SÃO AS URNAS DE VOTAÇÃO BRASILEIRAS, E CONSEQUENTEMENTE SEU SISTEMAELEITORAL, SEGUROS DE ATAQUES CIBERNÉTICOS OU DE *CRACKERS* ?

David Chaves.[1]

1 – Introdução

Em um ano de eleições municipais, como o que tivemos agora em 2020, reacendem as desconfianças à creca da segurança do sistema eletrônico de votação brasileiro, tal falto inflamou-se ainda mais após diversas declarações do Presidente Jair Bolsonaro questionar a segurança das urnas, que em sua opinião não teriam como passar por uma auditória, visto que os votos não são impressos depois de gravados no chip-set das urnas. Em resposta, o Tribunal Superior Eleitoral (TSE), afirmou que desde o inicio do seu uso em 1996, nunca houve registros de fraudes significativos que anulassem os benefícios do uso informatizado do sistema. Sob a temática, primeiramente aprofunda-se as discursões dos Poderes Executivo e Judiciário, referentes à confiabilidade do Sistema Eleitoral, posteriormente caracteriza-se as normas de Segurança Cibernética para as votações brasileiras nas urnas e na transmissão de dados pelo TSE, por fim, como forma de contribuição, o autor utiliza-se de seus conhecimentos teóricos, como técnico em informática e cientista político, para analisar a implementação do comprovante de voto, chamado popularmente de voto impresso, sua necessidade e segurança do Sistema Eleitoral.

2 – Aprofundamentos: a guerra entre Executivo Federal e Tribunal Superior Eleitoral sobre a confiabilidade do sistema eleitoral brasileiro.

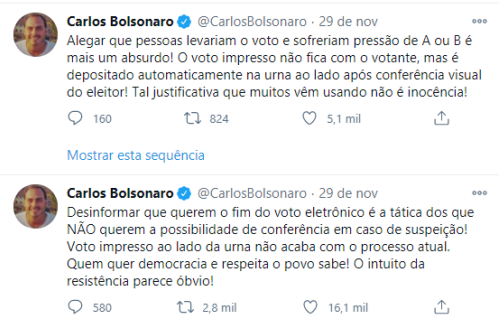
Sem dúvidas, o principal tema que marcou as eleições de 2020 fora a covid-19, em um país onde o número de abstenções já vinha em crescente vertiginosa, os brasileiros ficaram preocupados no ato de registrar seus votos, com medo de serem infectados pelo vírus que assolou o mundo neste ano pandêmico. Segundo informações obtidas pela Agência do Senado, 29,5% dos eleitores, aptos a votar, preferiram justificar seu voto, sendo a maior abstenção na recente história da redemocratização brasileira. Embora a discursão entre abstenções e obrigatoriedade do voto sejam pertinentes no quadro político nacional, não se tratará delas aqui, uma vez que nos interessa neste artigo a segurança de um outro tipo de vírus que pode adoecer a democracia brasileira, a segurança cibernética, dos eleitores que foram às urnas.

Destarte, logo após votar em segundo tuno, em seu seção eleitoral no Rio de Janeiro, em 29 de novembro de 2020, o Presidente Jair Bolsonaro voltou a defender o voto impresso como forma mais segura para garantir uma apuração presidencial justa e que seja auditável, em suas palavras, defendendo o citado afirmou:

> *"Está até na própria Constituição. A apuração tem que ser pública". Além disso estabeleceu duras críticas ao sistema eleitoral atual, atacando de fronte o Tribunal Superior Eleitoral; "Vou mostrar pra vocês [jornalistas]. A apuração minuto a minuto que acontecia no TSE [eleição geral de 2018]. Era alternado: em duas horas, no 1º minuto, eu ganhei, no 2º minuto, o Haddad ganhou, e assim intercalando. Estatisticamente, isso é impossível. Mesma coisa que eu contar as areias da praia de Copacabana agora, quantos grãos de areia têm lá (...). Não podemos continuar votando e não sabendo, não tendo a certeza daquele voto que foi dado para aquela pessoa."(BOLSANARO, JAIR MESSIAS, 2020)*

Ainda diante dos jornalistas, Bolsonaro afirmou que faria de tudo para que a reforma no processo eleitoral ocorresse para que nas eleições de 2022 o sistema de voto impresso seja implementado. Pelas redes sociais, um de seus filhos, o deputado federal Eduardo Bolsonaro, também se manifestou a favor do voto impresso.

[1] David Chaves é Mestre em Ciência Política/ Política Internacional pela Universidade Federal de Pernambuco (UFPE); Bacharel em Ciência Política com ênfase em Relações Internacionais (UFPE); Técnico em Manutenção e Suporte em Informática (ETEPAM). Graduando em Direito pela Universidade Federal da Paraíba (UFPB). E-mail: dvdchaves100@gmail.com



A resposta a seus apoiadores e ao Presidente não demorou muito a chegar, em coletiva de imprensa pós-divulgação dos resultados das eleições em segundo tuno, na noite de 29 de novembro de 2020, o Ministro do Supremo Tribunal Federal (STF) e então Presidente do TSE, Luís Roberto Barroso, afirmou que a volta do voto impresso traria o caos ao Sistema Eleitoral, ao poder Judiciário e a própria democracia brasileira. Defendera com unhas e dentes a confiabilidade da urna eletrônica e lembrou que o STF já formara jurisprudência, com a maioria de votantes, sobre a inconstitucionalidade de votar com uma caneta. Em suas palavra

> "*O presidente da República merece todo o respeito institucional e tem o direito de manifestar sua opinião. A verdade, porém, é que o STF já entendeu pela inconstitucionalidade do voto impresso. E não só pelo gasto, mas porque representaria um risco real para o sigilo de voto. Não existe hoje a possibilidade de voto impresso. Respeitando a opinião de todos, o voto impresso causaria grande tumulto, porque todo derrotado ia pedir recontagem, haveria impugnações, alegações de nulidade e judicialização do processo. Considero que traria um grande tumulto. Se o presidente tiver alguma comprovação de fraude de 1996 para cá, imediatamente designarei diligencias para apurá-la. Mas quero lembrar que sou juiz, não posso me impressionar com retórica política*" *(BARROSO, LUÍS ROBERTO, 2020)*

Continuando, com suas críticas ao líder do Executivo, de maneira ainda mais densa e com tons de ironia, Barroso referiu-se que "Na farmacologia" não existiria nenhum remédio para fazer qualquer pessoa parar de duvidar que é possível fraudar as urnas brasileiras. Para isso, argumentou que as urnas não são conectadas em rede e por isso não podem ser "crakqueáveis"; sendo carregadas individualmente e com seu programa operacional submetido a conferências de todos partidos políticos, Ministério Público, da Ordem dos Advogados do Brasil (OAB) e de outras entidades civis. Depois da conferência, em suas palavras, as urnas são lacradas em um cofre, que trava sob quaisquer tentativa de alteração e arrombamento, no final das votações cada urna emite um boletim com o resultado impresso, sendo ele entregue a todos os fiscais de partidos e colados nas paredes das seções eleitorais para que qualquer cidadão as veja. Ainda segundo barroso; "*Nunca, desde 1996, quando começou o voto eletrônico, ninguém demonstrou nenhum caso de fraude.*", Informou ainda que, a Organização dos Estados Americanos (OEA) considera o sistema de apuração brasileira, em suas palavras *"o mais ágil e seguro das Américas"*.

A convicção sobre a segurança do sistema eleitoral é tanta que na próxima secção discutirei, em profundidade, como o TSE elaborou as chamadas "Camadas de Proteção" das urnas eletrônicas brasileiras e como funciona a transmissão dos dados de cada Tribunal Regional Eleitoral (TRE), de cada estado da federação para o TSE em Brasília.

3 – As Camadas de Proteção Contra Ataques Cibernéticos do TSE.

Uma complexa redes de sistemas *on-line* e *off-line*, com fases de segurança mecânicas e virtuais, em várias camadas de proteção fazem do sistema de segurança eleitoral brasileiro um dos mais difíceis de ser "crakqueados" do mundo, fato que também contribui para a rápida divulgação dos resultados, correspondendo, com alto grau de paridade às pesquisas de boca de urna formuladas por cientistas políticos e institutos de pesquisas, destinados ao próprio TSE. Desta forma, explica-se aqui, por partes, para que fique mais compreensível ao leitor, o funcionamento deste complexo sistema, cuja fonte fora obtida através do site do próprio Tribunal Superior Eleitoral.

3.1 O uso da Criptografia.

A criptografia é essencial em todas as etapas das transmissões dos dados para o sistema que vai contabilizar , depois de encerrada a votação, o resultado dos pleitos. O conceito de criptografar dados fora inventada por Júlio César o grande líder romano, que usava em suas mensagens militares a troca de posições de três letras, a cada letra escrita, para que um possível interceptor da mensagem não soubera de seu conteúdo. Tão somente o receptor real saberia o código para descriptografar, refazer o texto substituído por 3 letras anteriores, par ter acesso ao conteúdo do qual César quisera que apenas o destinatário tivera. Evidentemente, com a evolução para um mundo globalizado, interconectado por redes, as formas de criptografias são muito mais avançadas e dificultosas para um possível, interceptor, *Hacker* ou *Cracker* do que a fora apresenta pela Cifra de César.

O TSE utiliza a criptografia através de assinaturas digitais para que seja garantido que os dados possam ser verificados, enquanto a sua integridade, buscando saber se estes não foram alterados ou modificados de forma intencional ou não, perdendo assim suas características originais, por falha de gravação ou de leitura. Garantindo que o arquivo não fora modificado em seu tráfego.

Da mesma forma, o Resumo Digital, ou *hash*, também feito por meio de criptografia, assemelha-se a um dígito verificador, que tem como função dos arquivos enviados por um conjunto de sistemas trabalhando em paralelo, em um algoritmo público, onde todas as pessoas podem ver as parciais das apurações de seus candidatos.

3.2 Ecossistema das Urnas.

O funcionamento de uma Urna eletrônica é totalmente *off-line*, com diversas camadas de proteções. Essas camadas são físicas e não físicas. Por camadas físicas entende-se todos os tipos de lacres, vedos, e proteção de cabeamento da urna. Por camadas não físicas, também conhecido como ecossistema da urna, define-se pelo conjunto de programas autônomos entre si, cada um com sua função específica para que a urna funcione. Caso exista algum tipo de falha em qualquer um desses programas a urna para sua atuação no exato momento, mas os votos que até então foram computados não se perdem, uma vez que estão armazenado na memória física de cada urna, em seu chip-set, um espécie de caixa-preta. Após isso são substituídas por urnas novas.

3.3 Registro Digital do Voto.

Depois que o eleitor digita os números de seus candidatos e aperta o botão de confirma são gerados dois arquivos, o primeiro é destinado para o sistema que vai processar os dados totais e dar os resultados das eleições já o segundo, permanece armazenado dentro da própria urna, sendo emitido no final como comprovante de total de votos, vale lembrar que neste comprovante também faz-se uso da criptografia, uma vez que dentro da urna existe um sistema que embaralha o nome do eleitor e se interessa apenas no quantitativo de dígitos registrados iguais, ou mais detalhadamente, no quantitativo de votos que cada candidato deteve.

3.4 Cerimônia de Assinatura Digital.

Antes das urnas serem lacradas, representantes dos partidos políticos, e da sociedade civil, são convidados para checarem os equipamentos e o processo de assinatura digital.

3.5 Votação Paralela e Auditória pela sociedade Civil.

Por votação paralela entende-se o ato de simular uma eleição previamente para constatar se todo o sistema está funcionando em harmonia, verifica-se também se o número digitado nas urnas, foram os mesmos computados e impressos nos boletins de final de expediente. A auditória pela sociedade surgiu em 2018, trata-se de mais uma etapa de verificação dos equipamentos por setores da sociedade, antes do início da eleição, qualquer eleitor poder ser apto a ser auditor.

3.6 Auditórias

Em 17 anos de utilização do sistema, inúmeras auditórias e pericias já foram realizadas, destacam-se as realizadas pela Unicamp em 2002, que concluiu que *"o sistema eletrônico de votação atende às exigências fundamentais do processo eleitoral, ou seja, o respeito à expressão do voto do eleitor e a garantia do seu sigilo".* e a da Polícia Federal de 2008 que em laudo técnico nas eleições municipais de Caxias (MA), descartou qualquer suspeita de fraude, ou enviesamento de dados das urnas.

Também em 2008 , o TSE contratou a Fundação de Apoio à Capacitação em Tecnologia da Informação (FACT) para prestação de serviços especializado e de suporte na especificação de programas par garantir ainda mais segurança ao sistema eletrônico brasileiro. Garantindo às urnas, características ergonômicas, de interferência eletromagnética e confiabilidade do *hardware,* gerando assim economia na compra de novas plataformas cada vez mais seguras.

3.7 Testes de Segurança

Os testes de segurança são espécies de *hackathon* – Junção de *hackers* em um mesmo espaço físico para tentar hackear os sistemas de segurança de determinada empresa ou instituição, com objetivo de aperfeiçoá-los – demostrando a importância dada pelo TSE ao melhoramento contínuo do sistema.

Nas ocasiões os investigadores inscritos, em grupo ou individualmente, apresentam planos de ataque e os executam, concernentes a componente externos e internos das urnas. No primeiro teste em 2009, nenhum especialista conseguiu adentrar o sistema, entretanto as ideias apresentas ali ajudaram o TSE a aperfeiçoá-lo, na segunda edição em 2012 e na Terceira edição em 2016, os especialistas tiveram acesso prévio ao código fonte. Já em 2017, dos 14 participantes dos testes, 10 conseguiram burlar o sistema de alguma maneira, ajudando o TSE a ampliar a segurança cibernética de seu sistema de votação.

Com a eficiência no melhoramento do processo com os testes, através da Resolução-TSE nº 23.444/2015, ficou determinado que os testes públicos de segurança sejam realizados antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecederem os pleitos eleitorais.

3.8 Votação Paralela.

Trata-se de uma auditória que ocorre no dia da eleição, na qual, ficais de partidos políticos, coligações, representante da Ordem dos Advogados do Brasil (OAB) e representantes da Sociedade Civil são convidados para participar e analisar os resultados. Os TREs designam um local após sorteio de duas a quatro urnas eletrônicas nas vésperas das eleições. A auditória acontece simultaneamente á votação oficial sendo apresentada a verificação do funcionamento das urnas sorteadas. Anteriormente à votação, o mínimo de 500 cédulas são entregues aos representantes dos partidos políticos que participarão do evento, que deverão preenche-las e em seguida deposita-las em urnas de lona lacrada. A comissão de votação paralela deve estar atenta ao caso de algum partido não entregar todas as cédulas, neste momento será pedido que representantes de outros partidos preencham os cédulas restantes. Os participantes recolhem um cédula da lona lacrada, revelam aos fiscais e demais presentes os candidatos escolhidos e em seguida digitam os números correspondentes no Sistema de Apoio a Votação Paralela e na Urna Eletrônica. Sendo todo o processo filmado e fiscalizado.

Os objetivos da votação paralela são: I – Verificação de assinatura digital; II – Verificação de resumo digital; III – Comparação do resultado da votação por cédula com o resultado do boletim da urna; IV – Verificação da filmagem do procedimento e do registro do sistema e V – Verificação do registro digital do voto.

4 – Reflexões Sobre o Uso do Voto Impresso, Suas Consequência e a confiabilidade do sistema eletrônico de votação.

Embora, costumeiramente, o Presidente Jair Bolsonaro venha batendo na tecla de que o voto impresso seria uma forma de garantir a confiabilidade das eleições brasileiras, um discurso mais político do que técnico, sua tese é respaldada por alguns cientistas políticos, que embora não defendam o voto impresso, assumem que não existem no Brasil uma maneira de se fazer um contrafactual, auditória, acerca dos resultados obtidos na urna eletrônica.

O autor, na posição de técnico em informática e cientista político, se coloca na ala contrária ao voto impresso, pelas inúmeras ineficácias que este pode trazer ao Sistema, já tão complexo, Eleitoral Brasileiro. Cita-se, seus argumentos em sequência.

4.1 Aumento dos Gastos com Compra de Papel e Tinta Pelo TSE.

De fato, o voto impresso já é inconstitucional, mas se fora adotado aumentariam em alguns milhões de reais os custos totais com a votação, uma vez que cada voto demandaria a impressão e o uso de papeis e tintas para serem registrados.

4.2 Falhas na Impressão dos votos e possíveis erros de dados registrados nos folhetins.

O voto impresso, daria margem para que possíveis erros de impressão acontecessem, sendo essas cédulas invalidadas. Exemplificando, em um segundo turno em que o eleitor deva votar entre os números 11 e 17, que são muito parecidos em termos estéticos, qualquer falha de impressão nestes números fariam por exemplo que os eleitores que votaram no número 17, tenham seu voto impresso registrado o número 11, gerando ainda mais transtorno quando comparados aos números da urna eletrônica.

4.3 Dificuldades Logísticas de Deslocamentos e Contagem dos Votos.

Em uma República Federativa continental como o Brasil, cercada de cantões com densos vazios demográficos e regiões com difícil acesso de chegada, como seria o transportes desses votos impressos para cada TRE, ou melhor, como todos esses votos impressos chegariam à Brasília? Teriam que sair comitivas de caminhões cercados de carros da polícia federal para deixarem os milhões de votos armazenados em algum lugar. Aumentando ainda mais os gastos com o sistema eleitoral. Além disso, a contagem dos votos impressos, demoraria deverás e custaria contratação de recursos humanos aos cofres públicos, além de deter uma margem de erro considerável, pois humanos são mais falhos do que computadores em atividades repetitivas.

4.4 Facilitação de Fraudes.

Ao contrário do que afirma o Presidente, com o voto impresso, ficara mais fácil fraudar o Sistema Eleitoral, uma vez que se abrange as possibilidades mecânicas de viagens dos dados. Imaginem que um grupo político consiga trocar uma pacote de determinada zona eleitoral com votos impressos, com um resultado que beneficie o candidato que eles apoiem, ou que os caminhões que carreguem os votos sofram qualquer tipo de troca de malotes ou sejam até mesmo assaltados, roubando-lhes os votos. Como proceder nestas situações ?

4.5 Aumento de pedidos de recontagem de votos, contestações do resultado de eleições e acúmulo de trabalho para um Judiciário que já caminha lento.

Com centenas de milhares de processos travados, o voto impresso, traria ainda mais demanda ao Judiciário, uma vez que vasta maioria dos partidos e candidatos derrotados recorreriam ao TSE para tentarem a recontagem dos votos impressos, gerando ineficácia, lentidão e acúmulo de trabalhos á justiça.

4.6 Estímulo ao Clientelismo, Coronelismo e Voto de Cabresto.

Chama-se em Ciência Política clientelismo, o fenômeno pelo qual os candidatos compram votos a seus eleitores, com se estes fossem seus clientes. Entretanto, a compra de voto não é garantia de que este candidato ganhará, tendo em vista que o voto é secreto, o eleitor pode pegar o dinheiro e votar em outro candidato, ou até mesmo nem ir votar. Com o voto impresso, a quebra do sigilo do voto ficaria em cheque, facilitando que os compradores de votos confiram quem, dos que foram pagos, realmente os votaram. Os mesmos argumentos são validos para o coronelismo e para o voto de cabresto.

Entretanto, embora o sistema de votação brasileira seja, inviolável e não “Hackavel” como afirmara o ministro Barroso, vislumbrou-se pós eleição, o acesso ao sistema do TSE, antes do primeiro turno, pelo grupo de *Crakers* portugueses denominados *CyberTeam,* cujo chefe corresponde pelo codinome *Zambrius*. Segundo, Barroso o episódio acontecera por motivação política para desacreditar o sistema eleitoral brasileiro, ainda sobre o episódio o ministro destacou que não houve acesso aos programas relativos às eleições de 2020, uma

vez que as urnas não ficam conectadas à internet e a transmissão para a totalização dos votos é feita por uma rede própria do tribunal e o processo da soma é feito por um supercomputador exclusivamente dedicado a esse processo.

Todavia, uma máxima que existe na informática, é "Tudo pode ser decodificado, "hackeável" ou acessado, basta a pessoa que estiver tentado fazê-lo deter mais conhecimento do que a que está sendo vítima". Neste trabalho, utiliza-se dessa máxima para reafirmar a necessidade de investimentos ainda mais sisudos na área de cibernética, no que diz respeito ao sistema informatizado do TSE. Argumento ainda, que seja necessário uma aproximação maior do TSE com o Comando de Defesa Cibernética do Exército Brasileiro, ComDCiber, ligado ao gabinete de segurança institucional e por último, abrir para a participação de testes mais rotineiros em parcerias com universidades brasileira renomadas no assunto de segurança da informação, para uma constante evolução do código e possíveis alterações de segurança.

5 Referências

Eleições/Urna eletrônica/Segurança, **Tribunal superior eleitoral**, Brasília, **[s.d.]** Disponível em: <https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca>. Acesso em : 16 de Dez. de 2020.

Presidente do TSE diz que volta do voto impresso traria o caos às eleições. **Jovem pan**, São Paulo, 29 de nov. de 2020. Disponível em:<https://jovempan.com.br/noticias/politica/eleicoes-2020/presidente-do-tse-diz-que-volta-do-voto-impresso-traria-o-caos-as-eleicoes.html >. Acesso em: 13 de Dez. de 2020.

Suspeito de ataque hacker ao sistema do TSE é preso em Portugal. **Uol**, Brasília, 28 de nov. de 2020. Disponível em: <https://noticias.uol.com.br/eleicoes/2020/11/28/pf-ataque-hacker-sistema-do-tse.htm>. Acesso em: 12 de Dez. de 2020.

TSE- Mecanismos de segurança da urna eletrônica, **Tribunal superior eleitoral**, Brasília, **[s.d.]** Disponível em: <https://www.tse.jus.br/videos/tse-mecanismos-de-seguranca-da-urna-eletronica>. Acesso em : 13 de Dez. de 2020.

Victor, Nathan. Bolsonaro volta a defender voto impresso depois de votar no 2º turno do Rio. **Poder 360**, Rio de Janeiro, 29 de Nov. de 2020.Disponível em: < https://www.poder360.com.br/governo/bolsonaro-volta-a-defender-voto-impresso-depois-de-votar-no-2o-turno-do-rio/>. Acesso em: 13 de Dez. de 2020.