ILUSTRÍSSIMA SENHORA PROCURADORA GERAL ELEITORAL, SENHORA
RAQUEL ELIAS FERREIRA DODGE, NO TRIBUNAL SUPERIOR ELEITORAL

O **Comitê Multidisciplinar Independente** – *CMInd* – neste ato representado por Pedro Antônio Dourado de Rezende, professor de Ciência da Computação da Universidade de Brasília (UnB) na área de segurança computacional, vem respeitosamente perante V.Exa. requer seja **designada audiência publica,** com a convocação dos técnicos da Secretaria de Informática que respondem pelo projeto do Sistema Eletrônico de Votação desse Egrégio Tribunal, para prestarem esclarecimentos quanto aos fatos abaixo:

Como é de conhecimento publico, ao participar dos testes públicos de segurança promovidos por este Tribunal no ano de 2012, o investigador Diego de Freitas Aranha, na ocasião professor da UnB, onde antes fora meu aluno, atualmente lecionando e pesquisando na Unicamp, detectou e relatou, dentre outras vulnerabilidades e/ou falhas no sistema eletrônico de votação em uso no Brasil, as seguintes:

1. *"Proteção inadequada do sigilo do voto: os votos são armazenados fora de ordem, mas é trivial recuperá-los em ordem a partir unicamente dos produtos públicos de uma eleição e conhecimento superficial do código-fonte, que também é de acesso público aos partidos políticos;"*

2. *"Cifração inadequada: a mesma chave criptográfica é utilizada para cifrar as mídias de todas as urnas eletrônicas. Utilizando a analogia clássica de um cadeado como abstração de técnica criptográfica, isto é equivalente a proteger meio milhão de cadeados com uma mesma chave, visto ser este o número aproximado de equipamentos em opera-ção. Além disso, a chave que decifra todas as mídias é armazenada às claras na porção decifrada das mídias. Utilizando a mesma analogia, isto equivale a esconder a chave do cadeado embaixo do tapete e confiar no segredo dessa localização como fonte de segurança* (...)" Extraído de https://sites.google.com/site/dfaranha/pubs/aranha-karam-miranda-scarel-12-pt, em 2/12/17

Segundo vários informes jornalísticos e oficiais desde então, o TSE já teria consertado tais problemas, incluindo para as eleições de 2014.

Porém, conforme informou o Sr Ministro Presidente do TSE em 01/12/2017, comentando resultados dos testes realizados em programas que poderão ser utilizados nas eleições de 2018, agora foram detectados os seguintes:

> *De acordo com a explicação técnica do coordenador de sistemas eleitorais do TSE, José de Melo Cruz, o grupo 1, que alcançou maior êxito, conseguiu decifrar o sistema de arquivo da urna. Na prática, eles obtiveram uma chave criptográfica que permitiu o acesso a arquivos da urna e conseguiram ler e transcrever as informações. A partir desse acesso, "eles fizeram algumas experiências e conseguiram acoplar um teclado e ecoar alguns dados desse teclado na urna eletrônica" (...)*
>
> *"Eles conseguiram acesso ao Log (registros de eventos do software da **urna eletrônica)**, que é um sistema que registra todos os eventos que ocorrem na máquina, comparado a*

uma caixa preta de um avião. A partir daí, "eles conseguiram acesso ao RDV (Registro Digital do Voto) (...)"

Isso mostra que os problemas encontrados em 2012 de alguma forma persistem, pois ressurgiram por outras vias nos mesmos pontos de penetração, ou seja, nos arquivos de Registro Digital de Votos (RDV) e na gestão de chaves criptográficas, exatamente como alertado pelo mesmo Professor Diego Aranha em seu relatório referente ao teste que coordenou no TSE em 2012.

Ademais, isso implica que a linha proposta pelo Professor Aranha para seus testes no sistema em 2017 teria sido em continuidade ao que ele e sua equipe anterior haviam descoberto em 2012, possivelmente considerando a natureza estrutural ou a origem sistêmica das vulnerabilidades encontradas, aludidas na parte supracitada do seu relatório pela analogia da chave mestra guardada debaixo de um tapete.

Os recentes êxitos nos testes de penetração executados nessa linha apontam fragilidades graves cuja natureza e origem já eram de conhecimento dos técnicos do TSE, mas que injustificadamente não foram corrigidas a contento, persistindo já por cinco anos e, com isso, conspurcando três ou – a menos de uma drástica mudança de rumo – talvez até quatro eleições.

O que se comentava durante o evento realizado pelo TSE no final de novembro foi que os investigadores do grupo 1 descobriram como obter chaves criptográficas, mesmo em condições restritas e censurantes sob as quais foram permitidos os tais "testes", e com elas desnudar ou alterar dados que deveriam estar protegidos por sigilo na urna, inclusive do arquivo RDV, bem como identificar voto de eleitor.

De fato, em entrevista divulgada em mídia nacional encontramos a confirmação da violação ao sigilo do voto por investigadores:

*'(...) Segundo o coordenador de sistemas eleitorais do Tribunal Superior Eleitoral (TSE), José de Melo Cruz, **"é possível**" que os técnicos tenham conseguido identificar como foi o último voto registrado numa urna. A informação foi passada pela manhã, quando os testes ainda estavam sendo feitos. (...)'* Extraído de https://g1.globo.com/politica/noticia/tecnicos-identificam-falhas-em-urna-eletronica-e-tse-diz-serao-corrigidas.ghtml, em 1/12/17

Assim, é necessário que o TSE explique à sociedade porque essas vulnerabilidades vêm persistindo, e sendo permitidas ao longo de tantas eleições. Inclusive por que, ante a precariedade do "conserto" que teria aplicado às falhas descobertas no seu sistema em 2012, ainda assim dois anos depois escolheu empresa inidônea com participação estrangeira para também manusear o metafórico tapete, aludido pelo professor Aranha em sua análise da natureza das vulnerabilidades encontradas (vide http://cic.unb.br/~rezende/trabs/relatorio-smart.html, acessado em 4/12/2017).

Temos que lembrar que o RDV foi introduzido em 2003 por um esforço desse mesmo Tribunal em eliminar da Lei Nº 10.402/2002 a obrigatoriedade do voto impresso em seu sistema eleitoral, sob a justificativa de que tal "invenção" seria um substituto adequado para fins de fiscalização. Não se justifica então

que 14 anos depois esse substituto ainda venha apresentando tantos problemas graves, sejam conceituais, de implementação ou operacionais.

A menos que tal curso, mantido com a impúdica derrubada do art. 5º da Lei 12.034/2009, seja ele o verdadeiro retrocesso democrático, camuflado de evolução teconógica. Porém, ainda trajando desenho vintagenário de sistema eleitoral eletrônico que todo o resto do mundo democrático já abandonou, pelas mesmas razões aludidas pelo professor Aranha.

Ante a gravidade da situação, solicita o peticionante seja convocada audiência publica para apresentação de justificativas quanto à persistência dessas vulnerabilidades, e debate sobre alternativas de rumo capazes de oferecer à sociedade lisura nas eleições em forma e em medida ansiadas por quem clama por democracia limpa com eleições verificáveis, inclusive exigida em Lei (13.165/2015), ao arrepio de protelações artificiosas e ampla propaganda de quem porventura insiste em um curso que vai se tornando cada vez mais perigoso para o Brasil.

Nestes Termos
Pede e Espera deferimento

Brasilia, 04 de dezembro de 2017

PEDRO ANTONIO DOURADO DE REZENDE
Professor de Ciência da Computação da UnB