipo de ação são nefastas e imprevisíveis.

Na era da informação, parece estar se transformando em padrão, a intromissão cibernética para turbar processos eleitorais. O grupo conhecido como *CyberBerkut*, curiosamente formado por hacktivistas russos, em 2014, executou uma operação que teve como alvo a Comissão Eleitoral Central da Ucrânia, fazendo com que a estrutura de rede da Comissão ficasse inativa por 20 horas. Além disto, no dia das eleições o grupo anunciou a vitória de um falso vencedor (SCHMITT, 2018, p. 37).

Existem indícios que apontam para um incremento na dinâmica das tentativas destas interferências. Tendo como exemplo as intervenções anteriores realizadas contra os EUA, cuja dinâmica quase sempre procurou influenciar a política interna e externa. No seu extremo, procuravam minar a legitimidade do processo democrático e destruir o tecido social do país. Tais interferências se materializavam de várias formas, incluindo panfletos, revistas, jornais, rádio, televisão e filmes (ACEVES, 2019, p.184-189). Com advento do ciberespaço, devido as suas características que favorecem o anonimato, tais intervenções atingiram o estado da arte e isto tem incentivado a ocorrência de mais tentativas de interferências em pleitos eleitorais.

Dois anos após as invasões da Comissão Eleitoral Central da Ucrânia, a Diretoria Principal de Inteligência do Estado-Maior Geral (GRU), órgão da Inteligência militar russa, mais precisamente sua unidade “APT-28”, executou uma operação maliciosa contra o *Bundestag* alemão, o Ministérios de Relações Exteriores e Finanças, e contra os sistemas da União Democrática Cristã (o partido da chanceler Angela Merkel). Da mesma

forma, a campanha[8] de Emmanuel Macron, em 2017, para a Presidência da França também foi alvo de operações cibernéticas maliciosas atribuídas aos GRU, que tentou implantar malware no site da campanha. (SCHMITT, 2018, p. 37).

Em novembro de 2017, ao mesmo tempo que a Comissão eleitoral do Reino Unido abriu investigação para investigar se a votação do *Brexit* tinha sido alvo de uma operação cibernética maliciosa, a Primeira Ministra, Thereza May, deu a seguinte declaração (THERESA..., 2017), se referindo às operações obscuras da Rússia: "Sabemos o que você está fazendo e você não terá sucesso, porque subestima a resiliência de nossas democracias, a atração duradoura de sociedades livres e abertas e o compromisso das nações ocidentais com as alianças que nos unem" (SCHMITT, 2018, p. 37, tradução nossa).

Nem mesmo a própria Rússia escapou de intromissão cibernética durante o pleito eleitoral presidencial de 2018, o site da Comissão Eleitoral Central Russa sofreu um ataque de negação de serviço (DDoS), originado em quinze países. Segundo o presidente da Comissão, o ataque não surtiu o efeito desejado em virtude do sistema eleitoral automatizado da Rússia não estar conectado à internet (SCHMITT, 2018, p. 37).

Desta forma, fica claro que os ataques cibernéticos contra pleitos eleitorais figuram como uma nova dinâmica pela qual atores estatais e não estatais procuram, com motivação escusa, infringir danos às democracias pelo mundo. Porém, nenhuma interferência foi tão contundente e eficaz como a realizada contra o pleito eleitoral dos EUA, em 2016. O que ocorreu naquela democracia, contra os cidadãos daquele país, precisa ser detalhadamente estudado por todos os Estados democráticos, com a finalidade de que sejam evitados novos ataques do mesmo tipo.

No próximo tópico será explorado, com detalhes, as ações realizadas pelos agentes russos e pela Cambridge Analítica, na visão do autor, tais ações se constituem em um verdadeiro ultraje ao sistema democrático.

[8] As "impressões digitais" desta operação na França se assemelhavam às impressões das operações contra o Comitê Nacional Democrático dos EUA e contra a campanha de Angela Merkel, no ano anterior (SCHMITT, 2018, p. 37).

A INTERFERÊNCIA NAS ELEIÇÕES DOS EUA EM 2016: A ASSOCIAÇÃO DE ATORES

Não existe precedente na história em relação a atuação de, em um mesmo pleito eleitoral, dois atores, um estatal e outro privado, no sentido de empreenderem ações sinérgicas e simultâneas para favorecer o mesmo candidato. A ação da Inteligência russa, somadas às ações da empresa Cambridge Analítica, criaram uma situação atípica, sinistra e perigosa.

A Rússia empregou todo seu obscuro potencial de Inteligência para atuar em favor da campanha do candidato republicano, ao mesmo tempo que o comitê de campanha[9] do referido candidato contratou os serviços de "assessoria" da empresa Cambridge Analítica. Ambos se utilizaram das facilidades do ciberespaço, mais precisamente das potencialidades das plataformas de redes sociais para empreender aquilo que pode ser considerado o maior golpe já perpetrado contra a democracia dos EUA.

A ATUAÇÃO DA INTELIGÊNCIA RUSSA

Os EUA reúnem um conjunto de características peculiares que tornam o país vulnerável para ações no ciberespaço e, desta forma, um alvo compensador para atividades cibernéticas maliciosas, principalmente na esfera da política. O sistema bipartidário norte-americano não tem familiaridade com o conceito de governo de coalização, desta forma, a dinâmica binária torna o efeito da manipulação do pleito, além de devastador, quantificável para os agentes maliciosos.

O princípio do "vencedor leva tudo", seguido pela maioria dos estados quando alocam seus delegados ao colégio eleitoral (que então elege o presidente), dá às pequenas intervenções, que modificam a convicção da maioria, um efeito desproporcional. Interferir marginalmente nos votos de um partido ou mover os votos de um campo para outro - apenas o suficiente para inclinar a balança - pode mudar o resultado para todo um estado (BUND, 2016, p. 2). Estas vulnerabilidades são multiplicadas pelas características inerentes ao ciberespaço.

[9] A empresa recebeu um investimento de US $ 15 milhões de Robert Mercer, o rico doador republicano, depois de assediar o conselheiro político do partido, Stephen K. Bannon, com a promessa de que suas ferramentas poderiam identificar os perfis, nas redes sociais, dos eleitores americanos e influenciar seu comportamento (ROSENBERG; CONFESSORE; CADWALLADR, 2018).

Quando o escândalo envolvendo Hilary Clinton, acusada de ter usado um servidor de e-mails do governo para veicular mensagens privadas, colocando assim em risco a segurança nacional, foi divulgado, a corrida eleitoral teve uma sensível guinada a favor de Donald Trump (VELDE, 2017, p. 4). Existem registros de que Donald Trump convidou os russos para a invasão das contas de e-mails de Clinton, como o exposto abaixo:

> Rússia, se você está ouvindo, espero que consiga encontrar os 30.000 e-mails que estão faltando", disse ele, acrescentando "A propósito, eles hackearam - eles provavelmente têm os 33.000 e-mails dela. Espero que sim. Eles provavelmente têm seus 33.000 e-mails que ela perdeu e excluiu porque você veria algumas belezas lá. Então, vamos ver (SHERMAN, 2016, s.n., tradução nossa).

As eleições norte-americanas, de 2016, sofreram interferência russa de duas maneiras diferentes: a primeira por meio de uma operação de hackeamento, que os russos realizaram contra os servidores do Comitê Nacional do Partido Democrata (DNC), com a subsequente divulgação dos e-mails; e a segunda se concretizou pela execução do "Projeto Lakhta", liderado por Yevgeniy Viktorovich Prigozhin, um aliado do governo russo (STEIGER, 2019, p. 5).

As investigações constataram que equipes de espionagem cibernética invadiram infraestruturas cibernéticas, com a finalidade de extrair informações classificadas. A mais exitosa destas intrusões foi realizada por uma equipe denominada "*Cozy Bear*", ou "A.P.T. 29", que logrou sucesso ao invadir os servidores do Comitê Nacional Democrata (DNC) e penetrar na conta de e-mail do então presidente da campanha eleitoral do partido, John Podesta. Outra equipe de espionagem cibernética conhecida como "*Fancy Bear*", ou "A.P.T. 28", invadiu o servidor do Comitê Nacional do Partido Republicano (RNC) (VELDE, 2017, p. 11). Centenas de milhares de servidores foram invadidos em todo o país, com a finalidade de furtar informações.

De posse das informações roubadas, os agentes russos passaram então a divulgar, seletivamente, o que interessava para a campanha de manipulação. Documentos extraídos dos servidores do DNC foram enviados, em julho de 2016, para publicação em sites como *WikiLeaks* e outros similares. Esta divulgação teve impacto imediato na campanha do Partido Democrata, principalmente na campanha dos parlamentares do partido, também em nível estadual. Debbie Wasserman Schultz, presidente do DNC, foi forçada a

renunciar, junto com seus principais assessores. Ressalta-se que os documentos extraídos dos servidores do RNC não foram divulgados pelos agentes russos (VELDE, 2017, p. 11).

Já o "Projeto Lakhta" se constituiu em uma grande e sistemática operação de propaganda, realizada com o largo emprego de operações cibernéticas maliciosas que, segundo a peça de acusação formal do Conselheiro Especial dos EUA, Robert Mueller, fazia uso de "*trolls*"[10] russos, que se passavam por cidadãos norte-americanos, ou, em algumas ocasiões, roubavam perfis on-line de cidadãos reais. Isto era feito para postar comentários ofensivos nas redes sociais. Em sua maioria, tais comentários assumiam posturas divergentes, com a finalidade de semear discórdia e divisão entre o povo americano. Segundo o Conselheiro Mueller, "a finalidade de tais postagens era a de dissuadir os eleitores a não votarem em Hillary Clinton e organizar o apoio a Donald Trump" (STEIGER, 2019, p. 5).

Um relatório de Inteligência classificado, elaborado pela Agência Central de Inteligência (CIA), Agência de Segurança Nacional (NSA) e o Bureau Federal de Investigação (FBI), construído sob a coordenação do Escritório do Diretor de Inteligência Nacional (ODNI), divulgado em 6 de janeiro de 2017, descreveu a campanha sistemática da Rússia (ACEVES, 2019, p. 201). Pelo documento, a campanha multifacetada de manipulação cibernética russa, teria sido aprovada nos níveis mais altos do governo russo, passando inclusive pelo o presidente, Vladimir Putin, que teria ordenado que ela fosse realizada por meio das mídias sociais e coordenada por agências de Inteligência. A responsabilidade pelas operações mais significativas ficou a cargo da Inteligência militar, mais precisamente do GRU (SCHMITT, 2018, p. 34).

Além disto, o referido relatório identificou que as duas principais metas da campanha eram (1) apoiar a campanha presidencial de Donald Trump e enfraquecer a campanha de Hillary Clinton; e (2) minar a fé pública no processo eleitoral dos EUA e, consequentemente, no sistema democrático. E por último, o relatório apontava que a campanha teria envolvido vários atores, além do governo, empresas civis, de mídia, financiadas pelo Estado russo, corporações privadas e indivíduos (ACEVES, 2019, p. 201). Em termos práticos, existem registros de uma campanha ativa, de propaganda

[10] Na rede o termo designa uma pessoa cujo comportamento tende a desestabilizar uma discussão e irritar outras pessoas. Acredita-se que o significado surgiu na década de 80 em um fórum de discussões chamado Usenet. Uma brincadeira no fórum propunha que as pessoas utilizassem o que a professora Judith Donath, do M.I.T, chama de tática "pseudo-naïve" (da falsa ingenuidade). Isto é, eles deviam fazer perguntas idiotas e usar argumentos levianos sobre algo sério para ver quem morderia a isca e realmente se irritaria (COUTINHO, 2013).

política, em vários meios de comunicação, incluindo as redes *RT* e *Sputnik*, que foi realizada juntamente com a campanha das mídias sociais (SCHMITT, 2018, p. 34).

Em 22 de março de 2018, o Comitê de Inteligência da Câmara dos Deputados divulgou um relatório detalhado sobre a campanha de mídia social da Rússia. Mesmo não tendo sido possível obter consenso entre os deputados da maioria e da minoria, sobre todas as questões do caso, houve consenso a respeito da realização da campanha obscura da Rússia para influenciar o pleito eleitoral de 2016, tal campanha teria sido realizada com a utilização de propaganda com forte teor psicológico, com larga utilização das redes sociais (ACEVES, 2019, p. 204). Segue abaixo, uma parte do referido relatório:

> A campanha de medidas ativas russas contra os Estados Unidos foi multifacetada. Ele alavancou ataques cibernéticos, plataformas secretas, mídia social, intermediários terceirizados e mídia estatal. O material hackeado foi disseminado por meio dessa miríade de atores com o objetivo de prejudicar a eficácia da futura administração. Essa disseminação funcionou em conjunto com mensagens irrisórias postadas nas redes sociais para minar a confiança na eleição e semear o medo e a divisão na sociedade americana. (HOUSE..., 2018, tradução nossa)

Em dezembro de 2018, o Comitê Especial de Inteligência do Senado divulgou o lançamento de dois relatórios, de grupos de pesquisa independentes, que analisaram a campanha de mídia social da Rússia contra os EUA, trazendo uma análise forense detalhada dos dados fornecidos pelo Comitê, tendo suas descobertas reforçado a conclusão de que os esforços da Rússia foram coordenados, sistemáticos e procuraram polarizar e dividir o público dos EUA (ACEVES, 2019, p. 208).

Porém, nada tem mais relevância jurídica do que as atividades de propaganda dissimulada empreendida nas redes sociais, com larga utilização *trolls*, que amplificaram os escândalos nos quais a candidata Hilary Clinton estava envolvida. "Fazenda de *Trolls*" era a forma pela qual era conhecida a Agência de Pesquisas da Internet (IRA)[11], de origem russa, sediada em São Petersburgo, ligada diretamente ao governo, que possuía um orçamento anual multimilionário e com ligações com a Inteligência Russa (SCHMITT,

[11] A IRA tinha como principal tarefa o apoio à agenda política doméstica e internacional da Rússia, mas não se pode precisar o grau de ligação da mesma com o governo e tal fato impede a atribuição de suas operações ao governo Putin. Sabe que a agência era composta por mais de noventa trolls, tendo gastado mais de dois milhões de dólares para comprar anúncios anti-Clinton e pró-Trump nas plataformas de redes sociais como Twitter, Facebook e Instagram (SCHMITT, 2018, p. 35).

2018, p. 34). Sua estrutura organizacional era sofisticada e tinha o apoio de centenas de funcionários (ACEVES, 2019, p.190).

Os relatórios de inteligência e o resultado das investigações encomendadas pela justiça norte-americana apontaram também para a existência de quatro tipos de atuação dos agentes russos: roubo de informações classificadas, disseminação seletiva de informações, campanha de propaganda manipulativa e tentativa de intrusão nos diversos sistemas de votação espalhados pelo país (VELDE, 2017, p. 10).

A missão primordial da IRA era a de empreender "guerra de informação contra os Estados Unidos da América" e "espalhar a desconfiança em relação aos candidatos e ao sistema político em geral"[12]. O staff da agência era subdividido em equipes, cada uma enfocando diferentes questões, referentes a política interna ou política externa. Com a finalidade de proteger a identidade da vigilância eletrônica, os russos se utilizavam de servidores de *proxie* que se comunicavam em inglês (ACEVES, 2019, p. 190). Para atingir seus propósitos, a agência utilizou mais de 120 grupos e contas nas redes sociais, atuando para convencer alguns indivíduos a votar, bem como tentando manter outros indivíduos longe das urnas (SCHMITT, 2018, p. 35).

A motivação encontrada para a ação de Putin foi a interferência do partido democrata na política interna russa, por ocasião da Revolução Rosa, na Georgia, de 2003; e a Revolução Laranja, na Ucrânia, em 2004. Para Putin, nestas duas ocasiões o então presidente Bill Clinton, para promover a democracia e a ascensão da sociedade civil, incentivou revoltas contra o governo russo. Acredita-se que a interferência da Rússia nas eleições de 2016 tenha sido uma retaliação contra o partido Democrata (VELDE, 2017, p. 10).

Um argumento no sentido de questionar se, no caso das eleições dos EUA, em 2016, o resultado das eleições teria realmente sido alterado com as ações russas e da Cambridge Analítica pode surgir, uma vez que não se tem como provar que tal fato ocorreu. Mas não se pode negar que um pleito eleitoral marcado pelo vício, provocado com as ações supramencionadas, coloca em dúvida a lisura do processo, a legitimidade do governo eleito e, consequentemente, suas futuras decisões. Tal fato pode levar o país alvo a entrar em um processo de infinita polarização política.

[12] Adrian Chen, The Agency, N.Y. TIMES MAG., June 6, 2015, at 57.

Os métodos apresentados no pleito americano de 2016 apontam para a utilização de técnicas assimétricas de emprego de força, que figuram como grave ameaça às democracias do globo. Na medida em que o voto é viciado, o coração do sistema democrático representativo é atingido. Com ações veladas que vieram à público e que visaram corromper a livre formação da intima convicção do eleitor, o sistema democrático foi exposto a uma situação de evidente perigo, provocado pelas facilidades e conquistas da era da informação. Conforme argumenta Steiger (2019), a "auto determinação" do cidadão é criminosamente sequestrada pela "outra determinação", prejudicando a legitimidade do Estado democrático de direito (STEIGER, 2019, p. 22).

O principal objetivo do Projeto Lakhta foi o de causar sérias fraturas no Estado democrático liberal. Os meios e métodos desse empreendimento malicioso estavam enraizados no engano e o efeito pretendido por seus perpetradores foi o da coerção velada: uma vez enganado o povo, o Estado democrático é forçado a aceitar o resultado contaminado ou a lidar com uma situação de legitimidade contestada. Assim, diferente da propaganda convencional que em geral não ultrapassa o limiar da coerção, o Projeto Lakhta e quaisquer atos semelhantes o fazem (STEIGER, 2019, p. 23).

A operação cibernética maliciosa russa também atacou vinte sistemas de registro eleitoral, em todo país. Quatro destes vinte foram comprometidos. Um relatório classificado da Agência de Segurança Nacional (NSA), publicado online pelo site *The Intercept*, afirma que *hackers* russos tentaram enviar e-mails de *spear-phishing*[13] para mais de 100 oficiais eleitorais da *VR Systems*, uma empresa de tecnologia com sede na Flórida, que vende equipamento e software para registro eleitoral (VELDE, 2017, p. 12).

Uma vez que ficou claro o objetivo das operações russas, o governo dos EUA respondeu com a imposição de sanções à várias entidades do país. Em paralelo, o Departamento de Justiça dos EUA apresentou acusação criminal contra várias organizações e indivíduos envolvidos na campanha obscura das redes sociais. Ocorreram audiências públicas no Congresso dos EUA, bem como foi feita proposta de criação de legislação específica para proteção do processo eleitoral. Nas redes sociais, as empresas excluíram as contas abertas pelos agentes russos e se comprometeram a evitar futuras tentativas de intervenções por parte de governos estrangeiros (ACEVES, 2019, p. 181).

---

13 *Spear phishing* é o nome que dá a um tipo de golpe aplicado por e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos. Embora tenha a intenção de roubar dados para fins mal-intencionados, os criminosos virtuais também podem tentar instalar malware no computador do usuário. Ver: https://www.kaspersky.com.br/resource-center/definitions/spear-phishing.

O Tribunal Distrital Federal do Distrito de Columbia, em 16 de fevereiro de 2018, por solicitação do Departamento de Justiça dos EUA, recebeu acusação contra a IRA, mais duas entidades e treze cidadãos russos[14]. Da peça constavam 8 acusações separadas: conspiração para fraudar os Estados Unidos, conspiração para cometer fraude eletrônica e fraude bancária e mais seis acusações de roubo de identidade com agravantes. Segundo a peça de acusação, os indiciados realizaram ações que visaram influenciar as eleições dos EUA e o sistema político, por meio de campanha obscura de mídias sociais. Ainda segundo a acusação, o teor da campanha era o de apresentar o candidato Donald Trump sob uma visão positiva e a candidata Hilary Clinton sob uma visão negativa (ACEVES, 2019, p. 202-203).

As evidências que apontam para uma interferência ilícita da Rússia são fortes e foram capazes de gerar medidas retaliatórias sumárias. Entretanto, a Rússia não atuou sozinha no sinistro contexto do pleito eleitoral de 2016. A empresa privada Cambridge Analítica foi protagonista da primeira ação de uma empresa privada que, com uso de ferramentas analíticas e inteligência artificial, agiu para influenciar a escolha de eleitores de uma Estado soberano, se aproveitando da ausência de regulamentação interna e internacional, que pudesse impedir o feito.

O TRABALHO SUJO DA CAMBRIDGE ANALÍTICA

Apesar de não existir uma definição pacífica sobre o que são as operações de *Big Data*, é correto dizer que a utilização de tais operações figuram como sérias ameaças à democracia. Ação como a "Trolagem Russa" se caracteriza como tipicamente conduzida por Estados, entretanto o trabalho que a Cambridge Analítica executou, no processo eleitoral de 2016, representa uma ação de ator não estatal operando na manipulação de votos de um pleito eleitoral. Ressaltando-se que tanto as operações russas, quanto as da empresa Cambridge Analítica foram executadas em ambientes privados (Instagram,

[14] Em 28 de setembro de 2018, o Departamento de Justiça entrou com uma ação criminal contra Elena Alekseevna Khusyaynova, no Tribunal Distrital federal do Distrito de Leste Virgínia. A denúncia alegava que a Sra. Khusyaynova era a contadora principal do Projeto Lakhta, uma operação russa que "estava envolvida interferência política e eleitoral" que teve como alvo os Estados Unidos e vários outros países (JURECIC, 2018).

Twitter e Facebook) que são suportados por grandes bancos[15] de *Big Data* (STEIGER, 2019, p. 4).

O trabalho da empresa foi exitoso o suficiente para afirmar que venceu as eleições presidenciais dos EUA, com o candidato Donald Trump. Esta lamentável atuação da empresa em um processo eleitoral, no qual os principais legitimados são os cidadãos, provou que os bancos de *Big Data*, localizados nas plataformas de redes sociais, podem ser usados para manipular os eleitores, durante pleitos eleitorais (STEIGER, 2019, p. 6).

Isto se torna mais preocupante, na medida em que a característica principal da pós-modernidade é a crescente indeterminação moral e cognitiva, como consequência do cada vez maior poder tecnológico. Este impacto ambíguo que a era da informação provocou na sociedade caracteriza aquilo que Simoncini (2016) chama de "paradigma tecnocrático". A expressão mais marcante desta ambiguidade se traduz no fato de por um lado a tecnologia figurar como expressão da liberdade criativa do ser humano, por outro ela traz consigo uma forma obscura de poder que não contém em si critérios claros de utilidade para a humanidade (SIMONCINI, 2016, p. 3). A inovação tecnológica carrega consigo um lado oculto, que tem o potencial de impactar negativamente na maneira pela qual as sociedades se relacionam e a democracia se encontra em rota de colisão com este lado obscuro.

A Cambridge Analítica atuou durante as eleições de 2016 dos EUA, efetuando perto de 1,5 bilhão de postagens favoráveis à campanha de Donald Trump. Tais postagens foram realizadas com o auxílio de ferramenta analítica que permitia a adaptação da postagem com o perfil psicológico do usuário alvo. Acredita-se que tal técnica tenha favorecido a vitória do candidato republicano (STEIGER, 2019, p. 3).

Considerando este tipo malicioso de uso do ciberespaço, existe uma relação de risco versus oportunidade, juridicamente falando, bem como uma relação de liberdade versus poder, do ponto de vista da filosofia política. Estes paradoxos não possuem soluções simples, como proibição absoluta ou liberdade plena, mas referindo-se ao princípio da precaução, é exigida uma normatização razoável, que encontre um ponto de equilíbrio entre o lado branco e o lado negro desta força (SIMONCINI, 2016, p. 3).

---

[15] *Google, Facebook, Amazon* vêm trabalhando na coleta e venda destes dados deixados para trás, desde a invenção da internet e para eles tais dados figuram como grandes minas de dinheiro. Com a ajuda de ferramentas analíticas, este tipo de "mineração" pode assinalar tendências, proporcionando a produção de perfis segmentados de usuários, facilitando assim prever e influenciar o comportamento de consumo na rede (STEIGER, 2019, p. 2).

A sistemática utilizada pela Cambridge Analítica teria sido a seguinte: primeiramente, a empresa reuniu o máximo de dados pessoais possíveis de serem coletados na internet, do maior número de pessoas possíveis, no caso em lide, de quase todos os cidadãos norte-americanos elegíveis para votar, cerca de 220 milhões de pessoas. Tais dados foram coletados de diversas fontes acessíveis ao público, principalmente redes sociais como Facebook, Instagram e Twitter. Após ter formado o banco de *Big Data*, uma classificação chamada *Ocean Score* foi atribuída a cada tipo de dado, dividindo as pessoas em categorias específicas (STEIGER, 2019, p. 6).

Neste sentido, o uso impróprio de dados pessoais não tem passado ileso pelo crivo da sociedade internacional, ao contrário, tem causado reações de vários organismos internacionais e regionais, bem como de governos, no sentido de que tal uso seja normatizado. Neste caminho, a Cambridge Analítica, depois de ter atuado em diversas campanhas eleitorais, foi envolvida num escândalo, em 2018, quando "foi acusada de ter adquirido e utilizado dados pessoais de 87 milhões de usuários do Facebook, obtidos de um pesquisador externo que, alegadamente, os recolhia para fins acadêmicos" (BARROSO, 2019, p. 1286).

Para se ter noção da capacidade analítica das ferramentas utilizadas pela empresa, o algoritmo[16] de inteligência artificial é capaz de classificar um perfil básico de uma pessoa considerando apenas 70 curtidas dela em posts no Facebook. Caso esta pessoa tenha dado 150 curtidas, o algoritmo é capaz de conhecê-la melhor do que os próprios pais da pessoa. E com 300 curtidas ele é capaz de conhecer a pessoa melhor do que o seu parceiro ou parceira. Com os resultados das análises realizadas pela ferramenta analítica da Cambridge Analítica, neste oceano de dados, se realiza a preparação do marketing direto e personalizado. O marketing então será realizado com a distribuição de "anúncios" denominados pelo Facebook de *Dark Posts*[17], porque podem ser vistos apenas pela pessoa-alvo e muitas vezes nem são divulgadas como anúncios (STEIGER, 2019, p. 6).

---

[16] Os algoritmos — processos definidos por codificadores para que computadores possam resolver problemas — são os componentes básicos de software. Os programadores podem combinar centenas ou milhares de algoritmos para criar um programa de software que toma decisões sem o conhecimento do usuário. Os usuários manipulam a interface gráfica que executa os scripts de uma linguagem de programação de um nível superior, que é, por sua vez, traduzida em entradas binárias para a unidade central de processamento. Esses níveis de abstração escondem do usuário o processo decisório real da máquina e as várias heurísticas, premissas e falhas que os codificadores incluem, intencional ou inadvertidamente, dentro dos programas (HURST, 2018, p.48).

[17] Por exemplo, se o *Ocean Score* identificou alguém como uma pessoa potencialmente medrosa e, além disso, esta pessoa curtiu a página de Facebook da *National Rifle Association* (NRA), um anúncio de Trump com uma imagem de homens invadindo uma casa era exibido no feed de notícias do Facebook dessa pessoa.

A tecnologia e a política não estão, até o presente momento, devidamente associadas de forma a permitir uma abordagem segura do impacto que ambos os conceitos exercem mutuamente (MINDUS, 2011, p. 5). A construção de postagens manipulativas serve para exemplificar um lado obscuro do uso do ciberespaço pela política, alertando para o fato de a tecnologia da informação tem o potencial de turbar o processo de convencimento do eleitor. Cerca de 4.000 *Dark Posts* (NATE PERSILY, 2017, p. 63-65) diferentes, alcançando entre 1,4 e 1,5 bilhões de espectadores, foram, supostamente, utilizadas na campanha eleitoral de 2016. Apenas no dia do terceiro debate televisivo entre os dois candidatos presidenciais dos EUA, teriam sido exibidos 175.000 *Dark Posts* diferentes[18].

Acredita-se que a era da informação trouxe consigo transformações na maneira pela qual o eleitor pode atingir o seu convencimento sobre as demandas políticas. A participação política e os processos de formação de consentimento e dissenso, realizados tradicionalmente por meio de partidos e movimentos políticos precisarão ser reinventados. Com as possibilidades oferecidas pelo ciberespaço, aspectos básicos de mobilização, pluralismo informacional, dinâmica da opinião pública, estrutura da esfera pública necessitam se adaptar à nova dinâmica. Ainda não existe consenso sobre os aspectos benéficos e maléficos, oriundos da associação da tecnologia da informação com a política, para uns a participação política está aumentando, juntamente com a deliberação, o que tem causado melhora das decisões, mas uma parte dos estudiosos acreditam que esta combinação pode ser extremamente perigosa (MINDUS, 2011, p. 16). A ação realizada pela Cambridge Analítica reforça a preocupação de que existe, realmente, um perigo extremo na associação da política com o ciberespaço, principalmente quando de tal simbiose saem ações maliciosas que atentem contra a democracia.

Sem a utilização das ferramentas analíticas de Big Data, seria impossível a realização destas operações obscuras, que, basicamente, capturaram, de forma intrusiva, a mente dos eleitores norte-americanos. Apesar dos efeitos não serem ainda bem

---

Outro exemplo, se o *Ocean Score* mostrasse que alguém com o perfil extrovertido, cujo pai e mãe gostassem da página de Facebook da NRA, um anúncio de Trump com a imagem de uma família feliz caçando patos era exibido (STEIGER, 2019, p. 6).

[18] Uma comparação dos *Dark Posts* com anúncios comerciais comuns mostra a eficácia dessa ferramenta: as taxas de cliques aumentam em 60% em comparação com a publicidade não personalizada, tecnicamente falando, a taxa de conversão, que indica o percentual de pessoas que clicam e realmente se tornam compradores, no caso dos *Dark Posts*, aumenta extraordinariamente em 1,400% (STEIGER, 2019, p. 6).

compreendidos, o impacto geral de tais operações se tornou conhecido neste último pleito eleitoral (STEIGER, 2019, p. 6). Mas as ferramentas de análise necessitam de um ambiente específico para serem utilizadas e este ambiente, para o caso em estudo, se caracterizou pelas plataformas de redes sociais.

O LADO OBSCURO DAS PLATAFORMAS DE REDE SOCIAIS

Antes de aludir propriamente a questão das plataformas de redes sociais, cabe uma abordagem técnica sobre os tipos de interferência que podem ser observados contra um pleito eleitoral. Normalmente, quando se alude a interferência nas eleições norte-americanas de 2016, costuma-se colocar todo o processo como se fosse uma única intrusão, realizada apenas de uma maneira. A análise mais detalhada do fato deixa claro que ocorreu uma grande operação de interferência, montada pela Rússia, constituída de várias operações cibernéticas maliciosas. Compreender isto se faz importante para que se tenha a noção da complexidade da situação e da dificuldade de se empreender uma resposta assertiva.

Velde (2017) faz uma divisão da ação russa em quatro categorias distintas de operações cibernéticas maliciosas: a primeira categoria é a operação cibernética maliciosa que promove a destruição física do equipamento de votação, tendo em vista que os sistemas eleitorais são sistemas eletrônicos que, na maioria das vezes, se comunicam pelo ciberespaço, um ataque cibernético que explore as vulnerabilidades de tais sistemas pode levar ao dano físico permanente do sistema ou a sua interrupção de funcionalidade, que pode equivaler a um dano físico, caso o sistema fique inoperante para o pleito; a segunda categoria trata-se da interferência na apuração dos votos, a operação cibernética realizada para transferir a totalização de votos das zonas locais para o centro de apuração nacional também está sujeita a interferência maliciosa, neste caso, o programa malicioso poderia criar um algoritmo para substituir as informações verdadeiras por falsas; a terceira categoria de interferência é aquela realizada com o furto de informações classificadas, que podem ser de forma a se buscar coação para algum objetivo político; e, finalmente, a quarta categoria está relacionada a realização de campanhas de informação, com a utilização sistemática de operações cibernéticas manipulativas (VELDE, 2017, p.17-19).

A operação de inteligência russa, bem como as ferramentas analíticas da Cambridge Analítica não seriam uteis se não existisse o ambiente perfeito para serem

empregadas: as plataformas de redes sociais. Apesar de haver indícios de ataques cibernéticos que visaram comprometer o bom andamento das seções eleitorais dos EUA, durante o pleito de 2016, foi por meio da intrusão e furto de informações, bem como pela sistemática campanha de propaganda, realizada pelas plataformas de redes sociais, que os atores obtiveram o êxito de suas ações.

A última categoria que Velde (2017) elenca diz respeito às operações voltadas para atingir o processo de convencimento do eleitor e esta será a categoria que vai tornar a operação cibernética de interferência eleitoral única, no universo dos ataques cibernéticos (VELDE, 2017, p. 19). Enquanto os ataques cibernéticos contra o setor privado visam um ativo comercial e os ataques de Estados contra ativos de outros Estados visam o dano cinético, furto de dados ou interrupção de funcionamento de infraestruturas cibernéticas, com seus alvos bem distintos, materialmente falando. A campanha de manipulação visa conquistar um alvo intangível, imensurável e iminentemente particularizado: as mentes e os corações dos eleitores.

A rede social tem extrema importância na análise do contexto geral, pois ela, com sua insipiente normatização, possibilita que tal manipulação ocorra. A dinâmica de tais operações de manipulação do convencimento se opera em três estágios diferentes. O primeiro é aquele conhecido como "doxing"[19], relacionado a disseminação de informações verdadeiras. Em um segundo estágio, são realizadas as campanhas de propaganda, propriamente ditas, com emprego de técnicas especializadas que operam com a disseminação de argumentos normativos[20]. No terceiro e último estágio, é realizada a obscura campanha de desinformação[21], por meio da ampla disseminação das chamadas

[19] Houve exemplos frequentes dessa prática durante a eleição de 2016 nos EUA. Por exemplo, o *WikiLeaks* postou 20.000 e-mails enviados ou recebidos por altos funcionários do DNC e divulgou uma série de e-mails hackeados do gerente de campanha de Clinton, John Podesta (VELDE, 2017, p. 20).

[20] Por exemplo, a *Voice of America* - e sua emissora afiliada Radio Martí, Radio *Free Europe* / Radio *Liberty* e Radio *Free Asia* - trabalham para "fornecer notícias confiáveis em múltiplas línguas para países que não possuem uma mídia independente viável e para promover os valores democráticos no exterior". Este tipo de campanha de propaganda pode ter como objetivo mudar as estruturas do regime, incentivar a participação democrática ou melhorar o acesso à informação. Nessa medida, a propaganda também é de natureza coerciva (FOLKENFLIK, 2016).

[21] Neste estágio, o elemento importante a ser observado é a natureza coercitiva da divulgação de informações. Ao espalhar informações que sejam falsas ou enganosas, os Estados indicam que seu único propósito é mudar mentes, ações ou inclinações dos eleitores. Por exemplo, durante a eleição presidencial dos EUA de 2016, documentos falsificados, que supostamente eram de um senador do Comitê de Segurança Interna do Senado, circularam. O documento incluía um falso aviso de um ataque cibernético que teria alterado a contagem de votos. Outra história que viralizou no Facebook foi a que dizia que o Papa Francisco tinha endossado a campanha de Donald Trump. Um outro tipo hipotético de *Fake News* que poderia impactar uma eleição seria a divulgação de que os locais de votação estariam fechados, ou informar aos eleitores sobre o local de votação, horário, requisitos ou até mesmo o dia da eleição de forma equivocada,

fake News, que busca turbar, em definitivo, o processo de construção do convencimento dos eleitores. Na prática, existe sobreposição destes estágios, realizada de forma minuciosa e calculada para que seja atingido o efeito desejado da campanha obscura (VELDE, 2017, p. 19).

A associação da política com o anonimato permitido pela virtualidade, uma vez utilizada para fins obscuros, tem o forte potencial de causar danos irreparáveis. As redes sociais são o terreno fértil para o florescimento de propaganda política obscura. Para a teoria social, ser virtual é uma extensão do distanciamento espaço-tempo, por meio do qual as relações entre os atores sociais são cada vez mais despersonificadas. Desta forma, isto se traduz em uma das características mais conspícuas da modernidade tardia, que dá origem a uma série de reconfigurações sociais altamente significativas. Porém, ainda se ignora como a tecnologia da informação está impactando o lado político desta virtualidade (MINDUS, 2011, p. 16).

Fato é que a democracia ainda se traduz em uma forma poderosa de governança, porém, com o advento do ciberespaço, tem demostrado sua fragilidade. Mesmo que sua legitimidade derive da vontade popular, seus princípios igualitários podem ser facilmente cooptados por uma agenda populista, por meio de uma "operação de influência". De acordo com Hollis (2018), uma "operação de influência" pode ser definida como "uma implantação de recursos para fins cognitivos que promovem ou mudam o comportamento de um público-alvo" (HOLLIS 2018, p. 4, tradução nossa). As operações de influência podem ser conduzidas por atores estatais ou não estatais e normalmente variam em termos de tamanho, finalidade, transparência e efeitos e seus alvos são "as percepções do adversário, que residem na dimensão cognitiva do ambiente de informação" (HOLLIS, 2018, p. 36-37, tradução nossa).

Quando os Estados estrangeiros lançam operações de influência, com larga utilização de plataformas de redes sociais, para manipular a vontade do eleitor, as democracias enfrentam riscos ainda maiores. Na era da informação, na qual a mídia social figura como uma maneira simples e rápida para atingir bilhões de pessoas, as consequências das ações russas e da Cambridge Analítica são evidentemente catastróficas para a democracia. Sem nenhuma dúvida, os avanços tecnológicos amplificam o potencial desta ameaça (ACEVES, 2019, p.184).

---

ou até mesmo a criar histórias falsas que alertem sobre a contaminação dos resultados eleitorais (VELDE, 2017, p. 20).

Tanto as operações russas, quanto às da Cambridge Analítica foram executadas com a utilização de "*bots* sociais" (robôs), ou seja, programas de software automatizados que executam postagens[22] automáticas nas redes sociais, se passando por seres humanos. Esses "*bots*" podem se comportar como *trolls*, se programados para postar comentários controversos em sites como o Facebook ou Instagram, ou para usar contas falsas do Twitter e outros meios com a finalidade de ampliar, automaticamente, os comentários feitos pelos *trolls*, tornando a trolagem, aparentemente, confiável e legítima. Todas estas operações maliciosas foram executadas com base em sistemas de Big Data e com o uso de *trolls*, que para os cidadãos americanos figuravam como pessoas reais. Foram criadas centenas de contas de mídia social e uma grande quantidade de diferentes grupos temáticos, que versavam sobre diversas questões, tais como o movimento *Black Lives Matter* e o de controle de imigração. Alguns desses grupos criados possuíam centenas de milhares de pessoas como seguidores (STEIGER, 2019, p. 5).

Uma grande parte das contas de mídias sociais utilizadas pela IRA foram criadas com informações pessoais roubadas de pessoas reais. As equipes de trabalho eram obrigadas a cumprir metas de publicação de novos posts e de realização de comentários sobre os posts já existentes. Os agentes mais produtivos recebiam bônus e os improdutivos eram sujeitos a multas. O processo de criação de posts falsos era baseado em dados reais e fictícios (ACEVES, 2019, p. 190).

Os "*bots*" do Twitter, por exemplo, são capazes de espalhar informações, de forma extremamente rápida para os eleitores com perfis na plataforma, sendo que a plataforma não possui capacidade de realizar a análise crítica deste conteúdo que está sendo veiculado, cabendo tal tarefa aos vulneráveis eleitores. Sites como *Facebook, Google e Twitter*, na ocasião do pleito de 2016, ainda não filtravam ou sinalizavam notícias falsas. Atualmente sinalizam, mas de forma tímida. Neste contexto, a divulgação de *fake news* gera aquilo que Bruno Kahl, chefe da Inteligência alemã, denomina de "incerteza política" (GILSINAN; CALAMUR, 2017), com um potencial claro de ocasionar

[22] Um exemplo clássico destas postagens foi a realizada numa suposta conta que pertencia ao movimento *Black Lives Matter* que, com a clara intenção de influenciar os votos dos cidadãos negros, dizia o seguinte: "'Um exagerado ódio, em particular por Trump, está enganando o povo e forçando os negros a votar em Hillary. Não podemos recorrer ao menor de dois demônios. Então, certamente estaríamos melhor sem votar NADA"[22]. Além dessas postagens, publicamente visíveis, também foram utilizadas mensagens individualizadas para criar confiança em grupos segmentados. Por fim, foram comprados anúncios nas plataformas de mídia social (STEIGER, 2019, p. 5, tradução nossa).

confusão na livre formação da convicção do eleitor e promover mudança de votos e de preferencias eleitorais (VELDE, 2017, p. 20).

A dinâmica de utilização das redes sociais, pelos agentes russos, se iniciava com a presença *on line* disfarçada, para a criação das contas falsas, após isto os perfis buscavam ganhar seguidores e construir credibilidade, ampliando cada vez mais o alcance das publicações e a segmentação do público-alvo por classes temáticas. As plataformas de mídia social permitiram que esses anúncios fossem direcionados a grupos específicos por meio de vários critérios, incluindo dados demográficos, localização, interesses e comportamento (ACEVES, 2019, p. 190).

Além do Facebook, a IRA usou o Twitter e o Instagram. Embora algumas das contas do Twitter tivessem sido operadas por seres humanos, a grande maioria foi operada pelos *bots*. O grupo chamado *Ten_Gop* tratava-se de uma conta falsa, particularmente ativa e influente, no Twitter. Fingia representar o *Tennessee GOP* (*Tennessee group of persons*). Esta conta tinha aproximadamente 136.000 seguidores, dez vezes mais seguidores que a conta real do grupo *Tennessee GOP*. O mais grave era que os *tweets* do falso grupo eram citados, rotineiramente, por veículos de notícias de todo o país (ACEVES, 2019, p. 199).

Mas foi no Instagram que a Rússia apresentou o lado mais obscuro de sua sinistra campanha. Duas contas específicas promoveram ralis de partidos antagônicos, no mundo real. O movimento foi marcado para ocorrer na sede da *National Football League*, em Nova York, às 8h do dia 16 de fevereiro de 2016 (ROMM, 2018). Os ralis foram convocados sob o pretexto de dar uma resposta ao desempenho da cantora Beyoncé, que no intervalo do Super Bowl realizou uma performance na qual reconheceu o movimento *Black Lives Matter*. Um dos ralis foi designado como *ProBeyoncé Protest Rally*, tendo como objetivo atrair indivíduos interessados em denunciar os "privilégios brancos". Já o rali concorrente foi denominado de *Anti-Beyoncé Protest Rally*, tendo como objetivo atrair pessoas interessadas em denunciar o racismo (ROGERS, 2016) da cantora (ACEVES, 2019, p. 199). Este não foi um evento isolado, em várias ocasiões, a campanha de propaganda russa passou do mundo virtual para o mundo real. Em algumas ocasiões, a IRA contratou indivíduos para organizar esses comícios, bem como contratou indivíduos para carregar cartazes, com mensagens pré-selecionadas (ACEVES, 2019, p. 200).

Para se ter ideia da força da rede social, a Rússia foi muito ativa na Flórida e organizou o comício *Florida Goes Trump*. Os anúncios para este evento atingiram uma audiência total de mais de 59.000 usuários do Facebook, somente na Flórida. Mais de 8.300 usuários do Facebook clicaram nos anúncios e, portanto, foram levados a uma página falsa do Facebook chamada "Ser patriótico" (STEIGER, 2019, p. 5). Conforme dados do próprio Facebook, entre janeiro de 2015 e agosto de 2017, contas falsas associadas a IRA compraram mais de 3.000 anúncios[23], que foram utilizados em cerca de 120 páginas no Facebook, incluindo mais de 80.000 posts, que atingiram cerca de 126 milhões de usuários. A escolha dos usuários alvo foi feita com a utilização de ferramentas analíticas de *Big Data*, tendo em vista os interesses registrados em seus perfis de Facebook (STEIGER, 2019, p. 6)

O Facebook (WEEDON; NULAND, STAMOS, 2017) descreve o processo de manipulação como sendo uma falsa amplificação, na qual a atividade coordenada entre contas, não autênticas e conectadas, busca manipular a opinião pública. Os objetivos desta manipulação seriam os seguintes: 1-*Amplificar ou explorar uma causa ou um problema específico*- Este é o principal efeito desejado de amplificadores falsos. Pode incluir uso deliberado de desinformação, utilização de memes e / ou notícias falsas. É comum que exista um gatilho, ou seja, um problema específico que será explorado e amplificado pela campanha obscura; 2- *Desacreditar as instituições políticas*- Com a aplicação desta dinâmica, os agentes adversos não particularizam um problema específico, mas buscam desgastar o status quo das instituições políticas ou até mesmo a sociedade civil em geral, em um nível mais estratégico; 3- *Espalhar a confusão*- Os controladores das redes de contas falsas visam um objetivo de longo prazo, com a finalidade de contaminar o discurso cívico e colocar os atores antagônicas da sociedade uns contra os outros, no caso em lide, atores oportunistas, com o uso do Facebook, se utilizaram de contas falsas, se engajaram ativamente em todo o espectro político com a aparente intenção de aumentar as tensões entre os apoiadores desses grupos e fraturar suas bases de apoio (ACEVES, 2019, p. 192).

A realização de marketing político faz parte da dinâmica dos pleitos eleitorais. Propagandas de rádio e televisão reforçam a campanha dos candidatos ao pleito e, em

[23] Cerca de 55% dos anúncios comprados pela IRA no Facebook versavam sobre questões raciais. Uma parte desses anúncios faziam referência explícita à corrida presidencial de 2016 ou aos candidatos, entretanto, muitos anúncios foram focados em questões discretas ou tinham como alvo grupos específicos, de ambos os lados do espectro ideológico da disputa (ACEVES, 2019, p .193).

países como o Brasil, são franqueadas pelo poder público e exibidas em horários pré-determinados, de forma obrigatória, na programação radio televisiva. Porém, as propagandas exibidas em mídias sociais são diferentes daquelas veiculadas em rádio e tv. A propaganda eleitoral radio televisiva possui um viés mais democrático, pois não permite a segmentação de público-alvo e direcionamento personalizado, desta forma permitem a formação da convicção e "pontos de vistas através da informação mais diversificada, profunda e equilibrada possível"[24] (STEIGER, 2019, p. 10, tradução nossa).

Para se ter uma noção de como o esquema funcionava, apenas um único anúncio de uma falsa comunidade denominada *Back the Badge*, criada no Facebook, recebeu 1.334.544 visualizações e 73.063 cliques. Foi o post, no Facebook, de maior sucesso feito pela IRA. Um outro anúncio, também Facebook, intitulado *Black Matters*, que recebeu 784.116 visualizações e 55.761 cliques, foi criado pela IRA, em 13 de julho de 2015, tendo custado, aproximadamente, 2.200 dólares americanos (ACEVES, 2019, p. 194).

Cabe ressaltar que os *Dark Posts* realizados pela Cambridge Analítica, para um público alvo previamente selecionado pelas poderosas ferramentas analíticas de Big Data e inteligência artificial, construídos na maioria das vezes com dados falsos ou tendenciosos, que visavam manipular o convencimento do eleitor, viciaram a cognição do eleitorado, prejudicando assim, a concorrência limpa e o processo político regular. Além disso, o pluralismo, a aceitação da decisão da maioria e o controle democrático também foram afetados pelas ações dos *trolls* russos e da Cambridge Analítica. Pois, os ambientes nos quais as propagandas manipuladas foram veiculadas são, comprovadamente, caracterizados como câmaras de eco e de bolhas de filtro, sendo, desta forma, ambientes iminentemente anti-pluralistas.

Tanto Twitter, como Instagram ou Facebook são ambientes que carecem de legitimidade e transparência, uma vez que possibilitam, pela particularidade de estarem baseados no ciberespaço, que usuários construam e trabalhem com contas falsas. Todas estas redes sociais permitem as comunicações ponto a ponto que não podem ser observadas por terceiros, não podendo, desta forma, serem desafiadas ou colocadas em debate. Ao contrário disto, os spots de TV são, por natureza, visíveis a todos e abertos ao desafio e controle do público. (STEIGER, 2019, p. 10).

[24] German Federal Constitutional Court ,BVerfGE 136, 9 [126] (separate opinion of Justice Paulus).

A técnica utilizada pelos agentes russos buscava oferecer perspectivas diferenciadas para diversos tipos de questões, desde o apoio aos aplicadores da lei, até críticas duras para estes mesmos aplicadores, passando posts que denunciavam o movimento *Black Lives Matter* e menosprezaram as causas de justiça social. Algumas ações foram ainda mais radicais e apoiaram grupos nacionalistas brancos, com apelos à violência. Além de postagens sobre questões raciais e de justiça social, os operativos russos também abordaram outras questões importantes e controversas, tais como imigração, direitos LGBT, controle de armas e religião. Portanto não há dúvidas de que se tratou de campanha de mídia social, projetada para promover tensões raciais e minar o tecido social dos Estados Unidos (ACEVES, 2019, p. 180).

Todo processo de análise do Big Data, que vai orientar a distribuição de postagens para os públicos-alvo segmentados, é realizado por um algoritmo de Inteligência Artificial, que normalmente se caracterizam como "caixas preta" não sujeitas a nenhum controle externo, o que pode representar um grande problema para o caso de uma responsabilização penal. Além disso, o indivíduo não sabe que uma conta no Twitter ou no Facebook é falsa e, provavelmente, não sabe que determinadas postagens foram pagas com finalidades escusas. Em 2016, por ocasião da corrida eleitoral, os termos e condições de uso do Facebook declaravam expressamente que a empresa nem sempre caracterizava serviços e comunicações pagos como tais. Esta diretiva foi modificada apenas em 2019 (STEIGER, 2019, p. 11).

Para Aceves (2019), não resta dúvida de que a campanha[25] russa empregou técnicas de propaganda, uma vez que visou influenciar, dissimuladamente, as opiniões e comportamentos de cidadãos norte-americanos. Sabe-se que a propaganda envolve "a comunicação de fatos, ficção, argumento e sugestão, muitas vezes com a supressão proposital de material inconsistente, com a esperança e intenção de implantar nas mentes do público 'alvo' certos preconceitos, crenças ou convicções" (WHITTON, 1974, p. 239, tradução nossa). Neste sentido, não é exagero dizer que as ações russas também podem

[25] De junho a dezembro de 2015, a IRA lançou entre 20 e 70 anúncios, no Facebook, com o foco na questão racial. Mesmo após o pleito eleitoral, esta dinâmica continuou, até ter uma diminuição em janeiro de 2017. O resultado desta campanha sinistra pode ser notado pela quantidade de interações que foram realizadas nos posts. Os posts com conteúdo racial receberam, aproximadamente, 25 milhões de visualizações, entre junho de 2016 e maio de 2017. São números que apontam para um alcance extraordinário da campanha russa. Dentre os diversos grupos criados pela IRA, sobressaíram os seguintes: *Blacktivist, Heart of Texas, United Muslims of America, Being Patriotic, Secured Borders e LGBT United*. Tais grupos geraram milhares de postagens, sendo estas postagens compartilhadas milhões de vezes (ACEVES, 2019, p. 194-198).

ser descritas como uma operação de informação sofisticada. Tais operações envolvem "ações tomadas por governos ou atores não-estatais organizados para distorcer o sentimento político interno ou estrangeiro, mais frequentemente para alcançar um objetivo estratégico e / ou resultado geopolítico" (WEEDON, 2017, p. 5, tradução nossa).

Os prepostos das empresas de mídia social Facebook, Twitter e Google foram convocados para uma audiência no Comitê de Inteligência da Câmara dos Deputados em 1º de novembro de 2017. Estes altos funcionários fizeram revelações impactantes sobre a IRA. Segundo o depoimento, a IRA teria gastado cerca de 2 milhões de dólares americanos para comprar mais de 3.000 anúncios, entre junho de 2015 e agosto de 2017, além de ter configurado 120 contas, que realizaram mais de 80.000 posts, durante o mesmo período, confirmando ainda que o conteúdo dos posts abordava temas relacionados a questões sociais e políticas, com intuito de causar divisão. O Facebook estimava que as postagens da IRA atingiram cerca de 126 milhões de usuários. Os Funcionários do Twitter identificaram cerca de 2.752 contas vinculadas à IRA, tendo estas contas postado cerca de 131.000 mensagens. Além disso, o Twitter identificou cerca de 36.000 contas engajadas em atividades suspeitas, relacionadas à corrida presidencial de 2016, que teriam postado cerca de 1,4 milhão de tuítes, entre setembro e novembro de 2016 e esses tuítes teriam recebido cerca de 288 milhões de visualizações. Em relação ao Google foram identificadas apenas duas contas que, aparentemente, faziam parte da campanha obscura (ACEVES, 2019, p. 202).

A utilização do ciberespaço para influenciar campanhas políticas é uma realidade que não pode mais ser negligenciada pelo direito. Atores estatais e não estatais, com intenções escusas e práticas maliciosas podem se utilizar das peculiares características do ambiente informacional, com a finalidade de perpetrarem ações ilícitas na busca de fins diversos. As plataformas de redes sociais oferecem uma ferramenta de poder para estes atores, as utilidades de tais redes para estes agentes vai muito além do entretenimento.

Desta forma, neste ponto do artigo encerra-se a apresentação do caso de estudo e passa-se a dedicar a análise dos reflexos que as operações cibernéticas maliciosas tiveram no direito. A análise sumária das principais teorias que se voltam para explicar o fenômeno que envolve a reunião do direito com a política e a tecnologia se faz importante para que, em seguida, sejam analisados os reflexos no direito interno.

O ATAQUE CONTRA A DEMOCRACIA E SEUS REFLEXOS PARA O DIREITO

O que mais causa espécie no caso apresentado é o fato de a campanha cibernética maliciosa ter atingindo um dos centros de gravidade da democracia: o voto. Uma vez afetado o livre convencimento do eleitor, a legitimidade deste solene ato democrático é colocada em dúvida. Portanto, já que as ações decorrentes do processo eleitoral estão sujeitas ao que preconiza a ordem jurídica, maculado o pleito, se pode concluir que manchada está também a democracia.

Nesta seção do artigo serão abordados os dois principais aspectos que afetam a ordem jurídica e a sua relação com o poder político. Inicialmente será realizada uma reflexão sobre alguns pontos relacionados à confluência do direito com a política e a tecnologia; e em seguida serão analisados aspectos que ressaltam a força simbólica que o voto possui para a democracia, bem como as consequências da manipulação do pleito de 2016 para os direitos fundamentais.

DIREITO, POLÍTICA E CIBERESPAÇO

Nos espaços nacionais o ciberespaço tem alterado a relação de poder existente entre o Estado e a sociedade e, juridicamente falando, o direito constitucional é o ramo das ciências jurídicas mais afetado, pelo fato de lidar diretamente com a Constituição e ter a finalidade de impor limites ao poder (individual e social). Uma vez que a sociedade é afetada pela inovação tecnológica, sendo a Constituição o testamento político mais elevado de uma sociedade, inevitavelmente, o direito constitucional também sofre influência do emergente fenômeno tecnológico. Do constitucionalismo antigo ao moderno e até mesmo no constitucionalismo contemporâneo, o direito constitucional tem procurado controlar o poder, seja estabelecendo um conjunto de direitos inalienáveis e fundamentais, seja estabelecendo certas regras de organização dos poderes públicos (SIMONCINI, 2016, p. 4), entretanto, a tecnologia fez surgir um ambiente ainda mais desafiador: o ciberespaço.

Muitos teóricos do direito, já há algum tempo, vêm tentando entender a relação que ocorre entre o direito e a política. Como já citado anteriormente, Kelsen figura nesta lista e sua Teoria Pura do Direito se esforça para subordinar o poder do Estado à existência de uma ordem jurídica legitima. O poder pelo poder não tem muito significado na arena

do direito e o direito sem o seu papel equalizador do poder também não significa muito para a sociedade. Entretanto, a era da informação chegou para colocar a tecnologia nesta já tensa relação entre poder e direito. O ciberespaço figura como o *locus* no qual o planeta vive nesta era contemporânea e, assim sendo, passou a figurar como ferramenta de uso para a política, para ações de manipulação e campanhas obscuras que visam afetar o comportamento do cidadão, normalmente com emprego de discurso de ódio. Sobre isto, Barroso (2019) afirma o seguinte:

> A internet e as redes sociais, por exemplo, deram lugar a desvios como discursos de ódio e campanhas de desinformação. Como proteger a comunicação no mundo das *fake news* e do *deep fake*, no qual vídeos falsos reproduzem imagem e voz de pessoas reais em situações inusitadas e inverídicas? As empresas que oferecem plataformas para as mídias digitais, compreensivelmente, relutam em funcionar como censores privados. Por outro lado, a interferência estatal no domínio da liberdade de expressão é sempre arriscada. Diante desse quadro, não há remédios jurídicos totalmente eficientes ou politicamente simples (BARROSO, 2019, p.1286).

A estrutura normativa que atualmente cerca a tecnologia da informação é multifacetada. Em uma primeira camada surge o nível subjetivo / moral, que tradicionalmente não está ao alcance dos juristas, mas não deve ser negligenciado. Uma vez que, em sua estrutura, o ciberespaço é, naturalmente, resiliente à regulamentação clássica, uma maneira eficiente de torná-lo um lugar mais seguro seria por meio da construção de um código moral do ciberespaço. O nível seguinte, intermediário, diz respeito ao conteúdo normativo ético-coletivo, representado por programas de pesquisas, convenções internacionais, legislação da União Europeia, manuais não vinculativos, melhores práticas e diretrizes gerais. A normatização deste nível figura como *soft law*, autorregulação, acordos voluntários ou regulamentos de autoridades privadas. Por fim, há um terceiro nível, público-jurídico, que envolve a regulação jurídica em sentido estrito, e que se materializa nas formas local, nacional, doméstico, constitucional, supranacional e internacional de regulamentos técnicos (SIMONCINI, 2016, p. 3).

Para Mindus (2011), a teoria do direito e a ciência política não dão a importância devida para a dimensão que o impacto da tecnologia causa em ambos os campos. Desta forma, uma observação atenta demonstra que existe “um vazio embaraçoso quando se tenta dar sentido ao que ocorre na infosfera”. Na visão da autora, a teoria da comunicação social e os estudos de ciência e tecnologia, também ignoram trabalho que tem sido

realizado, constantemente, na teoria jurídica e política sobre o conceito, limites e pré-condições da democracia (MINDUS, 2011, p. 6, tradução nossa). O conceito de democracia eletrônica tem se firmado em todo planeta, mas para sua operacionalização o direito deverá ter avançado no sentido de coibir as ameaças relacionadas ao uso malicioso do ciberespaço.

Neste caminho, existem algumas formas de encarar a relação entre o ciberespaço e a política que vão impactar no conceito da democracia eletrônica. Uma parte dos teóricos que se dedica ao tema acredita que o advento da tecnologia da informação, em relação a ciência política, é apenas uma continuação de experiencias anteriores, que não introduz mudança significativa. Já um outro grupo acredita que a tecnologia da informação é transformadora para a ciência política e induz a um novo paradigma representado pela democracia eletrônica (MINDUS, 2011, p.10).

A chegada da internet trouxe a esperança de que a participação da sociedade na vida política do país aumentaria, bem como o nível de responsabilidade dos governantes. Idealizou-se a criação de uma esfera pública digital, com o potencial de incrementar o exercício da democracia deliberativa, proporcionando um aumento na qualidade do debate público. Porém, o que se percebe, até o presente momento, é um efeito exatamente inverso, ao invés de fomentar o debate racional, sobre matérias relevantes para a sociedade, tem proporcionado a radicalização do debate e a prática da disseminação das *fake news*, em paralelo com o discurso de ódio. A realidade é que o ceticismo em relação à contribuição da rede para a melhora do sentimento democrático é grande, mesmo que ainda se acredite que possa haver, em médio ou longo prazo, “um avanço civilizatório paulatino rumo a uma maior racionalidade e tolerância” (BARROSO, 2019, p.1290-1291).

A ideia de que os níveis de democracia são diretamente proporcionais ao incremento do uso do ciberespaço não é verdadeira. Estados com regimes não democráticos possuem grande número de utilizadores, enquanto Estados democráticos se utilizam da rede para a realização de operações obscuras, como as denunciadas por Edward Snowden. Não obstante estas distorções, Estados democráticos (Inglaterra, França, Espanha) buscam aprovação de estratégias de cibersegurança, com a finalidade de protegerem-se do terrorismo e de interferências ilícitas realizadas por atores estatais e não estatais, pelo ciberespaço (SIMONCINI, 2016, p. 6).

Existem alguns que são extremamente céticos, como Hindman (2009), que depois de rastrear quase três milhões de páginas da internet, acredita que a ideia de que a Internet estaria "democratizando" a política, estaria completamente errada. O que ele denomina de "Googlearquia", se refere ao estado atual do ciberespaço e demonstra que a rede pouco fez para ampliar o discurso político, mas na verdade fortaleceu um pequeno conjunto de elites - algumas novas, mas a maioria já conhecida (HINDMAN, 2009, p. 3).

Fato é que não se consegue avaliar com precisão o impacto que o ciberespaço pode causar, especificamente, na democracia, nesta era da informação. Como o direito está intimamente ligado à organização da sociedade, para que seja mensurada a dimensão exata do impacto que o advento do ciberespaço tem causado nos ordenamentos jurídicos constitucionais é necessário primeiro medir o impacto que o fenômeno está tendo sobre a natureza do pensamento humano, portanto, as relações sociais e, eventualmente, sobre a própria antropologia humana. Desde os anos de 1970, a internet tem crescido em ritmo acelerado, tendo passado de 25 milhões de usuários, em 1970, para 3 bilhões em 2015. Atualmente, 40% da população atual se utiliza das facilidades oferecidas pelo ciberespaço, este percentual chega a 78% da população nos países desenvolvidos e 30% naqueles em desenvolvimento. No total, são mais de 7 bilhões de smartfones, capazes de se conectarem ao ciberespaço, na posse dos cidadãos do planeta (SIMONCINI, 2016, p. 1). Esta explosão de tecnologia tem seu reflexo na política e no direito.

Algumas correntes que analisam o impacto da tecnologia na política e no direito estão surgindo. Dentre aqueles que não veem nenhuma diferença a ser imposta pela tecnologia da informação na maneira pela qual o poder se apresenta na sociedade, existem duas principais correntes: 1- os escolásticos, que acreditam numa perspectivas que não leva em consideração a revolução digital e, portanto, não estão dispostos a operar com, ou mesmo notar, as mudanças atuais; e 2- os tradicionalistas, que acreditam numa abordagem que sustenta que estamos testemunhando novas versões de problemas antigos, se recusando a considerar que a atual conjuntura oferece recursos únicos e exclusivos (MINDUS, 2011, p. 10).

A corrente escolástica demonstra um apego meta-teoricamente acrítico a um cenário teórico incapaz de considerar novos dados, de forma a realizar uma abstração daquilo que realmente ocorre no ciberespaço. Tal abordagem chega perto do discurso arrogante de negacionismo, que crê que o poder continua sendo buscado como um fim em si mesmo, ignorando aquilo que Mindus (2011) denomina de "virada informacional".

Para estes, o mundo interconectado não tem o potencial de afetar as bases tradicionais da luta pelo poder. Tal abordagem é de uma completa cegueira para o novo ambiente moldado pelo ciberespaço, opondo-se totalmente a ideia de que a tecnologia da informação oferece potencial para uma redistribuição radical de poder (MINDUS, 2011, p. 9).

Naquilo que tange ao direito, ele procura abordar as novas conjunturas, com ubiquidade, universalidade e completude. Entretanto, não apenas pela complexidade do mundo, mas também por sua pluralidade e volatilidade, o direito se confronta, a todo momento, com um novo teste, pois o surgimento de dilemas éticos e impasses políticos é inevitável. Entretanto, é importante "manter o avanço tecnológico numa trilha ética e humanista, revitalizar a democracia, incorporando as potencialidades do mundo digital e redesenhando as instituições" (BARROSO, 2019, p. 1265). Desta forma, se faz importante, para a compreensão do fenômeno que envolve a política e o direito, trazer ao debate acadêmico novos tipos de abordagem.

No que tange a abordagem "Tradicionalista", cabe ressaltar que a palavra, para a abordagem em questão não possui nenhum significado politicamente carregado, apenas indica a capacidade cognitiva e epistemológica de uma teoria, já em uso, para explicar os fatos futuros. Desta forma, cabe notar que a principal diferença entre tradicionalistas e escolásticos estaria no fato de que os tradicionalistas aceitam o advento da era da informação, mas acreditam ter as respostas para o fenômeno, enquanto os escolásticos não aceitam. As perspectivas tradicionalistas, segundo Mindus (2011), na maioria das vezes, interpretam de forma assertiva a dinâmica pela qual as decisões políticas são tomadas, ao mesmo tempo em que a sociedade vai incorporando as práticas da tecnologia. Em geral, normativamente, os tradicionalistas recomendam que seja observado o inventário das experiências anteriores, a fim de explicar o impacto da tecnologia na política. No entanto, tal abordagem se arrisca a sobrecarregar a analogia, com a sugestão de um processo puramente mecânico de percepções e isto pode desconsiderar e distorcer decisões importantes que estão sendo tomadas na moldura das novas tecnologias que serão usadas na operação dentro do, politicamente carregado, mundo da experiência (MINDUS, 2011, p. 10).

Mas existe uma corrente teórica que acredita que o ciberespaço tem impacto decisivo nas relações políticas dos seres humanos, de modo que o advento da tecnologia aplicada às relações de poder deve ser objeto de investigação independente, capaz de

abordar a “singularidade” do “ciberespaço político” e da “democracia digital”. Os defensores desta corrente de investigação independente, assim como os céticos abordados anteriormente, desenvolvem perspectivas diferentes: a primeira centra-se na “transformação” provocada pela digitalização, enquanto a segunda se concentra na “revolução” em curso, fruto das novas tecnologias. No geral, os defensores desta correte acreditam que da mesma forma que a “era da informação”, que proporciona a existência de um Estado interconectado com seus cidadãos, impactou outros ramos do pensamento prático, como a ética, a economia e o direito, pelas perspectivas da transformação e da revolução, o planeta estaria testemunhando novas versões de velhos problemas, mas a questão não seria apenas de se realizar um nova contextualização, mas sim de aceitar que o advento traz características únicas e sem precedentes na história (MINDUS, 2011, p. 10).

A perspectiva de transformação é a que mais se percebe no planeta interconectado pelo ciberespaço. Provavelmente o primeiro domínio de conhecimento prático que considerou o potencial de transformação da era da informação foi a ética, que desde os anos de 1980 levanta questionamentos[26] sobre o impacto da informática nas relações sociais. O campo da economia também foi fortemente impactado pela capacidade de transformação da era da informação, de forma que os impactos[27] desta transformação foram notados na capacidade de reduzir custos de administração interna, agilizar a comunicação, reduzir custos de transmissão de dados. No campo da política, a tendência de transformação se fez presente com a transição[28] das administrações públicas para o chamado “governo eletrônico”, que simplificou, padronizou e transformou as administrações públicas de todo o globo. Entretanto, para Mindus (2011) isto não significou a “revolução” em direção à democracia digital. O potencial transformador do

[26] Perguntas do tipo: É ético um site colocar um cookie no disco rígido de quem o visita? A mineração de dados é moralmente aceitável? Os nomes de domínio da Internet estão sendo distribuídos de maneira justa? A cirurgia deve ser realizada remotamente com tecnologia de imagens médicas? Devem ser permitidas recriações gráficas de incidentes, como acidentes automobilísticos, em tribunais? É certo para um indivíduo reproduzir e alterar eletronicamente uma imagem artística que foi originalmente criada por outra pessoa? (MINDUS, 2011, p. 11).

[27] Todos os aspectos que significaram a redução do número de intermediários entre os fornecedores originais de bens e serviços e os consumidores finais sofreram impactos da tecnologia digital. Os futuristas acreditavam que a desintermediação desafiaria as funções econômicas tradicionais de atacadistas e varejistas, implicando em menos shoppings centers, escritórios, editoras etc. Este foco em funções econômicas renovadas é um bom exemplo da perspectiva focada na "transformação (MINDUS, 2011, p.12).

[28] Exemplos como prestação de serviços eletrônicos, o desenvolvimento de ferramentas de gerenciamento padronizadas para documentação legal e recuperação de informações, como padrões XML; ZTTs em vigilância e gerenciamento de congestionamento; cartões inteligentes em transporte público, como o London Oystercard (MINDUS, 2011, p.12).

ciberespaço também foi percebido pelos operadores do direito, principalmente com o surgimento de novos crimes cibernéticos e pela explosão[29] de legislações, a partir da década de 1990, que tentavam empreender a regulação desta nova tecnologia. Em resumo, segundo esta abordagem, o potencial transformador da era digital foi firmemente compreendido, bem como novas formas de lidar com as versões atualizadas da ética tradicional, das questões econômicas e jurídicas, notavelmente, se desenvolveram rapidamente (MINDUS, 2011, p. 12).

O potencial revolucionário da internet é indiscutível. Ao mesmo tempo que o ciberespaço é um ambiente de plena anarquia, se traduz no ambiente mais igualitário do planeta, no qual o rico e o pobre, o poderoso e o vassalo, o intelectual e o ignorante dividem o mesmo espaço, sem cerimônias. Pode-se apontar também para o surgimento da ética da informação, que vai além da ética da computação, uma vez que o tema fundamental desta ética não é mais considerado o ser humano, mas sim as entidades informacionais.

A revolução da informação, com sua impressionante velocidade: dos posts, dos *trolls*, dos *Dark Posts*, dos vídeos, dos documentos eletrônicos, que saem de Brasília para Tóquio em centésimos de segundos, a depender da largura de banda ou da capacidade do *Wi-Fi*. Aludindo-se aos fenômenos como o ciberterrorismo, o hackativismo e outros, que só existem devido ao potencial revolucionário da internet. E por fim, para o objeto deste artigo, a mudança na perspectiva do direito de privacidade e do direito a participação democrática, vítimas dos ataques de 2016, que hoje são considerados sob a força da virtualidade, nos quais efeitos revolucionários foram reverberados, no que tange ao exercício dos direitos fundamentais. Não foi sem motivos que Norbert Weiner, o precursor da noção do estudo da cibernética, quando comparou o ambiente cibernético com a bomba atômica de Nagasaki, afirmou que, em se tratando de capacidade, "estávamos na presença de outra potencialidade social de importância inédita para o bem e o mal" (WEINER, 1948, p. 27, tradução nossa).

Em suma, ainda aqui persiste a relação ambígua entre direito e tecnologia: se por um lado o ciberespaço é uma nova ferramenta poderosa para consecução dos objetivos do direito constitucional, traduzindo-se em uma forma inovadora de definir, controlar e

[29] Por exemplo, a Lei de Direitos Autorais do Milênio Digital de 1998, nos EUA, que definiu o regime de irresponsabilidade para ISPs sem o qual grande parte da web 2.0 não poderia ter se desenvolvido, com *Del.icio.us, Essembly, FB, Flickr, Gather, MySpace, Partybuilder, YouTube, Ning, Metacafe, Revver, Blip.tv, CHBN, vSocial, Tagworld, Collectivex, Bebo, Care2, Hi5, Xanga* (MINDUS, 2011, p.13).

regular o poder do Estado; por outro lado, o ciberespaço figura como um novo objeto da alçada deste mesmo direito, mais precisamente uma nova fonte de poder a ser definida, controlada e regulada (SIMONCINI, 2016, p. 4).

A MANIPULAÇÃO DO VOTO E SEUS REFLEXOS PARA OS DIREITOS FUNDAMENTAIS

O voto é revestido de uma característica hibrida e única, na democracia: por ele a vontade soberana da sociedade, porque não dizer o poder, seleciona e legitima o elemento político que terá a tarefa de representá-la.

Pode-se dizer que o voto é a expressão mais política do direito, como também a expressão mais jurídica da política. Por meio dele existe uma transposição de dimensões diferentes do poder, pois a vontade (poder) política da sociedade se submete à ordem jurídica (poder) do Estado. Cabe ressaltar que o poder político só tem legitimidade quando está subordinado a uma ordem jurídica. Não existe Estado sem que exista o direito. O poder do Estado só se legitima estando subordinado a uma ordem jurídica e a política é uma das expressões do poder estatal, mas precisa se submeter à ordem jurídica.

Desta forma, afirma Kelsen que o poder estatal só tem esta designação e se distingue de outras relações de poder pelo fato dele estar juridicamente regulado. Esta relação especial de poder que é atribuída ao Estado se trata da vigência de uma ordem jurídica estatal efetiva, pois "os indivíduos que, como governo do Estado, exercem o poder, recebem competência de uma ordem jurídica para exercerem aquele poder através da criação e aplicação de normas jurídicas - que o poder do Estado tem caráter normativo" (KELSEN, 1998, p. 202).

Quando a Constituição de 1988, em seu parágrafo único, do artigo 1.º expressa que "Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição", está se referindo ao poder soberano da sociedade, que, legitimado pela Carta política máxima, que é a Constituição, é transferido para os representantes, por meio do voto, e inserido no contexto do poder do Estado. O voto é o ponto híbrido do Estado democrático de direito. Se traduz no passaporte político que insere o representante do povo no contexto da ordem estatal.

O constitucionalismo democrático foi o paradigma de governo que prevaleceu no século XX. Dotado com características modernas que englobam poder limitado,

dignidade da pessoa humana, direitos fundamentais, justiça material, tolerância, respeito ao outro e, de certo modo, felicidade. Para que se chegasse a democracia como ela é, foi necessária a fusão do constitucionalismo, herdeiro da tradição liberal que remonta ao final do século XVII, que agrega no seu conceito a limitação do poder do Estado, por meio da ordem jurídica, e o respeito aos direitos fundamentais, com a democracia, cuja noção traduz a ideia de soberania popular, de governo da maioria, que somente se consolida, verdadeiramente, ao longo do século XX, com "a consagração do sufrágio universal e o fim das restrições à participação política decorrentes do nível de riqueza, do sexo ou da raça" (BARROSO, 2018, p. 16).

A Constituição figura como a máxima garantia da democracia, mas não se pode negligenciar que o voto livre é o cerne ontológico da representação. Na esfera da própria existência do sistema democrático, nada é mais verosímil com o que preconizam as teorias da representação do que o voto. Não existe sistema democrático representativo válido, sem que seja franqueada a possibilidade de livre escolha daqueles que irão representar a sociedade.

O Estado democrático se presta a "afastar a tendência humana ao autoritarismo e à concentração de poder" (MORAES, 2015, p. 5), pois no autoritarismo, onde a sociedade não tem voz, o poder se afasta do direito e se concentra nas mãos do tirano. Neste caminho, por mais complexo que seja o conceito de democracia, uma definição simples e assertiva afirma que democracia é o "regime em que governantes são escolhidos pelos governados, por intermédio de eleições honestas e livres" (DUVERGER, 1970, p. 387).

O pleito eleitoral possui uma posição de extrema relevância na democracia, sem querer menosprezar a importância da Constituição, que figura como a Norma Fundamental, da qual se irradia toda ordem jurídica. Não seria exagerado afirmar que para o Estado Democrático de Direito, que caracteriza o Estado Constitucional, a escolha dos representantes políticos, tanto para a função legislativa, quanto para a executiva, pela manifestação da vontade da sociedade, de forma livre, periódica, direta ou indiretamente, se traduz na essência do princípio democrático, "que exprime fundamentalmente a exigência da integral participação de todos e de cada uma das pessoas na vida política do país, a fim de garantir o respeito à soberania popular" (MORAES, 2015, p. 6). A ação de turbação do processo eleitoral de 2016 atingiu valores fundamentais caros para a democracia, dois, em especial, como o direito à participação democrática e o direito à

privacidade, que foram atacados contundentemente pela campanha de manipulação empreendida.

Em relação ao direito à participação democrática, cabe ressaltar que o voto livre, como todo direito fundamental, tem sua gênese em um direito da humanidade, desta forma, o Estado, que está diretamente relacionado a uma jurisdição pátria, tem suas obrigações com direitos que se servem para toda a humanidade. Pode-se perceber a relação entre direitos humanos e democracia, quando se compara o artigo[30] 25º, do Pacto Internacional sobre Direitos Civis e Políticos (CCPR), com o artigo[31] 3º, do Primeiro Protocolo Opcional à Convenção Europeia de Direitos Humanos (CEDH). Em ambos os artigos se percebe que existe a necessidade de os representantes serem escolhidos livremente. De acordo com o Conselho de Direitos Humanos da ONU (HRC), isso pressupõe que "a livre expressão da vontade dos eleitores" (UNITED..., 2005, p. 9) precisa ser garantida:

> [...] sem influência ou coerção indevida de qualquer tipo que possa distorcer ou inibir a livre expressão da vontade do eleitor. Os eleitores devem poder formar opiniões de forma independente, livres de violência ou ameaça de violência, compulsão, indução ou interferência manipuladora de qualquer tipo (UNITED..., 2005, p. 19).

O artigo 21° da Declaração Universal dos Direitos Humanos (DUDH) (DECLARAÇÃO..., 1948) diz que toda a pessoa tem o direito de tomar parte na direção dos negócios públicos do seu país, quer diretamente, quer por intermédio de representantes livremente escolhidos. Diz ainda que a vontade do povo é o fundamento da autoridade dos poderes públicos e deve exprimir-se através de eleições honestas a serem realizadas, periodicamente, por sufrágio universal e igual, com voto secreto ou segundo processo equivalente que salvaguarde a liberdade de voto.

É no preâmbulo da Constituição Federal de 1988 que está fundamentada a legitimidade do poder constituinte, pelo qual os representantes do povo brasileiro, eleitos

---

[30]Art. 25º "Todo cidadão terá o direito e a possibilidade, sem qualquer das formas de discriminação mencionadas no artigo 2º e sem restrições infundadas: 1. de participar da condução dos assuntos públicos, diretamente ou por meio de representantes livremente escolhidos; 2. de votar e ser eleito em eleições periódicas, autênticas, realizadas por sufrágio universal e igualitário e por voto secreto, que garantam a manifestação da vontade dos eleitores; 3. de Ter acesso, em condições gerais de igualdade, às funções públicas de seu país" (BRASIL, 1992)

[31] Artigo 3º- **Direito a eleições livres** –" As Altas Partes Contratantes obrigam - se a organizar, com intervalos razoáveis, eleições livres, por escrutínio secreto, em condições que assegurem a livre expressão da opinião do povo na eleição do órgão legislativo" (PROTOCOLO..., 2013)

pelo voto direto, instituíram o Estado Democrático, consagrando, assim, o princípio da participação popular na gestão da coisa pública, assegurando os direitos, garantias e liberdades individuais do povo brasileiro. A participação popular, enquanto princípio constitucional, é o direito de participação política, de compartilhar a administração da coisa pública, opinar sobre as prioridades e fiscalizar a aplicação de recursos públicos.

Desta forma, pela participação da sociedade, se dá a atuação do povo na esfera pública do Estado. Além da forma mais clássica, representada pelo sufrágio universal, a participação pode se caracterizar pelo referendo, consulta popular, ou iniciativa popular, no âmbito da atuação do Poder Legislativo, seja no âmbito do planejamento das políticas públicas e, igualmente, na esfera da atividade fiscalizadora da Administração Pública (SCHIER; MELO, 2017, p. 131).

Não se tem duvidadas de que "a democracia liberal, fundada no Estado de direito, no livre mercado, nas liberdades individuais e no direito de participação política, consagrou-se como o ponto culminante da evolução ideológica da humanidade (BARROSO, 2019, p. 1267). A noção de democracia está intimamente relacionada com a de equalização do poder e representação. Não obstante suas mazelas, a democracia é "o pior de todos os regimes, com exceção de todos os outros que foram experimentados de tempos em tempos"[32]. As democracias são regimes versáteis, pois somente nelas é possível demitir governantes, sem a necessidade de se usar a força. Bem como, por meio delas a sociedade se renova, pelo discursão livre, que leva a mudança de pensamentos. Muito além do simples ato de votar, nas datas eleitorais, a democracia permite, não apenas o acompanhamento do desempenho dos representantes, como também "da eficácia dos Poderes da República, em termos dos bens e serviços públicos que devem ser prestados à população" (MALAN, 2019, p. 15).

A democracia pode ser considerada sob um aspecto formal, que inclui a noção de governo da maioria e de respeito às liberdades públicas, mais relacionada as liberdades de expressão, associação e locomoção. Já em relação ao seu aspecto material, que segundo Barroso (2009), é o "que dá a alma ao Estado constitucional de direito", a democracia[33] representa mais do que o governo da maioria, sendo assim o governo para

[32] Winston S Churchill, 11 de novembro de 1947, ver: https://winstonchurchill.org/resources/quotes/the-worst-form-of-government/

[33] O funcionamento normal de uma democracia está diretamente relacionado à capacidade do Estado de abraçar todas as facções da sociedade. Quando se dá direitos à apenas uma suposta maioria e não se preocupa com as facções contra majoritárias, consequentemente a democracia estará prejudicada. "Deve-se anotar que a democracia liberal não é, por si, garantia de que as instituições políticas serão inclusivas. É

todos: minorias raciais, religiosas, culturais, mulheres, pobres e grupos afins. Neste aspecto material, o Estado promove, além do respeito aos direitos individuais, outros direitos de conteúdo social, que vão levar aos patamares aceitáveis de igualdade material, "sem o qual não existe vida digna e nem é possível o desfrute efetivo da liberdade" (BARROSO, 2009, p.41).

Com a manipulação realizada por meio da operação cibernética maliciosa a vontade majoritária se forma viciada e pode significar um sério problema para a democracia. Desta forma, Steiger (2019) entende que existam sete elementos principais, relacionados ao pleno exercício da democracia, que podem ser diretamente influenciados pelas operações cibernéticas maliciosas: o anonimato, a liberdade do eleitorado formar vontade política, o discurso aberto, a responsabilidade e o controle democrático, o acatamento da decisão majoritária, o pluralismo e a transparência (STEIGER, 2019, p. 9).

No caso em estudo, os elementos que são afetados mais diretamente são o anonimato e a liberdade de formação da vontade política, que uma vez capturados pelo engano das operações cibernéticas maliciosas, levam os demais elementos à derrocada. O anonimato é capturado para ser utilizado como meio de se chegar ao eleitorado, pela segmentação da propaganda, ele é ao mesmo tempo violado pelos russos e pela Cambridge Analítica. A liberdade de formação da vontade política figura como meta principal da campanha de manipulação e uma vez capturada, causa uma catástrofe democrática.

Com este cenário de engano, se chega à conclusão que a revolução digital não trouxe apenas benefícios e melhoria da qualidade de vida das sociedades, com ela veio "também, inconveniências, ameaças e perigos reais para a vida civilizada e a condição humana, que incluem novas táticas de guerra, como os ataques cibernéticos. O direito precisa lidar com desafios que testam os seus limites e suas possibilidades" (BARROSO, 2019, p.1285).

O direito está atrasado em encarar os desafios da era da informação, seguindo-se a dinâmica normal e corriqueira, a velocidade da inovação (para o mal) é extremamente maior do que a velocidade de adaptação da lei. A utilização do ciberespaço com intenções maliciosas é algo que necessita de reposta rápida e assertiva, principalmente quando a ação maliciosa é perpetrada contra a democracia, colocando-a em risco.

---

certo, porém, que eleições regulares, com competição política livre e plural, têm a tendência natural de produzir esse resultado" (BARROSO, 2019, p. 1274).

A liberdade de voto, em hipótese alguma, pode ser interferida, direta ou indiretamente, por indivíduos, Estados ou pessoas jurídicas. Isso serve também para mostrar que os Estados, de maneira geral, devem ter a diligencia de proteger suas próprias eleições contra interferências internas ou externas e, portanto, contra as manipulações do tipo que foram realizadas pela Cambridge Analítica e pelo Projeto Lakhta (STEIGER, 2019, p. 15).

E neste caminho, pode se afirmar que um dos pilares que sustentam a realização de competição eleitoral livre e sem vícios é o anonimato dos eleitores, pois além de garantir o voto livre de pressões, promove e garante a existência de uma sociedade aberta. Em relação as atividades realizadas pela Cambridge Analítica, a busca pela anulação do anonimato foi a forma utilizada para se conhecer o máximo possível dos eleitores e assim direcionar os *Darks Posts*. Já em relação ao *modus operandis* da propaganda dos *trolls* russos, o levantamento das identidades dos alvos não possui grande relevância, entretanto, os próprios trolls precisam permanecer anônimos para serem eficazes: se os eleitores dos EUA soubessem que seus tweets e postagens no Facebook eram da Rússia e não de americanos "comuns", as postagens não teriam a mesma influência que tiveram (STEIGER, 2019, p. 9).

As operações cibernéticas maliciosas, executadas com apoio de ferramentas analíticas de Big Data, quando aplicadas na dinâmica de uma corrida eleitoral, têm como meta desafiar a liberdade dos cidadãos de formar uma vontade política com convicção própria, por meio da manipulação psicológica que leve o eleitor a adotar uma conduta futura previsível. Desta forma, o *fair play* da disputa é diretamente prejudicado, bem como direito à participação democrática. Nas eleições norte-americanas de 2016, tanto a empresa Cambridge Analítica, como os *hackers* que agiram em nome da Rússia, se utilizaram de técnicas diferentes, que realizavam a pré-seleção dos alvos (eleitores), com a finalidade de obter informações privilegiadas para a realização ações pontuais que visavam influenciar o processo de formação de convicção dos eleitores para fraudar o resultado do pleito (STEIGER, 2019, p. 9).

Um dos grandes perigos destas condutas, quando realizadas no contexto de um pleito eleitoral, se traduz na utilização de pautas controversas, que naturalmente causam acirramento dos ânimos e levam a sociedade para uma extrema polarização. O abandono de visões políticas moderadas para se assumir posições de extremos é um fenômeno perigoso, que se espalha pelo planeta, principalmente em decorrência da onda de

populismo que se percebe em algumas democracias. Em relação a isto, Barroso (2019) afirma que "mesmo nas democracias mais maduras, um número expressivo de cidadãos tem abandonado visões políticas moderadas para apoiar minorias radicais, com aumento preocupante da tolerância para com soluções autoritárias" (BARROSO, 2019, p. 1265).

Não será o foco do artigo analisar o sistema eleitoral norte-americano que, apesar da vitória de Hillary Clinton no voto popular (ela obteve 65.844.610 votos contra os 62.979.636 votos de Trump), possibilitou que Donald Trump obtivesse a vitória, com os delegados do Colégio Eleitoral e se tornasse o quadragésimo quinto presidente dos Estados Unidos da América (VELDE, 2018, p. 4). Fruto da ação de manipulação, que visou turbar a liberdade de formação da vontade política, o direito fundamental de participação política dos cidadãos norte-americanos foi violado, no contexto das eleições de 2016.

O outro direito fundamental atingido, no caso em estudo, foi o direito à privacidade, violado por meio do ataque sistemático realizado contra o anonimato. Mesmo diante de todos os benefícios que a era da informação trouxe para o planeta, o direito à privacidade tem se destacado como uma das principais preocupações, não só da sociedade, mas também das autoridades do poder público.

A essência do direito de privacidade está relacionada com a existência, reconhecida pelo direito, de uma esfera na vida de todo indivíduo que deve ser protegida contra a invasão de outros indivíduos, do próprio Estado ou de empresas privadas. O presente momento se caracteriza pelo incremento, no direito à privacidade, de uma dimensão mais complexa, que envolve a tecnologia[34] com o uso do ciberespaço e das plataformas de redes sociais (BARROSO, 2019, p. 1286). O direito de privacidade é direito fundamental, garantido no inciso X, do artigo[35] 5° da Constituição Federal de 1988.

[34] Nesse cenário, há duas situações diversas a considerar: (i) a identificação pessoal do usuário, que inclui informações como nome, endereço, estado civil, ocupação, dados financeiros, declarações ao Fisco etc; e (ii) informações sobre comportamentos, preferências, interesses e preocupações de cada pessoa, obtidas a partir da navegação online. A internet é alimentada, em grande parte, pela exploração desses dados e o controle sobre eles se tornou uma das questões vitais do nosso tempo (BARROSO, 2019, p.1286).

[35] **Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: **X** - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

Várias disposições do Pacto Internacional sobre Direitos Civis e Políticos (ICCPR) podem ter sido violadas com interferência eleitoral ilícita no pleito de 2016 e o direito à privacidade figura como uma delas. O Pacto garante aos indivíduos o direito à privacidade, exigindo que os indivíduos não podem ser "sujeitos a interferência arbitrária ou ilegal em sua privacidade" (BRASIL, 1992). Nessa medida, em relação as operações maliciosas de intrusão, tanto os dados que foram tornados públicos, quanto os que não foram, dão margem para que tais operações sejam consideradas interferência arbitrária na privacidade de um cidadão (VELDE, 2017, p. 24).

Em relação ao direito de privacidade, a era da informação veio revolucionar a sua abrangência, incluindo na esfera da privacidade a titularidade dos dados pessoais que são criados e utilizados no ciberespaço, para diversas finalidades. A utilização do dado pode variar desde um simples registro, para a realização de uma transação comercial, até aqueles relacionados a atividades de entretenimento, como os dados utilizados nas redes sociais.

Muitos ordenamentos nacionais, bem como documentos internacionais, respaldam este direito de proteção de dados pessoais. O direito a proteção de dados é um direito específico, que decorre do direito de privacidade está cada vez mais presente nas legislações dos Estados. A Carta dos Direitos Fundamentais da União Europeia (EUROPEAN..., 2010) prevê um direito explícito à proteção de dados pessoais no artigo[36] 8°. Um outro órgão pioneiro neste tema é o Conselho da Europa, que já em 1981 adotou a Convenção sobre a Proteção de Pessoas no Tratamento Automático de Dados Pessoais (STEIGER, 2019, p. 15).

Com tudo que foi exposto até aqui, se percebe que as operações realizadas com o auxílio de ferramentas analíticas de Big Data possuem o potencial de violação dos dados de privacidades de indivíduos. A coleta, o armazenamento e a análise de grandes bancos de dados por empresas privadas ou órgãos públicos podem interferir gravemente no direito à privacidade. No caso do Facebook, os usuários consentem que seus dados possam ser utilizados pela empresa para fins diversos (STEIGER, 2019, p. 15). Neste sentido, é importante entender que o uso destes dados, com a utilização de ferramentas

[36] Artigo 8.o Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (Carta dos Direitos Fundamentais da União Europeia, tradução nossa).

de análise, gera novos dados, que, em princípio podem estar sendo utilizados sem o consentimento prévio de seus donos. Portanto, a compilação de dados e a segmentação de público alvo, conforme realizado com a classificação de *Ocean Score*, pode significar uma grave violação de dados pessoais e, consequentemente, ofensa ao direito fundamental à privacidade.

Neste sentido, a privacidade não deixou de ser o "direito de ser deixado sozinho" no significado do direito à não intromissão (por exemplo, sigilo de correspondência e de casa), mas também assumiu um significado até então desconhecido de um direito de controle sobre o tratamento de dados pessoais. Talvez o caso mais emblemático das novas formas de tensões, no equilíbrio de direitos fundamentais como privacidade e liberdade de expressão, seja oferecido por plataformas de redes sociais, como como o Facebook, Twitter e Instagram. Existem sérios questionamentos sobre a exposição exagerada dos usuários, sobre a qualidade e o tipo de dados que são armazenados na plataforma, bem como, se a noção de “consentimento informado” se aplica ao ato de “curtir” uma postagem. Para Mindus (2011), existe a premência de se dar atenção à estas questões, uma vez que as ferramentas de análise de Big Data disponíveis já permitem que tais dados sejam tratados com a finalidade de levantar informações estatísticas, não divulgadas abertamente, que permitem o levantamento de comportamentos específicos, principalmente em relação ao consumo (MINDUS, 2011, p. 13). Portanto, não existe nenhum impedimento que tal dinâmica de “mineração de dados” seja utilizada para mapear e manipular comportamentos eleitorais, o que foi provado em 2016.

CONCLUSÃO

As fascinações tecnológicas da era da informação, ao mesmo tempo que incrementaram a qualidade de vida da humanidade, introduziram no panorama da política um tipo de realidade sinistra, representada pelo mau uso da força virtual, capaz de figurar como grave ameaça à democracia. O uso malicioso do ciberespaço provou, com o pleito eleitoral de 2016, nos EUA, que existe premência de se construir uma base normativa sólida, que seja capaz de eliminar as comodidades das zonas cinzentas do direito internacional cibernético e garantir segurança jurídica para a utilização do ciberespaço.

As características do ciberespaço, sua divisão por camadas, bem como a dificuldade de nele se estabelecer o princípio da territorialidade favorecem que atores estatais e não estatais possam construir sinergia no sentido de prejudicar a democracia. Cabe ressaltar que esta ameaça pode estar localizada em solo pátrio ou em solo internacional. O caso de estudo demonstrou que a ação de grupos privados ou Estados, no ciberespaço, tem o potencial de violar direitos e garantias fundamentais. Ao se utilizarem de ações especializadas de Inteligência, bem como de ferramentas poderosas de análise de Big Data e inteligência artificial, para capturar o anonimato do eleitor, com a finalidade de exercer influência na formação da convicção do voto, tais atores violaram o direito à privacidade e a participação política do cidadão norte-americano.

Não obstante o advento do ciberespaço ser recente, se acredita que existe um descompasso entre a velocidade da inovação e a velocidade da normatização. No que tange ao estudo da política, tanto o negacionismo, quanto o ceticismo exagerado, que procuram não reconhecer o impacto do ciberespaço nas relações políticas contribuem para atrasar ainda mais os esforços de normatização. É preciso reconhecer os efeitos transformadores e revolucionários da era da informação.

O voto livre figura como algo sagrado para a democracia representativa. Uma vez violado, toda a democracia se macula. Desta forma, se faz de fundamental importância que as democracias do planeta, incluindo a do Brasil, voltem suas atenções para esta mais nova ameaça da era da informação. O Estado democrático de direito não pode ficar refém de atores antagônicos, estatais ou privados. A ordem jurídica precisa se adaptar e proporcionar os meios de defesa necessários para a democracia. Órgãos de controle e fiscalização devem ser criados com a finalidade de supervisionar a ocorrência de manipulação da sociedade, com a utilização do ciberespaço.

As redes sociais devem criar mecanismos capazes de identificar a ação de *Darks Posts, trolls, bots* maliciosos entre outros. Deve existir normatização para o emprego de ferramentas analíticas de Big Data e inteligência artificial. Isto deve ser exigido por parte do Estado. Depois do ocorrido no pleito eleitoral de 2016, nos EUA, se nada for feito, a democracia estará sempre à mercê de aventureiros cibernéticos, utilizados por oportunistas políticos.

REFERÊNCIAS

ACEVES, W. Virtual Hatred: How Russia Tried to Start a Race War in the United States. **Michigan Journal of Race & Law**, v. 24, n. 1, 2019. Disponível em: https://ssrn.com/abstract=3304223. Acesso em: 22 jul. 2020.

ALOUANE, R-S. The E-Citizen and the State: Towards a Democracy in 140 Characters? An Attempt to Elaborate a Method of Regulation of the Cyber-Democratic Space. *In*: WORLD CONGRESS OF CONSTITUTIONAL LAW, 2014, **Anais [...]**, Faculty of Law of Oslo (Norway), June 2014, Disponível: https://ssrn.com/abstract=2547862. Acesso em: 18 set. 2020.

BARROSO, L. R. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009.

BARROSO, L. R. O Constitucionalismo Democrático ou Neoconstitucionalismo como ideologia vitoriosa do século XX. **Revista Publicum Rio de Janeiro**, v. 4, ed. Comemorativa, 2018, p. 14-36. Disponível em: http://www.e-publicacoes.uerj.br/index.php/publicum. Acesso em: 19 jan. 2021.

BARROSO, L. R. Revolução tecnológica, crise da democracia e mudança climática: limites do direito num mundo em transformação. **Revista Estudos Institucionais**, [S.l.], v. 5, n. 3, p. 1234-1313, dez. 2019. Disponível em: https://estudosinstitucionais.com/REI/article/view/429. Acesso em: 19 jan. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Emendas Constitucionais. Brasília, DF: Presidência da República: 4. ed., São Paulo: Saraiva, 1990.

BRASIL. Decreto nº 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Brasília – DF: Presidência da República, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em 22 set 2020.

BUND, J. Cybersecurity and democracy Hacking, leaking and voting. **European Union Institute for Security Studies**, nov. 2016, Disponível em: https://www.iss.europa.eu/content/cybersecurity-and-democracy-hacking-leaking-and-voting. Acesso em: 10 set. 2020.

COUTINHO, M. O que são 'trolls' e o que é 'trollagem'? TechTudo, 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/06/o-que-sao-trolls-e-o-que-e-trollagem.html. Acesso em 17 agosto 2020.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Assembleia Geral das Nações Unidas em Paris. 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Introduction.aspx. Acesso em: 26 ago. 2020.

DUVERGER, M. **Os partidos políticos**. Rio de Janeiro: Zahar, 1970.

EUROPEAN UNION. Charter of Fundamental Rights of the European Union. **Official Journal of the European Union C83**. Vol. 53. Brussels: European Union. 2010.

FOLKENFLIK, D. An Obama-Backed Change at Voice of America has Trump Critics Worried. National Public Radio, 2016. Disponível em: http://www.npr.org/sections/thetwo-way/2016/12/14/505482691/an-obama-backedchange-at-voice-of-america-has-trump-critics-worried. Acesso em: 10 jul. 2021.

GILSINAN, K. CALAMUR, K. Did Putin Direct Russian Hacking? And Other Big Questions. The Atlantic, 2017. Disponível em: https://www.theatlantic.com/international/archive/2017/01/russian-hackingtrump/510689/. Acesso em 27 set. 2020.

HINDMAN, M. **The Myth of Digital Democracy**. Princeton Univ. Press, Princeton 2009.

HOFFMANN-RIEM, W. Inteligência Artificial como oportunidade para a regulação jurídica. **Direito Público**, [S.l.], v. 16, n. 90, dez. 2019. Disponível em: 4https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3756. Acesso em: 13 ago. 2020.

HOLLIS, D. The Influence of War; The War for Influence, Temple Journal of International & Comparative Law, v. 32, p 36 -39, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155273. Acesso em: 13 ago. 2020.

HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE. Report on Russia's active measures. 116. CONGRESS, 2018. Disponível em: https://intelligence.house.gov/uploadedfiles/final_ russia_investigation_report.pdf. Acesso em 27 set. 2020.

HURST, J. O Devido Cuidado com a Robotização do Campo de Batalha. **Military Review** - ed. brasileira, Quarto Trimestre, 2018. Disponível em: https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Quarto-Trimestre-2018/O-Devido-Cuidado-com-a-Robotizacao-do-Campo-de-Batalha/. Acesso em: 6 set. de 2020.

INTELLIGENCE COMMUNITY ASSESSMENT. Assessing russian activities and intentions in recent US elections. 2017. Disponível em: https://www.intelligence.senate.gov/sites/default/files/documents/ ICA_2017_01.pdf. Acesso em: 13 ago. 2020.

JURECIC, Q. Where in the World is Elena Khusyaynova? Lawfare – Federal Law Enforcement, 2018. Disponível em: https://www.lawfareblog.com/where-world-elena-khusyaynova. Acesso em: 16 jul 2020.

KELSEN, H. **Teoria pura do direito**. Tradução: João Baptista Machado. 6. ed. São Paulo: Martins Fontes, 1998.

MALAN, P. Uma perspectiva geral. *In*: BACHA, E.; FALCÃO J.; CARVALHO, J. M. *et al*. **130 Anos: em busca da república**. Rio de Janeiro: Intrínseca. 2019.

MINDUS, P. Updating Democracy Studies: Outline of a Research Program. Law, Technology and Society - Proceedings XXV WORLD CONGRESS OF IVR SPECIAL WORKSHOP ON "LEGITIMACY 2.0: E-DEMOCRACY AND PUBLIC OPINION IN THE DIGITAL AGE", 25., 2011, Frankfurt. **Anais Eletrônicos** [...], Goethe University, Frankfurt am Main, Paper series B, Ulfrid Neumann, ed., 2011. Disponível em: http://dx.doi.org/10.2139/ssrn.1970966. Acesso em: 1 ago. 2020.

MORAES, A. Direito Constitucional. 3 ed. São Paulo: Atlas, 2015.

NATE PERSILY, J. B. Can Democracy Survive the Internet? **Journal of Democracia**, v. 28, n. 2, p. 60-76, 2017.

PROTOCOLO ADICIONAL À CONVENÇÃO EUROPEIA DE PROTEÇÃO DOS DIREITOS DO HOMEM E DAS LIBERDADES FUNDAMENTAIS. Convenção Europeia dos direitos dos homens. Estrasburgo, 2013. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em 23 set. 2020.

ROGERS, K. Beyonce Faces Police Boycott of Her Concert in Miami. **New York. TIMES**, 2016. Disponível em: https://www.nytimes.com/2016/02/20/arts/music/beyonce-concertboycotted-by-police-group-over-halftime-show.html. Acesso em 05 set. 2020.

ROMM, T. “Pro-Beyoncé” vs. “Anti-Beyoncé:” 3,500 Facebook Ads Show the Scale of Russian Manipulation. The Guardian, 2018. Disponível em: https://www.theguardian.com/us-news/2018/may/10/russia-facebook-ads-us-elections-congress. Acesso em: 20 set. 2020.

ROSENBERG, M.; CONFESSORE, N. CADWALLADR, C. How Trump Consultants Exploited the Facebook Data of Millions. **New York Times**, 2018. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 17 ago. 2020.

SALDAN, E. **Os desafios jurídicos da guerra no espaço cibernético**. 2012. Dissertação (Mestrado em Direito Constitucional) - Instituto Brasiliense de Direito Público, Brasília, 2012.

SCHIER, A. C. R.; MELO, J. A. M. H. O direito à participação popular como expressão do Estado Social e Democrático de Direito. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 17, n. 69, p. 127-147, 2017.

SCHMITT, M. N. 'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. **Journal of International Law**, Chicago, v. 19, p. 30-67, 2018. Disponível em: https://ssrn.com/abstract=3180631. Acesso em: 5 set. 2020.

SHERMAN, A. Hillary Clinton Claims Donald Trump Invited Russian President Vladimir Putin to Hack Americans. Politifact, 2016. Disponível em:

http://www.politifact.com/truth-o-meter/statements/2016/sep/26/hillaryclinton/hillary-clinton-claims-donald-trump-invited-russia/. Acesso em: 3 set. 2020.

SIMONCINI, A. The Constitutional Dimension of the Internet: Some Research Paths. **EUI Department of Law Research Paper**. n. 2016/16, 2016. Disponível em: https://ssrn.com/abstract=2781496 or http://dx.doi.org/10.2139/ssrn.2781496. Acesso em: 23 ago. 2020.

STEIGER, D. International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process (2019). *In*: WITZLEB, Normann; RICHARDSON, Janice; PETERSON, Moira (eds.). **Big Data, Political Campaigning and the Law**: Privacy and Democracy in the Age of Micro-Targeting. Routledge: Forthcoming, 2019. Disponível em: https://ssrn.com/abstract=3430035. Acesso em 20 ago. 2020.

SUNSTEIN, C. Going to Extremes: How Like Minds Unite and Divide. ed. 3. USA: Oxford University Press, 2009.

THERESA MAY ACCUSES Vladimir Putin of Election Meddling. **BBC News**, 2017. Disponível em: https://perma.cc/HJ5P-5NAF. Acesso em: 17 ago. 2020.

UNITED NATIONS HUMAN RIGHTS COUNCIL. 'General Comment No 25' (n 69) para 9. US Department of Defense, The Strategy for Homeland Defense and Civil Support, 2005.

VELDE, V. Jacqueline. The Law of Cyber Interference in Elections. Paper SSRN, 2017. Disponível em https://ssrn.com/abstract=3043828. Acesso em: 20 set. 2020.

WEEDON, J.; NULAND, W.; STAMOS, A. **Facebook, Information Operations and Facebook**. 2017. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fi2.res.24o.it%2Fpdf2010%2FEditrice%2FILSOLE24ORE%2FILSOLE24ORE%2FOnline%2F_Oggetti_Embedded%2FDocumenti%2F2017%2F04%2F28%2Ffacebook-and-information-operations-v1.pdf&clen=845976&chunk=true. Acesso em: 18 jan. 2022

WEINER, N. Cybernetics or Control and Communication in the Animal and the Machine. **MIT PRESS**, Cambridge, 1948.

WHITTON, J. B. Aggressive Propaganda. I International Criminal law. BASSIOUNI, M. C.; NANDA, V. P. (eds.). 1974.

Recebido em: 05/07/2022

Aprovado em: 08/08/2022

Publicado em: 12/08/2022