Uma análise de conformidade da LGPD nas urnas brasileiras

Raphael Bernardino Ferreira Lima, Luis Antonio Kowada

[1]Instituto de Computação – Universidade Federal Fluminense (UFF)
Niterói – RJ – Brasil

raphaell@id.uff.br,luis@ic.uff.br

Abstract. *Our data-driven society requires rules to prevent abuse of personal information and misuse by agencies or companies. Therefore, several regulations are being created to protect sensitive data and regulate access to them. That said there is an imminent need for adequacy by the agents who perform the treatment of these data. This paper evaluates the compliance of the Brazilian electronic voting system through the Brazilian General Data Protection Law and critical security aspects that guarantee electoral rights. And last, but not least, the results obtained through the Public Security Test, and created by the Superior Electoral Court, are analyzed.*

Resumo. *A nossa sociedade orientada a dados necessita de regras para prevenir o mal uso de informações pessoais, seja por órgãos governamentais ou empresas privadas. Devido a esse problema diversas regulações estão sendo criadas com o objetivo de proteger os dados sensíveis e regulamentar acesso aos mesmos. Dito isso se evidencia uma iminente necessidade de adequação por parte dos agentes que realizam o tratamento desses dados. Esse trabalho tem como objetivo avaliar a conformidade do sistema de votação brasileiro sob a luz da Lei Geral de Proteção de Dados (LGPD) e os aspectos críticos de segurança que garantem os direitos eleitorais. Ao final são analisados os resultados obtidos através do Teste Público de Segurança criado pelo Tribunal Superior Eleitoral.*

1. Introdução

Com mais de 145 milhões de eleitores o Brasil representa uma das maiores democracias no mundo, segundo o [Tribunal Superior Eleitoral 2019]. Além disso, as urnas eletrônicas são utilizadas por cerca de 23 países e consideradas seguras pelo [Tribunal Superior Eleitoral 2018]; não apresentando assim ameaças à democracia do país. Apesar disso os países citados na nota de esclarecimento utilizam sistemas de votação muito diferentes dos propostos pelo Tribunal Superior Eleitoral (TSE). Podemos tomar como exemplo Canadá que utiliza dois sistemas de votação: um sistema de votação *online* e outro que realiza a leitura ótica nos papéis de votação. Essa última abordagem provê a garantia física do voto, que atualmente é inexistente nas urnas brasileiras.

O sistema brasileiro de votação atual, proposto em 1996 após diversas alegações de fraude no sistema anterior, utiliza urnas que registram de forma direta e eletrônica (*Direct Recording Electronic* - DRE) todos os votos sem impressão do voto físico. O voto impresso foi utilizado brevemente em 2002, porém representou um custo muito alto e que, segundo as autoridades eleitorais, não justificavam mantê-lo. Recentemente

o [Tribunal Superior Eleitoral 2017] propôs novamente que o voto fosse impresso a fim de prover uma eleição mais justa e confiável. A proposta foi suspensa sob alegações de inconstitucionalidade.

Por essas razões ultimamente têm se discutido muito os quesitos de segurança das urnas eletrônicas utilizadas nas votações brasileiras. Diversas falhas foram apontadas por diversos pesquisadores e técnicos nas últimas edições do Teste Público de Segurança (TPS) realizados pelo Tribunal Superior Eleitoral (TSE). Essas dúvidas colocam em risco a democracia de uma nação e podem gerar consequências desastrosas para seu povo. Portanto tais alegações devem ser analisadas minuciosamente e com cuidados a fim de que o tratamento seja respeitoso, honesto e justo com todas as partes envolvidas nos testes, desenvolvimento e usuários finais. Outro ponto que devemos ressaltar é que o TSE detém unicamente o poder legal para contratar empresas ou pessoas, organizar os locais de votação, implementar os *softwares* utilizados, decidir quais tecnologias ou *hardwares* serão utilizados, realizar as votações e, por fim, determinar se houve ilegalidades.

O Teste Público de Segurança (TPS) teve sua primeira edição em 2009 e se tornou um evento periódico com o objetivo de trazer mais confiança ao sistema proposto. Na primeira edição foram identificadas diversas falhas e, segundo o TSE, corrigidas antes das eleições. Nas demais edições também foram encontradas outras falhas e também, supostamente, corrigidas. Esse evento que atrai *hackers* e curiosos de todo o país acontece cerca de 6 meses antes das eleições, que ocorrem a cada 2 anos; alternando entre eleições municipais e gerais.

A Lei 13.709/2018 disposta pelo [Congresso Nacional 2018], e mais conhecida como Lei Geral de Proteção de Dados (LGPD), enuncia pontos essenciais para proteção de dados e altera a Lei 12.965/2014 também disposta pelo [Congresso Nacional 2014], e que é conhecida popularmente como Marco Civil da Internet, que tinha como objetivo proteger o cidadão brasileiro. A LGPD é mais abrangente e engloba empresas que lidam com processamento de dados, sejam sensíveis ou não. Além disso tem como objetivo regular o tratamento de dados pessoais, considerando meios digitais e físicos, para qualquer pessoa física ou jurídica de direito público ou privado a fim de proteger a liberdade, privacidade e livre desenvolvimento do cidadão.

Na Seção 2 é apresentada uma breve análise das leis relacionadas com a LGPD com foco no assunto tratado neste artigo. Na Seção 3 são apresentadas as falhas encontradas nas edições do [Tribunal Superior Eleitoral - TPS 2016] e [Tribunal Superior Eleitoral - TPS 2017b]. Na Seção 4 é feita a análise de conformidade das urnas com a LGPD. Por último, na Seção 5, são apresentadas a conclusão e alguns questionamentos que podem elucidar as questões discutidas neste artigo.

2. Análise da Lei 13.709

Inspirada no regulamento europeu GDPR (*General Data Protection Regulation*) a Lei 13.709/2018 regula a proteção de dados pessoais em âmbito nacional, concilia a proteção da pessoa, o interesse público e incentiva o desenvolvimento econômico ou tecnológico. Anteriormente esses dados eram relacionados ao direito à vida e à intimidade, consagrados no artigo 5º, X da Constituição e no artigo 21 do Código Civil. As questões relacionadas à tecnologia da informação estavam dispostas no Marco Civil da Internet.

Ao analisarmos os aspectos que englobam os direitos e deveres dos cidadãos bra-

sileiros no contexto de votação, podemos observar vários aspectos associados a manipulação de informações pessoais. Dentre outros, podemos destacar a questão do recadastramento biométrico, processo iniciado em 2007 pelo [Tribunal Superior Eleitoral 2007] e concluído em 2009 também pelo [Tribunal Superior Eleitoral 2009]. Os eleitores dos grandes centros urbanos adotaram, sem escolha, a inclusão de seus dados pessoais em banco de dados do Estado sob o pretexto de identificá-lo de forma única e evitar fraudes. Outros serviços prestados pelo Estado seguem a mesma abordagem, como é o caso da Carteira Nacional de Habilitação controlada pelo [CONTRAN 2007] e a renovação de passaportes pela Polícia Federal.

Recentemente foi aprovada no [Congresso Nacional 2017] a Lei 13.444/2017, ou Identificação Civil Nacional (ICN), que tem como objetivo integrar as bases de dados existentes e identificar a população através de sistemas biométricos. A ICN utilizará as bases de dados da Justiça Eleitoral, Sistema Nacional de Informações de Registro Civil (SIRC) e informações dispostas nas bases de dados dos institutos de identificação dos Estados e do Distrito Federal. O TSE será responsável por manter a base de dados atualizada e garantirá acesso gratuito aos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios. Os dados não podem ser comercializados, porém não impede o serviço de conferência de dados que envolvam a biometria prestado a particulares, a ser realizado exclusivamente pelo Tribunal Superior Eleitoral.

A política adotada nas Leis 13.444/2017 e 13.709/2018 difere na abordagem utilizada para o tratamento de dados. A LGPD trata dados sensíveis, como biometria, através do artigo 11 que determina "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;". Pode-se aplicar a Lei sem consentimento nos casos de "cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;". Dessa forma, esses dados, mesmo que sensíveis, recaem sob a administração do TSE devido a regulação da ICN. Em outras palavras temos que qualquer dado armazenado nas bases de dados da ICN está protegido pela LGPD. Por estes motivos a dispensa de consentimento se justifica para coleta, armazenamento e uso dos referidos dados.

Analisando ainda as leis supracitadas temos que o compartilhamento de dados sensíveis coletados pelo TSE é incompatível com a tutela jurídica de dados pessoais ou direito à privacidade. O armazenamento e coleta de tais informações não justificam o uso indiscriminado por órgãos públicos. O artigo 23 da LGPD enuncia que "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". Essas brechas dão margem a interpretações mal intencionadas sob o pretexto de garantir a segurança, integridade dos cidadãos ou eficiência do Estado.

Outro ponto que devemos ressaltar é o compartilhamento com instituições de segurança, como a Polícia Civil e Federal. Qualquer cidadão poderá ser investigado criminalmente devido a possuir sua biometria cadastrada e compartilhada com tais órgãos. O acesso irrestrito a essas bases de dados para fins de segurança pública é amparada pela Lei 13.444/2017. O [Ministério da Saúde 2018] determina na portaria 248/2018, de forma obrigatória, que recém-nascidos possuam a identificação palmar e biométrica da mãe.

A legitimidade destas autorizações pode, portanto, ser questionada ou avaliada através da LGPD. A coleta, por ser obrigatória ou não autorizada, pode criar precedentes na justiça. Os dados são obtidos com os fins de identificação civil e eleitoral, não podendo assim ser utilizada para outros fins sem autorização do titular; salvo os casos previstos na LGDP. O artigo 4 da referida Lei elucida que os fins de segurança pública não podem ser justificáveis através da mesma. Assim a alteração da finalidade não pode ser justificada através deste argumento. O mesmo ocorre no artigo 21 que diz "dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo", não havendo assim base legal para persecução criminal ou ações similares.

Outro ponto relevante relacionado com a disponibilização de dados pessoais pelo TSE é que alguns dos dados pessoais dos eleitores, como por exemplo, os dados biométricos e o CPF entre outros ficam residentes em terminais das urnas eletrônicas. E neste sentido, existe a possibilidade destes dados serem obtidos, por exemplo, se as urnas forem violadas.

3. Testes Públicos de Segurança

As urnas eletrônicas, desde o início da sua utilização, vêm sofrendo críticas sobre sua confiabilidade, transparência e segurança. Para minimizar tais críticas, o TSE realizou alguns testes de segurança, como por exemplo, em 2012 [Tribunal Superior Eleitoral 2012c]. E em 2015, através da resolução 23.444 de 30 de abril de 2015 instituiu o Teste Público de Segurança (TPS), que devem ser realizados antes de cada eleição ordinária, cujos detalhes são definidos por editais próprios [Tribunal Superior Eleitoral - TPS 2015].

No teste de 2012, um dos testadores mostrou que era possível quebrar o sigilo do voto, indicando em qual candidato cada eleitor estaria votando [Tribunal Superior Eleitoral 2012b]. Com isso, dados pessoais sensíveis de eleitores, como no caso voto poderiam ser comprometidos. Nos EUA, só o fato de o Facebook repassar dados que permitissem estimar posições políticas dos usuário para uma empresa (Cambridge Analytica) já foi considerado algo bastante grave, imagina se fosse possível repassar os votos propriamente ditos.

Os TPS realizados posteriormente em 2016 e 2017 revelaram várias falhas de segurança, conforme apresentamos a seguir. Por razões de espaço não será descrito ou discutido o funcionamento dos componentes presentes na urna eletrônica. É considerado que o leitor tenha conhecimento do funcionamento da urna eletrônica e seus componentes. Os procedimentos requeridos para participação nos Testes Públicos de Segurança também serão omitidos pelo mesmo motivo. Não são relatados os testes que resultaram em falhas ou insucessos, que quebram os procedimentos adotados como medidas preventivas à ataques ou que exigem envolvimento ilícito na disponibilização dos *flashes* de memória ou no transporte dos resultados.

O Teste Público de Segurança não abrange todas as funcionalidades do sistema. O [Tribunal Superior Eleitoral - TPS 2017a], por exemplo, enuncia que não são objeto de estudo os componentes descritos no artigo 2, e que abrangem:

- identificação e verificação biométrica do eleitor;
- preparação e infraestrutura para o Kit JE Connect;
- processamento dos arquivos de urna;

- totalização (TOT) e gerenciamento de totalização (GER);
- acesso às máquinas servidoras;
- acesso aos bancos de dados;
- ataques de negação de serviço;
- ataque destrutivo à urna eletrônica e demais recursos computacionais da Justiça Eleitoral;
- sistema de geração de chaves criptográficas;
- alteração do código-fonte dos sistemas;
- ambiente de compilação dos sistemas;
- lacre físico;

Note que grande parte dessas limitações são impostas apenas para os pesquisadores e interessados em melhorar a segurança da urna. Um atacante real não iria se ater aos cuidados de não burlar os ambientes ou componentes utilizados. Esses requerimentos resultaram no impedimento de participantes realizarem testes como a verificação do transporte de dados no sistema de votação. As restrições de tempo somadas às dificuldades criadas pelo próprio TSE impedem o prosseguimento de testes mais aprofundados.

Um ponto frágil identificado no teste de 2016 associado a obtenção de informações sensíveis, pela equipe liderada por Luis Fernando de Almeida, foi a quebra do sigilo do voto nos casos da votação para deficientes visuais. A transmissão do áudio foi feita nas urnas que possuem suporte nativo (disponibilizadas em locais que possuem inúmeros eleitores com deficiência visual), nos votos de deficiente visuais e nos casos onde o mesário, mediante decisão própria, habilitou tal funcionalidade. O vetor de ataque utilizado foi um Raspberry PI e o serviço IceCast que capturam o aúdio através da interface disposta na parte traseira da urna de votação. O áudio foi transferido utilizando *ethernet*, porém poderia ser feita via WiFi, para outro computador e reproduzido no mesmo. A miniaturização de tais componentes pode facilitar esse tipo de ataque futuramente. No caso de utilização de WiFi outros dispositivos como *smartphones* poderiam ser utilizados na recepção do conteúdo, exigindo apenas que o atacante esteja próximo da(s) urna(s) alvo.

Na edição posterior, de 2017, as limitações foram mais brandas e permitiram que [Aranha et al. 2018] identificasse que existem possibilidades para obtenção da chave criptográfica simétrica que protege os cartões *flash* de memória e que contém o *software* utilizado na votação, algumas bibliotecas não possuíam assinatura digital ou verificação de integridade, manipular as chaves criptográficas *on-the-fly* e a possibilidade de modificar o conteúdo das *strings*.

Ainda na edição de 2017 houve uma tentativa por parte do TSE de burlar o sistema removendo todas as chaves criptográficas do código-fonte. Essa modificação no código-fonte resultou em uma apresentação do sistema não fidedigna com a realidade. Através da análise do código a equipe liderada por Diego Aranha conseguiu identificar referências à chave criptográfica utilizando um *branch* não sanitizado pela equipe do TSE. Através de engenharia reversa foi possível obter a chave criptográfica e decifrar o arquivo *initje* [1] com o objetivo de escalar privilégios no sistema; esse arquivo foi escolhido devido ao cabeçalho ser conhecido pelos participantes.

Ao analisar a cadeia de confiança, ou *chain of trust*, foi identificado que certos arquivos não possuíam suas assinaturas verificadas e eram possíveis de burlar. As bibli-

[1] uma versão modificada do *daemon init* utilizada comumente no Unix.

otecas responsáveis pelo log *libapilog.so* e derivação de chaves criptográficas *libhkdf.so* foram modificadas e distribuídas nas urnas de votação. Foi analisado quais funções eram chamadas e a respectiva ordem de execução. A equipe modificou a primeira função, na ordem de chamada, para imprimir no terminal o texto "FRAUDE!". A biblioteca *libhkdf.so* também foi explorada como vetor de ataque forçando a ordem e quais números deveriam ser gerados pela mesma. Como estes números são utilizados para embaralhar os votos armazenados ou proteger as informações relacionadas, um atacante poderia quebrar o sigilo do voto usando a sequência previamente gerada e conhecida, disponibilizando uma informação sensível de eleitores.

Na tentativa de burlar as informações dispostas no terminal foi iniciado um ataque utilizando as vulnerabilidades encontradas na biblioteca *libhkdf.so* e usando a aplicação VOTA (Votação Oficial). Ao desativar a proteção criptográfica na VOTA, os pesquisadores puderam extrair os conteúdos da aplicação e modificar as *strings* contidas. O texto apresentado nos registros de voto e na memória de resultados foi modificado de “A Hora da Estrela” para “A Hora da Treta”. A tela inicial também teve seu texto modificado para apresentar “VOTE 99” ao invés de “SEU VOTO PARA”. Isto está relacionado com o vazamento de informações sensíveis dos eleitores, mas pode induzir os mesmos a votar diferente.

Dado o sucesso nos testes realizados os pesquisadores iniciaram uma tentativa de manipular os votos. Foi identificada uma função *AdicionaVoto()* na aplicação VOTA, que estava vulnerável. Um *payload* foi criado para sobrescrever a região fixa de memória utilizada para armazenar os votos. Ao executá-lo foram gerados erros de consistência após pressionar a tecla “CONFIRMA”. Outras tentativas com *payloads* mais simples foram elaborados. Por questões de tempo não houve sucesso completo. O *payload* completo utilizado na aplicação simulada funcionou corretamente e sem erros de consistência.

De forma resumida, em 2017, o primeiro achado possibilita que um atacante consiga inspecionar todos os dados secretos contidos no *software* das urnas e de qualquer urna, visto que todas utilizam a mesma chave criptográfica. O segundo achado permite que seja possível inserir diretamente código arbitrário em qualquer urna ou modificar as funções utilizadas pelas mesmas. O terceiro aumenta o dano causado pelos achados anteriores sendo capaz de adulterar *logs* e, possivelmente, apagar qualquer registro de invasão ou manipulação. O último achado abre a possibilidade de modificar os conteúdos apresentados na tela de votação, sendo assim capaz de favorecer algum candidato ou grupo político.

4. Conformidade com LGPD

Nesta seção são abordados os aspectos jurídicos relacionados à aplicação da Lei nos sistemas eleitorais, com base nos achados discutidos na Seção 3. [Aranha and van de Graaf 2018] enuncia os requerimentos para eleições justas, dentre os quais podemos citar: sigilo de voto, verificabilidade do voto, integridade das urnas, contagem pública ou transparência e a possibilidade de auditar o sistema utilizado.

É conhecido, por qualquer brasileiro, que as urnas atuais não conseguem prover mecanismos suficientes para verificar se o voto foi armazenado de forma correta. Em outras palavras, o cidadão realiza o voto através do terminal que apresenta a foto do candidato e pressiona “CONFIRMA”. Após ter feito isso não há garantias de que o voto

foi registrado corretamente, pois não é possível auditar as urnas ou recuperar através de um identificador único o seu voto. Os aspectos de integridade e transparência são questionáveis e, portanto, não serão discutidos.

A partir de 2008 o TSE começou a implantar tecnologias de biometria nas urnas eletrônicas sob o pretexto de identificar os votantes de forma única e prevenir irregularidades como, por exemplo, utilização dos votos de cidadãos ausentes. Essa abordagem tecnológica pode representar uma ameaça à privacidade. Nos TPS não são testadas tais tecnologias, apesar de estarem sendo desenvolvidas há mais de 10 anos e serem amplamente utilizadas em sistemas bancários, *smartphones*, aeroportos e outros sistemas similares. Vale ressaltar que a grande utilização não implica que são seguras ou que estão implementadas de forma correta nos sistemas eleitorais; por este motivo é necessário testá-las.

A tendência tecnológica anti-fraudes e individualização do cidadão aumenta o rastro de dados pessoais existente. A grande maioria dos sistemas nos dias atuais exigem cadastro, digital ou físico, com informações tais como CPF, RG e endereço. Outros sistemas trazem tecnologias que se beneficiam desse grande volume de dados como reconhecimento de faces, padrões de comportamento pessoal e previsões através de modelos matemáticos de forma a identificar o indivíduo. A chamada economia direcionada a dados (ou *data driven economy*) resultou no aumento de 1.134% nas reclamações pelo uso indevido de dados envolvendo questões de transparência e privacidade entre os anos de 2015 e 2017, como a pesquisa realizada pelo [IDEC 2018]. O principal fator reportado é referente à publicação, consulta e coleta de dados pessoais sem autorização do titular e corresponde a 63% dos casos. O segundo lugar é ocupado com 27% das reclamações e se referem ao respeito no acesso aos dados.

No modelo da urna atual existem dois terminais: identificação e votação. Esses terminais são conectados por um cabo que provê acesso aos dados armazenados no terminal de votação. O outro terminal, de identificação, portanto é capaz de, em teoria, determinar o eleitor e qual o voto foi executado. Além disso os dados são armazenados de forma redundante nos cartões *flash* externos e internos usados nas máquinas de votação. Essa abordagem evita que os votos se percam em caso de danos irreparáveis em qualquer uma das memórias *flash*.

Em 2014 o candidato Aécio Neves convocou a auditoria das urnas após ter perdido a eleição presidencial do mesmo ano. Para realizá-la foi necessária a coleta dos documentos físicos em 16 estados por diversos agentes ao custo de, aproximadamente, R$ 1 milhão de reais. Apesar do alto custo a significância estatística é muito inferior ao desejado; Segundo o [Tribunal Superior Eleitoral 2012a] existem cerca de 500 mil urnas, porém apenas 1.187 urnas utilizadas para votação foram verificadas. O tempo previsto para realização da auditoria era de 3 dias. Devido a diversas complicações após 3 meses não foi possível determinar se houve fraude ou não. As mídias convencionais reproduziram a informação de que não havia ilegalidades na eleição e a auditoria teria sido realizada.

A geração de BUs falsos e aceitos pelo SA representa um risco à integridade da votação. E caso a colisão fosse gerada poderíamos afirmar de que há fortes indícios do sistema estar comprometido. Por razões de tempo e limitações do teste não houve a com-

provação de tais fatos. No ataque com foco na quebra do sigilo através da interceptação do áudio pode-se notar que não há um tratamento adequado neste quesito. As informações são transmitidas em canais inseguros e podem ser interpretadas por qualquer agente mal intencionado. Recomenda-se a utilização de outro meio para que deficientes visuais possam exercer o direito ao voto sem terem seu sigilo quebrado.

O ataque realizado na biblioteca *libhkdf.so* com o objetivo de quebrar o sigilo do voto é complexo pois exige que o cartão de memória seja removido a cada voto. Uma abordagem mais provável é que outras partes do sistema sejam comprometidas. Após cada voto realizado uma região auxiliar armazenaria a sequência cronológica dos votos. Ao fim da votação esse conteúdo seria copiado e decifrado pelo atacante. As aplicações que poderiam ser afetadas são, por exemplo, SCUE (Sistema de Carga da Urna Eletrônica) e VOTA (Votação Oficial).

A chave criptográfica é conhecida por todos os desenvolvedores envolvidos no projeto e armazenada em texto claro dentro dos cartões de instalação. Mesmo que o acesso seja restrito não é recomendável que essa abordagem seja utilizada. Funcionários mal intencionados podem vazar o conteúdo dos arquivos ou vendê-la para *hackers* que têm o objetivo de fraudar as eleições. Como vimos ao longo do artigo, a posse da chave criptográfica possibilita diversos outros ataques prejudiciais para a integridade dos sistemas e legitimidade da votação. Esses problemas são comuns em sistemas que usam chaves fixas e compartilhadas entre diversos dispositivos. Na edição de 2012 esse problema já havia sido identificado pelo pesquisador Diego Aranha; o que comprova que o TSE não conseguiu mitigar tais ataques ou elaborar novas estratégias nos 5 anos existentes entre as edições de 2012 e 2017.

A função de geração de números pseudoaleatórios (PRNG) não é suficientemente segura para ser utilizada na urna, como indica o próprio autor [Levin 2005]. Apesar disso o TSE insiste em utilizá-la para garantir a segurança no embaralhamento dos votos. A outra abordagem utilizada, e que apresenta menos riscos, é realizar leitura dos dados gerados pela */dev/urandom*. [Aranha et al. 2018] recomenda que o Registro Digital do Voto seja eliminado e a lei modificada.

Podemos notar que o sistema atual de votação em comparação com os princípios enunciados na LGPD, em respeito aos dados biométricos e votos, possui conformidade em alguns aspectos e não os atende em outros casos. Abaixo são descritos os 10 princípios dispostos no artigo 6 da referida lei e qual o parecer técnico a respeito de cada um:

- **Finalidade:** O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular. Esse princípio é subjetivo, visto que os mesários devem informar os eleitores no momento do cadastramento dos dados biométricos para qual finalidade serão utilizados. Se os dados forem utilizados somente para fins eleitorais não há dúvidas de sua finalidade, porém nos casos de compartilhamento a finalidade pode ser confundida ou utilizada de forma errônea.
- **Adequação:** As finalidades informadas ao titular devem ser compatíveis com o tratamento realizado e contexto. O sistema eleitoral parece estar em conformidade pois as informações biométricas e informações cadastrais, como CPF, auxiliam na identificação do eleitor e o armazenamento dos votos é necessário para contagem ou auditoria.

- **Necessidade:** Deve-se limitar o tratamento ao mínimo necessário para a realização de suas finalidades. Como o sistema biométrico ainda não foi explorado nas edições do TPS, será considerado que o tratamento realizado é mínimo e atende à necessidade imposta.
- **Livre acesso:** Os titulares devem possuir meios de consulta facilitada e gratuita a respeito de seus dados, assim como a integralidade de seus dados pessoais. A consulta da biometria não é facilitada e o eleitor não possui quaisquer mecanismos ao sair da zona eleitoral para verificar se o voto foi computado corretamente. Portanto, esse aspecto não está em conformidade em nenhum dos casos.
- **Qualidade dos dados:** Os dados coletados ou tratados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e finalidade de seu tratamento. Não há conformidade neste princípio devido ao recadastramento da biometria não ocorrer de forma facilitada. O eleitor poderá ter passado por alguma doença, uso de produtos químicos e ter danificado ou "apagado" parcialmente sua digital.
- **Transparência:** Informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento devem ser disponibilizadas para os eleitores. A transparência é subjetiva porque as leis discutidas neste artigo possuem acesso gratuito e *online*. Por outro lado, o compartilhamento destas informações não é feita de maneira transparente entre os órgãos, como prevê a ICN. O eleitor não conseguirá manter o controle dos dados.
- **Segurança:** Medidas técnicas e administrativas aptas devem ser utilizadas a fim de proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. O uso de criptografia pode ser interpretado como cumprimento da lei. Apesar dos algoritmos serem seguros e aptos, o sistema não é seguro devido a estrutura utilizada possuir falhas.
- **Prevenção:** Medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais devem ser adotadas. Esse princípio é cumprido através do Teste Público de Segurança, do Registro Digital do Voto e as mídias *flash* utilizadas no processo de votação.
- **Não discriminação:** Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Não há nenhuma informação a respeito do uso de biometria ou votos para fins discriminatórios, portanto há conformidade com este princípio.
- **Responsabilização e prestação de contas:** Demonstração da adoção de medidas eficazes e capazes de comprovar a observância, cumprimento das normas de proteção de dados pessoais e eficácia dessas medidas. No site do TSE existem diversas estatísticas relacionadas às eleições, incluindo dados do eleitorado e dados eleitorais.

É importante ressaltar que o sistema atual de votação utilizado pelo TSE pode não estar conforme com a LGPD em duas vertentes: uma pelo tratamento indevido dos dados dos eleitores pelo próprio poder público, conforme comentado nos parágrafos anteriores, mas também devido a possibilidade de dados pessoais sensíveis dos eleitores poderem ser disponibilizados de forma indevida devido a ataques.

O artigo 46 da LGPD diz: "Os agentes de tratamento devem adotar medidas de

segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." [Congresso Nacional 2018]. O TSE, restringindo o escopo e as possibilidades para o único teste permitido sobre as urnas, não adota as medidas de segurança necessárias para proteger os dados pessoais. Em concreto, não é possível afirmar que sistema de biometria é seguro e, consequentemente, se os dados biométricos podem ser vazados ou não, visto que o sistema de biometria não faz parte do escopo do TPS.

Os sistemas avaliados nas edições anteriores dos Testes de Segurança mostraram várias falhas. Conforme comentado anteriormente, no TPS 2016, foi mostrada a possibilidade de quebra de sigilo nos votos de deficientes visuais. No último TPS, em 2017, uma chave criptográfica que permite decifrar parte do sistema operacional foi obtida e, com isso, também seria possível violar o sigilo dos votos, neste caso para todos votantes em uma determinada urna. O TSE afirma que corrigiu essa vulnerabilidade, mas não houve teste posterior para tal verificação.

5. Conclusão

O artigo aborda os diferentes aspectos das leis, suas consequências e suas brechas. Uma análise de conformidade com o sistema atual de votação é feito e são apresentados as falhas identificadas nos TPS 2016 e 2017. Cada princípio da LGPD é analisado levando com consideração os dados sensíveis.

As próximas edições do TPS devem dar total liberdade aos pesquisadores, *hackers* e especialistas em segurança a fim de que o sistema, em sua totalidade, seja testado e avaliado. A escolha de segurança por obscuridade não representa uma razão técnica positiva. Sistemas que possuem sua segurança baseados em razões de desconhecimento são facilmente burlados e dependem somente do fator temporal.

A partir das vulnerabilidades encontradas nos Testes Públicos de Segurança e notícias de vazamentos de dados nos mais diversos sistemas, o leitor pode também se questionar a respeito da segurança, tecnologias e os riscos à privacidade existente em tais sistemas. O questionamento, portanto, é se os sistemas e tecnologias propostas possuem maturidade suficiente para prover ou tratar os dados envolvidos e se os órgãos possuem competência para cumprir suas obrigações sem se evadir dos questionamentos técnicos.

Outras perguntas que devem ser feitas são como o eleitor pode verificar seu voto atualmente, se a pessoas física é capaz de controlar os dados coletados, há garantias de anonimização nos conteúdos compartilhados entre as diversas entidades e quais são as motivações que justificam a separação de empresas privadas e públicas nas normas regulatórias previstas nas leis. A questão de anonimização é elucidada devido ao perigo inerente no transporte de tais dados sensíveis, que não podem ser compartilhados de forma direta. E, se essa for feita, qual será a utilidade do dado para o órgão requerente?

Ainda podemos ressaltar que as decisões judiciais, geralmente, não são baseadas em pesquisas científicas ou por juízes que possuem conhecimento elevado das tecnologias utilizadas. O desconhecimento dos impactos tecnológicos causados por suas ações são, por vezes, maiores que aqueles causados pelos próprios desenvolvedores ou responsáveis pelo sistema.

Podemos concluir que as leis discutidas neste trabalho podem auxiliar no avanço tecnológico através das regulações impostas sobre o tratamento de dados. Os legisladores poderiam utilizar o conhecimento científico disponível nos próprios órgãos públicos a fim de elaborar regras mais claras sobre, por exemplo, o sistema de votação.

Referências

[Aranha et al. 2018] Aranha, D. F., Barbosa, P. Y. S., Cardoso, T. N. C., de Araújo, C. L., and Matias, P. (2018). The return of software vulnerabilities in the brazilian voting machine. *Relatório Técnico*.

[Aranha and van de Graaf 2018] Aranha, D. F. and van de Graaf, J. (2018). The good, the bad, and the ugly: Two decades of e-voting in brazil. *IEEE Security & Privacy*, 16(6):22–30.

[Congresso Nacional 2014] Congresso Nacional (2014). Marco civil da internet. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 18 de junho de 2019.

[Congresso Nacional 2017] Congresso Nacional (2017). Identidade civil nacional. "http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/Lei/L13444.htm". Acessado em 18 de junho de 2019.

[Congresso Nacional 2018] Congresso Nacional (2018). Lei geral de proteção de dados. "http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm". Acessado em 18 de junho de 2019.

[CONTRAN 2007] CONTRAN (2007). Resolução contran nº 249, de 27 de agosto de 2007. https://www.normasbrasil.com.br/norma/resolucao-249-2007_106036.html. Acessado em 18 de junho de 2019.

[IDEC 2018] IDEC (2018). Reclamações sobre cadastros financeiros de consumidores crescem 1.344% entre 2015 e 2017. https://idec.org.br/release/reclamacoes-sobre-cadastros-financeiros-de-consumidores-crescem-1344-entre-2015-e-2017. Acessado em 18 de junho de 2019.

[Levin 2005] Levin, I. (2005). Sapparot-2. http://www.literatecode.com/sapparot2. Acessado em 18 de junho de 2019.

[Ministério da Saúde 2018] Ministério da Saúde (2018). Portaria 248. "http://bvsms.saude.gov.br/bvs/saudelegis/gm/2018/prt0248_05_02_2018.html". Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2007] Tribunal Superior Eleitoral (2007). Resolução tse nº 22.688 de 13 de dezembro de 2007. https://www.normasbrasil.com.br/norma/resolucao-22688-2007_107293.html. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2009] Tribunal Superior Eleitoral (2009). Resolução tse nº 23.061, de 26 de maio de 2009. http://www.tse.jus.br/legislacao/codigo-eleitoral/normas-editadas-pelo-tse/resolucao-nb0-23.061-de-26-de-maio-de-2009-brasilia-2013-df. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2012a] Tribunal Superior Eleitoral (2012a). Depósito de urnas. http://www.tse.jus.br/o-tse/cultura-e-historia/o-tse/sede-atual/videos-nova-sede/deposito-de-urnas. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2012b] Tribunal Superior Eleitoral (2012b). Relatório dos resultados do grupo 01 - tps 2012. http://www.justicaeleitoral.jus.br/arquivos/relatorio-dos-resultados-da-realizacao-dos-testes-publicos-de-seguranca-da-urna-eletronica-plano-1-grupo-1. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2012c] Tribunal Superior Eleitoral (2012c). Teste público de segurança 2012. http://www.tse.jus.br/eleicoes/eleicoes-anteriores/eleicoes-2012/testes-publicos-de-seguranca-do-sistema-eletronico-de-votacao. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2017] Tribunal Superior Eleitoral (2017). Minuta sobre adição de voto impresso. http://www.justicaeleitoral.jus.br/arquivos/tse-audiencias-publicas-voto-impresso. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2018] Tribunal Superior Eleitoral (2018). Esclarecimentos sobre utilização das urnas eletrônicas. http://www.tse.jus.br/hotsites/esclarecimentos-informacoes-falsas-eleicoes-2018/somente-3-paises-utilizam-urnas-eletronicas.html. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral 2019] Tribunal Superior Eleitoral (2019). Consulta quantitativa de eleitores no brasil. "http://www.tse.jus.br/eleitor/estatisticas-de-eleitorado/consulta-quantitativo". Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral - TPS 2015] Tribunal Superior Eleitoral - TPS (2015). Resolução 23.444 de 30 de abril de 2015. http://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/arquivos/resolucao-no-23-444-de-30-de-abril-de-2015. Acessado em 12 de agosto de 2019.

[Tribunal Superior Eleitoral - TPS 2016] Tribunal Superior Eleitoral - TPS (2016). Compêndio tps 2016. http://www.justicaeleitoral.jus.br/arquivos/tse-testes-publicos-de-seguranca-2016-compendio. Acessado em 18 de junho de 2019.

[Tribunal Superior Eleitoral - TPS 2017a] Tribunal Superior Eleitoral - TPS (2017a). Edital tps 2017. http://www.justicaeleitoral.jus.br/arquivos/tse-edital-testes-publicos-de-seguranca-2017. Acessado em 15 de agosto de 2019.

[Tribunal Superior Eleitoral - TPS 2017b] Tribunal Superior Eleitoral - TPS (2017b). Relatório técnico tps 2017. Acessado em 18 de junho de 2019.