1 Introdução

Pretenda-se neste artigo explorar com apropriado grau de profundidade, a relação que têm a comunicação, com a labor que realizam as equipes dos políticos em campanha, e o exercício do sufrágio, principalmente, desde um olhar comunicacional. Para isto, serão utilizadas as teorias de Manuel Castells. Segundo o autor (191-192, tradução minha), o conceito de "significação" tem um importante lugar na teoria política, tal como o indica em sua obra *"Comunicación y poder":*

> A comunicação se produz através da ativação das mentes para compartilhar significado. A mente é um processo de criação e manipulação de imagens mentais (visuais ou não) no cérebro. As ideias podem ser vistas como configurações de imagens mentais. Em toda a probabilidade imagens mentais correspondem a padrões neurais. Padrões neurais são configurações da atividade nas redes neurais. As redes neurais conectam neurônios que são células nervosas. Os padrões neurais e as imagens correspondentes ajudam o cérebro a regular a sua interação com o próprio corpo e seus arredores. Padrões neurais formam-se para a evolução da espécie, e o conteúdo do cérebro no nascimento e experiências do sujeito.

De acordo com este fragmento, o sociólogo Manuel Castells se apoia numa variada gama de argumentos para demostrar, que efetivamente a comunicação têm uma profunda relação com a função de significação das pessoas, isto é, com o papel que ostenta o indivíduo de conceber-se e compreender assim seu entorno. Neste contexto, a teoria de Castells serve como base para refletir sobre alguns aspectos, os quais encontram-se razoavelmente ligados às ações comunicativas realizadas pelo ser humano, como a política e o poder. Frente a isto Castells (2009, p.292, tradução minha) menciona:

> Isso não significa que os meios de comunicação ostentem o poder. Eles não são o quarto poder. Eles são muito mais importantes: são o espaço onde o poder é criado. A mídia é o espaço onde as relações de poder entre atores políticos e sociais rivais são decididas. Portanto, para atingir seus objetivos, quase todos os atores e as mensagens devem passar através da mídia. Eles têm que aceitar as regras do jogo midiático, a linguagem da mídia e dos seus interesses. Os meios de comunicação como um todo não são neutros, como o proclama a ideologia do jornalismo profissional; nem são instrumentos diretos do poder do Estado, com a exceção óbvia dos meios de comunicação em regimes autoritários. Os atores dos meios criam plataformas de comunicação e produzem mensagens em linha com os seus interesses

> profissionais e de negócios específicos. Dada a diversidade de atores nos meios de comunicação, esses interesses também são diversos.

Os meios de comunicação são então para o autor muito mais importantes que o poder, pois "são o espaço onde o poder é criado". Sob o entendimento dessas circunstâncias, é preciso começar a questionar-se pelo lugar onde verdadeiramente residem a soberania e o poder. Então diante disso, é verdadeiramente sobre o povo ou sobre os meios de comunicação que reside o poder? Para Castells a pergunta já está resolvida, porque segundo ele a soberania pode ser usurpada pelo poder mediático. Neste sentido, Castells (2009, p.87-88, tradução minha) indica que é necessário compreender como funcionam as comunicações, pois detalha que:

> Começando com *o âmbito do próprio processo,* deve distinguir-se entre a comunicação interpessoal e comunicação social. No primeiro caso, os emissores e receptores são designados são os sujeitos da comunicação. Na segunda, o conteúdo da comunicação pode ser difundido em toda a sociedade: é o que nós geralmente chamamos *comunicação de massa.* A comunicação interpessoal é interativa (a mensagem é enviada de um para outro com loops de feedback), enquanto a comunicação de massas pode ser interativa ou unidirecional. A comunicação de massas tradicional é unidirecional (a mensagem é enviada de um para muitos, livros, jornais, filmes, rádio e televisão)

Assim Castells explica como a "mensagem [dos meios de comunicação de massas] é enviada de um para muitos", isto redistribui de maneira desproporcionada e desigual os efeitos sociais da comunicação, e faz com que o processo de significação seja redistribuído de forma desigual. Desta forma é que são criados os laços de poder de modo imperceptível. Isto parece estar bem definido para Castells, pois para ele os meios de comunicação de massas, são uma forma de controlar aos outros, ainda que, em forma indireta. Embora, com isso claro, é necessário estabelecer se os outros meios de comunicação trabalham na mesma linha, por exemplo, acontece de igual forma com a Internet? Também é um meio de controle? A soberania também é usurpada pela Internet? Com relação à formação de poder da Internet Castells (2009, p.535, tradução minha) assinala:

> O poder está essencialmente confinado construindo significado na mente humana, usando os processos de comunicação que acontecem nas redes multimídia global-local de comunicação de massas, incluindo a autocomunicação de massas. Embora as teorias sobre o poder e a observação histórica apontam à importância crítica do monopólio da violência por parte do estado como fonte de poder social,

> argumentando que a capacidade de empregar com sucesso violência ou intimidação, exige o emoldurado individual e coletivo das mentes.

Sendo assim, o poder mais que na força, reside na mente, na psicologia e, no poder de emoldurar as mentes. Isto faz que os meios de comunicação de massas tradicionais e a Internet possam usurpar o poder politico que deve recair no povo. Mas então, como intervierem realmente os atores, por exemplo, nos processos de criação de poder politico através de um meio de comunicação como a Internet? Esta situação em palavras do próprio Castells (2009, p.538-539, tradução minha) foi resolvida da seguinte forma:

> [...] Por si sós, as redes multimídia como estruturas de comunicação não têm poder de ligar a rede, poder em rede ou poder para criar redes, mas dependem das decisões e instruções de seus programadores. Na minha estrutura conceitual (Capítulo 1), o poder da ligação em rede (networking power) é a capacidade de deixar que um meio ou uma mensagem entrar na rede, filtrando os procedimentos de acesso (gatekeeping). [...] No entanto, a rede de comunicação de gerenciamento de rede opera de acordo com os termos de um metaprograma que projetou alguém fora da rede. Este "alguém" intrigante é o assunto da forma mais decisiva do poder: o poder de criar redes.

A criação e o gerenciamento das redes dependem deste modo de duas figuras fundamentais: os *metaprogramadores* e os *gatekeepers*. Os primeiros, os *metaprogramadores* políticos, são agentes externos da rede que estampam seus interesses e valores. Em uma comunidade política têm-se tantos *metaprogramas* como propostas políticas, sendo que ganha finalmente a proposta política mais forte, detrás da política existe uma verdadeira guerra comunicacional. Os *gatekeepers* são muito importantes também, por ser pessoas com muito poder dentro da rede política, pois geralmente são pessoas com bastos conhecimentos técnicos que lhes permitem gerenciar eficientemente a rede em favor dos interesses dos *metaprogramadores*.

Diante do exposto, para plantear uma problemática específica, pode-se dizer que os *hackers* são um exemplo da manipulação mediática na rede. Os *hackers* são pessoas com grandes habilidades e conhecimentos técnicos para manipular os sistemas cibernéticos, para obter e administrar informações privilegiadas e manejá-las segundo sua vontade. Em outras palavras, os *hackers* são verdadeiros *gatekeepers* da Internet, perfeitos para administrar os *metaprogramas* dos candidatos políticos.

Um caso prático que pode esclarecer o problema planteado, pode ser o caso do "*hacker* político" Andrés Sepúlveda. Este interferiu mediante diferentes técnicas de *hacking* nas eleições políticas de sete países da América latina, como são Panamá, Honduras, El Salvador, Colômbia, México, Costa Rica, Guatemala e Venezuela (BLOMBERG, 2016, par.6).

Entre as atividades desenvolvidas pelo hacker, estão, por uma parte, os atos de violação da segurança cibernética, como os roubos dos planos de campanha, controle remoto de dispositivos eletrônicos alheios, monitoramento das estratégias financeiras dos partidos políticos, o monitoramento de conversas privadas e o uso indevido de informações confidenciais (BLOMBERG, 2016, par.6-51).

Por outro lado, estão os mecanismos de manipulação psicológica, os ataques contra a sociedade civil, especialmente contra a opinião pública, palpável em questões como a manipulação massiva de perfis falsos em redes sociais, atentados de difamação e de degradação de figuras públicas, a suplantação de identidades, geração de propaganda negra, rumores e notícias falsas ou *fake news* (BLOMBERG, 2016, par.6-51).

Contudo, o *hacker* Sepúlveda foi acusado e sentenciado a 10 anos de prisão em 09 de abril de 2015, pelo Juizado 22 de Conhecimento do Circuito Especializado de Bogotá, Colômbia, pelos delitos de espionagem, *concierto para delinquir*, *acceso abusivo a sistema informático*, *violación agravada de datos personales y utilización de software malicioso*[1] contra os membros negociadores do processo de paz na Colômbia e o ex-vice-presidente da Colômbia, Francisco Santos (FISCALIA GENERAL DE LA NACIÓN DE COLOMBIA, 2015, pr.1-3).

A intenção então desta pesquisa é fazer evidente uma problemática social latente, mas velada: a Internet como meio de massas também é uma fonte de perda de soberania e legitimidade dos estados democráticos, isto, leva ainda mais a representatividade a sua crise. Assim sendo, é necessário que estes acontecimentos sejam especialmente analisados e estudados, por isso, sob o *status quo* formulado propõe-se o seguinte questionamento de pesquisa: Como é que os *hackers*[2] interferem nos resultados das eleições políticas, e quais são as consequências jurídico-políticas de essa influência? Deste modo, o objetivo principal da

[1] Segundo o direito penal colombiano

[2] *Hackers* compreendidos como aqueles especialistas em programação de redes informáticas

presente pesquisa, é ajudar a determinar no âmbito jurídico como se formam os laços de poder na Internet por meio do *hacking* e contribuir nessa medida para a defesa da democracia.

Para resolver a problemática formulada é proposta a seguinte hipótese: Detrás da Internet, em forma oculta, existe um forte poder que reside nas pessoas que têm o conhecimento técnico necessário para manipular a rede, os *hackers* ou *gatekeepers* da rede. Estas pessoas de forma intencional discriminam a informação que passa pela rede em favor ou prejuízo de um ator politico determinado, realizando ataques cibernéticos ou alterando a opinião publica[3] . Em virtude dos interesses politico de um candidato ou movimento politico (o *metaprogramador*). Isto leva à democracia a uma crise de representação, e implica que os *hackers* sejam judicializados não somente por seus crimes econômicos e técnicos, mas também, por seus crimes políticos.

Para comprovar esta hipótese a pesquisa se desenvolverá em seis momentos principais: no primeiro momento, será apresentado o tema introdutório, a sociedade em rede e a segurança cibernética; no segundo momento, se explicará o papel do *hacking*, a cultura *hacking* e em forma geral as principais técnicas de *hacking* que existem, num terceiro momento, se aprofundará sobre uma das técnicas de *hacking* mais importantes nesta pesquisa, a engenharia social e seu relação com os ataques psicológicos; num quarto momento, se falará de psicologia de massas, inconsciente coletivo e determinismo comunicacional; no quinto momento, se expor a relação que têm o direito com o hacking politico; finalmente, no sexto momento, será falado sobre os efeitos do *hacking* politico na crise da representatividade.

Com o objetivo de cumprir tais fins, a abordagem metodológica que será utilizada nesta pesquisa para resolver a pregunta principal será qualitativa, pois, através desta, pretende-se entender os sinais e signos expostos na realidade, assim como também entender sua causa, sua origem, desenvolvimento e possíveis consequências. Além disso, trabalha-se dentro de uma pesquisa teórica, explicativa e analítica, em virtude de que, por médio dela, poderão se identificar em grande medida os fatores que determinam a realidade do fenômeno comunicacional que está sendo estudado, logrando finalmente uma compreensão e uma resolução integral do problema.

[3] Alterando não somente a opinião publica sino também os processos de significação das pessoas, e com isso a percepção dos sujeitos mesmos.

2 Desenvolvimento

Inicia-se a análise da presente pesquisa a partir da abordagem técnica. Portanto, desenvolvem-se reflexões sobre categorias como: sociedade em rede, segurança cibernética, engenharia social, determinismo comunicacional, psicologia de massas e ataques psicológicos.

2.1 A sociedade em rede e o conceito de segurança cibernética

Em primer lugar é preciso compreender que a Internet foi um dos descobrimentos mais importantes e revolucionários da história da humanidade, pois interligou a milhões de pessoas em todo o mundo, isto produziu uma importante transformação econômica, politica e cultural em diferentes dimensões[4], no entanto, essa interligação também produziu um conjunto de riscos desconhecidos até então pela humanidade, pois nunca se experimentou esse nível de exibição. Agora, com uma alta exposição da Internet o verdadeiro valor está no intercambio de informação, mas então, como respondeu a sociedade em rede aos novos riscos digitais?

É assim como para proteger ao individuo na era digital, no processo de construção social, nasce o conceito de segurança cibernética. Para definir apropriadamente o conceito de cibersegurança pode ser citado a Equipe de Resposta a Emergências de Computação do Departamento da Defesa e Segurança Nacional de Estados Unidos (CERT-US, s.d., p.3) quem define a segurança cibernética como:

> Toda a gama de políticas e atividades de redução de ameaças, redução de vulnerabilidade, dissuasão, engajamento internacional, resposta a incidentes, resiliência e recuperação, incluindo operações de rede de computadores, garantia de informações, aplicação da lei, diplomacia, militares e inteligência relacionadas à segurança E estabilidade da infraestrutura global de informação e comunicações.

Deste modo, pode entender-se, que a cibersegurança procura o design de métodos, técnicas e procedimentos destinados para fazer um sistema de informação seguro e confiável, o que leva a assumir três elementos necessários no conceito de segurança informática: o

[4] Castells (2009, p.166) identificou quatro principais trocas culturais: a globalização cultural, o individualismo cultural, o individualismo e comunalismo.

primeiro, a proteção dos diferentes elementos que comporem o sistema da informação, o segundo, a procura de possíveis perigos, e o terceiro, a adoção de medidas para conhecer, prevenir, impedir, detectar, reduzir o controlar os riscos potencias (AGUILERA, 2015, p.8). Embora, ainda o conceito de segurança está incompleto, pois a segurança só têm sentido à luz de uma ameaça, mas então, é necessário compreender quais são essas ameaças.

2.2 *Hacking*

2.2.1 Conceito de *hacker* e cultura *hacking*

O termo *hacker* é um termo discutível e difuso, pois não há uma autoridade, instituição ou fonte formal que seja responsável de determinar exatamente o conceito, não obstante, é possível entender que a palavra não responde só a um sujeito, senão a um contexto ou para ser mais específicos a um movimento cultural (WIKIPEDIA, s.d., par. 1).

Por outro lado, existem diferentes tipos de *hackers* dependendo da forma em que utilizem seus conhecimentos, seja para o beneficio ou prejuízo dos outros. Os *hackers* que utilizam seus conhecimentos positivamente, por exemplo, para encontrar e solucionar problemas e vulnerabilidades de algum sistema são denominados "*whitehackers", "whitehats"* ou "*hackers* éticos". Ao contrário, os *hackers* negativos, os que utilizam seus conhecimentos (de forma professional ou *amateur*) para danificar aos outros ou para obter benefícios financeiros são chamados *"blackhackers", "blackhats"* ou *"crackers*. Finalmente, encontram-se os *hackers* que são uma mistura dos anteriores, pois trabalham indistintamente para organizações legais e criminais (INTEC, s.d., par.16-20).

Com tudo, é necessário para compreender o verdadeiro papel que desempenham os *hackers* na política e analisar as diferentes técnicas com que a rede é manipulada.

2.2.2. Principais técnicas de *hacking*

Entender as diferentes técnicas de *hacking* é fundamental para poder compreender qual é o papel que tem o *hacking* na politica, para isso, serão expostas superficialmente as principais técnicas de *hacking*. A saber, no *hacking* há seis principais técnicas e são: o *spoofing*, o *sniffing*, os MITM, os *malware*, os *Dos* e a engenharia social. As diferentes técnicas serão explicadas a continuação.

O *Spoofing* para Babu, Bhaskari e Satyanarayana (2010, p.1) é uma prática que pode assumir diferentes formas no mundo digital, o *spoofing* como sua própria tradução sugere, trata-se de uma falsificação, que, de tal forma, envolve algum tipo de falsa representação de informações pela vítima. Segundo Babu[5] há uma variedade de métodos e tipos de *spoofing* entre os que podem indicar-se o *spoofing* IP, a ARP *spoofing*, *o spoofing* de e-mail, a web *spoofing* e o *spoofing* de DNS (BABU, BHASKARI e SATYANARAYANA et al, 2010, p.1).

O *sniffing* é uma técnica que permite capturar o tráfico que passa por uma rede. Spangler (2003, p.1, tradução minha) descreveu esta técnica assim:

> O sniffing de pacotes é uma técnica de monitoramento de todos os pacotes que atravessam a rede. Um sniffer de pacote é uma peça de software ou hardware que monitora todo o tráfego de rede. Isso é diferente dos hosts de rede padrão que recebem apenas o tráfego enviado especificamente para eles. A ameaça de segurança apresentada por sniffers é sua capacidade de capturar todo o tráfego de entrada e saída, incluindo senhas de texto claro e nomes de usuário ou outro material sensível. Em teoria, é impossível detectar as ferramentas de sniffing porque são de natureza passiva, significando que coletam somente dados. Embora, alguns deles não são totalmente passivos e possam ser detectados.

A intenção do atacante com os MITM é ganhar acesso á informação de forma passiva, isto é, sem que a vítima tenha sequer conhecimento da intromissão, a essência do assalto é interceptar a comunicação (OPPLIGER et al, 2005, p.2-3). O ataque começa quando o *hacker* leva a aceitar um certificado gerado de forma ilegítima a sua vítima, então, o agressor coloca-se no meio da rota de rede entre o computador da vitima e o servidor, no momento quando a vítima envia uma solicitação para estabelecer uma nova conexão com o servidor, a assaltante intercepta e responde sua solicitação com um certificado falso. Se a vitima aceita esse certificado, então completa a configuração maliciosa (DACOSTA, AHAMAD e TRAYNOR, p.4).

Aqui o *hacker* tem duas conexões simultâneas, uma com a vítima e outra com o servidor. Agora, o *hacker* pode decifrar, voltar a cifrar e reenviar todas as mensagens que sejam trocadas entre a vitima e o servidor. Desta forma, como resultado deste procedimento, o atacante tem acesso a toda a informação privada do adversário inclusive tem até capacidade de fazer qualquer alteração (DACOSTA, AHAMAD, TRAYNOR, s.d., p.4-5).

[5] Id.

Pode falar-se de modo geral que os *malware* são componentes de software colocado em um sistema para provocar danos (BAILEY et al, 2007, p.179). A *Organization for Ecnonomic Co-operation and Developed* OECD (2007, p.10, tradução minha) resume o conceito de malware da seguinte forma:

> Malware é um termo geral para um software inserido num sistema de informação para causar dano a esse sistema ou outros sistemas, ou subvertê-los para uso diferente do pretendido por seus proprietários.
>
> O malware pode obter acesso remoto a um sistema de informação, gravar e enviar dados desse sistema para um terceiro sem a permissão ou conhecimento do usuário, ocultar que o sistema de informação foi comprometido, desativar medidas de segurança, danificar o sistema de informação ou de outra forma afetar os dados e a integridade do sistema.
>
> Diferentes tipos de malware são comumente descritos como vírus, worms, cavalos de tróia, backdoors, keystrokeloggers, rootkits ou spyware. Estes termos correspondem à funcionalidade e ao comportamento do malware (por exemplo, um vírus se auto-propaga, um worm se autorreplica). Especialistas costumam agrupar o malware em duas categorias: família e variante. "Família" refere-se ao pedaço distinto ou original de malware; "Variante" refere-se a uma versão diferente do código malicioso original, ou família, com pequenas alterações.

Por sua parte, o principal objetivo que tem uma ofensiva *Dos* ou *DDos* é a interrupção da transmissão da informação (MIKOVIC e REIHER, 2004, p.1). Taghavi (et al, 2013, p.1, tradução minha) estabeleceu de forma concisa como é o procedimento técnico para um ataque *DDos*, destacando:

> Hoje, os ataques DDoS são frequentemente lançados por uma rede de computadores Zombies ou Botnet controlados remotamente, bem organizados e amplamente dispersos que enviam simultaneamente e continuamente uma grande quantidade de solicitações de tráfego e / ou serviço para o sistema de destino. O sistema alvo responde tão lentamente que é inutilizável ou falha completamente. Zumbis ou computadores que fazem parte de uma Botnet são geralmente recrutados através do uso de worms, cavalos de Tróia ou backdoors. Empregar os recursos de computadores recrutados para executar ataques DDoS permite que os atacantes lancem um ataque muito maior e mais perturbador. Além disso, torna-se mais complicado para os mecanismos de defesa reconhecerem o atacante original devido ao uso de endereços IP falsificados (isto é, falsificados) por zumbis sob o controle do atacante.

Finalmente, a engenharia social é uma técnica que é utilizada pelos *hackers* para atacar o ponto mais fraco do sistema informático, o ser humano, principalmente através de ataques

psicológicos. É por isso, que esta técnica está profundamente integrada com a política e merece um especial desenvolvimento.

2.2.3 A engenharia social e os ataques psicológicos

A engenharia social necessariamente não tem uma conotação negativa ou maliciosa, há engenheiros sociais que utilizam positivamente seus conhecimentos para encontrar falhos, com o objetivo de corrigi-los, por exemplo, como o sistema educativo de uma comunidade (PAPAZOV, s.d., p.2). A engenharia social não é uma má prática *per se*, os resultados que sejam obtidos com ela dependeram das pessoas e não da própria ferramenta. Assim sendo, PAPAZOV (s.d., p.3, tradução minha) estabeleceu de forma amplia que:

> A engenharia social é um conjunto de fenômenos principalmente psicológicos, aplicados predominantemente no contexto da computação e da segurança das informações. Desta forma, contrasta com a natureza principalmente técnica do domínio, que muitas vezes foi incompreendida ou negligenciada por especialistas técnicos. [...] A engenharia social é "sempre psicológica e, às vezes, técnica", "o aspecto psicológico da engenharia social é o que faz o ataque, não o técnico". De fato, um dos desafios de lidar com a engenharia social é precisamente a origem não técnica da ameaça, inibindo soluções puramente técnicas. No entanto, [...] existem algumas abordagens técnicas para as defesas de engenharia social.

Quando trata-se de engenharia social, fala-se de ferramentas de manipulação psíquica no nível individual ou social. Acerca dos principais âmbitos de aplicação da engenharia social Papazov (s.d., p.2) assinala dois usos: o primeiro para ataques de segurança informática e o segundo na ciência política[6]. O primeiro, enfocado geralmente à manipulação através de ferramentas técnicas e dispositivos e, o segundo, focado principalmente à manipulação do inconsciente coletivo por meio de dispositivos eletrônicos ou tradicionais (). Com relação à engenharia social, Kevin Mitnick[7] e William Simon (2002, p.12, tradução minha) argumentaram acerca da ilusão dos sistemas informáticos dizendo que:

> A segurança é muitas vezes apenas uma ilusão, uma ilusão que piorada quando a incredulidade, ingenuidade ou ignorância entra em jogo. O cientista mais respeitado

[6] Estes dois âmbitos não são excludente pois podem complementar-se
[7] Kevin Mitnick é considerado o pai da engenharia social

> do século XXI, Albert Einstein, é citado dizendo: "Somente duas coisas são infinitas, o universo e a estupidez humana, e não tenho certeza sobre o primeiro". No final, os ataques de engenharia social podem ter sucesso quando as pessoas são estúpidas ou, mais comumente, simplesmente ignorantes sobre as boas práticas de segurança. Com a mesma atitude do um proprietário de casa consciente da segurança, muitos profissionais de tecnologia da informação (TI) apegam-se à ideia de que eles fizeram suas empresas amplamente imunes a ataques porque implantaram produtos de segurança standard - firewalls, sistemas de detecção de intrusões ou dispositivos de autenticação, como fichas baseadas no tempo ou cartões inteligentes biométricos. Qualquer pessoa que pense que os produtos de segurança oferecem uma segurança verdadeira está estabelecendo a ilusão de segurança. É um caso de viver em um mundo de fantasia: inevitavelmente, mais tarde, se não antes, sofrer um incidente de segurança.

Desta forma, Mitnick encontrou que hackear a mente das pessoas, é similar a *hackear* os sistemas informático e inclusive mais fácil ainda. Deste modo, para Mitnick (2002 p.12, tradução minha), "o fator humano é verdadeiramente o elo mais fraco na segurança", depois acrescenta que, "os seres humanos –tu, eu e todos os outros- continuam sendo a ameaça mais severa para a segurança de cada um" (Mitnick, 2002, p.17, tradução minha). Assim sendo, em sínteses pode dizer-se que a engenheira social pode-se basearem estratégias como a manipulação, fraude, armadilhas e nas mentiras provenho-as e eticamente reprocha-lhes.

Assim, destaca-se que uma das principais formas técnicas de lograr a manipulação psicológica, e através das denominadas Operações Psicológicas ou PSYOS, como são conhecidas por sua contração em inglês. Segundo Bates e Mooney (2014, p.1) as PSYOS têm uma amplia aplicação em campos particulares e públicos, especialmente militares, pois anotam:

> As operações psicológicas estão planejadas para transmitir informações e indicadores selecionados ao público para influenciar emoções, motivos, raciocínio objetivo e, finalmente, o comportamento de organizações, grupos e indivíduos (Rouse, 2012). As operações psicológicas envolveram uma variedade de táticas e tecnologias para influenciar os públicos-alvo (FM 33-1-1, 2003).
>
> Uma campanha de guerra psicológica é uma guerra da mente. O PSYOP pode ser divulgado por meio de comunicação cara a cara, meios audiovisuais (televisão), mídia de áudio (rádio ou alto-falante), mídia visual ou o domínio digital. A arma não é o sistema de entrega, mas a mensagem que ela carrega e como essa mensagem afeta um público-alvo é a arma (Rouse, 2012).

Deste modo, há diferentes forças, publicas e particulares no mundo que utilizam suas armas psicológicas para influenciar no pensamento das pessoas, por exemplo, na revista

MILITARY REVIEW, foi publicado um artigo escrito pelo comandante Randall G. Bowdish da Armada de Estados Unidos, onde documenta que os ataques psicológicos são:

> [...] Operações planejadas para transmitir informações e indicadores selecionados para o público estrangeiro para influenciar suas emoções, motivos, raciocínio objetivo e, em última instância, o comportamento do governo estrangeiro, organizações, grupos ou indivíduos. [...] PSYOP Não só abrangem o espectro militar completo de conflitos, mas também têm aplicabilidade fora da arena militar [...].

Em suma, até aqui, é possível apontar que a Internet é um meio de comunicação ideal para ataques psicológicos, pois entre outros aspetos, a rede é econômica, permite a segmentação, tem um rápido nível de propagação, os destinatários contribuem à difusão das mensagens, é propicia para a produção de boatos, têm audiências amplias e variadas, a mensagem produz confiabilidade, os ataques não estão limitados por tempo, espaço, instituições publicas nem por fronteiras, todo isto, adicionado com as outras técnicas de *hacking* como o *spoofing*, o *sniffing*, os *malware*, os *DDos*, os *MITM* e o *phishing* conformam o espaço perfeito para a manipulação e o controle dos votantes (SALVADOR, 2011, p.15).

Afinal, os engenheiros sociais têm um imenso poder para construir a sociedade desde sua base, começando desde a própria mente das pessoas e fazendo delas realidades sociais, mas então, qual é a responsabilidade jurídica que têm os engenheiros sociais?

2.3 Direito e *hacking* politico

Em consideração ao desenvolvimento precedente, ficou clara a forma em que é praticado o *hacking* desde o ponto de vista técnico, mas, verdadeiramente como isso está integrado com o direito? Para responder essa pergunta, será realizado uma análise jurídica, especialmente aplicada ao contexto normativo brasileiro.

Para começar a análise jurídica é necessário entender exatamente a que conduta típica corresponde o *hacking* político no ordenamento jurídico brasileiro. Neste sentido, é viável dizer que no ordenamento brasileiro há uma variada gama de normas que regulamentam

diferentes aspectos de segurança informática[8], não obstante, pode falar-se que as principais são a lei 9,100/1995, que em seu artigo 67 modificou os sistemas de votação e tipificou crimes eleitorais, a lei 9,983/2000 que modificou o código penal, a lei 11,829/2008 que proíbe diferentes aspectos do abuso infantil na rede, a lei 12,737/2012 que caracterizou de modo especial os delitos informáticos, o decreto 7845/2012, que neste aspecto, principalmente regulamentou a proteção dos sistemas de votação e a lei 13.260/2016 que tipificou os crimes cibernéticos como atos de terrorismo.

Porém, os ataques de segurança cibernética ou *hacking* que estão sendo analisados nesta investigação, não são os de *hacking* tradicional, usado com fines maliciosos[9], o *hacking* que está sendo analisado é hacking político. Em outras palavras, o objeto deste estudo é o *hacking* que é realizado com o fim de alterar um exercício eleitoral, por este motivo, a forma em que o ato é julgado, não pode ser igual ao de *hacking* entendido de forma tradicional, pois os efeitos sociais, políticos e econômicos que produz são muito diferentes.

Sendo assim então, sob as circunstancias técnicas explicadas anteriormente, pode-se interpretar que o *hacking* politico é uma obstrução deliberada no processo de eleição, com o proposito de alterar a vontade dos votantes, favorecendo ou prejudicando de alguma forma algum ator politico por médio de ataques comunicacionais e a manipulação da opinião publica. Essa atuação dos *hackers* sociais parece ajustar-se muito bem ao conceito de fraude eleitoral. Para isso, é conveniente compreender verdadeiramente o conceito de fraude eleitoral no contexto brasileiro. Toffoli (2009 apud TRIBUNAL SUPERIOR ELECTORAL, 2013, p.7) explica o fraude a partir de dois elementos:

> [...] Um de ordem objetiva (eventus damni) e outro subjetivo (consilium fraudis). No entanto, já se tem desconsiderado, em muitos casos, o elemento subjetivo, principalmente quando está em confronto o interesse público. [...] [E continua:] a fraude no Direito Eleitoral independe da má-fé ou do elemento subjetivo, perfazendo-se no elemento objetivo, que é o desvirtuamento das finalidades do próprio sistema eleitoral.

[8] Entre elas se encontram: a lei 8,137/1990, Art. 2 (regulamenta aspectos tributários), a lei 9,296/1996, Art. 10 (proíbe as interceptações telefônicas), a lei 11,829/2008 (proíbe diferentes âmbitos de abuso infantil na rede), a lei 9,504/1997 (estabelece normas para as eleições eleitorais) e a lei 12,735/2012, Art.4 (modifica leis sobre faculdades da força publica).

[9] Para fazer dano a outro ou obter benefícios econômicos

Por outra parte, acerca do conceito de fraude eleitoral López-Pintor (2011 apud DOČEKALOVÁ, 2012, p.2) argumentasse que é "qualquer ação intencional de manipular as atividades eleitorais e os materiais eleitorais para afetar os resultados de uma eleição, o que pode interferir ou frustrar a vontade dos eleitores". Neste sentido, Fabrice Lehoucq (2003 apud DOČEKALOVÁ, 2012, p.3) agrega que em ultimas o fraude eleitoral é “um esforço clandestino para moldar os resultados eleitorais". Finalmente, o *Instituto Interamericano de Derechos Humanos* (s.d., p.1) sintetiza que o fraude eleitoral é:

> Conduta que, por meio de engano, manipulação, falsificação, distorção, despojamento, evasão, obstrução ou violência, exercida em qualquer fase do processo eleitoral, visa impedir a realização de eleições livres, periódicas e equitativa, ou afetar o caráter universal, igual, livre e secreto voto cidadão.

É evidente que a conduta dos *hackers* políticos está ajustada ao tipo de fraude eleitoral. Entendendo a base da conduta, pode ser exposto o possível fundamento normativo do problema. Assim, desde a Constituição Politica do Brasil, a norma fundacional da federação, estabelece em seu artigo 14 § 10 que “O mandato eletivo poderá ser impugnado perante a Justiça Eleitoral no prazo de quinze dias contados da diplomação, instruída a ação com provas de abuso do poder econômico, corrupção ou fraude”.

Esta norma da Constituição é bastante abstrata, mas pode ser interpretada sob o artigo 222 do Código Eleitoral que assinala que “É também anulável a votação, quando viciada de falsidade, fraude, coação, uso de meios de que trata o art. 237, ou emprego de processo de propaganda ou captação de sufrágios vedados por lei”. Nesse sentido, o artigo prevê uma remissão ao artigo 237 que adverte que “A interferência do poder econômico e o desvio ou abuso do poder de autoridade, em desfavor da liberdade do voto, serão coibidos e punidos [...]”.

Assim sendo, de chegar-se a comprovar um caso de *hacking* politico no contexto jurídico brasileiro e de acordo com este desenvolvimento, as consequências poderiam ser muito graves, pois o efeito direito de que seja comprovado o fraude por meio de ataques de *hacking* para alterar de alguma maneira a decisão de voto dos eleitores poderia abrir a possibilidade de que seja anulada a eleição, nessa medida, também podem começar a ser previstos novos mecanismos para fazer mais rigoroso o laxo regímen que têm os

comunicadores, para que desta forma, seja exercida a liberdade de expressão de forma mais responsável, em conformidade com o risco social que representa o exercício da profissão desde o ponto de vista da engenharia social.

Entretanto, antes de continuar com o estudo político do problema, é necessário analisar a forma em que a filosofia interpreta esta situação.

2.4 Inconsciente coletivo, determinismo comunicacional e psicologia de massas

Para compreender a influencia que sobre as pessoas exercem os meios de comunicação, pode apresentar-se o apontado por Marshall McLuhan[10] (1967, p.26-41), quem explica a profundidade a forma em que os indivíduos são atacados pelos meios de comunicação, pois explica que:

> Todos os meios batem-nos minuciosamente. Eles são tão penetrantes em suas consequências pessoais, políticas, económicas, estéticas, psicológicas morais, éticas e sociais que não deixam parte de nós intacta, inalterada.
>
> O meio é a mensagem. Nenhuma compreensão de uma mudança social e cultural é possível quando não é conhecida a maneira em que os indivíduos funcionam em ambientes.
>
> Todos os meios são a extensão de alguma faculdade humana, física ou mental. A roda... é uma extensão do pé [,] o livro é uma extensão do olho... a roupa, é uma extensão da pele... o circuito elétrico é uma extensão do sistema nervoso central.

Certamente, McLuhan estabeleceu fortes bases para a interpretação da influência dos meios de comunicação nas pessoas, pois apoiado na cibernética social, logrou explicar como nossa consciência fica alterada depois de estar em contato com os meios de comunicação, finalmente asseverou, “quando essas proporções [comunicacionais] mudam, as pessoas mudam” (McLuhan, 1967, p.41, tradução minha). Assim apresentam-se os ataques psicológicos, em forma inconsciente e “minuciosa”. Isto é conhecido também como determinismo comunicacional.

[10] Livro em versão gráfica

No entanto, para poder entender depois disso, que acontece com os condicionamentos do sujeito, podem plantear-se as propostas do inconsciente coletivo de dois psicanalistas: Jacques Lacan e Carl Jung. Ambos acreditavam que a realidade dependia de uma interação da internalidade com a externalidade, por isso, elaboraram duas teorias diferentes do inconsciente.

Para o professor Lacan (1959, p.140, tradução minha) o inconsciente é um ponto meio entre dois, pois explicou que existe "[…] um mundo entre os dois porque é precisamente em contato com a palavra […]". Nesse sentido, o inconsciente para Carl Jung (1970, p.146, tradução minha) dependia de uma interação do interior com o exterior, pois explicou que:

> Em suma, a quê tende este recorrido que regressa sobre si mesmo na enunciação analítica, pelo tanto, eu diria libertado ao princípio, a regra fundamental da associação livre? Valorar como possível o que tem incluso em todo discurso, uma cadeia significativa de tudo o que sabe cada um, de forma fragmentada, noutras palavras, de elementos interpretáveis. Aqueles elementos interpretáveis, um tanto fragmentados, aparecem na medida em que o sujeito tenta reconquistar-se em sua originalidade, de tornar-se aquilo que a demanda definiu nele e capturando suas necessidades, encontra-se primitivamente relacionado às necessidades próprias da demanda, que se encontram essencialmente fundadas pelo fato de que já o jeito da demanda está modificada, alienada: pelo fato de que devemos pensar sob esta forma de linguagem, é já no registro do Outro como tal, no código do Outro, que ela deve inscrever-se.

Deste modo, a manipulação do inconsciente coletivo pode ser o mais precioso tesouro dos engenheiros sociais no campo politico. No obstante, ainda falta entender como os ataques psicológicos adquirem determinado nível de sociabilidade. Para explicar isso, Hanna Arendt (2009) escreveu acerca da opinião pública que "[...] para nós, a aparência –algo que vem e ouvem os outros da mesma forma como nós– é a realidade [...]" (p,59, tradução minha). Assim é como se tornam sociais os ataques psicológicos. Como origem destas teorias, pode-se expor a de Gustave Le Bon (2004, p.18, tradução minha) quem explicou como em ultimas, para bem ou para mau, a consciência individual pode desaparecer na consciência do grupo:

> [...] A massa é sempre intelectualmente inferior ao indivíduo isolado, mas do ponto de vista dos sentimentos e ações que esses sentimentos causar, a massa pode, dependendo das circunstâncias, ser melhor ou pior do que o individuo. Tudo depende da sugestão de que a massa está exposta. Este é o ponto que foi

> completamente mal interpretado por escritores que só estudaram as massas de uma vista criminal. Sem dúvida alguma, uma massa é muitas vezes criminal, mas também muitas vezes é heroico. São as massas invés de indivíduos as que podem ser induzidos a correr um risco de morte para garantir o triunfo de um credo ou uma ideia; que pode ser inflamado com entusiasmo para a glória e honra; que pode ser conduzido - quase sem armas como na época das Cruzadas - para recuperar o túmulo de Cristo das mãos dos infiéis ou, como em noventa três, para defender o país. Um heroísmo como esse é certamente inconsciente até certo ponto, mas de esse tipo de heroísmo está feita a História. Se os povos foram levados em conta apenas para atos cometidos a sangue frio, os anais do mundo iriam registrar apenas muito poucos deles.

Este desenvolvimento mostra, o complexo que se pode tornar o evitar a manipulação. Mas então, porque acontece todo isto? Que respostas poder ser feitas para explicar como aconteceu isto na filosofia politica? Afinal, a sustância de todo isto é a acumulação de poder, ao respeito, assinalou Michael Foucault (1987, p.218, tradução minha) que "[...] o poder produz; ele produz realidade; produz campos de objetos e rituais da verdade. O indivíduo e o conhecimento que dele pode-se ter originam-se nessa produção [...]". Instalando-se finalmente o poder na filosofia com as teorias de Nietzsche (2002, p. 9), quem fala:

> O que é bom? – Tudo que aumenta, no homem, a sensação de poder, a vontade de poder, o próprio poder.
> O que é mau? – Tudo que se origina da fraqueza.
> O que é a felicidade? – A sensação de que o poder aumenta – de que uma resistência foi superada.
> Não o contentamento, mas mais poder; não a paz a qualquer custo, mas a guerra; não a virtude, mas a eficiência (virtude no sentido na Renascença, virtude desvinculada de moralismos). [...]

Assim, para Nietsche o que move aos homens é a vontade de poder, toda esta orquestra de técnicas e estratégias não tem outro objeto que o de sobrepor-se e dominar aos outros. Contudo, finalmente, que acontece com a politica neste caso?

2.5 Aspectos políticos do problema: a crise da representatividade y da legitimidade

De tal modo, para Nietzsche a própria natureza do ser humano está constituída por um profundo desejo de dominação e superposição sobre os outros. Em complemento com Nietzsche, no campo político-econômico, Anthony Downs (2001, p.136) estabeleceu que o sistema politico em conformidade com os princípios econômicos está baseado no egoísmo e,

por conseguinte, o funcionamento das eleições politicas é egoísta, pois depende da administração de recursos escassos, em função dos interesses privados de cada pessoa.

Nesse sentido, é possível entender que a prática da politica não está baseada na liberdade, muito pelo contrário, na dominação. Esse egoísmo desmente até certo ponto a viabilidade da democracia como sistema politico, embora, agrega Downs (2001, p.136, minha tradução) que "grande parte da teoria econômica consiste essencialmente em provar que os homens que perseguem o seu próprio fim podem não entanto desempenhar suas funções sociais com grande eficiência, pelo menos sob certas condições".

Como é descrito por Hanna Pitkin (1985, p.15-46), o Estado Hobbesiano controla ao Leviatán em virtude da autoridade que simboliza a representação. Não entanto, a representatividade atualmente está em crise, pois como foi assinalado por Pippa Norris (1999, p.12) os cidadãos confiam na democracia, mas não, em seus autoridades publicas.

Essa pesquisa é também prova dos postulados de Norris, pois a representatividade está efetivamente em crise, já que o sistema político-econômico descrito por Downs obriga aos atores a comportar-se em contra da própria democracia, atacando ao elo mais fraco, para o ser humano (como foi analisado na pesquisa), e é através dos meios de comunicação onde é mais eficiente este ataque.

Esta manipulação indiscriminada e sistemática é o que ocasiona a crise da representatividade, pois as eleições políticas são feitas sem legitimidade. Os candidatos políticos não trabalham para representar os ideais, senão para dobrar seu oponente politico na arena da opinião publica, por conseguinte, os cidadãos não votam realmente numa democracia, os cidadãos votam num sistema hibrido, onde a soberania radica em cidadãos manipulados, representados só pela formalidade (DIAMOND, 2004, p.118).

É aqui onde as teorias filosóficas apresentadas têm maior valor, já que podem ser uma forma apropriada de entender o problema da crise da representatividade, podendo ser proposta a seguinte análise: o sistema politico, como todos os outros sistemas depende em grande parte da informação que é compartida e dos processos de retroalimentação das partes do sistema. Conforme foi analisado com Castells, o intercâmbio de informação não é só um ato, é realmente um processo, o qual implica na "significação" do sujeito, similar às propostas do Jung e do Le Bom, esse processo não e isolado, pelo contrario é um processo social.

Fazendo uma síntese geral dos pensadores antes citados, pode-se dizer que segundo as análises feitas com Jung e Lacan a mente do ser humano, depende em grande parte de um espaço subconsciente mais ambivalente, ou seja, com uma dimensão tanto interna como externa. De forma similar Arendt, propôs que a construção interna dependia da realidade social, enquanto que para Foucault, o sujeito é construído desde a influência externa das realidades criadas pelos discursos disciplinares dos poderosos.

Seja assumida uma explicação desde o pensamento dos autores, Arendt, Lacan, Jung e Foucault, estes têm um espaço teórico coincidente, pois para eles, na zona social acontece a comunicação, as instituições, a disciplina, os estabelecimentos, a opinião publica, e com eles, os condicionamentos que vão a determinar a realidade do individuo e em consequência sua realidade social. Tem-se então uma externalidade de corpos intangíveis, por exemplo, a moral, a religião, o pudor sexual, o patriotismo, a nacionalidade, a família, mas com efeitos tangíveis, sanções, guerras, triunfos eleitorais; estas podem ser interpretadas como tecnologias sócias que não são perceptíveis pelos sentidos, mas que enquadram o mundo cognoscível pelo sujeito e que ao ser sutil o fazem vulnerável.

Em resumo, pode que uma das principais causas da crise da representatividade nos sistemas democráticos contemporâneos radique num problema de segurança informática, pois o elo mais fraco do sistema é o ser humano, já que o cidadão, não conta com os mecanismos necessários para se defender de ataques psicológicos dos meios de comunicação, e muito menos, é consciente de suas vulnerabilidades, morando no terreno da ignorância dos riscos políticos de que é susceptível. Deste modo, sob os resultados obtidos com este trabalho é possível estabelecer que para tentar solucionar o problema da representatividade da democracia é necessário assumir medidas políticas e jurídicas de segurança informática para alcançar cidadãos mais conscientes, e reduzir as possibilidades de manipulação negativa dos engenheiros informáticos.

3. Conclusões

As conclusões desta pesquisa podem ser resumidas da seguinte forma:

a) Ao longo do artigo, foram expostos diferentes argumentos para demostrar que os profissionais em programação de redes informáticas ou *hackers* ou também engenheiros sociais, estão desempenhando uma função fundamental nas campanhas eleitorais, filtrando e gerenciando a informação que recebem os

eleitores (verdadeiros *gatekeepers*), condicionando a forma em que pensam os cidadãos, e por tanto, a forma em que assumem suas decisões políticas. Por isso, é imprescindível começar a ampliar o conceito de segurança informática, para incluir as vulnerabilidades politicas de que são susceptíveis os usuários da rede.

b) É necessário que a sociedade seja consciente das vulnerabilidades que têm e dos diferentes riscos de que são susceptíveis nos diferentes meios de comunicação, especialmente na Internet. A manipulação apresentada nos meios de comunicação é sumamente frívola e calculada, no entanto, é indireta e por isso mais forte, exigindo que os cidadãos sejam mais conscientes, ativos e críticos. Também, as diferentes entidades publicas e de controle estão involucrados nesta problemática e devem encará-la, assumindo as medidas jurídicas e politicas que sejam necessárias para a proteção da ordem democrática.
c) Este problema não pode significar uma tendência em direção a uma tecnofobia, também no, a entrada numa centralização da Internet, uma vez que isso representaria uma desnaturalização própria da rede, pois a Internet nasceu como uma rede de redes livre, autônoma e independente e uma decisão de centralização unilateral dos estados significaria sua desfiguração.
d) Deve-se proteger "à vida, à liberdade, à igualdade, à segurança e à propriedade" como supremos valores jurídicos e sociais da comunidade brasileira consagrados no artigo 5º. da Carta Magna, por isso, os *hackers* políticos, bem como os candidatos políticos a quem estão ligados, devem ser julgados não só por seus delitos econômicos e técnicos, mas também, por seus delitos políticos, como a fraude eleitoral, tipificado no artigo 222 do Código Eleitoral Brasileiro (Lei 4.747/1965).
e) É muito apressado concluir absolutamente que, de forma velada e detrás da ordem das campanhas politicas, existe uma guerra cibernética de forma dissimulada, pois para isso, ainda seria necessária uma pesquisa com maior profundidade e tal vez um enfoque mais qualitativo. No entanto, até aqui, é possível concluir que o processo competitivo das campanhas políticas, representa um forte conflito mediático que pode em determinado momento trasladar-se a espaços cibernéticos, deste modo, é obrigação da academia, das instituições públicas e da sociedade em geral zelar para que essas ações não violem os princípios éticos, não sirvam para agredir, para manipular, nem para controlar ou dominar aos outros.

REFERÊNCIAS

AGUILERA, L. **Seguridad Informática**. [S.l]: Editex, 2015. Disponível em: <https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf>. Acesso em: 02 jun. 2017, 18:57:13.

ARENDT, H**. La condición humana.** Buenos Aires: Paidós, 1 ed 5, 2009.

BABU, R; BHASKARI, L; SATYANARAYANA; CH. A Comprehensive Analysis ofSpoofing. **International Journal of Advanced Computer Science and Applications**, [S.l.] vol. 1, n.6 p.157-152, dez. 2010.

BATES, R, A; MOONEY, M. Psychological Operations and Terrorism: The Digital Domain. **The Journal of Public and Professional Sociology.** Morrow, Clayton State University, vol. 6, [n.1.], jul. 2014.

BILEY, M. et al. **Automated Classification and Analysis of Internet Malware.** Michigan: University of Michigan, 2007.

BOWDISH, G. R. Information- Age Phychological Operations. **MILITARY REVIEW**, US Navy, Lincoln, p.28-36, fev. 1999.

BRASIL. Constituição (1988) Constituição da republica federativa do Brasil: promulgada em 5 do outubro de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm>. Acesso em:

BRASIL. Decreto n. 7845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 14 de novembro de 2012, Disponível e <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>. Acesso em: 05 jun. 2017.

BRASIL. Lei n. 12,737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 30 de novembro de 2012, Disponível e < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 jun. 2017.

BRASIL. Lei n. 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5o da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nos 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 16 de março de 2016, Disponível e

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm>. Acesso em: 05 jun. 2017.

BRASIL. Lei n. 4,737, de 15 de julho de 1965. Institui o Código Eleitoral. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 15 de julho de 1965, Disponível e < http://www.planalto.gov.br/ccivil_03/leis/1950-1969/L4747.htm>. Acesso em: 05 jun. 2017.

BRASIL. Lei n. 9,100, de 29 de setembro de 1995. Estabelece normas para a realização das eleições municipais de 3 de outubro de 1996, e dá outras providências. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 29 de setembro de 1995, Disponível e <http://www.planalto.gov.br/ccivil_03/leis/L9100.htm>. Acesso em: 05 jun. 2017.

BRASIL. Lei n. 9,983, de 14 de julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Diário oficial da União, Poder Executivo, Brasília, DF, Promulgada em 14 de julho de 2000, Disponível e <http://www.planalto.gov.br/ccivil_03/leis/L9983.htm>. Acesso em: 05 jun. 2017.

CASTELLS, M. **Comunicación y poder.** Tradução de María Hernández, Madrid: Alianza Editorial, 2009.

CERT-US. **Common Cyber Security Language.** [S.l. : s.d. : s.n.]

DAKOSTA, I; AHAMAD, M; TRAYNOR . P**. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties.** Georgia: Georgia Institute of Technology, [s.d.].

DIAMOND, L. Elecciones sin democracia A propósito de los regímenes híbridos, **Estudios Politicos,** Tradução de Darío López, Baltimore, Universidad Johns Hopkins, p.117-134, 2004.

DOČEKALOVÁ, P. **Comparative Research of Electoral Fraud: Limits and Opportunities.** Hradec Králové: University of Hradec Králové, 2012.

DOWNS, A. An economic theory of political action in a democracy. **The Journal of Political Economy**, vol.65, n.2, p.135-150, abr. 1957.

FISCALÍA GENERAL DE LA NACIÓN (COLOMBIA)**. Es condenado hacker Andrés Sepúlveda**, [S.l.]: 2016. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi8q--JoaDUAhUHx5AKHcIgCFIQFggsMAE&url=http%3A%2F%2Fwww.fiscalia.gov.co%2Fcolombia%2Ftag%2Fcaso-hacker%2Ffeed%2F&usg=AFQjCNFkECz28JUD3V4LInYVCV0H0ETrjw&sig2=aXJB5XfKWwjfXUGqm1s6rw>. Acesso em: 04 mar. 2017, 17:57:43.

FOCAULT, M. **Vigilar y castigar.** Buenos Aires: Siglo XXI editores, 2002.

INTECO. ¿QUÉ ES Y QUÉ NO ES UN HACKER? **Cuaderno de notas del OBSERVATORIO.** [S.l.: s.d.] Disponível em:

<http://www.egov.ufsc.br/portal/sites/default/files/cdn_hacking_v2.pdf>. Acesso em: 19 mai. 2017, 22:30:15

JUNG, C. G. **Arquetipos e inconsciente colectivo.** Barcelona: Ediciones Paidos, 1970.

LACAN, J. **Seminario 6**: **El deseo y su interpretación**. Paris: Psikolibro, s/d. Disponível em: <http://www.bibliopsi.org/docs/lacan/08%20Seminario%206.pdf>. Acesso em: 19 mai. 2017 22:08:05.

LE BOM, G**. Psicologia de masas.** Buenos Aires: [S.n], 2004.

MCLUHAN, M. **El medio es el mensaj**e: **un inventario de efectos.** Nueva York: Paidós Studio, 1967.

MIRKOVIC, J. REIHER, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. **Computer Communications Review**, Los Angeles, vol. 34, p.39-54, abr. 2004.

MITNICK, K. SIMON, W. **The art of deception.** [S.l : s.n.], 2002.

NIETZSCHE, Friederich. **O anticristo**, 2002.Disponível em: <http://www.ebooksbrasil.org/adobeebook/anticristo.pdf> Acesso em: 19 mai. 2017, 13:21:09.

NORRIS, P. **Critical Citizens: Global Support for Democratic Government.** Oxfordshire: OUP Oxford, 1999.

OPLIGGER, R. et al. **A Proof of Concept Implementation of SSL/TLS Session-Aware User Authentication (TLS-SA).** Zurich: [S.l.] 2010.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Malicious Software (Malware): A Security Threat to the Internet Economy.** Seoul [S.l.], 2008.

PAPAZOV, Y**. Social Engineering.** NATO OTAN: Sofía, s.d.ROBERTSON, J. RILEY, M. WILLIS, A. **Cómo Hackear una Elección** [S.l.]: Bloomberg Businessweek, 2016. Disponível em: <https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/>. Acesso em: 02 jun. 2017, 17:55:27.

PITKIN, H. **El concepto de representación.** Madrid: Centro de estudios constitucionales, 1985

SALVADOR, L. Ingeniería social y operaciones psicológicas en internet. **Ieee.es**, [S.l.], vol. 74, p.1-21, oct. 2011.

SPANGLER, R. **Packet Sniffer Detection with AntiSniff.** Wisconsin: University of Wisconsin, 2003.

TAGHAVI, S, Z. et al. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. **IEEE COMMUNICATIONS SURVEYS & TUTORIALS,** Pittsburgh, University of Pittsburgh, p.1-24, [s.d.].

TRIBUNAL SUPERIOR ELEITORAL. **Ilícitos Eleitorales.** Brasília: Seprov/Cedip/SGI, 2013.

WIKIPEDIA**. Cultura hacker.** [S.l: s.d.] Disponível em: https://pt.wikipedia.org/wiki/Cultura_hacker>. Acesso em: 02 jun. 2017, 18:59:09.