Tribunal Superior Eleitoral

ESTUDOS ELEITORAIS

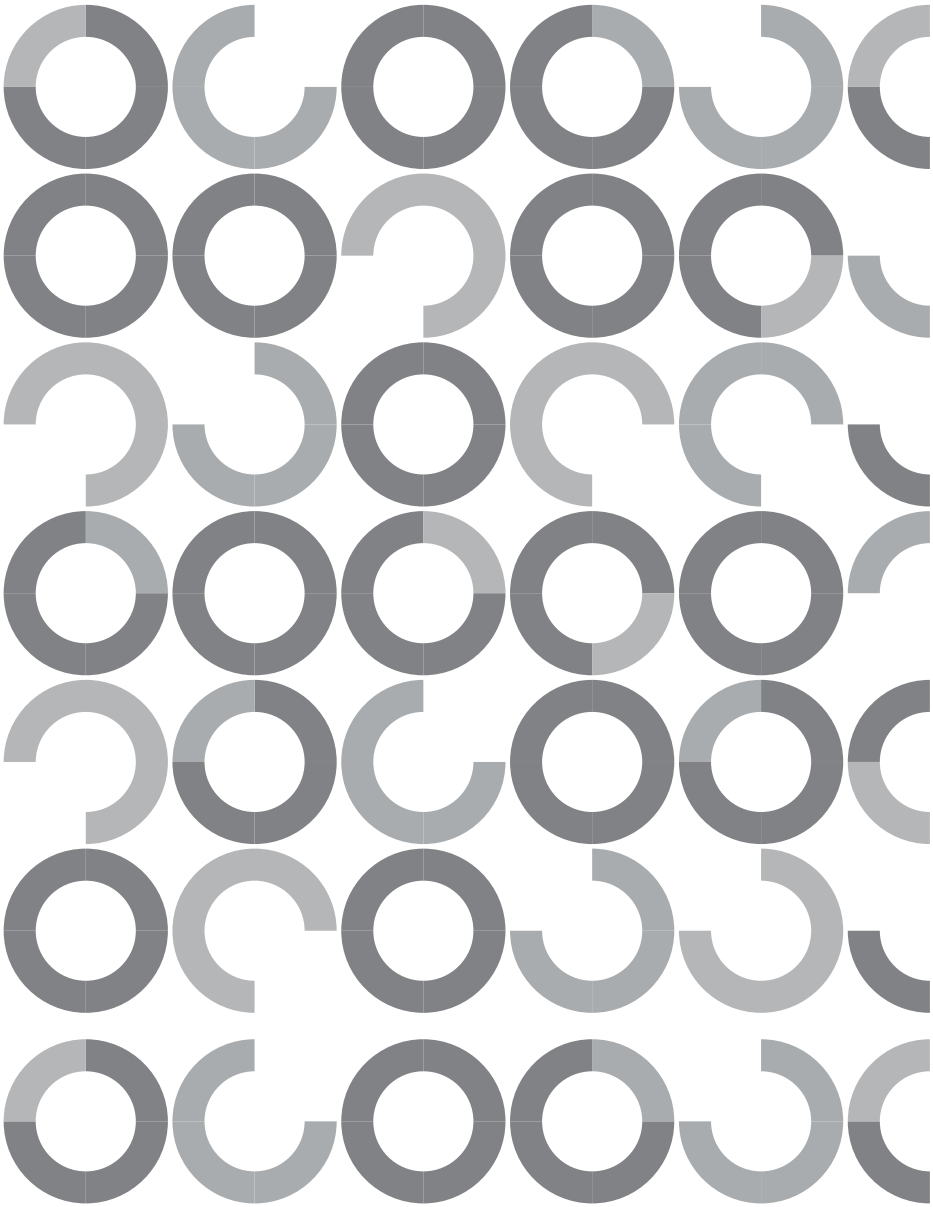
VOLUME 13 – NÚMERO 3
SETEMBRO/DEZEMBRO 2018

BRASÍLIA – 2019

ESTUDOS ELEITORAIS

A segurança da democracia e a *blockchain*

Matheus Passos Silva



A segurança da democracia e a *blockchain*[1]

The security of democracy and the blockchain

Matheus Passos Silva[2]

RESUMO

Este artigo pretende analisar a impressão do voto do eleitor para fins da confirmação estabelecida pelo art. 59-A da Lei nº 9.504/1997. Objetiva apresentar solução tecnológica que responda aos argumentos daqueles que são favoráveis e dos que são contrários a essa medida e que seja capaz de garantir os direitos fundamentais dos cidadãos. A resposta se apresenta por meio da propositura de utilização da tecnologia *blockchain* no sistema eletrônico de votação. A redação tem como base os métodos monográfico, tipográfico e estruturalista, conforme definição de Lakatos e Marconi. Conclui-se que a utilização de tal tecnologia concretiza os direitos fundamentais vinculados à capacidade eleitoral ativa.

Palavras-chave: Democracia. Processo eleitoral. Voto impresso. Voto eletrônico. *Blockchain*.

---

[1] Artigo recebido em 22.8.2018 e aprovado para publicação em 24.2.2019. https://seer.tse.jus.br/index.php/estudoseleitorais/article/view/120

[2] Doutorando em Direito, com especialização em Ciências Jurídico-Políticas pela Universidade de Lisboa (Portugal). Pesquisador da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes). Investigador voluntário do Centro de Investigação & Desenvolvimento sobre Direito e Sociedade (Cedis) da Universidade Nova de Lisboa (Portugal). Mestre em Ciência Política pela Universidade de Brasília (UnB). Pós-graduado em Direito Eleitoral pelo Instituto Brasiliense de Direito Público (IDP) e em Ética, Direito e Pensamento Político pela Universidade de Lisboa (Portugal).

ABSTRACT

This article intends to analyze the printing of the citizens' vote for confirmation purposes, as established in the art. 59-A of Law nº 9504/1997. The aim is to present a technological solution that responds to the arguments of those who are favorable and of those who oppose the printed vote and that guarantee the fundamental rights of citizens. The answer is presented through the introduction of the use of blockchain technology in the Brazilian electronic voting system. The article is based on the monographic, typographic and structuralist methods, as defined by Lakatos and Marconi. It is concluded that the use of such technology concretizes the fundamental rights linked to the active electoral capacity.

Keywords: Democracy. Electoral process. Printed vote. Electronic vote. Blockchain.

1 Introdução

Um dos aspectos mais destacados em relação à democracia atual diz respeito à ideia de voto. Significa dizer, em outras palavras, que a teoria político-jurídica dominante identifica as eleições – de maneira geral – e o voto – de maneira específica – como elementos fundamentais para o bom desenvolvimento de qualquer regime que se intitule democrático.

Para além das críticas que podem ser feitas a tal posicionamento, é necessário destacar que a democracia pressupõe, de uma forma ou de outra, a garantia ao cidadão de que sua voz será ouvida por aqueles que exercem o poder político em seu nome. Dada a atual estrutura da democracia, a qual se apresenta como representativa, é inegável que o processo eleitoral adquire importância basilar nesse mesmo processo de representação.

A estrutura constitucional-eleitoral do Brasil se vincula a tal modelo de democracia representativa. É assim que o primeiro Código Eleitoral brasileiro, de 1932, já estabelecia, em seu art. 56, o sufrágio universal, voto direto e representação proporcional – sistema que, em seu núcleo, permanece até os dias de hoje. O item 2 do inciso I desse mesmo artigo falava sobre a cédula de papel, a qual seria utilizada pelo eleitor para a emanação de seu voto.

Passados pouco mais de 60 anos da instituição desse Código Eleitoral, passou-se a utilizar, a partir de 1996, a urna eletrônica no Brasil. Com objetivo inicial de dar mais segurança e agilidade ao processo eleitoral, ao mesmo tempo em que buscava evitar a intervenção humana e eventuais fraudes, a utilização da urna eletrônica se consolidou nas eleições brasileiras desde então. As cédulas de papel ainda são utilizadas, mas apenas de maneira subsidiária quando tanto a urna eletrônica principal quanto a de substituição apresentam falhas.

Entretanto, a despeito da presença recorrente da urna eletrônica no cenário eleitoral brasileiro há praticamente duas décadas – já que as cédulas em papel foram abandonadas a partir do ano 2000 –, existem questionamentos frequentes sobre a segurança do mecanismo. O principal se refere à possibilidade de fraudes no sistema informático empregado na urna, já que, em princípio, técnicos do Tribunal Superior Eleitoral (TSE) poderiam reescrever o código de maneira a beneficiar o candidato A ou B. Nessa perspectiva, o eleitor não teria a certeza de que seu voto foi realmente computado para o candidato em quem votou. É por tais razões que determinados grupos na sociedade defendem a impressão do voto, o que viabilizaria comprovação física do resultado final da eleição em caso de contestação.

Por outro lado, outros grupos sociais argumentam que a implantação adicional do voto impresso ao voto eletrônico constituiria afronta à inviolabilidade do voto, já que possibilitaria alguém verificar em quem o cidadão votou. Além disso, argumenta-se também que o voto impresso gera custos elevados ao Estado brasileiro, o que seria inviável em tempos de restrições orçamentárias.

Nesse contexto, surge a relevância da utilização de novas tecnologias no processo eleitoral. Fala-se especificamente da tecnologia *blockchain*, que se apresenta como solução viável para garantir, por um lado, a inviolabilidade do voto e, por outro, a certeza do resultado eleitoral – sendo tais vantagens concretizadas por meio das características técnicas dessa tecnologia.

Este artigo traz argumentos favoráveis à implantação da tecnologia *blockchain* no processo eleitoral brasileiro. Para tanto, inicialmente, serão apresentadas as condicionantes jurídicas do voto no Brasil no momento atual. Em seguida, será feita explanação dos principais argumentos pró e contra o voto impresso, além de breve introdução à tecnologia *blockchain*. Por fim, serão realizados apontamentos argumentativos acerca da sua

utilização no caso brasileiro, momento em que se mostrará como tal tecnologia concretiza direitos fundamentais no âmbito da capacidade eleitoral ativa do cidadão brasileiro.

2 Aspectos jurídicos do sistema eletrônico de votação no Brasil

A principal premissa do conceito de democracia é a ideia de que tal regime político corresponde à expressão da vontade popular no exercício do poder político do Estado. É nessa perspectiva que o voto do cidadão se transforma em um dos principais pilares da democracia contemporânea.

O Estado brasileiro claramente se fundamenta em tal visão de democracia. Isso é visível já no *caput* do art. 1º da Constituição: "A República Federativa do Brasil [...] constitui-se em Estado democrático de direito [...]", texto complementado pelo parágrafo único desse mesmo artigo: "Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição" (BRASIL, 2017a, p. 11). Complementa-se tal visão, ainda sob a perspectiva constitucional, com o *caput* do art. 14, pelo qual se verifica que "a soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos" (BRASIL, 2017a, p. 21).

Já em perspectiva infraconstitucional, a importância do voto como mecanismo para concretizar o exercício do poder político por parte do cidadão encontra-se presente em alguns diplomas. Destaca-se aqui, desde já, a Lei nº 4.737, de 15 de julho de 1965, conhecida como Código Eleitoral, que, em seu art. 1º, já indica que tal diploma "[...] contém normas destinadas a assegurar a organização e o exercício de direitos políticos precipuamente os de votar e ser votado", no que é complementada pelo art. 2º: "Todo poder emana do povo e será exercido, em seu nome, por mandatários escolhidos, direta e secretamente, dentre candidatos indicados por partidos políticos nacionais [...]" (BRASIL, 1965).

Impossível não destacar também a Lei nº 9.504, de 30 de setembro de 1997, a chamada Lei das Eleições – diploma fundamental por ser o regulador de todo o processo eleitoral brasileiro, tanto em sentido amplo quanto restrito. Mais que isso: para além das disposições gerais elencadas em seus artigos iniciais, a Lei das Eleições se afigura como relevante porque é nela que se apresenta a regulamentação jurídica do sistema eletrônico de votação no Brasil, pelo que se torna necessário fazer análise mais aprofundada do seu conteúdo normativo.

O art. 59 da Lei das Eleições indica que "a votação e a totalização dos votos serão feitas por sistema eletrônico [...]" (BRASIL, 1997), ainda que o TSE possa autorizar, se assim for necessário e apenas em caráter excepcional, a utilização de cédulas impressas em papel, conforme as regras fixadas nos arts. 83 a 89. O art. 59 traz em seus parágrafos os detalhes desse sistema eletrônico, tais como a maneira de votar, o cômputo dos votos, a exibição de detalhes ao eleitor, dentre outros.

Destaca-se também o art. 61, que indica que "a urna eletrônica contabilizará cada voto, assegurando-lhe o sigilo e inviolabilidade, garantida aos partidos políticos, coligações e candidatos ampla fiscalização" (BRASIL, 1997). Esse mecanismo merece referência por buscar concretizar a perspectiva proposta no art. 14 da Constituição, que estipula a necessidade do sigilo do voto com o objetivo de garantia da liberdade do cidadão.

Importante também chamar a atenção para o art. 66, especificamente seus parágrafos, já que é nessa parte do diploma que são estabelecidos os critérios de segurança e de auditoria dos sistemas informáticos utilizados na eleição. O § 1º garante que os programas de computador do TSE poderão ser auditados por "técnicos indicados pelos partidos políticos, Ordem dos Advogados do Brasil e Ministério Público, até seis meses antes das eleições"; o § 2º indica que o TSE é obrigado a mostrar o código-fonte dos programas, bem como estes últimos, a representantes

dos partidos e coligações, para conferência; o § 3º regula a possibilidade de impugnação do código-fonte e dos programas por parte dos partidos e coligações, com novo conhecimento, por parte destes últimos, na forma do § 4º; o § 5º convoca fiscais de partidos e coligações a testemunharem a preparação das urnas, após o que serão lacradas; o § 6º fala da realização de votações paralelas com o objetivo de auditoria de verificação do funcionamento das urnas, sempre por amostragem e com presença de fiscais de partidos e coligações; e, por fim, o § 7º garante aos partidos a possibilidade de montarem sistemas próprios de fiscalização, apuração e totalização dos resultados eleitorais, inclusive recebendo os resultados oficiais da eleição (BRASIL, 1997).

Outro aspecto relevante está no art. 67 da Lei das Eleições, o qual indica:

> Os órgãos encarregados do processamento eletrônico de dados são obrigados a fornecer aos partidos ou coligações, no momento da entrega ao juiz encarregado, cópias dos dados do processamento parcial de cada dia, contidos em meio magnético. (BRASIL, 1997).

O objetivo, claramente, é o de garantir a lisura do processo eleitoral por meio da transparência na divulgação dos resultados finais, dando a todos os envolvidos a possibilidade de checar, por conta própria, tais resultados e, se for o caso, solicitar auditorias nos termos do já citado art. 66.

Por fim, importa destacar a Lei nº 13.165, de 29 de setembro de 2015, conhecida como minirreforma eleitoral, que alterou inúmeros dispositivos do Código Eleitoral e da Lei das Eleições. Mais que isso, vale indicar que é justamente esse o dispositivo que trouxe o elemento aqui em análise: o voto impresso. É o que diz o art. 2º da minirreforma eleitoral, que criou o art. 59-A na Lei das Eleições, cuja redação é a seguinte: "No processo de votação eletrônica, a urna imprimirá o registro de cada voto, que será depositado, de forma automática e sem contato manual

do eleitor, em local previamente lacrado". É relevante também indicar o texto do parágrafo único desse mesmo art. 59-A: "O processo de votação não será concluído até que o eleitor confirme a correspondência entre o teor de seu voto e o registro impresso e exibido pela urna eletrônica" (BRASIL, 1997).

Vale destacar, a título de esclarecimento, que o dispositivo não altera o sistema eletrônico de votação, como às vezes é divulgado. O que o dispositivo passa a exigir é a impressão do voto depois de o eleitor votar normalmente na urna eletrônica, como já ocorre atualmente. "Todo o conteúdo digitado aparecerá numa impressora e, posteriormente e de modo aleatório, todos aqueles votos vão cair numa urna, que ficará passível de auditagem" (BRASIL, 2018b, p. 7). Dessa forma, o voto impresso passaria a ser uma espécie de comprovante de que o cidadão efetivamente votou naqueles candidatos, atuando, dessa forma, como mecanismo de segurança para que sejam evitadas fraudes de informática.

Tendo em vista a aplicação, nas eleições de 2018, do já citado art. 59-A da Lei das Eleições, e considerando-se que, no ano de 2016, não houve a impressão do voto, conforme exigido por tal dispositivo, devido a dificuldades técnicas à época, o TSE aprovou, em 1º de março de 2018, a Resolução nº 23.521, que "regulamenta os procedimentos nas seções eleitorais que utilizarão o módulo impressor nas eleições de 2018" (BRASIL, 2018a). Esse normativo reitera alguns elementos já indicados no próprio art. 59-A, ao mesmo tempo em que o complementa com indicações explícitas que visam à garantia do sigilo do voto do eleitor, evitando sua identificação. São também descritos todos os procedimentos em relação à segurança física dos equipamentos, tais como lacres, e aos seus procedimentos de instalação.

Em suma, o procedimento eleitoral ocorrerá da seguinte maneira: 1) o eleitor escolhe na urna eletrônica seus candidatos, da mesma forma que já faz atualmente; 2) será exibida tela-resumo na qual o eleitor poderá

conferir se seus votos foram realmente direcionados aos candidatos escolhidos; 3) uma vez de acordo, o eleitor pressiona a tecla "Confirma", ocorrendo então o registro do voto eletrônico, a impressão do voto e o depósito automático da impressão na urna. Se o eleitor não estiver de acordo, deverá então pressionar a tecla "Corrige", sendo impresso o comprovativo de cancelamento – o qual também será depositado automaticamente na urna – com o reinício do procedimento (BRASIL, 2018a, p. 4-5).

É de se destacar, ainda com base na Resolução nº 23.521, que o voto impresso busca garantir ao eleitor que efetivamente há correspondência entre o que foi por ele digitado na urna eletrônica e os dados que são processados por este equipamento. Apenas de maneira subsidiária, considera-se a possibilidade de recontagem de votos em caso de eventuais impugnações. Da mesma maneira, o voto impresso só terá validade para ser utilizado como definidor do resultado eleitoral caso haja perda total dos resultados eletrônicos (BRASIL, 2018a, p. 19). Reitera-se, portanto, o caráter eletrônico da votação, conforme *caput* do art. 59 da Lei das Eleições.

Entretanto, a despeito da existência de resoluções do TSE referentes à implantação do sistema de voto impresso e da legislação a respeito do tema, o Supremo Tribunal Federal (STF) deferiu liminar que suspende a aplicação do art. 59-A nas eleições de 2018. A Ação Direta de Inconstitucionalidade nº 5889, proposta pela Procuradora-Geral da República (PGR), argumenta que tal artigo coloca em risco o sigilo e, consequentemente, a liberdade do voto. Argumentou-se também que "a adoção do modelo impresso provoca risco à confiabilidade do sistema eleitoral, fragilizando o nível de segurança e eficácia da expressão da soberania nacional por meio do sufrágio universal" (BRASIL, 2018c, p. 2).

A decisão do STF, fundada no voto do Ministro Alexandre de Moraes, apontou que a regra "coloca em risco o sigilo da votação" e que, com isso, estaríamos arriscando também "a outra característica: o voto secreto,

universal e livre". O Ministro indicou ainda que "o registro impresso e sua conferência pelo eleitor possibilita que seu conteúdo seja acessado por outras pessoas, até mesmo mesários, trazendo de volta memórias do 'voto de cabresto' existente no Brasil". Por tais motivos, a cautelar foi concedida nos termos do pedido feito pela PGR (BRASIL, 2018d).

Uma vez feita a caracterização jurídica da situação referente ao voto impresso, bem como delineada a situação fática em que esse processo se encontra no momento de redação deste artigo (junho de 2018), é interessante destacar os prós e contras desse sistema. É a isso que se dedica a próxima seção.

3 Os prós e contras do voto impresso

Uma vez estabelecida a impressão do voto do eleitor pela minirreforma eleitoral, surgiram inúmeros questionamentos a respeito do tema, tanto de maneira favorável quanto de maneira contrária. A seguir, será feita síntese dos principais argumentos favoráveis e também dos desfavoráveis ao voto impresso.

3.1 Os argumentos a favor do voto impresso

A defesa do voto impresso se dá principalmente em torno da questão da segurança do resultado eleitoral, que pode, nessa perspectiva, estar comprometida devido à possibilidade de fraudes no sistema eletrônico utilizado pelo TSE para a totalização e apuração dos votos.

Um dos principais representantes daqueles que consideram que a urna eletrônica é extremamente vulnerável é o professor Diego Aranha[3]. Atualmente vinculado à Universidade Estadual de Campinas (Unicamp),

[3] Existem outros críticos do atual sistema informático utilizado pelo TSE. Entretanto, os argumentos, em geral, são os mesmos. É por esse motivo que se optou aqui pela centralização das críticas em torno do prof. Diego Aranha.

Aranha participou de testes públicos promovidos pelo TSE em 2012 e em 2017. O objetivo de tais testes, conduzidos pelo próprio Tribunal, é o de buscar vulnerabilidades tanto no hardware quanto no software da urna eletrônica.

No teste de 2012, o professor, em conjunto com sua equipe, conseguiu efetivamente quebrar o protocolo de segurança da urna eletrônica. Ficou comprovado, à altura, que era possível a ocorrência de infrações no que diz respeito ao sigilo do voto. Segundo o professor, foi possível, depois da realização de eleição simulada, "recuperar os votos em ordem, baseado apenas em informação pública. A hora de emissão da zerésima[4] era a informação que a gente precisava para descobrir como votou o primeiro eleitor, o segundo eleitor, o terceiro eleitor e assim por diante". Ainda segundo ele, em seus testes, não foi efetivamente possível descobrir quem eram o primeiro, o segundo e o terceiro eleitores – o que permitiria identificar em quem cada eleitor havia votado –, mas isso seria fácil de ser obtido "com a ajuda de um mesário malicioso" (PAYÃO, 2017).

Outra forma identificada pelo professor de descobrir em quem um cidadão teria votado diz respeito ao fato de que a urna armazena o horário de votação de cada um dos eleitores. Consequentemente, de posse do horário de emissão da zerésima de determinada seção eleitoral – que é informação pública –, de arquivo que se chama Registro Digital do Voto[5] (que coloca os votos embaralhados e também é informação pública para os partidos) e do horário em que tal cidadão votou, uma pessoa seria capaz de descobrir em quem esse cidadão teria votado (PAYÃO, 2017).

[4] A "zerésima" corresponde ao relatório que traz toda a identificação da urna eletrônica, sendo emitido no momento em que a urna é ligada no dia da eleição. O relatório comprova que estão registrados todos os candidatos e que não há voto computado, ou seja, a urna tem "zero votos". Após a impressão da zerésima, o presidente da seção, os mesários e os fiscais dos partidos ou coligações que estiverem presentes devem assiná-la.

[5] Criado pelo § 4º do art. 59 da Lei das Eleições: "A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor" (BRASIL, 1997).

O professor Diego Aranha identificou ainda outra possível vulnerabilidade: o software de criptografia estava embutido no próprio programa das urnas eleitorais. Significaria dizer, segundo o professor, que, ainda que tal problema não tivesse sido efetivamente verificado por falta de tempo, já que os testes públicos duraram apenas três dias naquele ano de 2012 (PAYÃO, 2017), existiriam "ao menos 500 mil cópias dessa informação às claras em cartões de memória", ao que acrescenta: "não dá nem para chamar isso de segredo". O professor, entretanto, acredita que, desde 2012, o TSE já deve ter realizado mudanças para prevenir tais vulnerabilidades.

Outro aspecto relevante destacado por Aranha diz respeito ao custo de eventual invasão aos sistemas eleitorais do TSE. Segundo ele, "os mecanismos de segurança que estavam no sistema não ofereciam custo proibitivo para algum atacante minimamente sofisticado". Além disso, o professor destaca também que "se você compromete alguém, por exemplo, que esteja dentro do TSE para escrever software que vai roubar votos para alguém, isso tem (em tese) custo muito mais barato do que comprar 100 mil votos em uma cidade", sendo esse, portanto, "um ponto tentador de ataque, que concentra risco" (PAYÃO, 2017).

Como o registro do voto no Brasil é exclusivamente eletrônico, o professor Diego Aranha acredita que o sigilo e a segurança do voto, bem como a real correspondência entre a intenção do eleitor e o resultado da eleição, são elementos que dependem "diretamente da qualidade do software de votação e de sua resistência contra manipulação por agentes internos e externos". Com base em tais argumentos, o professor defende o surgimento de um sistema eleitoral que seja "minimamente auditável e transparente". Em sua visão, isso só ocorreria se houvesse não apenas a melhoria da segurança do software de votação e dos seus processos de auditoria, "mas também da implantação de mecanismos que permitam

ao eleitor verificar se o sistema registra sua intenção corretamente" (PAYÃO, 2017), sendo o professor defensor declarado do voto impresso.

Vale destacar que a visão do professor não se alterou após os testes de 2017. Em palestra realizada na Unicamp em 2018, Diego Aranha voltou a afirmar que, tanto em 2012 quanto em 2017, nos testes públicos do TSE, foram constatadas falhas na urna eletrônica. Nestas duas edições, foram encontradas "múltiplas vulnerabilidades nos sistema", o que "permitiu explorar e violar as principais propriedades de segurança do equipamento, que são o sigilo do voto e a integralidade do *software* de votação para que não se comporte de maneira honesta durante a eleição" (PAIVA, 2018).

Duas dessas falhas são vistas como gravíssimas. A primeira delas diz respeito à possibilidade de modificação dos arquivos do sistema informático sem a necessidade de autenticação via assinatura digital. A segunda se refere à facilidade com que o grupo do professor da Unicamp conseguiu rodar outros programas que poderiam manipular e alterar o funcionamento do que controla a votação, sendo possível, por exemplo, interferir na contagem final dos votos (MARTINS, 2018).

Além disso, como os programas do TSE contêm mais de 13 milhões de linhas de código, seria plenamente possível que algum servidor interessado no resultado A ou B das eleições inserisse linha maliciosa no programa, o qual seria distribuído em todas as urnas em todo o país. Como é praticamente impossível auditar tal quantidade de códigos – segundo Diego Aranha –, a votação exclusivamente eletrônica seria perigosa para o resultado eleitoral (MARTINS, 2018).

Em síntese, pode-se afirmar que a grande preocupação daqueles que se posicionam contra o voto exclusivamente eletrônico se fundamenta especialmente na possibilidade de fraudes informáticas. Conforme fica demonstrado, o atual sistema utilizado pelo TSE contém vulnerabilidades

que são preocupantes, especialmente quando se considera o voto secreto presente no *caput* do art. 14 da Constituição/1988. Além disso, a própria alegação do TSE, responsável por corrigir os erros para as próximas eleições, confirmaria, a contrario sensu, que existem falhas no sistema atual (BRUNAZO FILHO, 2018). É por tal motivo que, nessa visão, o voto impresso se torna ferramenta indispensável à lisura do processo eleitoral.

3.2 Os argumentos contrários ao voto impresso

Os principais argumentos daqueles que se apresentam como contrários ao voto impresso fundamentam-se principalmente em questões de ordem econômica, sem desconsiderar, é claro, eventuais infrações a princípios constitucionais. Nesse sentido, as principais críticas estão sintetizadas na já citada ADI nº 5889, de autoria da PGR.

Sob perspectiva jurídica, argumenta-se, na ADI, que o sistema de voto impresso infringe frontalmente "o direito fundamental do cidadão ao sigilo de voto", fragilizando, consequentemente, a soberania popular. Além disso, a proposta iria também contra o princípio da eficiência presente no art. 37 da Constituição (BRASIL, 2018c, p. 2). Isso se dá porque, segundo a PGR, o art. 59-A da Lei das Eleições "não explicita quais dados estarão contidos na versão impressa do voto, o que abre demasiadas perspectivas de risco quanto à identificação pessoal do eleitor, com prejuízo à inviolabilidade do voto secreto" (BRASIL, 2018c, p. 3).

Outro argumento elencado diz respeito a eventuais falhas mecânicas no equipamento de impressão, o que levaria à necessidade de intervenção humana para solução e, assim, à violação do sigilo do voto do cidadão. O mesmo ocorreria, ainda segundo a PGR, com as pessoas com deficiências visuais e analfabetas, que necessitariam de auxílio de terceiros e, consequentemente, teriam o sigilo do voto violado (BRASIL, 2018c, p. 3).

Por conseguinte, afirma-se que "a reintrodução do voto impresso como forma de controle do processo eletrônico de votação caminha na contramão da proteção da garantia do anonimato do voto e significa verdadeiro retrocesso", já que a implantação da urna eletrônica ocorreu, dentre outros argumentos, justamente para garantir e reforçar o princípio do sigilo ao voto (BRASIL, 2018c, p. 3).

Reforça o Parquet a argumentação ao afirmar que, a despeito das inúmeras alegações de fraudes, nenhuma jamais foi comprovada, o que reforça a impossibilidade de – em suas palavras – retrocesso ao voto impresso (BRASIL, 2018c, p. 4). Ainda, argumenta-se que a reintrodução do voto impresso levaria ao surgimento de novas vulnerabilidades no processo eleitoral – como, por exemplo, a manipulação das cédulas impressas –, as quais poderiam ser exploradas em benefício particular e em detrimento da coletividade (BRASIL, 2018c, p. 6).

Como o art. 59-A da Lei das Eleições cria "um ônus material, técnico e, sobretudo, financeiro para a realização do direito do voto, que não se mostra apto para o objetivo a que visa – a maior idoneidade do pleito", tornando, ao contrário, "mais complexo, custoso, demorado, problemático e suscetível de desconfianças e questionamentos o sistema que [...] alterou" (BRASIL, 2018c, p. 6), deve-se considerar a sua inconstitucionalidade. Reforça-se o pedido indicando que o voto impresso vai contra o princípio da eficiência do aparelho estatal, com base nos argumentos já apresentados anteriormente.

Para além dos argumentos constitucionais, há ainda os de ordem econômica. Em fevereiro de 2017, o TSE estimou em 1,8 bilhão de reais o custo total para a implantação do sistema com voto impresso (BRASIL, 2017b). Por sua vez, em julho do mesmo ano, o TSE estimou que o gasto total em dez anos seria de 2,5 bilhões de reais (MOURA; PIRES, 2017).

Há de se destacar ainda os argumentos referentes à demora no processo eleitoral. Argumenta-se que a existência do voto impresso fará com que aumente o tempo gasto pelo cidadão na cabine eleitoral, já que ele precisará não apenas digitar os números mas também conferir se tudo está correto antes da impressão do voto. Assim, há a preocupação com o aumento de filas e de incômodos ao cidadão, além de eventuais problemas para o processo como um todo.

Outro aspecto destacado por aqueles que são contrários ao voto impresso diz respeito às especificidades da aplicação do art. 59-A. A legislação não define, por exemplo, por quanto tempo devem ficar armazenados os votos impressos, nem mesmo onde isso ocorreria, o que leva a questionamentos acerca da privacidade dos dados ali contidos (FLORES, 2018).

Vale destacar ainda que, na visão dos críticos ao sistema de voto impresso, esse sistema abre a possibilidade de coação do cidadão, por parte de terceiros, a votarem em candidatos específicos. Em consequência, seriam violados inúmeros princípios constitucionais, o que viria a fragilizar, em última instância, a democracia brasileira.

O último aspecto a ser indicado diz respeito à intervenção humana no processo eleitoral, o que facilita a ocorrência de fraudes. Se aqueles que são favoráveis ao voto impresso indicam a mão humana como sendo a fonte de possíveis fraudes no código do sistema eletrônico, os grupos contrários ao voto impresso também a responsabilizam por problemas de "lentidão, erro e fraude" (ZANINI, 2018).

Segundo um dos criadores da urna eletrônica, Giuseppe Janino, "o risco de fraude na produção das urnas não existe", já que todo o projeto é desenvolvido pelo TSE. Além disso, a fabricação das urnas é supervisionada e acompanhada por técnicos do órgão, evitando eventuais alterações. Ele reforça ainda que "o cartão de memória que

carrega os resultados é protegido por um lacre especial feito pela Casa da Moeda", sendo, portanto, impossível haver qualquer tipo de violação sem a existência de rastros que indiquem quem cometeu tal violação. A segurança da urna, segundo seu criador, é garantida ainda pelo fato de ela não se encontrar conectada a nenhuma rede, o que impede a sua violação (ZANINI, 2018).

Percebe-se, por todo o exposto, que os argumentos contrários e favoráveis ao voto impresso são, cada qual à sua maneira, razoavelmente plausíveis e robustos. Dessa forma, torna-se necessário encontrar um sistema tecnológico que, por um lado, concretize os direitos fundamentais dos eleitores e, por outro, garanta toda a lisura no processo eleitoral. É a respeito disso que se falará a seguir.

4 A tecnologia *blockchain* pode trazer benefícios ao processo eleitoral(?)

Como foi mostrado na seção anterior, existem vários – e bons – argumentos a favor do voto impresso. Entretanto, o mesmo pode ser dito daqueles que se posicionam de maneira contrária a tal sistema. Independentemente do lado escolhido, fato é que as inovações tecnológicas que surgem a cada dia podem se transformar em soluções para a garantia de princípios constitucionais, tais como o sigilo do voto e a eficiência do Estado, de um lado, ao mesmo tempo em que buscam solucionar problemas atualmente existentes, nomeadamente a própria possibilidade de quebra desse sigilo existente no sistema atual. É em direção a uma dessas inovações tecnológicas que este artigo caminha agora, indicando não apenas a própria inovação em si mas também as possibilidades técnicas e jurídicas de sua aplicação no sistema eletrônico de votação no Brasil.

4.1 O que é a tecnologia *blockchain*?

O ano de 2017 viu o surgimento avassalador na mídia do tema das moedas digitais, capitaneado pela principal delas – o Bitcoin (BTC). Vale dizer, a título exemplificativo, que essa moeda digital chegou a valer R$69.912,00 no dia 17 de dezembro daquele ano. O furor com as moedas digitais era justificado: exatamente um ano antes dessa data o BTC valia R$2.760,00[6] – crescimento de 2.535% em um único ano, muito superior a qualquer outro tipo de investimento.

Outras moedas digitais tiveram um desempenho ainda melhor que o BTC. A Ether (ETH), conhecida como a "prata" das moedas digitais, valia 9,92 dólares em 13 de janeiro de 2017. De maneira surpreendente, exatamente um ano depois, a ETH chegou a 1.385,00 dólares – ou seja, uma valorização de 13.955% em um único ano[7]. Não há dúvida de que os números impressionam.

Entretanto, há algo que está para além dos números e das próprias moedas e a respeito do qual pouco se fala: qual é a tecnologia que elas utilizam? Considerando-se que são moedas digitais, necessariamente precisa haver algo que as crie no mundo virtual. Esse algo a que se faz referência diz respeito à chamada tecnologia *blockchain*, que vai muito além de transações financeiras e das moedas digitais.

De maneira simplificada, uma *blockchain* corresponde a uma cadeia de blocos armazenados de maneira sequencial, ou seja, "uma estrutura de dados feita como uma grande corrente com blocos encadeados e validados entre si" (ORIGINALMY, 2018). Cada bloco é composto

[6] Informação obtida por meio da plataforma TradingView, conforme valores negociados na corretora Mercado Bitcoin. Disponível em: https://br.tradingview.com/chart/?symbol=MERCADO:BTCBRL. Acesso em: 20 jun. 2018.

[7] Informação obtida por meio da plataforma TradingView, conforme valores negociados na corretora Coinbase. Aqui foi utilizado o valor em dólar por não haver negociação de ETH em reais nas corretoras brasileiras. Disponível em: https://br.tradingview.com/chart/?symbol=COINBASE:ETHUSD. Acesso em: 20 jun. 2018.

por transações diversas, as quais, por sua vez, podem conter os mais diferentes tipos de informação. O exemplo geralmente utilizado associa a *blockchain* a um livro-razão, já que as diversas informações são anotadas sequencialmente e dependentes umas das outras – ou seja, por um lado, o bloco de informações "B" necessariamente depende do bloco "A" e, por outro, é a base do bloco "C", que será incluído posteriormente.

A princípio, pode-se dizer que essa descrição da tecnologia não difere muito do que se tem na atualidade. Se alguém estiver, por exemplo, registrando, em maio, seu planejamento financeiro – gastos com água, luz, telefone, alimentação, etc. –, basta abrir planilha do Excel e indicar em uma coluna o quanto recebeu de salário e, em outra, o quanto gastou, fazendo a conta ao final. Ao passar para o mês de junho, tal pessoa simplesmente copiaria o crédito (ou débito) do mês anterior e recomeçaria os cálculos. Nessa lógica, também estão presentes os elementos definidores da *blockchain* – a ideia de sequência e a ideia de dependência de um dado em relação a outros.

Entretanto, tal lógica do Excel é válida apenas se considerarmos que os dados são centralizados – como é o caso no exemplo dado. Mais que isso, é importante destacar que o sistema atual de armazenamento de dados[8] se fundamenta também na ideia de confiança: é necessário acreditar que aquele que grava e armazena os dados seja confiável para mantê-los seguros e imutáveis no tempo. Mas o que ocorreria com os dados se ocorresse pane no computador dessa pessoa? Mais ainda: em se tratando de dados públicos, é possível confiar em instituições?

É nessa perspectiva que surge a segunda característica da tecnologia *blockchain*: os dados gravados nos blocos são descentralizados. Significa dizer que não será uma única pessoa ou instituição a responsável por

[8] Por "sistema atual de armazenamento de dados" deve-se compreender qualquer tipo de tecnologia que não a *blockchain*.

armazenar e proteger os dados contidos nos blocos: todos aqueles que tiverem acesso à rede *blockchain* armazenarão cópia exatamente igual a todas as outras armazenadas por todos os outros membros daquela rede. O princípio por trás da descentralização é o da segurança: ocorrendo falhas técnicas em um dos computadores ligados à *blockchain*, os dados não serão perdidos, já que todos os outros possuem cópia.

Uma terceira característica da tecnologia *blockchain* diz respeito também à segurança, mas em outro sentido: os dados gravados na *blockchain* são imutáveis. A título de exemplo, imagine o leitor a existência do bloco "A" contendo dados "X". O bloco "A" contém espécie de assinatura eletrônica – o chamado *hash*, que é único e dependente de cálculos matemáticos que foram feitos quando de sua criação.

Quando um novo bloco (o bloco "B") está pronto para ser gravado na *blockchain*, os computadores conectados à rede vão utilizar o *hash* do bloco "A" para verificar se ele é válido. Uma vez que os computadores conectados à rede realizem os mesmos cálculos matemáticos e comprovem que o *hash* é válido, o bloco "B" é gravado no banco de dados, vinculando-se, por um lado, ao bloco "A" e, por outro, criando seu próprio *hash*, que poderá ser utilizado futuramente quando da gravação de um novo bloco "C" em sequência.

A partir do momento em que número suficiente de computadores – geralmente 51% – aceita a gravação do bloco "B" no banco de dados, tal bloco passa a ser imutável dentro da *blockchain* – é o que se chama de confirmação. A imutabilidade é decorrente não apenas do número crescente de confirmações, mas também – e principalmente – pelo fato de que, como cada bloco tem seu próprio *hash* (que depende do conteúdo ali armazenado), eventuais tentativas de alteração do conteúdo do bloco gerariam novo *hash*, conflitando com o original. Verifica-se, portanto, que a decisão de gravar ou não um novo bloco na *blockchain* depende do consenso entre os usuários e não apenas da "vontade" da entidade controladora da rede.

A título de exemplo, imagine o leitor que seja gravada, no bloco "A", a palavra "lápis", identificando-se tal objeto como um "mecanismo que permite a escrita em papel". O bloco "A" criaria, nesse exemplo hipotético, o *hash* número 5, correspondente ao número de letras da palavra "lápis". Os computadores conectados a essa rede verificariam que a palavra realmente possui cinco letras e, portanto, confirmariam que o *hash* do bloco "A" corresponde ao número 5.

Entretanto, suponha-se que alguém mal intencionado decidisse alterar o conteúdo do bloco "A" de "lápis" para "caneta", argumentando que o segundo objeto também é um "mecanismo que permite a escrita em papel". Se tal alteração fosse válida, o cálculo matemático indicaria que agora o *hash* do bloco "A" seria 6. Porém, já foram feitas inúmeras confirmações referentes ao *hash* do bloco "A" como sendo 5, não 6. Tal alteração, portanto, seria invalidada pelos próprios computadores pertencentes à rede, pois todos eles já gravaram o número 5 como sendo o *hash* do bloco "A".

Usando o exemplo prático do BTC, sua rede *blockchain* estabelece que "após 6 blocos serem adicionados no topo da cadeia, é impossível alterar qualquer transação anterior a eles no bloco, uma vez que a capacidade de processamento requerida para isso torna inviável a mudança" (GATES, 2017, posição 279-80). Portanto, justamente em razão desse encadeamento dos blocos, para se fraudar uma operação na rede BTC seria necessário alterar as informações de todos os blocos anteriores. Se uma transação está registrada no bloco 10, por exemplo, quando for colocado o 16º bloco na cadeia, aquele 10º bloco se tornará tecnicamente imutável. A quantidade de blocos pode variar de rede para rede, mas o importante é compreender que, depois de certo número de novos blocos, a operação se torna imutável, garantindo-se, portanto, a segurança do conteúdo ali gravado.

A importância da tecnologia *blockchain* reside também no fato de que ela pode ser utilizada para registrar qualquer coisa de valor, tais como moedas digitais, identidades digitais, dados de redes sociais e, inclusive, registros eleitorais de votação. Portanto, não se pode nunca confundir o BTC – a moeda digital mais conhecida – com a *blockchain*: o BTC se fundamenta na tecnologia *blockchain* para funcionar. Existe, portanto, a *blockchain* do BTC, a *blockchain* do ETH e assim sucessivamente.

Em síntese, portanto, vale destacar os seguintes benefícios da tecnologia *blockchain*: 1) transparência, pois as operações realizadas nos blocos são visíveis a todos que fazem parte da rede[9]; 2) remoção de intermediários, já que as transações são feitas diretamente pelos membros da rede; 3) descentralização, posto não haver um centro específico no qual estão armazenados os dados – o que evita ataques de *hackers* bem como as consequências indesejadas pela queda de um servidor e perda de dados; 4) confiança, pois a manutenção dos dados na *blockchain* depende da atuação conjunta de todos os membros da rede; 5) segurança decorrente da imutabilidade dos dados, prevenindo fraudes e manipulações, sendo que alterações ou remoções do conteúdo não são possíveis depois de um número "X" de confirmações – inclusive com facilidade de auditoria, já que o bloco posterior sempre conterá elementos identificadores do bloco anterior e também dos computadores que o alterou; 6) custos reduzidos, já que a remoção de intermediários e de vários estágios na prestação do serviço ou do produto permite a redução significativa de custos; e 7) rapidez nas transações, justamente pela ausência de intermediários (GATES, 2017, posição 682-709).

[9] Não confundir a ideia de transparência na realização das transações com possibilidade de saber o conteúdo dos dados. A transparência diz respeito ao fato de que todos os computadores conectados a uma *blockchain* irão ver que estão sendo gravados os blocos A, B e C, mas não conseguirão ver o conteúdo que está gravado em tais blocos de informação.

É claro que a tecnologia tem também seus pontos negativos. Nesse sentido, destaca-se: 1) a falta de privacidade, especialmente se a *blockchain* for pública e/ou aberta; 2) a preocupação de perda de conteúdo, principalmente quando o indivíduo perde ou esquece sua chave privada[10]; 3) a ausência de controle central, já que a aceitação depende do consenso da rede; 4) o risco do chamado "ataque de 51%", situação na qual agentes mal intencionados obtêm o controle de mais de 51% do poder computacional da *blockchain* e, portanto, poderiam confirmar alterações no conteúdo que não condizem com a realidade; 5) o fato de a *blockchain* ser uma tecnologia nova, ainda não testada em médio e longo prazos; 6) os gastos de energia elétrica em alguns tipos de *blockchain*, com possíveis consequências ambientais; 7) os problemas de escala, especialmente no que diz respeito ao volume de transações por segundo; 8) as questões referentes à reputação da tecnologia, que muitas vezes é associada exclusivamente às criptomoedas e ao lado negativo destas; 9) a falta de compreensão da tecnologia, não apenas por parte do público em geral mas também por parte razoável dos próprios analistas de TI; 10) a ausência de regulação e de integração aos sistemas atuais; e 11) a exagerada propaganda sobre a tecnologia, que é muitas vezes apresentada como panaceia para todos os problemas atuais (GATES, 2017, posição 904-289).

Feitas essas considerações, vale agora responder à pergunta: as vantagens da tecnologia *blockchain* podem suplantar suas desvantagens e, assim, solucionar os problemas existentes na seara eleitoral apresentadas na seção 1? É o que será respondido a seguir.

[10] Para uma explicação sucinta, mas bem fundamentada, da distinção entre chaves públicas e privadas ver Figueiredo, 2018, p. 12-4.

4.2 A viabilidade da *blockchain* nas eleições brasileiras

A resposta à pergunta apresentada na subseção anterior passa necessariamente por dois aspectos: o técnico e o jurídico. É necessário verificar, por um lado, se a tecnologia *blockchain* pode ser devidamente utilizada no processo eleitoral brasileiro, nomeadamente nas eleições; por outro, é necessário também verificar se a utilização dessa tecnologia infringe normas do sistema eleitoral brasileiro, bem como se há algum impedimento constitucional à sua utilização.

Tal questionamento é interessante, especialmente quando se transfere o exemplo do Excel, anteriormente apresentado, para o âmbito público, nomeadamente para a questão das eleições. Verifica-se que, no caso brasileiro, os dados eleitorais são, por um lado, necessariamente centralizados no TSE, mas, por outro, não há a necessária confiança de que tais dados referentes ao resultado das eleições se mantenham imutáveis – ou seja, que o voto dado pelo eleitor ao candidato "A" seja efetivamente computado para esse mesmo candidato, como mostrado na seção 2.1.

Do o ponto de vista técnico, parece não haver dúvidas a respeito da possibilidade de uso da tecnologia *blockchain* em âmbito eleitoral. Os argumentos técnicos se fundamentam especialmente nas características da imutabilidade dos dados, da segurança, por ser um sistema descentralizado, e pela garantia da confiança no momento de gravação dos dados.

É claro que eventual sistema eleitoral baseado em *blockchain* precisaria de determinados ajustes e considerações específicas. Em primeiro lugar, é importante destacar que a "*blockchain* do TSE" precisaria ser do tipo privada, não pública. Em resumo, uma *blockchain* privada é aquela em que apenas membros autorizados por autoridade central podem encadear os blocos, gravando dados no sistema, enquanto que, na *blockchain* pública, qualquer

pessoa pode ter acesso a tais dados. É também possível, na *blockchain* privada, restringir os dados de leitura, permitindo ou não que seja lido o conteúdo dos dados nos blocos (PILKINGTON, 2016, p. 10-11).

Em segundo lugar, é necessário decidir o tipo de sistema que seria utilizado no que diz respeito à participação do eleitor: se ele continuaria votando pelo sistema atual, em que se dirige a uma cabine eletrônica colocada na seção eleitoral – sendo a urna eletrônica conectada à "*blockchain* do TSE" – ou se seria permitida a votação a distância, sem a presença do eleitor – por exemplo, via algum aplicativo de celular ou via algum *website*.

Um terceiro aspecto relevante diz respeito à identidade do eleitor: é importante garantir que a pessoa que estiver votando seja realmente ela mesma. A existência de uma espécie de identidade digital é elemento central em um sistema descentralizado baseado em *blockchain*, já que a gravação dos dados precisaria necessariamente passar pela comprovação de que aquela pessoa é realmente ela, e não alguém votando em seu lugar.

Por fim, mas não menos relevante, é fundamental garantir a privacidade do voto do eleitor. Por esse motivo, mencionou-se acima a necessidade de utilização de rede privada, não pública, para o eventual uso da tecnologia *blockchain* em eleições. Entretanto, o problema aqui não é tanto técnico, senão cultural: em eventual sistema fundado em *blockchain*, o cidadão nunca poderá compartilhar a chave privada de sua identidade digital. É na distinção entre chaves públicas e privadas que se garantem ao cidadão a privacidade e o sigilo de voto.

Por sua vez, sob a perspectiva jurídica, parece também não haver nenhum impedimento à utilização da tecnologia *blockchain* na área de votação e totalização de votos. O art. 59 da Lei das Eleições, referido na seção 1 deste artigo, indica apenas que a votação e a totalização serão realizadas por sistema eletrônico, sem indicar explicitamente qual tipo de

sistema eletrônico será utilizado. O § 5º desse mesmo artigo dispõe que "caberá à Justiça Eleitoral definir a chave de segurança e a identificação da urna eletrônica de que trata o § 4º" (BRASIL, 1997), tendo este último já sido referido também na seção 1. Ainda no mencionado artigo, o § 6º está devidamente adequado à *blockchain*, já que exige o registro do horário e do arquivo de boletim da urna eletrônica, elementos cuja segurança pode ser reforçada por meio da própria lógica da *blockchain* acima explicada, nomeadamente a questão da imutabilidade dos dados.

Já o art. 61 da mesma lei, que trata do sigilo e da inviolabilidade do voto, ao mesmo tempo em que garante a fiscalização por parte de partidos e coligações também permite a aplicação da *blockchain*, especialmente considerando-se o fato de que apenas aqueles que forem autorizados poderão gravar dados em uma rede privada – mais que isso, apenas outros autorizados poderão confirmar a autenticidade desses dados sem, contudo, identificar quem é o eleitor.

Da mesma forma, sob a perspectiva constitucional – e considerando-se as preocupações elencadas pela PGR e indicadas na seção 2.2 deste artigo –, a tecnologia *blockchain* também se apresenta como solução viável aos problemas ali indicados. A partir do momento em que apenas os cidadãos têm acesso às suas chaves privadas – ou pelo menos assim se espera que seja, como atualmente se espera que as pessoas não divulguem aos outros o seu voto ou que não divulguem sua senha de banco a terceiros –, apenas eles saberão em quem votaram, garantindo o sigilo e a liberdade de voto. Por outro lado, considerando-se a imutabilidade dos dados que são registrados na *blockchain*, as preocupações com fraudes eletrônicas perdem a razão de ser – desde que, novamente, utilize-se uma *blockchain* privada.

A exemplificação mais clara desse argumento encontra-se em algo que está presente no início deste artigo. O leitor atento deve ter percebido que a autoria foi indicada tendo-se por base a chave pública do autor,

disponível na *blockchain ID* de determinada empresa que cria identidades digitais no Brasil. O leitor é livre para fazer a busca dessa chave pública em redes *blockchain* por inúmeros sites na internet. Ao fazê-lo, encontrará o número de transações realizadas por este ID. Também poderá ver todo o histórico de transações realizadas por este ID, sem, entretanto, saber qual é o conteúdo de tais transações. Da mesma forma, o leitor não saberá a quem pertence este ID. Aplicando-se tal raciocínio a uma eleição, significa dizer que seria possível verificar a quem o voto se dirige sem, contudo, identificar o eleitor. Garante-se, dessa forma, o sigilo do voto e, ao mesmo tempo, a impossibilidade de fraudes em uma eleição.

5 Considerações finais

É inegável que o sistema eletrônico de votação e de apuração de votos no Brasil precisa de melhorias. Por mais que o TSE sempre afirme que o sistema é seguro e que é impossível a existência de grandes fraudes, fica sempre o questionamento: e as pequenas fraudes? E aquelas situações em que, sob o sistema eletrônico atual, o cidadão não comparece à cabine de votação, mas depois verifica que foram computados votos em seu nome? Tais situações precisam ser solucionadas para que a democracia brasileira se robusteça e faça jus ao seu título.

Por outro lado, as mudanças precisam, sem dúvida alguma, levar em consideração direitos fundamentais basilares de todos os cidadãos brasileiros, seja de maneira individual – nomeadamente o direito ao sigilo de voto –, seja de maneira coletiva – como a eficiência do Estado. É necessário pensar a respeito de um sistema tecnológico que garanta tais direitos, os quais são ainda reforçados pela própria ideia de soberania popular que fundamenta toda a estrutura constitucional-eleitoral do Brasil.

É nessa perspectiva que se verifica a possibilidade, tanto técnica quanto jurídica, de implementação da tecnologia conhecida por

blockchain no sistema eletrônico de votação no Brasil. As características que são intrínsecas à tecnologia, como transparência nas operações realizadas, descentralização e imutabilidade dos dados, permitem a melhoria da qualidade das eleições no Brasil, já que possibilitam suplantar o atual problema da possibilidade de fraude ao mesmo tempo em que concretizam os direitos fundamentais acima relacionados.

É claro que, como mencionado no item 3.1 deste artigo, a tecnologia é nova – apareceu efetivamente em 2008 – e precisa de testes para que seja verificada a sua real eficácia no processo eleitoral brasileiro. Isso, porém, não pode ser visto como empecilho à sua eventual utilização, especialmente porque parece claro que tal mudança não poderia ocorrer em curto período de tempo.

Da mesma forma, não devem prosperar as críticas que se fundamentam na necessidade de "reeducação do eleitor". Em primeiro lugar, porque tais críticas partem do princípio de que as pessoas não teriam a devida capacidade para compreender eventual mudança no sistema eletrônico com a utilização de chaves públicas e privadas, por exemplo. Em segundo lugar, porque toda mudança necessita, obrigatoriamente, de esclarecimento junto à população, da mesma maneira como ocorreu na ocasião da implantação da urna eletrônica e como continua ocorrendo até os dias de hoje – basta verificar as constantes campanhas educativas feitas pelo TSE nesse sentido.

Haverá também aqueles que se posicionarão contra a implantação de tal tecnologia por considerarem que ela se relaciona "apenas às moedas digitais", o que, como já mostrado, carece de total fundamentação. Basta ver, em exemplo que vale por todos[11], a iniciativa da empresa Sony de utilizar a tecnologia *blockchain* para controle de direitos digitais (BASTIANI, 2018).

[11] Alguns exemplos de outros usos da tecnologia *blockchain* – como serviço de câmbio baseado em *blockchain*, soluções para o mercado de energia ou armazenamento de registros de saúde com segurança – podem ser vistos em Akhtar (2018).

Vale ainda argumentar que a experiência não seria inovadora, ao menos em âmbito mundial. A Estônia, país que está na vanguarda da tecnologia na Europa, estabeleceu o i-Voting desde 2005. O i-Voting "é um sistema que permite que os eleitores votem a partir de qualquer computador conectado à internet em qualquer lugar do mundo" (REPUBLIC OF ESTONIA, 2018a, tradução nossa).

O sistema funciona da seguinte maneira: durante determinado período prévio às eleições, o eleitor faz login no sistema utilizando certificado digital – o qual é fornecido a todos os cidadãos pelo governo estoniano – e vota nos candidatos escolhidos. Em seguida, a identidade do eleitor é dissociada do voto antes que ele chegue à Comissão Eleitoral Nacional para a totalização, garantindo o anonimato.

Vale destacar que o próprio governo estoniano reconhece a possibilidade de os eleitores serem forçados a votar em determinado candidato. Por tal motivo, o sistema estoniano permite que o cidadão vote quantas vezes quiser durante a fase pré-eleitoral. Como cada voto cancela o anterior, o eleitor sempre terá a opção de alterar o seu voto posteriormente, resistindo a eventuais pressões que venha a sofrer. Importa ainda indicar que o governo da Estônia utiliza a tecnologia *blockchain* para guardar também os registros médicos de todos os cidadãos. No momento, 95% dos dados referentes à saúde dos cidadãos estonianos já estão digitalizados (REPUBLIC OF ESTONIA, 2018b).

Para concluir, importa destacar outros dois exemplos práticos de eleições que utilizaram a tecnologia *blockchain*. Em março de 2018, Serra Leoa realizou aquela que é considerada a primeira eleição no mundo totalmente baseada em *blockchain* (BIGGS, 2018). Por sua vez, em maio de 2018, ocorreram as primeiras eleições registradas em *blockchain* nos Estados Unidos (REESE, 2018). Ainda que nos dois casos

o número de votantes tenha sido proporcionalmente pequeno, é inegável que o resultado positivo obtido consolida a tecnologia *blockchain* como elemento promissor para a solução dos problemas aqui apresentados.

Como foi apresentado, a tecnologia existe e está à disposição para a melhoria da qualidade da democracia brasileira. Da mesma maneira, a implantação da tecnologia *blockchain* poderá reforçar ainda mais os direitos fundamentais do cidadão. É assim que se torna possível afirmar que a *blockchain* conseguirá, futuramente, garantir a segurança da democracia.

Referências

AKHTAR, Tanzeel. Tecnologia *Blockchain*: não É mais Apenas para Criptomoedas. *Money Times*. Disponível em: https://moneytimes.com.br/tecnologia-blockchain-nao-e-mais-apenas-para-criptomoedas. Acesso em: 20 jun. 2018.

BASTIANI, Amanda. Sony Mira *Blockchain* para Controle de Direitos Digitais. *Criptomoedas Fácil*. 27 de abril de 2018. Disponível em: https://www.criptomoedasfacil.com/sony-mira-blockchain-para-controle-de-direitos-digitais. Acesso em: 20 jun. 2018.

BIGGS, John. Sierra Leone just Ran the First Blockchain-Based Election. *Techcrunch*. 15 de março de 2018. Disponível em: https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/?guccounter=1. Acesso em: 21 jun. 2018.

BRASIL. Supremo Tribunal Federal. *Certidão de Julgamento*. Medida Cautelar na Ação Direta de Inconstitucionalidade 5.889. 6 de junho de 2018. 2018e. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=14994632&prcID=5346547#. Acesso em: 19 jun. 2018.

_____. Tribunal Superior Eleitoral. Código Eleitoral – *Lei no 4.737, de 15 de julho de 1965*. Institui o Código Eleitoral. Disponível em: http://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965. Acesso em: 19 jun. 2018.

_____. *Constituição da República Federativa do Brasil:* Texto Constitucional Promulgado em 5 de outubro de 1988, com as Alterações Determinadas pelas Emendas Constitucionais de Revisão nºs 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 99/2017 e pelo Decreto Legislativo nº 186/2008. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2017a.

_____. Tribunal Superior Eleitoral. Lei das Eleições – *Lei no 9.504, de 30 de setembro de 1997*. Estabelece Normas para as Eleições. Disponível em: http://www.tse.jus.br/legislacao/codigo-eleitoral/lei-das-eleicoes/lei-das-eleicoes-lei-nb0-9.504-de-30-de-setembro-de-1997. Acesso em: 19 jun. 2018.

_____. Tribunal Superior Eleitoral. *Lei no 13.165, de 29 de Setembro de 2015*. Altera as Leis nºs 9.504, de 30 de setembro de 1997, 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 – Código Eleitoral, para Reduzir os Custos das Campanhas Eleitorais, Simplificar a Administração dos Partidos Políticos e Incentivar a Participação Feminina. Disponível em: http://www.tse.jus.br/legislacao/codigo-eleitoral/leis-ordinarias/lei-no-13-165-de-29-de-setembro-de-2015. Acesso em: 19 jun. 2018.

_____. Supremo Tribunal Federal. *Liminar Suspende Regra da Minirreforma Eleitoral que Prevê Voto Impresso*. 6 de junho de 2018. 2018d. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=380571. Acesso em: 19 jun. 2018.

_____. Ministério Público Federal. Procuradoria-Geral da República. *nº 14/2018 – SFCONST/PGR*. Sistema Único nº 11.597/2018. Ação Direta de Inconstitucionalidade. 2 de fevereiro de 2018. 2018c.

Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=14308709&prcID=5346547#. Acesso em: 19 jun. 2018.

_____. Tribunal Superior Eleitoral. *Resolução nº 23.521*. Instrução nº 0600194-15.2018.6.00.0000 – Classe 19 – Brasília – Distrito Federal. 1º de março de 2018. Regulamenta os Procedimentos nas Seções Eleitorais que Utilizarão o Módulo Impressor nas Eleições de 2018. 2018a. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23521-sobre-voto-impresso. Acesso em: 19 jun. 2018.

_____. Tribunal Superior Eleitoral. *Resolução nº 23.564*. Processo Administrativo nº 0600351-85.2018.6.00.0000 – Classe 26 – Brasília – Distrito Federal. 3 de maio de 2018. Estabelece os Critérios para Distribuição dos Conjuntos de Impressão de Votos a Serem Utilizados nas Eleições 2018. 2018b. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/modulo-impressor-distribuicao-por-estado-r-23564-pa-060035185. Acesso em: 19 jun. 2018.

_____. Tribunal Superior Eleitoral. *Série Voto Impresso*: TSE Estuda Modelo de Urna com a Impressão de Voto e Avalia Custos. 14 de fevereiro de 2017. 2017b. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2017/Fevereiro/serie-voto-impresso-tse-e-instituto-de-pequisas-tecnologicas-estudam-modelo-de-urna-com-a-impressao-de-voto. Acesso em: 19 jun. 2018.

BRUNAZO FILHO, Amilcar. Em Defesa do Voto impresso. Crítica Técnica e Jurídica à ADI 5889. *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 23, n. 5346, 19 fev. 2018. Disponível em: https://jus.com.br/artigos/64166. Acesso em: 19 jun. 2018.

FIGUEIREDO, José. *Introdução à Tecnologia Blockchain*. Lisboa: Blockbird Ventures, 2018.

FLORES, Paulo. Voto Impresso: Quais os Argumentos de Defensores e Críticos. *Nexo*. 9 de fevereiro de 2018. Disponível em: https://www.nexojornal.com.br/expresso/2018/02/09/Voto-impresso-quais-os-argumentos-de-defensores-e-cr%C3%ADticos. Acesso em: 19 jun. 2018.

GATES, Mark. *Blockchain*: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. [S.L.]: Createspace Independent Publishing Platform, 2017. Edição Kindle.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia Científica*. São Paulo: Atlas, 2017. Edição Kindle.

MARTINS, Rafael. Voto Impresso: Desconfiança nas Urnas Eletrônicas Vale 2 Bilhões? *Revista Exame*. 19 de fevereiro de 2018. Disponível em: https://exame.abril.com.br/brasil/a-desconfianca-das-urnas-eletronicas-vale-2-bilhoes-de-reais. Acesso em: 19 jun. 2018.

MOURA, Rafael Moraes; PIRES, Breno. Impressão de Voto Vai Custar R$ 2,5 Bi, diz TSE. *O Estado de S. Paulo*. 22 de julho de 2017. Disponível em: https://politica.estadao.com.br/noticias/geral,impressao-de-voto-vai-custar-r-2-5-bi-diz-tse,70001900669. Acesso em: 19 jun. 2018.

ORIGINALMY. *Afinal, o que É Blockchain?* Descubra aqui! 15 de junho de 2018. Disponível em: https://blog.originalmy.com/afinal-o-que-e-blockchain-descubra-aqui. Acesso em: 20 jun. 2018.

PAIVA, Valério. Pesquisadores Avaliam Limitações de Segurança das Urnas Eletrônicas. *Comunidade Interna*. Unicamp. 10 de abril de 2018. Disponível em: https://www.unicamp.br/unicamp/noticias/2018/04/10/pesquisadores-avaliam-limitacoes-de-seguranca-das-urnas-eletronicas. Acesso em: 19 jun. 2018.

PAYÃO, Felipe. Urnas Eletrônicas: Falhas, Vulnerabilidades e Fraudes do Mesário. *TecMundo*. Segurança. 18 de setembro de 2017. Disponível em: https://www.tecmundo.com.br/seguranca/122152-urnas-eletronicas-falhas-vulnerabilidades-fraudes-mesario.htm. Acesso em: 19 jun. 2018.

PILKINGTON, Marc. Blockchain Technology: Principles and Applications (sept. 18, 2015). *Research Handbook on Digital*

Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. Disponível em: <https://ssrn.com/abstract=2662660>. Acesso em 20 jun. 2018.

REESE, Adam. America's First Partially Blockchain-Based Election Takes Place in West Virginia. ETHNews. 10 de maio de 2018. Disponível em: https://www.ethnews.com/americas-first-partially-blockchain-based-election-takes-place-in-west-virginia. Acesso em: 21 jun. 2018.

REPUBLIC OF ESTONIA. *e-Governance. i-Voting. e-Estonia.* Disponível em: https://e-estonia.com/solutions/e-governance/i-voting. 2018a. Acesso em: 20 jun. 2018.

_____. Healthcare. e-*Estonia*. Disponível em: https://e-estonia.com/solutions/healthcare. 2018b. Acesso em: 20 jun. 2018.

ZANINI, Fábio. Pai da Urna Eletrônica Preocupa-se com Futuro de sua Cria. *Folha de S.Paulo*. 14 de abril de 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/04/pai-da-urna-eletronica-preocupa-se-com-futuro-de-sua-cria.shtml. Acesso em: 19 jun. 2018.