
DEMOCRACIA DOS
DADOS

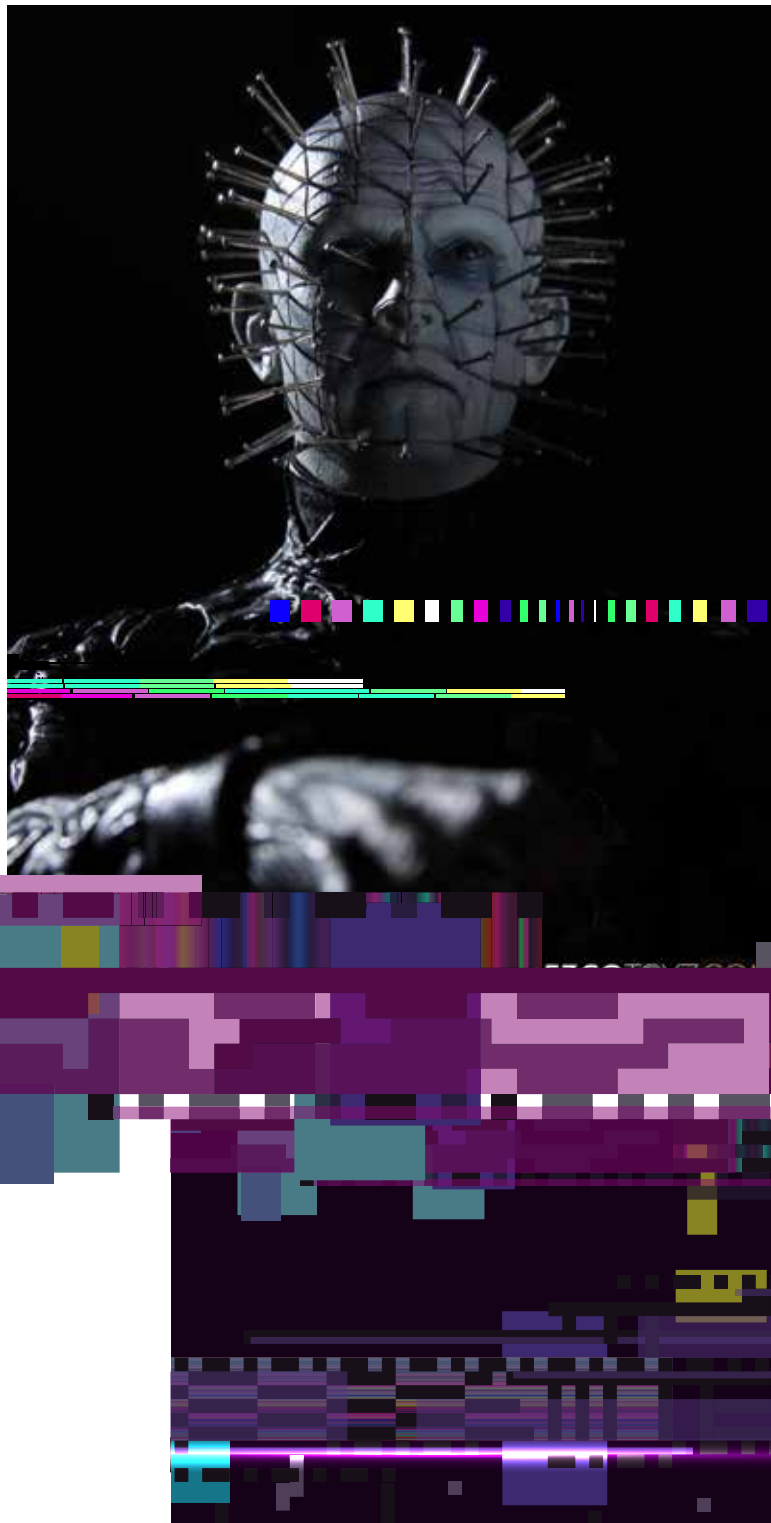
POR QUE DIZER NÃO ANTES QUE ALGUÉM DIGA SIM POR VOCÊ

Leidi Priscila Figueiredo Vilela
Advogada

Há mais de duas décadas o Brasil tem passado por um gradativo processo de modernização por todos os seus Poderes e esferas político-administrativas rumo à inserção do Estado na Era da Informação. Nesta nova Era, o Estado pode ganhar maior eficiência e se aproximar do cidadão, seja oferecendo novas formas de prestação de serviços públicos, seja atribuindo maior transparência e ferramentas de participação popular na gestão da *res publica*.

No entanto, a imersão do Estado na Era da Sociedade da Informação também traz desafios relacionados aos limites da prestação de serviços públicos em meio eletrônico, bem como aos limites do interesse público sobre a vida privada. Sob este último aspecto, pondera-se que o uso de tecnologias da informação viabiliza uma alta concentração de informações privadas pelo Estado, além da possibilidade de compartilhamento e cruzamento de informações atualmente amparadas pela Lei Geral de Proteção de Dados – LGPD – e por outras leis e atos infralegais que vêm estruturando uma grande "Transformação Digital" baseada na concentração de informações.

A alta concentração de dados pessoais no âmbito do Poder Público, assim chamada Govtech, ainda que não seja exatamente o foco do presente artigo, é um ponto que merece absoluta atenção em razão do risco de vigilantismo sobre a vida privada, em violação ao direito da privacidade e da intimidade, além do risco de violação ao direito do devido processo legal, do contraditório e da ampla defesa. Não obstante, a concentração de informações pessoais



em bases centralizadas oferece risco aos titulares dessas informações, uma vez que passam a ser alvos de cibercriminosos com o objetivo de explorar suas fragilidades e obter benefícios através de seus ataques em prejuízo aos direitos dos cidadãos.

No âmbito privado, a alta concentração de informações pessoais, especialmente pelas Bigtechs, além dos riscos de ataques de cibercriminosos e vazamentos de dados, também potencializa a manipulação de massas, direcionamento político e possibilidade de que estas grandes corporações colaborem com o Estado no fornecimento de ainda mais dados e informações pessoais quando solicitados.[1]

Todo esse pano de fundo somado nos traz questionamentos quanto à segurança e à neutralidade de muitos dos serviços públicos prestados eletronicamente, uma vez que são passíveis de manipulação e de excessos, servindo aos seus administradores eleitos ou não eleitos, e não propriamente ao cidadão. Além disso, questiona-se o alcance do Poder Público na vida privada – seja das informações que já possui ou que compartilha com outros entes públicos – ou aquelas que são requeridas para entes privados sob fundamento do interesse público para persecução criminal, segurança do Estado ou para combate à fraude.

Dentro desse complexo cenário, questiona-se a legalidade do alcance do Poder Público na vida privada que recai sobre informações que, muito embora estejam protegidas sob sigilo constitucional, possam ser fragilizadas em sede de compartilhamento de informações e/ou no bojo de processos imaturos de modernização que possam vir a violar o direito ao sigilo. Nessa esteira, chegando ao foco da discussão deste artigo, considerado como uma cláusula pétrea da Constituição Federal, o voto é um dos sigilos que o Estado tem obrigação de manter incólume, sem que exista qualquer previsão de relativização desse sigilo.

Ainda que diante de uma cláusula pétrea, o Tribunal Superior Eleitoral (TSE) vem analisando alternativas desenvolvidas por entes privados para que as urnas eletrônicas possam ser substituídas e para permitir o exercício do voto remotamente por meio de dispositivos móveis, ou seja, sem a necessidade de que o cidadão compareça presencialmente à sua seção eleitoral.

Não obstante os estudos sejam importantes para pavimentar debates e eventuais aprimoramentos ao sistema eleitoral brasileiro, é preciso entender quais são as bases que pretendem ser utilizadas para fomentar uma inovação tecnológica para o exercício da soberania popular em que o sigilo pode ser objeto de frontal violação. Isso porque a potencial utilização dos dispositivos móveis para registro dos votos e para identificação dos cidadãos traz à tona cenários que poderão fragilizar a democracia brasileira e a soberania nacional, haja vista que toda a interação eleitoral desse modelo tenderá a ser realizada pela internet de forma desassistida por colaboradores da Justiça Eleitoral, onde o eleitor e as urnas eletrônicas seriam substituídos por dados pessoais e dispositivos móveis.

A concepção do sufrágio exercido por meio da validação de dados pessoais e dados biométricos gera enormes inseguranças em meio a inúmeras notícias de vazamentos

de dados pessoais em massa. Em janeiro de 2021, foi identificado que mais de 220 milhões de pessoas tiveram seus dados pessoais e biométricos expostos e colocados à venda,[2] sem que seja possível rastrear os imediatos efeitos desse e de outros vazamentos e de ataques cibernéticos recorrentes e seus impactos a um projeto de democracia baseada em dados. Além disso, os riscos de transposição do processo eleitoral para a internet também esbarram sobre potenciais manipulações, induções, adulterações e ataques oriundos de qualquer parte do globo, inclusive mediante o uso de ferramentas e serviços prestados por Bigtechs, potencialmente removendo o cidadão do centro da democracia e inserindo a tecnologia em seu lugar.

Vale registrar que todas as reflexões trazidas neste artigo são em tese, ou seja, levando em consideração cenários ainda hipotéticos apesar de altamente prováveis.

QUANDO OS DADOS PESSOAIS SE TORNARAM CIDADÃOS?

A Lei nº 13.709/2018 (denominada Lei Geral de Proteção de Dados – LGPD) veio estabelecer importantes princípios, diretrizes e regras para proteção dos dados pessoais dos cidadãos, sua intimidade e privacidade. O conceito de dados pessoais[3] previsto na Lei é amplo, e mesmo aqueles dados que não pareçam relevantes ou que não façam referência direta a alguém, quando cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, inclusive com aspectos sensíveis,[4] motivo pelo qual merecem proteção.

A Justiça Eleitoral, para o alistamento dos eleitores, coleta informações pessoais, dentre elas, o nome, filiação e endereço, mediante apresentação de documentos de identificação elencados na Resolução TSE nº 21.538/2013. O alistamento eleitoral nada mais é do que o cadastro do eleitor para que possa desempenhar os seus direitos políticos. Com a implementação do processamento eletrônico de dados no alistamento eleitoral (Lei nº 7.444/1985) evidenciou-se que o alistamento e a atualização de dados de inscritos consistem em cadastros mantidos em computador, cuja competência de regulamentar o seu fiel cumprimento é do TSE. Nesse sentido, o Tribunal editou a Resolução nº 22.688/2007, que implementou em caráter experimental a atualização de dados constantes no cadastro eleitoral com dados biométricos em meios informatizados. A partir desse momento, a Justiça Eleitoral passou a coletar informações pessoais sensíveis, aos olhos da LGPD – dados biométricos –, com o objetivo específico de identificação dos eleitores.[5]

Em 2019, o TSE editou a Resolução nº 23.595, alterando a Resolução nº 23.440/2015, para permitir a coleta de dados de georreferenciamento e a identificação dos eleitores por intermédio do aproveitamento de dados mantidos por outros órgãos, mediante validação da identificação biométrica por ocasião do comparecimento para votação ou por meio de outras soluções tecnológicas.

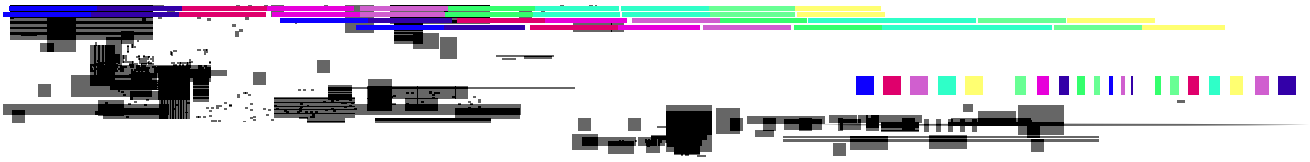
Adicionalmente, no interregno entre as Resoluções de 2015 e de 2019, foi editada a Lei nº 13.444/2017, que dispõe sobre o a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados, sob gestão do TSE. Trata-se de lei que veio a convalidar a base biométrica do TSE, inicialmente instituída por atos infralegais, como uma das fontes para expedição do Documento Nacional de Identificação – DNI.

Nota-se que as normas eleitorais que visavam a manutenção de cadastros de eleitores foi se expandindo com o passar dos anos, de modo a exigir a coleta de dados biométricos, dados de georreferenciamento e aproveitamento de cadastros de terceiros, inclusive sem necessidade de comparecimento presencial para fins de identificação de eleitores. Ainda que a identificação do eleitor perante a Justiça Eleitoral não tenha validade apenas para fins do exercício do voto, mas também para requerimentos diversos e para fins de candidaturas de cidadãos para cargos eletivos, é certo que as normas não tiveram o condão de suprir a necessidade de que o cidadão manifeste sua vontade perante as seções eleitorais, a partir do registro de seu voto em uma urna eletrônica.

A partir do contexto narrado, temos que o TSE é um órgão que efetua tratamento de dados pessoais e de dados pessoais sensíveis nos termos da LGPD.

Pois bem. A concepção de um modelo de votação eletrônica remota no Brasil seria integralmente baseada no tráfego de dados pessoais e dados pessoais sensíveis onde, resumidamente, em uma ponta, o cidadão coletaria dados biométricos e registraria o seu voto e, de outro lado, a Justiça Eleitoral conferiria a identidade do indivíduo e contabilizaria o voto encaminhado. Em que pese possam existir mecanismos seguros para a comunicação entre essas duas partes, não é possível afirmar que o registro do voto não assistido por colaborador da Justiça Eleitoral possa garantir (i) a inviolabilidade do sigilo do voto; (ii) a privacidade no momento do sufrágio; (iii) a livre manifestação de vontade do eleitor, e, diante de recentes relatos de vazamentos de dados pessoais em massa; (iv) assegurar a identidade do eleitor, quando utilizadas tecnologias que não garantam critérios robustos de identificação do cidadão.

É PREOCUPANTE QUE A INOVAÇÃO TECNOLÓGICA TENHA POR PRINCIPAL OBJETIVO A REDUÇÃO DE CUSTOS E NÃO O AUMENTO DA SEGURANÇA



Os dados pessoais sempre foram objeto de tratamento da Justiça Eleitoral, posto indispensável para a consecução de suas atividades e para identificação dos eleitores para fins de alistamento e para o exercício da cidadania. No entanto, com o passar dos anos e com a modernização do cadastro eleitoral, inclusive mediante coleta de dados biométricos, a Justiça Eleitoral passou a acessar e incorporar outras informações que não aquelas originalmente coletadas quando do alistamento, seja em razão do aproveitamento de informações advindos de outras bases públicas, seja na construção da base de dados do DNI. A questão a se refletir no caso recai sobre a finalidade da coleta e do tratamento de dados pessoais que pode ir além dos interesses e das prerrogativas legais da Justiça Eleitoral.

Em coletiva de imprensa realizada em 15/11/2020, o presidente do TSE, Ministro Luis Roberto Barroso, afirmou que os estudos em fomento à utilização de dados pessoais e de tecnologias no processo democrático ainda são "puramente especulativos" e uma eventual substituição das urnas eletrônicas somente aconteceria de forma progressiva.[6] Mesmo que em sede de estudos especulativos, o tema abre espaço para reflexões e exige posicionamento técnico e jurídico, principalmente diante de fragilidades e violações de direitos que poderão ser concretizados gradualmente e de forma desapercebida.

ELEIÇÕES DO FUTURO?

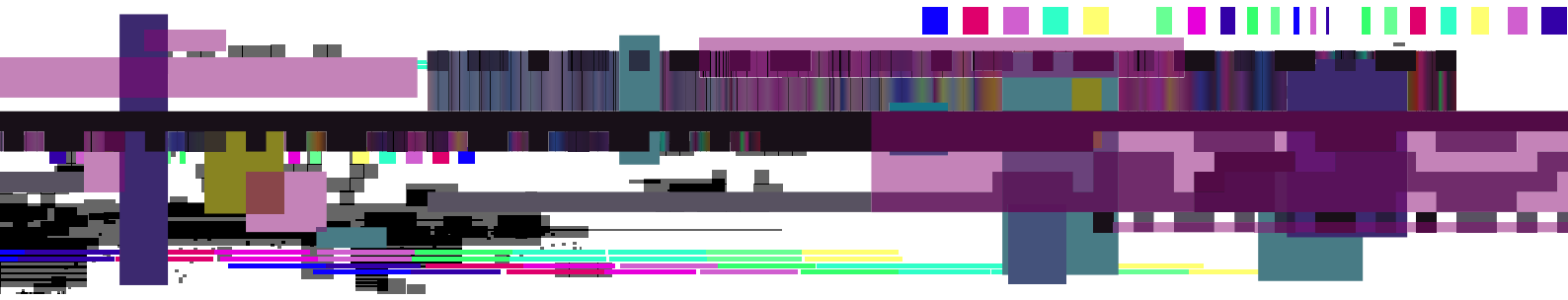
Na esteira de medidas de modernização que vêm sendo implementadas em serviços públicos diversos, a Justiça Eleitoral brasileira instituiu um programa denominado "Eleições do Futuro", que prevê a possibilidade da utilização de novas tecnologias para o exercício da cidadania em substituição às urnas eletrônicas.

Por meio da Portaria TSE nº 527, de 14 de julho de 2020, o Tribunal instituiu grupo de trabalho incumbido de pesquisar e implementar inovações no Sistema Eletrônico de Votação, em especial quanto à redução dos custos de aquisição e manutenção dos equipamentos de votação. Em desdobramento, foi publicado edital de chamamento público (Edital de Chamamento Público nº 01/2020) que estabeleceu as regras para participação de entidades interessadas em apresentarem soluções tecnológicas e que definiu os requisitos técnicos mínimos para a solução tecnológica.[7]

Ao justificar o projeto e a realização de testes com empresas privadas para apresentação de soluções, o presidente do TSE, ministro Luis Roberto Barroso, em coletiva de imprensa realizada em 15/11/2020, ponderou que

> [...] a proposta "eleições do futuro" é para que empresas de tecnologia apresentem modelos de votação que possam no futuro substituir as urnas – que funcionam muito bem e são confiáveis – porém elas têm um custo elevado, têm uma necessidade de reposição constante a cada 2 anos e nós precisamos repor cerca de 20% das urnas [...] e, portanto, para minimizar esse custo, nós estamos tentando um modelo alternativo, de preferência de voto pelo dispositivo pessoal. [...] evidentemente, se tiver alguma proposta relevante e factível, nós vamos começar a pensar a forma de implantação de um novo modelo.[8]

É desejável que o TSE busque informações que possam aprimorar o sistema eleitoral. No entanto, é preocupante que a inovação tecnológica tenha por principal objetivo a redução de custos e não o aumento da segurança



do cidadão e da democracia, principalmente a partir de incidentes graves de megavazamentos de dados de 220 milhões de brasileiros e de ataques à sistemas públicos como do STJ.[9] Sobre este último ponto, ao analisarem as extensões do ataque ao STJ ocorrido em 2020, os pesquisadores da FGV Direito-SP concluem que as medidas de prevenção não podem ser dispensadas pelo seu custo, porque "em um mundo digitalizado, segurança cibernética e segurança em sentido amplo se confundem, de forma que a primeira deve ser tratada com a mesma seriedade que a segunda. Do contrário, a marcha pela digitalização, desburocratização e eficiência dos serviços públicos só pode resultar em um abismo de vulnerabilidade".

Dada a natureza das soluções almejadas, a votação digital se daria mediante a utilização de dispositivos móveis privados para o registro de votos pela internet, delineando uma fragilidade insuperável para o sistema eleitoral, que é a garantia do sigilo do voto.

AS MÚLTIPLAS FACETAS DO SIGILO DO VOTO

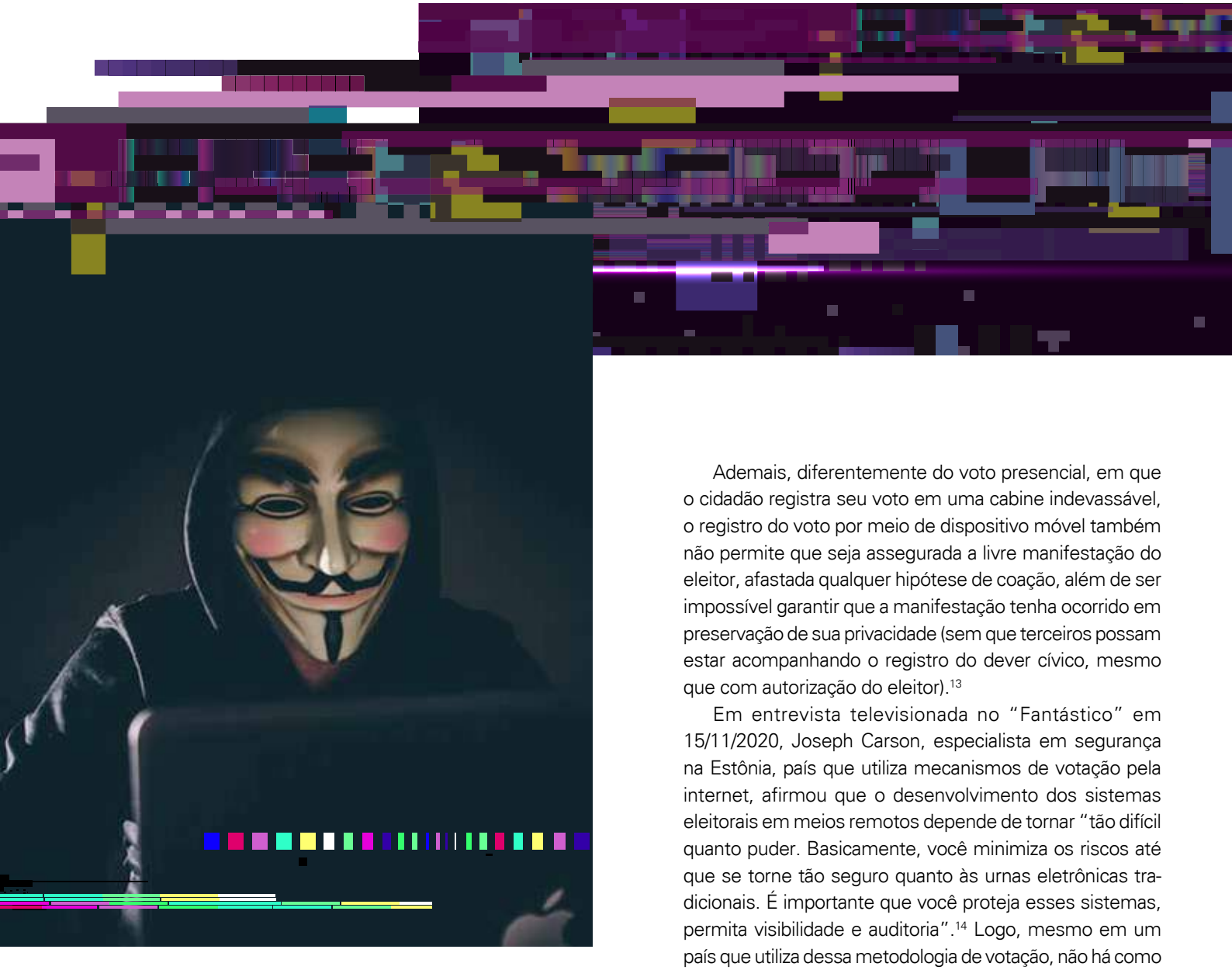
As urnas eletrônicas brasileiras são grandes referências mundiais de sucesso, eficiência e celeridade na apuração de votos.[10] Uma das principais características das urnas é o seu funcionamento desconectado das redes, o que garante a impossibilidade de que os equipamentos possam ser manipulados por ataques realizados pela internet.[11] Ao considerarmos a possibilidade de que os cidadãos brasileiros possam votar remotamente por intermédio dos seus dispositivos pessoais, o uso da internet torna-se obrigatório, mesmo que mediante redes teoricamente seguras. Contudo, é certo que a Justiça Eleitoral brasileira não possui absolutamente qualquer controle sobre esse meio, exponenciando os riscos relacionados ao seu uso e que atualmente são mitigados pelas urnas eletrônicas offline.

Aliás, uma das peculiaridades da internet é a ausência de fronteiras e de controlador central, restando aos Estados a pretensão de regularem os efeitos e as regras das relações que são decorrentes de seu uso, se possível e viável, correndo-se o risco de esbarrar em direitos fundamentais, como o da liberdade.

Essa liberdade é a mesma que permite que a internet também seja o meio para a prática de ilícitos de todas as naturezas, por brasileiros e estrangeiros (inclusive Estados estrangeiros), da qual a ausência de regulação efetiva favorece o anonimato e manipulação de informações que inviabilizem a localização, a identificação e a punição de seus agentes.

O Marco Civil da Internet (Lei nº 12.965/2014) prevê que o acesso à internet é essencial ao exercício da cidadania, garantida a inviolabilidade e o sigilo do fluxo de suas comunicações e das comunicações privadas armazenadas pela internet, salvo por ordem judicial (art. I, II e III). Nota-se que, a inviolabilidade do sigilo das comunicações pela internet é relativa, haja vista a possibilidade de quebra por determinação judicial. Contudo, no caso hipotético em análise, os votos remotos, por trafegarem pela internet estariam no rol de comunicações que poderiam ser interceptadas por determinação judicial. Eis que, a Constituição Federal não prevê nenhuma exceção ao sigilo do voto dos cidadãos, considerado como cláusula pétrea, evidenciando a incompatibilidade do meio para o fim pretendido.

O segundo aspecto ponderado recai sobre o controle do dispositivo utilizado para a votação, que, no caso de uma votação por meios remotos, seriam os telefones celulares (smartphones) dos cidadãos. Não é preciso aprofundar ponderações sobre a impossibilidade jurídica de que a Justiça Eleitoral controle dispositivos privados dos cidadãos. Logo, não é possível garantir a segurança do dispositivo utilizado e evitar que a comunicação seja interceptada, monitorada ou qualquer outra ação que viole o seu sigilo. Inclusive, diferentemente das urnas eletrônicas que permanecem lacradas e armazenadas para auditorias após a realização



das eleições, os dispositivos móveis privados não estariam submetidos a esse nível de auditabilidade. Ainda, é necessário considerar que, em sendo um instrumento de utilidades particulares diversas, os dispositivos móveis podem ser importantes provas digitais e sujeitos a perícias, apreensão e outras medidas judiciais e legalmente previstas para investigações e repressões de ilícitos penais.[12] Nesse aspecto, em havendo a possibilidade de que os votos realizados por meio dos smartphones ficassem registrados em logs no aparelho, por exemplo, novamente estaríamos diante de fragilização do sigilo.

Ademais, diferentemente do voto presencial, em que o cidadão registra seu voto em uma cabine indevassável, o registro do voto por meio de dispositivo móvel também não permite que seja assegurada a livre manifestação do eleitor, afastada qualquer hipótese de coação, além de ser impossível garantir que a manifestação tenha ocorrido em preservação de sua privacidade (sem que terceiros possam estar acompanhando o registro do dever cívico, mesmo que com autorização do eleitor).[13]

Em entrevista televisionada no "Fantástico" em 15/11/2020, Joseph Carson, especialista em segurança na Estônia, país que utiliza mecanismos de votação pela internet, afirmou que o desenvolvimento dos sistemas eleitorais em meios remotos depende de tornar "tão difícil quanto puder. Basicamente, você minimiza os riscos até que se torne tão seguro quanto às urnas eletrônicas tradicionais. É importante que você proteja esses sistemas, permita visibilidade e auditoria".[14] Logo, mesmo em um país que utiliza dessa metodologia de votação, não há como se eliminar integralmente os riscos de fraudes, de ataques e incidentes de quaisquer naturezas no processo eleitoral eletrônico, apenas de mitigação.

Sob esta ótica, ao comparar o Brasil e a Estônia, o cientista computacional, professor e especialista em segurança da informação e infraestrutura, Edilson Osório Jr., vê que a utilização das eleições por dispositivos pessoais no Brasil poderá ter "problemas de tentativa de hacking e indisponibilidade de sistemas. A criptografia os sistemas abertos podem ter toda a segurança do mundo, mas a infraestrutura precisa aguentar uma carga de tentativas de acessos e ataques – a Estônia tem 1,3 milhão de habitantes, o Brasil mais de 200 milhões".[15]

Apesar das considerações dos especialistas, nota-se em diversas iniciativas de modernização do Estado

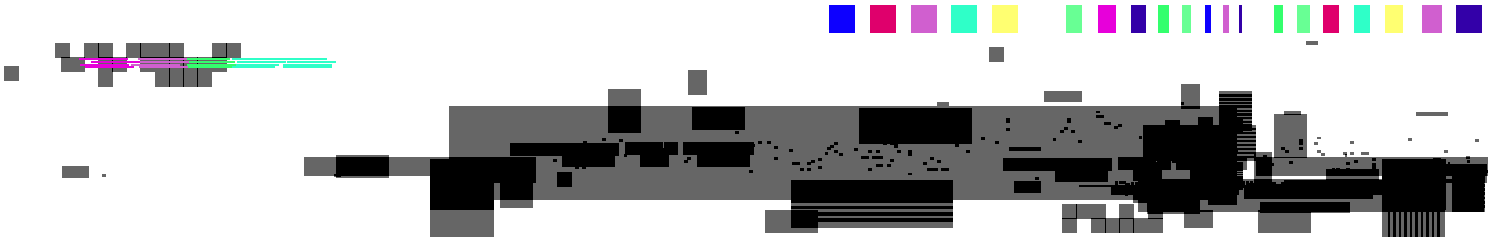
brasileiro, especialmente dos últimos anos sob condução do governo federal, que há um especial interesse em aproximação de práticas de governo eletrônico às práticas implementadas na Estônia.

A Estônia é um país referenciado em termos de modernização de serviços públicos e permite que o cidadão possa registrar o voto em eleições por meio da internet, com uso de seus dispositivos pessoais e mecanismos de identificação eletrônica. Contudo, sem prejuízo aos elogios que devem ser traçados ao país a partir de seus êxitos, há de se convir que as realidades da Estônia e do Brasil são diferentes. Além da história, da cultura, dos aspectos econômicos, a exemplo do que foi mencionado pelo pesquisador ao citar os riscos da implementação de votações online no Brasil, a população da Estônia é de pouco mais de 1,3 milhão de pessoas em 45.227 km² de área.[16] Isolado, o estado de São Paulo possui mais de 44 milhões de pessoas em sua base populacional e 248.209 km² de área, o que exponencia, apenas nesse corte de comparação, os desafios de um país com mais de 200 milhões de habitantes e 8.516.000 km² de área.[17] Ainda assim, não faltam iniciativas para implementar as mesmas soluções da Estônia em um país de extensão e de complexidades continentais.

Outra vertente do sigilo do voto recai sobre a privacidade do momento do exercício do dever cívico. O voto é a externalização de uma manifestação de vontade que deve permanecer secreto justamente para que possa ser livre. A liberdade de votar sem que o voto possa ser identificado empodera a população para que possa fazê-lo e, para tal, depende da garantia de privacidade necessária para o ato. Nessa linha, ainda antes da implantação das urnas eletrônicas (1996), a legislação eleitoral já dispunha sobre a necessidade de que o eleitor proferisse seu voto em cabine indevassável, para que pudesse fazer a sua escolha em isolamento (art. 103, II e 138 do Código Eleitoral). No mesmo sentido, com o uso das urnas eletrônicas, o registro do voto também deve ser realizado em cabine indevassável, onde fica situado o equipamento de registro dos votos dos eleitores.

O texto constitucional e a Lei Eleitoral atualmente exigem forma específica para formalização do voto: secretamente, em cabine de votação indevassável, mediante comparecimento pessoal. Em analogia à validade dos negócios jurídicos prevista no Código Civil brasileiro (art. 104), em que a inobservância de uma solenidade determinada por lei pode tornar o ato nulo (art. 166, IV e V), o exercício do voto em inobservância às suas formalidades legais também poderá anular o exercício cívico. Assim, ainda que se cogite a possibilidade de implantação de inovações tecnológicas no processo eleitoral, qualquer modificação que altere as bases do sigilo do voto depende de alteração da Constituição Federal e da Lei, inobstante sejam valiosos os estudos que venham a pavimentar reflexões no âmbito legislativo.

Contudo, o voto é um direito político altamente sensível e não pode ser tratado, principalmente em sede de debates voltados à simplificação de procedimentos e redução de despesas, como um serviço público que necessite de mo-



O VOTO É UM DIREITO POLÍTICO ALTAMENTE SENSÍVEL E NÃO PODE SER TRATADO COMO UM SERVIÇO PÚBLICO QUE NECESSITE DE MODERNIZAÇÃO A QUALQUER CUSTO

dernização a qualquer custo. Isso porque, primeiramente, os direitos políticos são direitos e não serviços públicos.

A República Federativa do Brasil tem como fundamento a soberania popular em que "todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente" (Art. 1º, I e parágrafo único da CF/88). Se a soberania popular é exercida por meio do voto obrigatório e secreto, qualquer aspecto relacionado à segurança e à inviolabilidade do exercício da soberania popular merece os necessários e adequados investimentos. Ademais, em tendo regras próprias e claras, não pode um direito político ser levado à "Sandbox",[18] a exemplo de segmentos econômicos regulados que permitem o desenvolvimento e o oferecimento à população de produtos e serviços com a flexibilização de normas para que sejam experimentadas inovações sem observância à carga regulatória ordinária.

O voto é a base da democracia, e é inquietante que uma das principais motivações externadas pelo TSE para a experimentação de inovações tecnológicas que possam fragilizar o sigilo do sufrágio tenha sido puramente para a redução de custos. O sigilo está intrinsecamente relacionado à livre manifestação de vontade do eleitor, que não pode ser assegurada mediante votação remota e não assistida por colaboradores da Justiça Eleitoral ou por mecanismos eletrônicos frágeis, manipuláveis e que ainda possam possibilitar e fomentar o uso indevido de credenciais baseadas em dados que foram colocados à venda.

DADOS PESSOAIS INSEGUROS

O contexto narrado merece reflexão especialmente porque mais de 220 milhões de brasileiros tiveram seus dados pessoais vazados e comercializados na internet[19] este ano. Nome, CPF, telefone, e-mail, foto de rosto, título de eleitor, renda mensal, classificação de crédito e participação no programa Bolsa Família, incluindo dados de pessoas falecidas, são algumas das informações que foram colocadas à venda e que, uma vez vazadas, não podem ser necessariamente apagadas da internet ou da darkweb.

Diariamente temos convivido com notícias relacionadas à grandes vazamentos de dados pessoais, ataques a bases e sistemas públicos e privados e uma série de outras situações que colocam o cidadão em situação de extrema fragilidade em meio eletrônico. Isso tudo sem considerar os riscos de ataques transnacionais direcionados à desestabilização da soberania popular brasileira. Ronaldo Lemos, advogado especialista em direito e tecnologia, pondera que os dados pessoais seriam como o novo petróleo e que, assim como o petróleo, quando os dados são vazados, também provocam danos de enorme escala, às vezes irreversíveis.[20]

Até o momento não foi possível mensurar os danos sofridos pela população que teve seus dados pessoais vazados e é possível que seus efeitos ainda possam perdurar por muitos anos. Isso porque muitos dos dados que foram objeto de divulgação e comercialização são estáticos (como o nome, título de eleitor e o CPF) e não se alteram durante a vida de uma pessoa. Contudo, são dados muito utilizados para abertura de cadastros, criação de contas, solicitação e contratação de serviços e uma infinidade de outras possibilidades. A utilização desses dados estáticos, inclusive aliada às informações biométricas que também foram alvo de vazamento, como as fotografias da face dos cidadãos, também dão a prerrogativa de que as pessoas formalizem manifestações de vontade e obtenham acesso às informações sigilosas em meio eletrônico, com o uso de assinaturas eletrônicas fornecidas pelo governo federal, denominadas assinaturas simples e avançadas.[21]

Ciente do risco de utilização para fins fraudulentos, Ghassan Dreibi, diretor de cibersegurança da Cisco, afirma que "se não podemos mudar nossos CPFs precisamos repensar a autenticação das pessoas".[22] A colocação do diretor de cibersegurança é absolutamente verdadeira, haja vista que além do CPF, título de eleitor, nome e outras informações pessoais, também não podemos alterar as nossas características biométricas e, todas essas informações foram vazadas, podendo ser manipuladas tecnologicamente para permitir um inestimável número de fraudes e ilícitos ao longo dos próximos anos.

Sob este aspecto, as medidas de cibersegurança devem ser prioridade de todas as pautas públicas e privadas, especialmente porque, nas palavras dos advogados pesquisadores da FGV Direito SP, João Pedro Favaretto Salvador e Tatiane Guimarães, "os custos de prevenção, por maiores que possam parecer, são ínfimos frente aos danos que podem decorrer da paralisação desses sistemas".[23] E não apenas da paralização dos sistemas, mas também dos custos relacionados ao ressarcimento de danos sofridos pelos titulares de dados vazados, bloqueados e indisponibilizados por ataques ou por fragilidades sistêmicas.

No contexto das fragilidades relatadas, grande parte dos cidadãos desconhece a amplitude e a densidade dos riscos relacionados ao uso da internet e sequer tem condições técnicas suficientes para agir preventivamente. Aliás, as camadas de segurança a determinados atos usualmente são confundidas com burocracias desnecessárias. Muitas vezes, o próprio poder público dá a conotação de que existem formalidades excessivas e que uma série de mo-

dernizações estariam sendo implementadas com o objetivo de "desburocratizar" a vida do cidadão. Ocorre que há uma linha tênue entre desburocratizar e desproteger a vida, os bens, os dados pessoais, a privacidade, a propriedade e os direitos do cidadão. E, geralmente, o cidadão não tem o entendimento e o alcance de todos os riscos relacionados ao processo de "desburocratização", sendo facilmente convencido pelos benefícios da inovação e da comodidade, renunciando à segurança e à privacidade.

AUTODETERMINAÇÃO DEMOCRÁTICA E DEMOCRACIA NO CIBERESPAÇO

A legislação brasileira ressalta o direito à autodeterminação informacional, ou seja, à capacidade do cidadão em ter conhecimento e controle de seus dados e informações pessoais. Contudo, quando os dados são coletados e tratados por entes públicos, a consecução da finalidade pública definida em lei ou em regulamento permite um sem-número de possibilidades de tratamento de dados sem consentimento e, quiçá, sem conhecimento do titular. Afora as discussões sobre o alto grau de subjetividade da LGPD para tratamento de dados pessoais por entes públicos, que pode dar a impressão de uma possibilidade de tratamento ilimitado e até mesmo fora das finalidades que tenham sido originalmente coletadas, no bojo da prestação de serviços eleitorais da Justiça Eleitoral brasileira, o voto é um dado pessoal sensível por determinação da LGPD, e sigiloso, por determinação constitucional.

Todos os dados pessoais são passíveis de proteção, contudo, nem todos eles são sigilosos no aspecto de seu conhecimento estar limitado ao seu próprio titular, existindo pessoas físicas e jurídicas, de direito público ou privado, que fazem o seu respectivo tratamento. Nesse caso, ao tratarem de dados pessoais, esses agentes devem dispor de todos os mecanismos necessários para assegurar o sigilo e a proteção desses dados, com informações claras e precisas sobre eventual compartilhamento. Contudo, a LGPD elenca como sensível a opinião política, a filiação a sindicato e a participação em organizações de cunho político como dados pessoais sensíveis, uma vez que são dados capazes de gerar discriminação e exclusão social.

O voto é uma opinião política, uma escolha, uma manifestação de vontade, um dado sensível e um direito político. Na era da "sociedade da classificação".[24] a fragilização do sigilo do voto, seja qual for o meio utilizado, poderá gerar efeitos catastróficos para a liberdade e para a democracia. Se para as opiniões políticas a Lei atribui uma proteção mais forte ao considerá-la informação sensível, é justamente para evitar discriminações e exclusões.[25]

No caso hipotético da legislação brasileira vir a permitir que as eleições possam ocorrer por meios remotos, ainda que se evidenciem os mais robustos sistemas de votação eletrônica, não existem garantias de que os votos não poderão ser objeto de interceptação, manipulação ou mesmo que não serão utilizados para definição de perfis de eleitores a partir dos cadastros mantidos pela Justiça Eleitoral e por outros entes públicos mediante compartilhamento. A partir de cruzamentos de informações coletadas pelo Poder Público juntamente com a possibilidade de quebra do sigilo dos votos, quais poderiam ser os impactos e os danos à democracia brasileira? Sem prejuízo, como proteger os cidadãos de representantes autoritários que possam vir a utilizar as informações extraídas desse processo vulnerável de votações?

Muito além das informações eleitorais, o Poder Público (no qual se inclui a Justiça Eleitoral) estará de posse de um conjunto de informações privadas, que favorecerão o medo de retaliação, repressão ou de aplicação de penalidades em razão de escolhas pessoais (desde opiniões até o exercício do voto), além da alta rastreabilidade de atividades eletrônicas que poderia vir a anular ou reduzir a participação popular por meio das tecnologias, oferecendo grande risco ao processo democrático brasileiro.[26]

A amplitude do conhecimento do Poder Público sobre o cidadão foi objeto de reflexões de Miriam Wimmer, apontando que, ao mesmo tempo em que o Estado necessita conhecer seus cidadãos como pré-requisito para o exercício da cidadania, a expansão e a quantidade da variedade de dados custodiados pelo Estado trazem à tona riscos de violações de direitos, aumentam a capacidade de intervenção do Estado, tanto com o objetivo de atingir finalidades sociais justas – como, por exemplo, a distribuição de benefícios sociais – como para finalidades nefastas".[27] Com vistas a coibir os efeitos nefastos do conhecimento de informações altamente sensíveis por parte do Poder Público, seja quem for o seu representante, é importante que o legislador mantenha os votos sob o mais alto grau de sigilo, ainda que sob custos muito elevados, pois o custo do autoritarismo e da fragilização da democracia brasileira serão impagáveis e poderão nos conduzir para um caminho sem volta.

As preocupações sobre novos rumos da democracia na Era da Sociedade da Informação foram muito bem delineadas por Rodotá, ao afirmar que a amplitude de dados pessoais coletados pelo Estado é impulsionada sob a argumentação de que tudo pode se revelar útil para a tutela da saúde, da segurança etc. Contudo, em suas palavras

> [...] A democracia é também sobriedade, até mesmo renúncia, quando pode existir um risco para a liberdade dos cidadãos. [...] A democracia é antes de tudo discussão, confronto, pesquisa. As tecnologias da informação devem exaltar esse aspecto, e não oferecer atalhos enganosos [...]"[28]

Diante de todo o panorama traçado, na atual maturidade tecnológica do país e da realidade socioeconômica brasileira, é preciso dizer não à democracia dos dados antes que alguém diga sim por você; antes que as identidades eletrônicas sejam roubadas para manipulações de eleições; antes que os dados pessoais dos cidadãos sejam colocados à serviço do Estado e seus representantes eleitos e não eleitos; antes que a legislação seja alterada sem o devido debate e preparo; antes da população perder seu direito à opinião e ao voto; antes de sepultarmos uma democracia funcional e sistemicamente exemplar para darmos espaço à empolgação de metodologias não adequadas à realidade jurídica e fática do Brasil.

CONSIDERAÇÕES FINAIS

As reflexões aqui registradas apontam as fragilidades da democracia baseada em dados pessoais e a importância de que o cidadão proteja a sua única ferramenta de poder: o seu voto exercido pessoalmente e a integridade e a autenticidade de sua declaração de vontade ainda que realizada em meio eletrônico. Não se rechaçam inovações que possam vir a aprimorar a segurança e a agilidade do processo eleitoral, mas é fundamental que a democracia continue sendo feita pelas pessoas e para as pessoas e não sendo feita pela tecnologia e para a tecnologia (e para aqueles que a controla).

A inovação é importante e desejada à medida que se deve aumentar o rigor e a segurança do processo eleitoral, não sendo possível concordar com a implementação de novas tecnologias apenas para fins de redução de custos quando o poder do povo está correndo o risco de ser fragilizado. Ademais, não é cabível nenhuma forma de relativização do sigilo do voto – considerado um dado pessoal sensível –, capaz de gerar discriminações e exclusões, caso se torne público por qualquer tipo de incidente de segurança.

A LGPD é aplicável tanto para entes públicos quanto para entes privados e, em razão de sua natureza, a responsabilidade decorrente do tratamento dos dados pessoais tratados pelos entes públicos – dos quais estão incluídos os votos – deve ser distinta dos entes privados, por possuir aspectos muito mais abrangentes do que os dados tratados em âmbito privado.[29] Por esse motivo, o sigilo que recai sobre o voto não permite ao Poder Público que inovações imaturas venham a expor os cidadãos brasileiros e a soberania nacional.

Muito mais do que um dever, o voto é um direito poderoso de mudar o futuro. ●

A autora é pós-graduanda em Compliance na FGV e Mestre em Direito da Sociedade da Informação pelas Faculdades Metropolitanas Unidas – FMU. Dedica-se ao estudo da democracia e dos direitos civis no ciberespaço
figueiredo.priscila@uol.com.br

BIBLIOGRAFIA

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Urna eletrônica: 20 anos a favor da democracia. – Brasília: Tribunal Superior Eleitoral, 2016. Disponível em: https://www.justicaeleitoral.jus.br/arquivos/tse-urna-eletronica-20-anos-a-favor-da-democracia/rybena_pdf?file=. Acesso em 3 de mar/2021.

FOLHA DE S. PAULO. LEMOS, Ronaldo. O vazamento de dados do fim do mundo. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml?origin=uol. Acesso em 4 de mar/2021.

FUNDAÇÃO GETULIO VARGAS. SALVADOR, João Paulo Favaretto; GUIMARÃES, Tatiane. O ataque ao STJ é mais um grito de socorro da segurança cibernética no Brasil. Disponível em: https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil . Acesso em 4 de mar/2021.

LOPES, Alan Moreira; TEIXEIRA, Tarcísio. O direito das tecnologias móveis. In: LOPES, Alan Moreira; TEIXEIRA, Tarcísio (coord.). Direito das novas tecnologias: legislação eletrônica comentada, mobile law e segurança digital. São Paulo: Editora Revista dos Tribunais, 2015

RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Mara Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo (coord.) et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 117-118.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: Tratamento de dados pessoais na LGPD sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo (coord.) et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

NOTAS DE RODAPÉ

1. Cite-se, como exemplo, o caso da empresa Cambridge Analytica, que juntamente com o Facebook, fez propaganda e direcionamento político a mais de 50 milhões de pessoas, a partir do conhecimento de seus perfis e interesses extraídos pela mídia social. BBC NEWS. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em 6 de mar/2021.

2. CISO ADVISOR. Vazamento expõe dados pessoais de milhões de brasileiros. Disponível em: https://www.cisoadvisor.com.br/vazamento-expoe-dados-pessoais-de-milhoes-de-brasileiros/. Acesso em 6 de mar/2021.

3. A Lei considera como dado pessoal a informação relacionada a pessoa natural identificada ou identificável e como dado pessoal sensível o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5, incisos I e II).

4. VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo (coord.) et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 117-118.

5. Tal como se verifica no artigo 1º da Resolução nº 23.440/2015, senão vejamos: "Art. 1º A atualização dos dados constantes do cadastro eleitoral, visando à implantação da identificação com inclusão de impressões digitais dos dez dedos, ressalvada impossibilidade física, fotografia e assinatura digitalizada do eleitor, será realizada por meio do serviço ordinário de alistamento eleitoral e de revisões de eleitorado".

6. "Entrevista do presidente do TSE: eleições 2020". Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-brasil/2020/11/15/eleicoes-2020-acompanhe-entrevista-do-presidente-do-tse-ao-vivo.htm. Acesso aos 02 de mar/2021.

7. BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Edital de Chamamento Público nº 01/2020. Disponível em: https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/audiencia-publica/arquivos/edital-de-chamamento-publico-n1-2020-servico-de-votacao-on-line/rybena_pdf?file= Acesso em 3 de mar/2021.

8. UOL. "Entrevista do presidente do TSE: eleições 2020". Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-brasil/2020/11/15/eleicoes-2020-acompanhe-entrevista-do-presidente-do-tse-ao-vivo.htm. Acesso em 2 de mar/2021.

9. SUPERIOR TRIBUNAL DE JUSTIÇA. STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-informacoes-digitais-do-tribunal-apos-o-ataque%E2%80%AFhacker.aspx . Acesso em 4 de mar/2021.

10. BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Apresentação – Urna Eletrônica. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica. Acesso em 3 de mar/2021.

11. "*A grande vantagem da urna eletrônica, demais disso, são seus vários mecanismos de segurança, que impedem adulterações e garantem o sigilo do voto. A impossibilidade de identificação do eleitor, aliada à inexistência de ligação da urna com a Internet ou com qualquer dispositivo de rede, entre outras medidas, tornam-na um mecanismo confiável para evitar violações nas várias fases do processo de votação*". BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Urna eletrônica: 20 anos a favor da democracia. – Brasília: Tribunal Superior Eleitoral, 2016. p. 19. Disponível em: https://www.justicaeleitoral.jus.br/arquivos/tse-urna-eletronica-20-anos-a-favor-da-democracia/rybena_pdf?file. Acesso em 3 de mar/2021.

12. LOPES, Alan Moreira; TEIXEIRA, Tarcísio. O direito das tecnologias móveis. In: LOPES, Alan Moreira; TEIXEIRA, Tarcísio (coord.). Direito das novas tecnologias: legislação eletrônica comentada, mobile law e segurança digital. São Paulo: Editora Revista dos Tribunais, 2015. p. 278.

13. Além disto, a legislação eleitoral veda que o eleitor porte aparelho de telefonia celular, máquinas fotográficas e filmadoras, dentro da cabine de votação (parágrafo único do art. 91 da Lei nº 9.504/1997).

14. GLOBO. Fantástico. TSE estuda viabilidade de realizar eleições pela internet e faz testes em três cidades. Disponível em: https://globoplay.globo.com/v/9025989/?s=0s. Acesso em 4 de mar/2021.

15. Idem.

16. Disponível em: https://pt.wikipedia.org/wiki/Est%C3%B3nia. Acesso em 4 de mar/2021.

17. Disponível em: https://pt.wikipedia.org/wiki/Brasil. Acesso em 4 de mar/2021.

18. Um exemplo de Sandbox regulatório é o que ocorre no âmbito do Banco Central do Brasil, para que instituições já autorizadas ou não possam testar projetos inovadores – produtos ou serviços inovadores – com clientes reais, sujeitos a requisitos regulatórios específicos. BRASIL. BANCO CENTRAL DO BRASIL. Sandbox regulatório BACEN. Disponível em: https://www.gov.br/startuppoint/pt-br/programas/sandbox-regulatorio. Acesso em 4 de mar/2021.

19. G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em 3 de mar/2021.

20. FOLHA DE SÃO PAULO. LEMOS, Ronaldo. O vazamento de dados do fim do mundo. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml?origin=uol. Acesso em 4 de mar/2021.

21. BRASIL. Decreto nº 10.543, de 13 de novembro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10543.htm. Acesso em4 de mar/2021.

22.VALOR ECONÔMICO. Vazamento requer ação do governo, diz especialista. Disponível em: https://valor.globo.com/empresas/noticia/2021/02/01/vazamento-requer-acao-do-governo-diz-especialista.ghtml. Acesso em 4 de mar/2021.

23. FUNDAÇÃO GETULIO VARGAS. SALVADOR, João Paulo Favaretto; GUIMARÃES, Tatiane. O ataque ao STJ é mais um grito de socorro da segurança cibernética no Brasil. Disponível em: https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em 4 de mar/2021.

24. RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Mara Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 234.

25. Idem. p. 145.

26. Idem. p. 126.

27. WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: Tratamento de dados pessoais na LGPD sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo (coord.) et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 273

28. Ibidem. p. 162.

29. WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: Tratamento de dados pessoais na LGPD sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo (coord.) et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 274.