UNIVERSIDADE DE SÃO PAULO

Missão de Observação Eleitoral 2022

USP

UNIVERSIDADE DE SÃO PAULO

Missão de Observação Eleitoral
2022

Administração da Universidade de São Paulo

Carlos Gilberto Carlotti Junior
Reitor

Maria Arminda do Nascimento Arruda
Vice-Reitora

Aluisio Augusto Cotrim Segurado
Pró-Reitor de Graduação

Marcio de Castro Silva Filho
Pró-Reitor de Pós-Graduação

Paulo Alberto Nussenzveig
Pró-Reitor de Pesquisa

Marli Quadros Leite
Pró-reitora de Cultura e Extensão Universitária

Fernando Facury Scaff
Superintendente Jurídico

Marina Helena Cury Gallottini
Secretária Geral

Arlindo Philippi Junior
Chefe de Gabinete

Edmilson Dias de Freitas
Coordenador Executivo do Gabinete do Reitor

UNIVERSIDADE DE SÃO PAULO

Missão de Observação Eleitoral 2022

Relatório final

Sumário

1. A Equipe da MOE USP **7**

2. Relatos **9**

2.A. O período pré-eleitoral 9

2.B. O 1º turno das eleições 12

2.C. O 2º turno das eleições 14

2.D. O período pós-eleitoral 17

3. Análise Conclusiva **19**

4. Recomendações da MOE USP para as próximas eleições **21**

Agradecimentos **23**

ANEXOS

Anexo 1. Comentários sobre alegações infundadas ou falsas sobre as urnas eletrônicas brasileiras **26**

Anexo 2. Considerações sobre os logs das urnas eletrônicas brasileiras usadas nas eleições de 2022 ..... **40**

Apêndices ao Anexo 2 ..... **69**

Apêndice I – Passo a passo para realizar a "impossível" tarefa de verificar a correspondência entre logs de urnas e as urnas correspondentes. Siga o que pedem as figuras 70

Apêndice II – Como encontrar o código de identificação da urna no BU e no RDV 80

Apêndice III – Modificação de log da urna eletrônica: desmentindo que ID_UE tem alguma relevância quando comparado com assinatura digital 89

Apêndice IV – VAR UE – Verificando as Assinaturas de Resultados da Urna Eletrônica 93

Referências 95

1. A Equipe da MOE USP

Atendendo ao Edital de Chamamento Público nº 01/2022, do Tribunal Superior Eleitoral, a USP organizou uma Missão de Observação Eleitoral – MOE com a seguinte equipe (em ordem alfabética):

1. **Bruno de Carvalho Albertini, Professor Doutor da Escola Politécnica**, do Departamento de Engenharia de Computação e Sistemas Digitais;
2. **Daniel Macedo Batista, Professor Associado do Instituto de Matemática e Estatística**, do Departamento de Ciência da Computação;
3. **Edson Satoshi Gomi, Professor Doutor da Escola Politécnica**, do Departamento de Engenharia de Computação e Sistemas Digitais;
4. **Fátima de Lourdes dos Santos Nunes Marques, Professora Titular da Escola de Artes, Ciências e Humanidades**;
5. **Fernando Facury Scaff, Professor Titular da Faculdade de Direito**, do Departamento de Direito Econômico, Financeiro e Tributário, que exerce a função de **Coordenador desta Missão de Observação Eleitoral**, conforme designação do Magnífico Reitor da USP (Portaria Interna 634, 05/07/22);
6. **Flávio Luiz Yarshell, Professor Titular da Faculdade de Direito**, do Departamento de Direito Processual;
7. **Floriano de Azevedo Marques Neto, Professor Titular da Faculdade de Direito**, do Departamento de Direito do Estado;
8. **Graça Bressan, Professora Doutora da Escola Politécnica**, do Departamento de Engenharia de Computação e Sistemas Digitais;
9. **Jó Ueyama, Professor Titular do Instituto de Ciências Matemáticas e de Computação**;
10. **Marcos Antonio Simplicio Junior, Professor Associado da Escola Politécnica**, do Departamento de Engenharia de Computação e Sistemas Digitais;
11. **Ronaldo Porto Macedo Junior, Professor Titular da Faculdade de Direito**, do Departamento de Filosofia e Sociologia do Direito; e
12. **Wilson Vicente Ruggiero, Professor Titular da Escola Politécnica**, do Departamento de Engenharia de Computação e Sistemas Digitais.

A tônica da USP na MOE foi a de congregar docentes de diferentes áreas de atuação, oriundos da Faculdade de Direito, da Escola Politécnica, da Escola de Artes, Ciências e Humanidades e do Instituto de Matemática e Estatística, contando com o apoio do EGIDA – Escritório de Gestão de Indicadores de Desempenho Acadêmico e sob a coordenação da Superintendência Jurídica. As áreas de conhecimento desse grupo abarcam alguns dos principais aspectos que estavam em xeque na disputa eleitoral: ciência da computação, envolvendo conhecimento de redes de informática, tecnologia de *software* e de *hardware* das urnas eletrônicas e estatística, além de diversos aspectos jurídicos.

Para evitar dispersão em sua atuação, o grupo decidiu concentrar esforços na eleição presidencial e na dinâmica de todo o processo eleitoral, seja no período pré-eleitoral, seja nos desdobramentos da eleição. Dessa forma, diversos aspectos que são usualmente abordados pelas MOEs nacionais e internacionais foram apenas observados lateralmente, tais como o comparecimento dos eleitores às urnas ou o comportamento dos mesários no dia da eleição.

Este Relatório analisa as eleições de 2022, tendo por base a disputa presidencial, contextualizando o período pré e pós-eleitoral, e não apenas os dias em que foram realizadas as votações em 1º e 2º turnos. Tal enfoque amplia a ótica de análise, a fim de que se possa compreender a dinâmica do processo, e não apenas fatos isolados, servindo para informar *urbi et orbe* ("para a cidade e o mundo") o que se passou nas eleições presidenciais de 2022, sendo um Relatório *independente*, que deve *obrigatoriamente* ser apresentado ao *Presidente do TSE* e *às Chefias dos Poderes da República* (Resolução TSE 23.678/21, art. 24, §3º). Foram observados, em especial, aspectos referentes à segurança das urnas eletrônicas e o âmbito jurídico da eleição presidencial de 2022, contendo, ao final, algumas recomendações para o aperfeiçoamento do sistema.

2. Relatos

2.A. O período pré-eleitoral

Não há como compreender o ambiente eleitoral de 2022 sem analisar a questão da prisão e da soltura do ex-Presidente Luiz Inácio Lula da Silva, fruto das acusações que lhe haviam sido formuladas pela denominada Operação Lava Jato.

O ex-Presidente havia sido condenado em julho de 2017 pelo então juiz federal Sergio Moro, que estabeleceu pena de 9 anos e 6 meses de prisão pelos crimes de corrupção passiva e de lavagem de dinheiro. Foi interposto recurso ao TRF da 4ª Região, que em janeiro de 2018 manteve a condenação, com aumento de pena. A despeito da interposição de diversos outros recursos, o ex-Presidente foi recolhido à prisão em abril de 2018, onde passou 580 dias. Naquela ocasião, o ex-Presidente liderava as pesquisas eleitorais para Presidência que ocorreriam em outubro de 2018, mas foi impedido de disputar.

Em novembro de 2019, o STF decidiu que a Constituição prescrevia que presunção de inocência só poderia cessar após o trânsito em julgado das ações penais propostas, e, com isso, o ex-Presidente foi libertado.

Em março de 2021, o STF decidiu pela anulação de todos os atos decisórios praticados pelo então magistrado Sérgio Moro no âmbito da Ação Penal que havia condenado o ex-Presidente, incluindo os atos praticados na fase pré-processual.

Com isso, o ex-Presidente Lula da Silva pôde concorrer novamente à Presidência da República nas eleições que ocorreram em outubro de 2022.

Desde o início das pesquisas eleitorais para a disputa de 2022 dois candidatos à Presidente da República despontavam como favoritos: o Presidente da República, Jair Bolsonaro, candidato à reeleição, e o ex-Presidente Luiz Inácio Lula da Silva, em busca de um terceiro mandato.

O ambiente pré-eleitoral foi caracterizado por uma escalada de agressões, tendo como centro a inviolabilidade das urnas eletrônicas, tema constantemente apontado pelo candidato à reeleição.

As urnas eletrônicas são usadas no Brasil desde 1996, encerrando um período em que o voto impresso dava margem a incontáveis manipulações, fraudando a expressão da vontade popular. No sistema eletrônico os votos são registrados e apurados na própria urna, que os consolida e apresenta a totalização do resultado em um documento impresso denominado Boletim de Urna – BU, que fica disponível ao público em geral em cada Seção Eleitoral. Em 2022, para apuração do voto de 156

milhões de eleitores, existiram 2.637 Zonas Eleitorais, divididas em 496.512 Secções Eleitorais, que utilizaram mais de 577.000 urnas eletrônicas, cujo BU fica acessível *on-line* e em tempo real, para quaisquer interessados, que podem somar os resultados urna a urna antes mesmo do TSE, sendo possível desta forma realizar uma verdadeira contagem paralela. De cada urna eletrônica surgem quatro documentos: o BU, a tabela de registro digital dos votos, o rol de eleitores que não compareceram e os ***logs*** (registros de eventos) do *software* – registros que são públicos e passíveis de auditoria.

Mesmo com todo esse histórico de utilização das urnas eletrônicas e do sistema de controle e auditoria descrito, foram incontáveis as imprecações realizadas contra esse sistema pelo candidato à reeleição, em múltiplos discursos, como o ocorrido em abril de 2022, quando o candidato à reeleição promoveu um "ato cívico pela liberdade de expressão" no Salão Nobre do Palácio do Planalto, atacando o TSE e alegando nele existir "uma sala secreta", na qual "meia dúzia de técnicos dizem no final: 'Olha, quem ganhou foi este.'" Por esse motivo havia recomendado às Forças Armadas realizar contagem paralela dos votos. Embora fizessem parte da Comissão de Transparência Eleitoral, a convite do próprio TSE, as Forças Armadas, através do Ministro da Defesa, Paulo Sérgio Nogueira, comunicaram ao TSE que mandariam representantes para fiscalizar a eleição. O então Presidente do TSE, Ministro Edson Fachin, determinou que inscrevessem seus representantes na forma da legislação eleitoral aplicável e afirmou que "Quem trata de eleições são forças desarmadas e, portanto, as eleições dizem respeito à população civil que, de maneira livre e consciente, escolhe seus representantes". O TSE informou na ocasião que mais de 70% das propostas da Comissão de Transparência Eleitoral foram acolhidas para as Eleições 2022, pois, das 44 sugestões apresentadas, 32 foram implementadas e 11 seriam analisadas para o novo ciclo eleitoral (2023-2024), tendo sido rejeitada apenas uma.

De fato, a busca era para ser adotado o voto impresso, mantendo o voto eletrônico, isto é, cada eleitor sairia da cabine de votação com um documento comprovando em quem havia votado, o que poderia ensejar o retorno ao sistema de *voto de cabresto*, através da intimidação daqueles eleitores que tivessem votado em candidatos distintos dos que haviam sido recomendados pelos apoiadores eleitorais. Observe-se que, diversamente do alegado, tal procedimento não permitiria a totalização dos votos, em face de sua enorme fragmentação. Ocorre que a Proposta de Emenda Constitucional que previa o retorno do voto impresso havia sido rejeitada na Câmara dos Deputados em agosto de 2021, tendo sido computados 229 votos favoráveis, 218 contrários e 1 abstenção, o que levou ao seu arquivamento por não ter conseguido o quórum mínimo de 308 votos favoráveis. No dia dessa votação, com claro intuito intimidatório ao Congresso, foi realizado um inusitado desfile de tanques blindados em Brasília, a pretexto de convidar o Presidente para um exercício militar que ocorreria nas cercanias, o que jamais havia sido visto, nem no período da ditadura militar.

Registre-se ainda que o candidato Bolsonaro já havia sido eleito inúmeras vezes deputado federal pelo Estado do Rio de Janeiro, bem como Presidente da República em 2018, através do sistema de urnas eletrônicas. Seu rotineiro discurso contra o sistema de apuração eletrônico de votos foi objeto de uma transmissão ao vivo em julho de 2021, com mais de duas horas, visando apresentar as provas de fraude nas urnas eletrônicas, porém jamais as demonstrou, tendo declarado no minuto 47 do vídeo que "Não temos provas".

Esse discurso foi repetido em uma peculiar reunião realizada em julho de 2022, para a qual foram convocados todos os Embaixadores de países estrangeiros creditados no Brasil, para demonstração de uma suposta fragilidade do sistema de urnas eletrônicas. Ocorre que nenhuma fragilidade ficou evidenciada, o que ocasionou um constrangimento internacional para a imagem do Brasil no mundo. Na mesma ocasião, foi elevado o tom das críticas contra o TSE e o STF, o que se manteve até o final das eleições.

No dia 11 de agosto, a Faculdade de Direito da USP, com a presença de mais de 13.000 pessoas, promoveu a leitura da *Carta às Brasileiras e aos Brasileiros em defesa do Estado Democrático de Direito*, que foi subscrita por 3.400 Instituições da sociedade civil e mais de 1.087.000 indivíduos, com amplíssima repercussão na imprensa e mídias sociais. Nessa mesma linha, centenas de Faculdades de Direito por todo o Brasil promoveram a leitura do documento, movimentando a população em prol da defesa da Democracia.

Às vésperas do dia da votação alguns fatos geraram forte comoção. Um apoiador do candidato Bolsonaro invadiu uma festa de aniversário que estava sendo realizada por apoiadores do candidato Lula, em um condomínio privado, em Foz do Iguaçu, no Paraná, e matou o aniversariante a tiros. O ex-deputado Roberto Jefferson, também apoiador do candidato à reeleição, que cumpria prisão domiciliar, abriu fogo contra viaturas da Polícia Militar do Rio de Janeiro, inclusive jogando granadas de mão, e conclamando a insurgência civil contra a realização das eleições, que, segundo ele, estariam sendo manipuladas. Logo após, a deputada federal Carla Zambelli, igualmente vinculada ao candidato Bolsonaro, perseguiu um manifestante com arma em punho no Centro de São Paulo, pois ele a havia constrangido minutos antes.

Sobrepairando esse clima belicoso subsistiam dois Decretos exarados pelo Presidente Bolsonaro (Decreto nº 10.627 e Decreto nº 10.628, ambos de 12 de fevereiro de 2021), facilitando de forma significativa o processo de aquisição, cadastro, registro e posse de armas de fogo e de munições, retirando diversas barreiras e exigências para a aquisição e registro de armas e munições de maior potencial danoso. Tais Decretos foram objeto de diversas Ações Diretas de Inconstitucionalidade (ADI 6139, 6466 e 6119, entre outras) propostas logo após sua edição, sendo que, durante a sessão de julgamento, o Ministro Nunes Marques pediu vistas (em 28/09/21), sendo o julgamento prosseguido após um ano, com a concessão da liminar suspendendo os efeitos dessas normas por infringirem diversas leis que disciplinavam a matéria – porém a disseminação armamentista na sociedade já estava concretizada.

O ambiente eleitoral era tenso, fruto da escalada de agressões e de escaramuças armadas que se via pontualmente pelo Brasil, segundo divulgado pela imprensa tradicional e pelas mídias sociais.

2.B. O 1º turno das eleições

Ainda no sábado, 1º de outubro, véspera do 1º turno das eleições, no bojo da programação organizada para os observadores internacionais, a MOE USP esteve presente no TRE, em São Paulo, e no TSE, em Brasília, tendo constatado *in loco* um Judiciário firmemente empenhado em dar a mais ampla publicidade possível às práticas que realiza e aperfeiçoa há anos.

Em São Paulo, o plenário do Tribunal Regional Eleitoral ficou tomado na manhã de sábado, para escolha das urnas que deveriam ser objeto dos Testes de Integridade, uma das principais ferramentas de auditoria do sistema eleitoral. Esse processo foi feito com a direta participação das inúmeras entidades que ali se fizeram representar, que incluíam partidos políticos e outras entidades representativas da sociedade. A elas se facultou, em sistema de sorteio, a escolha dos locais tomados como referência para aquele controle, o que se fez a partir de uma divisão espacial do Estado. Essa abordagem assegurou isonomia e representatividade nas amostras, com o objetivo de conferir maior credibilidade aos resultados. Os trabalhos transcorreram de forma séria, eficiente e serena e, em alguns momentos, até descontraída.

Seguiu-se a essa atividade a execução de urnas em modo de eleição simulada, durante a qual foi possível observar a emissão da denominada "zerézima" dos sistemas. Mais adiante, houve ainda uma sessão destinada à apresentação do sistema eletrônico de votação, com demonstração a partir das urnas.

Os trabalhos do domingo, dia do 1º turno das eleições, dia 02 de outubro, no TRE, em São Paulo, começaram logo cedo, com o acompanhamento do início da votação na Universidade Mackenzie, seguidos da observação do Teste de Integridade das urnas no Centro Cultural São Paulo e de visita ao local de votação organizado na UNIP/Paraíso, para vistoria do projeto-piloto do teste de integridade com biometria. Na parte da tarde, houve nova reunião para que fosse acompanhado o encerramento da votação, o que se deu em escola próxima ao TRE-SP, ao que se seguiu o acompanhamento da divulgação da apuração e resultados na sala de imprensa da Corte. Atuação similar aconteceu na UNIP/Paraíso, com acompanhamento da conclusão do teste de integridade com biometria, o qual não revelou qualquer discrepância entre os votos lançados e os computados nas urnas averiguadas.

No TSE, em Brasília, os trabalhos se desenvolveram com a mesma tranquilidade na apuração dos votos, não havendo qualquer registro de irregularidades. Todas as Missões foram convidadas a conhecer a sala de apuração da votação, na qual existiam inúmeros computadores e servidores envolvidos com o acompanhamento do ritmo da votação.

Não há dúvida de que a observação realizada pela Comissão – assim como aquela feita pelos demais que a tanto se dispuseram – proporciona visão limitada de um fenômeno complexo,

quer porque se trata uma eleição nacional, voltada à escolha de diferentes cargos, quer pelo ambiente político de notória e excepcional ebulição. Outros mecanismos certamente são aptos, com objetividade e maior grau de segurança, a constatar e medir os acertos e desacertos. Entre os últimos, ganhou notoriedade a questão da implantação do sistema de biometria, que teria sido um dos fatores determinantes do aumento do tempo de espera para votação durante o 1º turno.

Outro ponto observado como fonte de algum questionamento refere-se ao voto em trânsito, o que levou os boletins de urna das seções afetadas a apresentar um número maior de eleitores aptos a votar para o cargo de Presidente do que para outros cargos. Embora esse fato em nada possa ser considerado como um indicativo de irregularidade ou falha, ele acabou gerando algum ruído entre eleitores, suscitando o interesse em deixar mais clara a informação do número de eleitores em trânsito diretamente no Boletim de Urna – informação que hoje já pode ser obtida como uma mera subtração do número de eleitores aptos para votar em Presidente e em outros cargos.

É preciso considerar que eventuais queixas relacionadas à demora do processo de votação, bem como a eventuais dúvidas sobre as informações fornecidas pelas urnas ao final do pleito, rigorosamente em nada respaldam alegações que têm por objetivo colocar em dúvida a credibilidade do sistema de votação. Por exemplo, no caso da biometria, o que se implantou foi mais um mecanismo que tem por objetivo aumentar a lisura do processo eleitoral e, como na vida, pode ocorrer que dado progresso demande esforço e algum tempo – investimentos que a sociedade deve fazer com a compreensão de que a conquista da Democracia se faz todo dia, a um custo infinitamente menor do que qualquer alternativa autoritária e não democrática.

Após a divulgação dos resultados surgiram dúvidas em razão das alegações feitas no documento intitulado "Relatório preliminar de análise das urnas eletrônicas usadas na eleição presidencial do Brasil no primeiro turno – 02 de outubro de 2022", de autoria desconhecida, mas amplamente divulgado na Internet.

A equipe da USP, com *expertise* na área de computação e cibersegurança e com experiência na análise do ecossistema da urna eletrônica brasileira, concentrou-se na análise de três alegações falsas ou que carecem de qualquer embasamento ou fundamento, conforme se pode verificar no Anexo 1 deste Relatório.

Em apertada síntese, as alegações formuladas foram as seguintes:

A. "As urnas de modelo anterior a 2020 não têm qualquer documentação de auditoria recente, e relatórios anteriores referem não serem passíveis de auditoria. Não há documentação comprobatória acerca dos modelos 2009/2010/2011/2013/2015", justificativa usada no documento para comparar "o modelo 2020 (auditado) *versus* os demais";

B. A observação de que há "diferenças sutis entre os arquivos de 'log' (...) das urnas", levando à alegação de que "há, confirmadamente, ao menos dois *softwares* nas urnas, em diferentes modelos, não dependentes de determinado modelo", pois supostamente "jamais poderia haver sequer uma diferença nesta sequência" e "nada mais explica essa diferença que não ao menos duas versões de *softwares*"; e

C. A existência de uma suposta "trava que não deixa a soma [do total de votos lançados para os candidatos Lula e Bolsonaro] ultrapassar determinado número", o que leva a observações como "Modelos não-2020 têm ângulo fixo 'máximo', do qual os votos do Bolsonaro (ou do Lula) 'não podem passar'. Nesta 'faixa limite', a soma dos votos Lula + Bolsonaro é fixa: 300+0, 200+100 ou 100+200, por exemplo. Este jamais seria um comportamento esperado."

Os dois primeiros aspectos recaem sobre a área de *expertise* dos docentes, enquanto o último tem muito mais relação com matemática básica e, portanto, não requer conhecimentos técnicos especializados.

Em suma, as conclusões da análise foram:

1. Alegação A: não tem qualquer embasamento, dada a existência de análises de segurança bastante recentes tanto para as urnas modelo 2020 e 2015, enquanto modelos mais antigos foram alvo de análises similares no passado;
2. Alegação B: embora seja levantada uma possibilidade interessante a partir da observação realizada, essa hipótese de existência de dois códigos fontes revela-se falsa, já que foi possível reproduzir em laboratório o mesmo comportamento observado com um **único código fonte** (a saber, o próprio código fonte da urna eletrônica); e
3. Alegação C: a afirmação de suposta estranheza nos dados carece de qualquer fundamento, pois o gráfico obtido é um resultado natural do fato de que cada urna tem um número máximo de eleitores aptos a votar (em geral, da ordem de 400 eleitores, podendo chegar a cerca de 500 em alguns casos).

A íntegra da análise da MOE USP acerca dessas alegações envolvendo a segurança das urnas eletrônicas encontra-se no Anexo 1 deste Relatório.

2.C. O 2º turno das eleições

No dia 31 de outubro foi encerrado o 2º turno das eleições em todo o país, com a vitória definitiva de 12 governadores e de um candidato à Presidência da República. A MOE USP esteve presente no TRE, em São Paulo, e no TSE, em Brasília.

As quatro semanas que intercalaram os dois turnos eleitorais foram acirradas entre os contendores e verificou-se o uso intensivo de dinheiro público com intuito reeleitoral, como se pode verificar pela seguinte cronologia: *03/10*: anúncio de antecipação do Auxílio Brasil de outubro; *04/10*: inclusão de 500 mil novos beneficiários no Auxílio Brasil; *06/10:* Caixa Econômica Federal lança campanha de refinanciamento de dívidas em até 90%; *07/10*: anúncio de antecipação do Benefício Caminhoneiro e Benefício Taxista de outubro; *11/10*: início da concessão de empréstimos consignados do Auxílio Brasil e inclusão de 300 mil novos beneficiários do Auxílio Gás; *18/10:* aprovado o uso de crédito futuro do FGTS para financiamento de imóveis. É difícil dizer que estas, entre outras irresponsabilidades fiscais, foram tomadas sem ter como alvo impactar o resultado das eleições.

Além disso, com absoluta falta de transparência, constatou-se o uso das verbas decorrentes das emendas de relator (RP9) com nítido intuito reeleitoral, no que ficou conhecido como *orçamento secreto*, que consistia no uso ampliado das emendas do relator-geral do orçamento, para efeito de inclusão de novas despesas públicas ou programações no projeto de lei orçamentária anual da União. Em 2022, o uso desse tipo de emenda chegou ao montante de R$ 16,5 bilhões, e R$ 19,4 bilhões haviam sido reservados para este fim no orçamento de 2023. Apenas passadas as eleições, em dezembro de 2022, é que as Arguições de Descumprimento de Preceito Fundamental (ADPFs) 850, 851, 854 e 1014 foram julgadas, tendo sido declarado inconstitucional esse mecanismo financeiro.

Por parte do candidato à reeleição foram mantidos os ataques verbais ao sistema de apuração do voto eletrônico, enquanto ambos os candidatos amplificaram a disseminação de notícias falsas nas mídias sociais, o que gerou reação por parte do Tribunal Superior Eleitoral – TSE, que em 20/10/22 aprovou por unanimidade a Resolução 23.714/22, vedando a divulgação ou compartilhamento nas redes sociais de fatos sabidamente inverídicos ou gravemente descontextualizados que atingissem a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos (art. 2º), e permitindo que a Presidência do TSE determinasse a extensão da decisão colegiada para outras situações com idênticos conteúdos (art. 3º), podendo haver a suspensão automática de perfis, contas ou canais mantidos em mídias sociais (art. 4º).

Isso gerou inúmeros protestos ancorados na *liberdade de expressão* nas redes sociais, considerando que este deveria ser amplíssimo e estava sendo restringido pelo TSE, e concentradamente nas mãos de seu Presidente, Ministro Alexandre de Moraes.

O debate sobre a constitucionalidade desta Resolução foi objeto da ADI 7261, proposta pela Procuradoria Geral da República junto ao STF e relatada pelo Ministro Edson Fachin, que negou a liminar pleiteada em 22/10/22, submetendo-a de imediato ao Plenário, que a confirmou em 26/10/22.

Ultrapassada a questão da constitucionalidade da Resolução, sua aplicação foi efetiva. O Presidente do TSE registrou em seu pronunciamento, ocorrido logo após a proclamação dos resultados do 2º turno, que foram gerados 19 processos, cujas decisões foram replicadas para outros procedimentos, sendo que, nas últimas 36 horas antes do início do pleito, foram retirados do sistema 354 impulsionamentos e 7 *sites* foram desmonetizados, observando que isso se caracterizava como propaganda paga, além de terem sido removidos 701 URLs, com idêntico conteúdo. Foram também banidos 5 perfis do *Telegram* contendo 580 mil usuários, com disseminação de propaganda de ódio. As plataformas colaboraram, tendo retirado o conteúdo em até 15 minutos, prazo inferior ao que havia sido determinado pela norma.

Na tarde do dia da votação do 2º turno, 30/10/22, ocorreu uma operação da Polícia Rodoviária Federal – PRF para alegadamente fiscalizar os ônibus que transportavam eleitores entre cidades, principalmente no Nordeste (foram noticiadas 272 ações, 49,50% do total de 549), o que gerou muito ruído nas mídias sociais. Foi informado pelo Presidente do TSE em seu pronuncia-

mento que tal fato não acarretou impacto na taxa de abstenção no Nordeste, região onde se concentravam os eleitores do candidato Lula da Silva, pois, a despeito do problema, todos os eleitores conseguiram chegar aos seus pontos de votação.

Em geral, houve redução da abstenção nestas eleições, considerados os dois turnos de votação. Tradicionalmente a taxa de abstenção aumenta, como se viu em 2018, quando a abstenção no 1º turno foi de 20,33% e no 2º turno, 21,30%. Em 2022, no 1º turno a abstenção foi de 20,95% e, para o 2º turno, a abstenção foi reduzida para 20,56%. Houve também redução dos votos em branco e nulos, o que gerou o número recorde de 75,86% dos eleitores escolhendo o Presidente da República.

Diferentemente do turno anterior, não foram observados grandes atrasos nas seções mesmo com a verificação digital do eleitor e o tempo de espera entre a digitação e a habilitação da tecla de confirmação. Isso leva a crer que o atraso percebido no 1º turno não foi fortemente influenciado por razões de cunho tecnológico, mas principalmente pela complexidade da votação, que demandava a digitação dos números dos cinco cargos em disputa. Como no 1º turno, a apuração foi realizada em tempo real assim que os dados chegavam no TSE, sem qualquer distinção. Não foi percebido qualquer problema relacionado à conexão dos TREs ou Zonas Eleitorais com o TSE.

Não houve relatos relevantes de problemas tecnológicos, e os casos que aconteceram estavam dentro da previsão do TSE, sendo resolvidos por meio dos procedimentos-padrão: reinicialização do equipamento ou substituição por equipamento reserva. Os Testes de Integridade, tanto o tradicional como aquele que faz uso de biometria, foram também realizados no 2º turno, o qual foi acompanhado por membros da MOE USP na cidade de São Paulo, inclusive com a verificação manual de que os votos lançados na urna correspondiam ao resultado por ela informado, com o objetivo de eliminar qualquer dúvida sobre o processo de validação dos resultados. Na ocasião, também foi observado o esforço legítimo de agentes da Justiça Eleitoral em convencer o maior número possível de eleitores a participar dos Testes de Integridade com biometria, com o aumento considerável de pessoal dedicado a essa tarefa. De fato, embora tenha sido mantido o seu cunho voluntário, o índice de participação nesses testes foi bastante superior ao observado no 1º turno. Mais uma vez, a lisura das urnas eletrônicas foi comprovada, não se observando qualquer indício de que elas estivessem fazendo algo distinto do esperado: o registro do voto do brasileiro com integridade e sigilo.

Todos os governadores eleitos reconheceram e cumprimentaram o candidato presidencial vitorioso, bem como o fez o Vice-Presidente da República, já tendo havido amplo reconhecimento internacional sobre a lisura do pleito e seu resultado. O Presidente da República, dias após a proclamação do resultado, também reconheceu o veredito das urnas.

No discurso realizado ao final da apuração do 2º turno, o Presidente do TSE, Ministro Alexandre de Moraes, expressamente saudou a USP, em nome da qual agradeceu a todas as Missões Eleitorais Nacionais.

Registra-se que, logo após o resultado do 2º turno das eleições ter sido proclamado, o Partido Liberal (PL) e o Instituto Voto Legal (IVL) realizaram Impugnação formal junto ao TSE

acerca dos *logs* das urnas eletrônicas utilizadas, usando tal fato como base para o pedido de anulação parcial de votos. Foi alegado que "*os arquivos log de Urna são inválidos para todas as urnas eletrônicas de modelos antigos não 2020*", ou que "*não há como realizar uma associação fiel do arquivo log com uma urna específica e, para além disso, também não há como relacionar tal arquivo com os demais elementos de auditoria de votos (BU e RDV) supostamente emitidos pelo mesmo equipamento*".

Os docentes da área tecnológica da USP demonstraram que as conclusões daquela Impugnação são infundadas, havendo diversas alegações que careciam de rigor técnico, conforme se pode verificar pelo Anexo 2 deste Relatório, aqui sintetizadas:

1. São corretas as observações de que o "Código de identificação UE" não está presente nos *logs* das urnas de modelos anteriores ao UE2020.
2. Como consequência da observação anterior, concluíram que não seria válido afirmar que *"nos arquivos LOG que não contêm o código de identificação da urna eletrônica correto, é impossível correlacionar univocamente esse arquivo LOG com o arquivo BU, invalidando a garantia de integridade do conteúdo do BU."*

   Tal ilação não tem qualquer fundamento técnico. Na realidade, o que se comprova experimentalmente é que o "Código de identificação UE" não é o único (ou sequer o mais importante) produto gerado pelas urnas eletrônicas para vinculá-las aos resultados produzidos, ou para permitir a verificação da integridade desses resultados. Assim, o que fica demonstrado é que qualquer pessoa pode correlacionar um dado *log* com o Boletim de Urna correspondente, independentemente do modelo da urna e a despeito do problema relatado.
3. Em síntese: várias afirmações realizadas são infundadas, por carecerem de rigor técnico, conforme exposto no documento constante do Anexo 2 deste Relatório.

2.D. O período pós-eleitoral

Embora o país se encontrasse na mais absoluta normalidade, existiram iniciativas isoladas, fruto de pequeno número de descontentes com o resultado eleitoral, que realizaram piquetes pontuais nas estradas brasileiras, bem como diversos grupos acamparam defronte dos quartéis, com vários manifestantes pedindo intervenção das Forças Armadas visando evitar a posse do Presidente eleito. O esforço governamental para reverter estas manifestações foi mínimo ou inexistente.

No dia 12 de dezembro de 2022 foi realizada no TSE, sem qualquer intercorrência, a cerimônia de diplomação dos candidatos eleitos para cumprir o mandato de Presidente da República, Luiz Inácio Lula da Silva, e de Vice-Presidente, Geraldo Alckmin.

No período entre a diplomação e a posse foi ampliada a presença de manifestantes defronte de quartéis pedindo intervenção pelos militares no âmbito *federal*, contestando apenas a eleição presidencial, com foco na manutenção do candidato derrotado à frente da Presidência da República. O caráter antidemocrático dessas manifestações era patente, mas nenhuma providência foi realizada pelo governo para dissuadir os envolvidos.

O clima de beligerância foi sendo ampliado pouco a pouco. Foram registrados tumultos nas proximidades de um *shopping center* em Brasília, com explosão de veículos que estavam estacionados, tendo sido identificada e desarmada uma bomba instalada ao lado de um caminhão tanque repleto de combustível nas proximidades do aeroporto de Brasília, visando criar um tumulto e buscar a intervenção militar.

No dia 1º de janeiro de 2023, foi realizada a posse dos eleitos, em cerimônia que contou com a presença de dezenas de missões estrangeiras, bem como com ampla participação popular. A tradicional troca de faixa presidencial não ocorreu, pois o candidato derrotado se negou a fazê-la, viajando de véspera para os Estados Unidos da América.

No dia 08 de janeiro, domingo, a Praça dos Três Poderes foi tomada por manifestante que invadiram os prédios do Supremo Tribunal Federal, do Senado Federal, da Câmara dos Deputados e o Palácio do Planalto, depredando-os vastamente, pretendendo, com isso, aplicar um golpe de Estado e reverter o resultado das eleições presidenciais.

No dia imediatamente posterior foram realizados incontáveis atos em todo o Brasil em prol da Democracia e repudiando veementemente a depredação ocorrida, com destaque para o realizado pela USP, na Faculdade de Direito, que reuniu múltiplos representantes de organizações da sociedade civil, clamando pela apuração dos atos de vandalismo e se posicionando contra a tentativa de golpe que havia sido perpetrada.

O governo recém-empossado debelou a rebelião, sem derramamento de sangue, e com a responsabilização dos culpados até aqui identificados, na forma da lei. A apuração segue seu curso.

3. Análise Conclusiva

As eleições de 2022 foram realizadas sob um clima tenso e acirrado, prenhe de ataques às Instituições Judiciárias, em especial ao TSE e ao STF, vários deles diretamente dirigidos aos Ministros dessas Cortes, pelos partidários dos principais candidatos à Presidência da República, tendo como principal tema a liberdade de expressão e o controle das mídias sociais.

A Resolução 23.714/22 do TSE, que regulava a matéria, foi considerada constitucional pelo STF e aplicada de forma indistinta a todos que a infringiram.

A despeito do clima beligerante e das inúmeras contestações dos partidários dos dois principais candidatos, o TSE conduziu o pleito com absoluta normalidade, não obstante pequenos grupos insatisfeitos terem promovido badernas e buscado implementar um golpe de Estado, visando anular as eleições e manter no poder o candidato derrotado, que então exercia a Presidência da República.

O intento golpista, que se manifestou mais fortemente após a proclamação das eleições e, de forma bárbara, após a posse dos eleitos, com a invasão da Praça dos Três Poderes, em 08 de janeiro de 2023, naquele que foi denominado pelo Ministro Gilmar Mendes como o *dia da infâmia brasileiro*, está sendo devidamente apurado e seus responsáveis processados na forma da lei. Vários prédios foram vandalizados, com depredação de instalações, obras de arte e objetos históricos.

No dia 1º de fevereiro de 2023, os deputados federais e os senadores eleitos tomaram posse e elegeram suas Mesas Diretoras, com os prédios do Senado e da Câmara ainda sendo recuperados. Na mesma data foram iniciados os trabalhos do Poder Judiciário, com uma cerimônia no Plenário do Supremo Tribunal Federal ainda sob reconstrução.

Impera no Brasil o Estado Democrático de Direito, a despeito das tentativas de golpe de Estado que ocorreram, que estão sendo apuradas na forma da lei.

4. Recomendações da MOE USP para as próximas eleições

Fruto da Missão realizada, e considerando que *este Relatório deve ser apresentado ao Presidente do TSE e às Chefias dos Poderes da República*, consoante a Resolução TSE 23.678/21, art. 24, § 3º, a MOE USP, visando ao aperfeiçoamento do processo eleitoral brasileiro, com vistas à regular continuidade democrática, *recomenda*:

- Mudança no art. 14, § 6º, da Constituição, para alterar o sistema de reeleição, pois atualmente o Chefe do Poder Executivo, em todos os níveis federativos, não se licencia do cargo para disputar o mesmo cargo, apenas se vier a disputar cargo diverso. Isso dá margem a diversos abusos que podem ser reduzidos caso haja desincompatibilização. Isso tem urgência, em face das eleições municipais de 2024, na qual grande parte dos mais de 5.500 Prefeitos estarão aptos a disputar sua reeleição;
- Buscar mudanças na legislação para que existam formas justas de atribuir responsabilidade, ainda que não absoluta, às plataformas de mídias sociais pela divulgação de propaganda desinformativa ou de caráter golpista. Por certo, o paradigma para esse tipo de dispositivo legal ainda está em aperfeiçoamento em vários países, que procuram avançar nessa direção. Embora não sejam veículos convencionais de imprensa, que podem ser responsabilizados pelos conteúdos que apuram, editam e difundem, as plataformas digitais podem ser também responsabilizadas pela divulgação de certos conteúdos e essa é uma meta legítima das sociedades contemporâneas;
- Aperfeiçoar o atual sistema de controle das finanças públicas, visando coibir a utilização dos recursos públicos com finalidades reeleitorais;
- Aperfeiçoar o sistema de prestações de contas das verbas recebidas pelos partidos políticos e utilizadas pelos candidatos eleitos e não eleitos, aproximando o controle adotado pela Justiça Eleitoral ao dos Tribunais de Contas, que são especializados nesses procedimentos;
- Criar centros de estudos e pesquisas sobre direito eleitoral, com foco na análise de sistemas correlatos em outros países, visando ao aperfeiçoamento do processo eleitoral brasileiro;
- Aproximar as MOEs Nacionais e as Internacionais, amplificando a exitosa experiência.

Agradecimentos

É imperioso consignar diversos agradecimentos.

No âmbito do TRE-SP, ao seu Presidente, Desembargador Paulo Galízia e a todos os servidores, o que se faz na pessoa de Fernanda Diniz, que recepcionou o grupo que esteve presente nas atividades desenvolvidas perante aquela Corte.

No âmbito do TSE, deve-se agradecer ao seu Colegiado, o que se faz na pessoa dos Ministros Alexandre de Moraes e Ricardo Lewandowski, respectivamente Presidente e Vice-Presidente daquele Tribunal, pela fidalguia com que esta Missão foi recebida, bem como ao Ministro Edson Fachin, ex-Presidente do TSE, que tomou a iniciativa de institucionalizar as Missões de Observação Nacionais. Deve-se agradecer também ao Secretário-Geral da Presidência do TSE, José Levi Mello do Amaral Júnior, sempre cordial e eficaz, e aos servidores do Tribunal, o que se faz nas pessoas de José Gilberto Scandiucci e Vinícius Quintino de Oliveira, responsáveis pela recepção às Missões Eleitorais nacionais e internacionais.

São Paulo, março de 2023.

Missão de Observação Eleitoral

UNIVERSIDADE DE SÃO PAULO

ANEXOS

Anexo 1. Comentários sobre alegações infundadas ou falsas sobre as urnas eletrônicas brasileiras

11 de novembro de 2022

LARC-PCS-EPUSP

Autores (em ordem alfabética):

- **Felipe Kenzo Shiraishi**, Engenheiro e Aluno de Mestrado na Escola Politécnica da Universidade de São Paulo (USP);
- **Lucas Lago**, Mestre em Engenharia da Computação pela Escola Politécnica da Universidade de São Paulo (USP);
- **Marcos Antonio Simplicio Junior**, Professor Associado da Escola Politécnica da Universidade de São Paulo (USP);
- **Paulo Matias**, Professor Adjunto do Departamento de Computação da Universidade Federal de São Carlos (UFSCar);
- **Tiago Barbin Batalhão**, Doutor em Física pela Universidade Federal do ABC (UFABC); e
- **Wilson Vicente Ruggiero**, Professor Titular da Escola Politécnica da Universidade de São Paulo (USP).

Resumo Executivo

O presente documento tem por objetivo elucidar algumas dúvidas que surgiram recentemente sobre o processo eleitoral brasileiro, em particular devido a algumas das alegações feitas no documento intitulado "Relatório preliminar de análise das urnas eletrônicas usadas na eleição presidencial do Brasil no primeiro turno – 02 de outubro de 2022", de autoria desconhecida, mas amplamente divulgado na Internet. As análises foram realizadas por pesquisadores da Universidade de São Paulo e UFSCar, todos com expertise na área de computação e cibersegurança e também experiências prévias com análise do ecossistema da urna eletrônica brasileira, concentrando-se em três **alegações falsas ou que carecem de qualquer embasamento ou fundamento:**

A. A alegação de que "As urnas de modelo anterior a 2020 não têm qualquer documentação de auditoria recente, e relatórios anteriores referem não serem passíveis de auditoria. Não há documentação comprobatória acerca dos modelos 2009/2010/2011/2013/2015", justificativa usada no documento para comparar "o modelo 2020 (auditado) *versus* os demais".

B. A observação de que há "diferenças sutis entre os arquivos de 'log' (...) das urnas", levando à alegação de que "há, confirmadamente, ao *menos* dois softwares nas urnas, em diferentes modelos, não dependentes de determinado modelo", pois supostamente "Jamais poderia haver sequer uma diferença nesta sequência" e "Nada mais explica essa diferença que não ao menos duas versões de *softwares*".

C. A existência de uma suposta "trava que não deixa a soma [do total de votos lançados para os candidatos Lula e Bolsonaro] ultrapassar determinado número", o que leva a observações como "Modelos não-2020 têm ângulo fixo 'máximo', do qual os votos do Bolsonaro (ou do Lula) 'não podem passar'. Nesta 'faixa limite', a soma dos votos Lula+Bolsonaro é fixa: 300+0, 200+100 ou 100+200, por exemplo. Este jamais seria um comportamento esperado".

Cabe notar que os dois primeiros aspectos recaem sobre a área de expertise dos autores, enquanto o último tem muito mais relação com matemática básica e, portanto, não requer conhecimentos técnicos especializados.

Em suma, as conclusões da análise foram:

1. Alegação A: não tem qualquer embasamento, dada a existência de análises de segurança bastante recentes tanto para as urnas modelo 2020 e 2015, enquanto modelos mais antigos foram alvo de análises similares no passado.
2. Alegação B: embora seja levantada uma possibilidade interessante a partir da observação realizada, essa hipótese de existência de dois códigos-fonte revela-se falsa, já que foi possível reproduzir em laboratório o mesmo comportamento observado com um único código-fonte (a saber, o próprio código-fonte da urna eletrônica).
3. Alegação C: a afirmação de suposta estranheza nos dados carece de qualquer fundamento, pois o gráfico obtido é um resultado natural do fato de que cada urna tem um número máximo de eleitores aptos a votar (em geral, da ordem de 400 eleitores, podendo chegar a cerca de 500 em alguns casos).

Este relatório tem teor técnico, mas tenta na medida do possível trazer para uma linguagem mais próxima do público em geral as observações realizadas, buscando demonstrar claramente as conclusões apresentadas.

Introdução

O TSE e a USP firmaram o Convênio 14/2021, com a finalidade de permitir ao Laboratório de Arquitetura e Redes de Computadores (LARC) do Departamento de Engenharia de Computação e Sistemas Digitais (PCS) da Escola Politécnica da Universidade de São Paulo (USP) planejar e executar testes de segurança sobre as urnas eletrônicas brasileiras. Como parte desse convênio, foram disponibilizadas para a Universidade de São Paulo: duas unidades do modelo UE2015 e três unidades do modelo UE2020; a documentação correspondente ao ecossistema das urnas; e os códigos-fonte e respectivos códigos compilados para realizar a carga das urnas para fins de testes.

Como essa parceria é de conhecimento público, membros do LARC-USP têm mantido um canal de comunicação aberto com diversas pessoas e entidades interessadas no tema "segurança das urnas eletrônicas", incluindo parceiros em universidades no Brasil (e.g., a Universidade Federal de São Carlos – UFSCar) e no exterior. Em uma dessas interações, no dia 02/Novembro/2022, chegou ao conhecimento de pesquisadores da USP e da UFSCar o documento intitulado "Relatório preliminar de análise das urnas eletrônicas usadas na eleição presidencial do Brasil no primeiro turno – 02 de outubro de 2022". Embora de autoria desconhecida, o documento fazia alegações diversas sobre supostas fraudes nas eleições de 2022, com base em dados públicos disponibilizados pelo TSE. Pouco tempo depois, foi realizada uma apresentação desse relatório por meio de uma *live*, por alguém identificado pela mídia como o argentino Fernando Cerimedo. Por essa razão, o relatório (ainda de autoria desconhecida) ficou conhecido em alguns meios como o "Relatório Argentino". Por comodidade, esse relatório é também assim referenciado neste documento.

Embora o teor do Relatório Argentino parecesse duvidoso desde o princípio, decidiu-se investir algum tempo na sua análise, com o objetivo de confirmar ou refutar as alegações ali feitas de forma independente. Em particular, considerando a expertise dos pesquisadores na área de computação e cibersegurança, bem como experiências prévias com análise da urna eletrônica brasileira, as análises iniciais buscaram se concentrar em dois aspectos principais:

A. A alegação de que "As urnas de modelo anterior a 2020 não têm qualquer documentação de auditoria recente, e relatórios anteriores referem não serem passíveis de auditoria. Não há documentação comprobatória acerca dos modelos 2009/2010/2011/2013/2015", justificativa usada no documento para comparar "o modelo 2020 (auditado) *versus* os demais".

B. A observação de que há "diferenças sutis entre os arquivos de 'log' (...) das urnas", levando à alegação de que "há, confirmadamente, ao menos dois *softwares* nas urnas, em diferentes modelos, não dependentes de determinado modelo", pois supostamente "Jamais poderia haver sequer uma diferença nesta sequência" e "Nada mais explica essa diferença que não ao menos duas versões de *softwares*".

Assim, em princípio, decidiu-se não abordar as discussões que, ao menos em teoria, envolveriam análises estatísticas de dados. A razão para isso é dupla. A primeira é que, embora estatística seja parte da formação dos pesquisadores, esta não é exatamen-

te a sua área de expertise. A segunda é que várias reportagens na mídia já analisaram o perfil demográfico de ao menos parte das 147 seções eleitorais em que um único candidato recebeu votos, o que corresponde a 4 casos para Bolsonaro (totalizando 124 votos) e 143 casos para Lula (somando 16.579 votos); o que se observou nessas análise é que a unanimidade para o candidato Lula, considerada improvável por alguns grupos, em geral ocorreu em aldeias indígenas, comunidades ou povoados: conforme reportagem em https://g1.globo.com/politica/eleicoes/2022/eleicao-em-numeros/noticia/2022/11/07/secoes-em-que-so-um-candidato-a-presidente-foi-votado-somam-001percent-dos-votos-validos-no-2o-turno.ghtml, "em 22 delas, o local de votação tem 'aldeia' no nome; em 27, tem 'comunidade' e, em 51, tem 'povoado'". Argumentar se esse comportamento amplamente favorável ao candidato Lula era ou não o esperado de tais grupos não faz parte do escopo desta análise.

Após a análise dos pontos acima, decidiu-se então incluir um novo ponto à análise, embora, ao menos em teoria, ele fizesse parte da porção "estatística" do Relatório Argentino. Especificamente, como muitas das observações nessa porção envolvem equívocos de matemática básica na interpretação de gráficos (algo que, portanto, não exige qualquer conhecimento de estatística), decidiu-se por analisar uma alegação adicional:

> C. A existência de uma suposta "trava que não deixa a soma [do total de votos lançados para os candidatos Lula e Bolsonaro] ultrapassar determinado número", o que leva a afirmações como "Modelos não-2020 têm ângulo fixo 'máximo', do qual os votos do Bolsonaro (ou do Lula) 'não podem passar'. Nesta 'faixa limite', a soma dos votos Lula+Bolsonaro é fixa: 300+0, 200+100 ou 100+200, por exemplo. Este jamais seria um comportamento esperado".

A seguir, são apresentados os resultados das análises de cada um desses pontos.

Alegação A: Sobre documentações de auditoria dos diferentes modelos de urnas

Como parte da parceria entre USP e TSE, membros do LARC-USP acompanharam os Testes Públicos de Segurança (TPS) realizados no período de 22 a 27 de novembro de 2021, ocasião em que um grupo de 26 investigadores (incluindo membros da Polícia Federal que costumeiramente participam do evento) puderam realizar testes de segurança diversos sobre urnas do modelo UE2015. Acompanhamento similar ocorreu no Teste de Confirmação, realizado de 11 a 13 maio de 2022, em que 5 grupos de investigadores que obtiveram algum sucesso durante o TPS voltaram ao TSE para repetir os ataques e avaliar as contramedidas propostas. Detalhes sobre o evento, incluindo os relatórios correspondentes, encontram-se publicamente disponíveis em https://www.justicaeleitoral.jus.br/tps/.

Em paralelo às análises realizadas por investigadores no TPS 2021, e mesmo antes da realização do evento, pesquisadores do LARC-USP já tinham tido a oportunidade de avaliar a segurança do modelo UE2015, inclusive propondo melhorias ao sistema por meio de relatórios internos ao convênio entre USP e TSE. Apoiando-se nos conhecimentos adquiridos em tais testes, e ten-

do em vista que as urnas eletrônicas do modelo UE2020 não haviam sido disponibilizadas pelo fabricante para serem avaliadas no período estabelecido do TPS 2021, foi solicitado ao LARC-USP que fizesse uma análise de segurança e relatório público também para a UE2020. As atividades realizadas nesse sentido foram planejadas para serem compatíveis com os padrões dos TPS, e dentro da disponibilidade de tempo que atendesse as eleições do calendário 2022. O relatório dessa atividade foi entregue em Agosto de 2022, ocasião na qual o resumo executivo correspondente foi publicado juntamente com análises independentes realizadas por pesquisadores da Universidade de Campinas (Unicamp) e da Universidade Federal de Pernambuco (UFPE). Esses relatórios encontram-se publicamente disponíveis em https://www.tse.jus.br/comunicacao/noticias/2022/Agosto/universidades-validam--nova-urna-e-codigos-fonte-dos-sistemas-eleitorais-357621.

Ainda, toda eleição conta com os chamados "Testes de Integridade", durante os quais as urnas sorteadas são colocadas em um ambiente de votação simulada. Durante esse teste, são lançados diversos votos nas urnas, sem qualquer proteção de sigilo, e, então, confere-se se o resultado obtido nos boletins de urna corresponde aos votos efetivamente lançados. Os votos em questão não vão para a totalização oficial, mas servem apenas para verificar que as urnas testadas não estão de alguma forma "desviando votos". Contanto que a simulação seja próxima o suficiente de um ambiente de votação real, seria difícil para um "*software* fraudador" saber que está sob testes, e então um eventual desvio de votos poderia ser detectado. Como os Testes de Integridade acontecem em todos os Estados do Brasil, e com urnas selecionadas aleatoriamente, eles acabam cobrindo diversos dos modelos de urna sendo utilizados naquela eleição. De fato, uma equipe da USP acompanhou, em 2022, os Testes de Integridade realizados na cidade de São Paulo durante os dois turnos da eleição, ambos ocorridos no Centro Cultural São Paulo e na Universidade Paulista (Unip) do Paraíso, e observou diferentes modelos sob testes. A Figura A1 ilustra esse fato para os testes ocorridos no Centro Cultural, no 2º turno das eleições de 2022. Nota: essa imagem foi escolhida por mostrar claramente os dois modelos em bancadas vizinhas, facilitando a visualização; imagens de outros lugares do País também permitem constatar essa variedade, em ambos os turnos.

Figura A1 – Imagem do Teste Público de Integridade no 2º turno das Eleições de 2022, realizado no Centro Cultural de São Paulo. Pode-se observar o uso de urnas modelo 2020 (verde) e de um modelo anterior (vermelho), aproveitando a diferença visual entre elas. Fonte: https://www.youtube.com/watch?v=DpoTL7Nbhyo

Dado esse contexto, a análise da afirmação de que "As urnas de modelo anterior a 2020 não têm qualquer documentação de auditoria recente", enquanto as urnas modelo 2020 teriam sido auditadas, parece exigir uma breve discussão sobre o que seria uma "auditoria". O dicionário Michaelis define o termo de forma bem ampla, como o "Procedimento de análise, investigação e validação de um sistema, atividade ou informação". Comumente, entretanto, o termo "auditoria" é reservado no meio técnico para análises de um sistema após seu uso, para avaliar alguma denúncia ou suspeita, por exemplo. Logo, a rigor, as análises de segurança feitas nos TPS e pelas equipes de universidades não poderiam ser consideradas "auditorias", por terem acontecido antes das eleições apenas. Além disso, pode-se argumentar que os Testes de Integridade que ocorrem durante as eleições também não entrariam estritamente na definição de "auditoria", por ocorrerem durante (e não após) as votações. Nesse sentido, até um pouco pedante, provavelmente seriam classificadas como "auditoria" nas eleições de 2022 somente análises como aquela feita pelo TCU (https://portal.tcu.gov.br/imprensa/noticias/tcu-finaliza-analise-de-boletins-de-urna-do-1-turno-das-eleicoes.htm) sobre 4.161 boletins de urna, em busca de divergências entre o resultado divulgado pelo TSE e o fornecido pelas urnas. Porém, nesse caso não se trataria de uma auditoria de urnas *per se*, mas sim do processo de totalização.

Isso posto, é difícil saber exatamente o que seria considerada uma "auditoria" pelo Relatório Argentino (nenhuma referência é ali fornecida para a mencionada "auditoria das urnas modelo 2020"). Portanto, assume-se aqui que o autor utiliza a definição mais ampla, de modo que tanto o TPS como o Teste de Integridade são considerados exemplos de auditoria. Se não for essa a definição utilizada, provavelmente seria necessário argumentar (novamente, de forma pedante) que nenhum modelo de urna passou por auditoria no contexto das eleições de 2022.

Dado esse esclarecimento/simplificação, não parece haver qualquer embasamento técnico na comparação do modelo de urna 2020 com modelos anteriores: a afirmação de que "As urnas de modelo anterior a 2020 não têm qualquer documentação de auditoria recente" é incorreta. Afinal, os relatórios públicos do TPS de 2021 testaram a segurança das urnas do modelo 2015, enquanto modelos anteriores à UE2015 foram analisados em edições anteriores dos Testes Públicos de Segurança, que normalmente ocorrem a cada dois anos. Ao mesmo tempo, tanto a UE2015 como a UE2020 foram e continuam sendo analisadas pela USP, e relatórios deste último modelo foram publicados não apenas pela USP, mas também pela Unicamp e UFPE. Já os Testes de Integridade cobrem modelos diversos de urnas, via sorteio. Finalmente, ao afirmar que "relatórios anteriores referem não serem passíveis de auditoria", o autor parece se referir ao Relatório de Auditoria das Eleições de 2014, disponível em http://www.brunazo.eng.br/voto-e/arquivos/RelatorioAuditoriaEleicao2014-PSDB.pdf. As conclusões desse relatório incluem essencialmente (1) uma listagem de pontos que puderam ser auditados, e para os quais não foram encontrados indícios de fraude, e (2) uma listagem de pontos que não puderam ser auditados a contento, com correspondentes sugestões de melhoria para sanar as lacunas observadas. Em nenhum momento o Relatório de Auditoria das Eleições de

2014 faz (ou sequer tenta fazer) qualquer distinção entre modelos de urnas, exceto para discutir características técnicas como a presença de *hardware* de segurança (presente em todas as urnas posteriores ao modelo 2009, ou seja, em todo o parque de urnas utilizadas nas eleições de 2022) e de mecanismo de biometria (o qual se encontrava e ainda se encontra disponível em vários modelos de urna). Portanto, novamente, não se justifica a divisão artificial entre modelos de urna feita no relatório sob análise.

Dessa forma, do ponto de vista técnico, é difícil entender a razão pela qual o autor do Relatório Argentino decide fazer uma comparação entre [urnas modelo 2020] *vs*. [urnas mais antigas] como premissa das análises, assumindo (erroneamente) haver uma diferença clara da confiabilidade de cada modelo. Consequentemente, é bem provável que quaisquer conclusões tiradas a partir dessa comparação não tenham relação direta com o modelo em si, contrariamente àquilo que o relatório sob análise dá a entender. Por exemplo, ao menos em alguns casos, pode haver correlação entre o modelo de urna e o perfil demográfico da população (vide Figura A2, na qual se observa que no Nordeste do Brasil houve uma maior concentração de urnas modelo 2020 em áreas próximas a capitais). Logo, as eventuais diferenças observadas podem ser reflexo desses perfis demográficos, bem como ideologias, perfis psicológicos, crenças e outros fatores, não do modelo de urna: seria necessária grande dose de cautela para controlar essa grande diversidade de fatores em eventuais análises e, pela ausência de detalhes no Relatório Argentino, não é possível dizer se isso foi de fato feito.

Figura A2 – Distribuição de urnas modelo 2020 (azuis) e de modelos anteriores (vermelho) na região do Nordeste. Fonte: autores, com base nos dados disponíveis em https://dadosabertos.tse.jus.br/.

Alegação B: Sobre diferenças em arquivos de log implicarem a existência de códigos-fonte distintos

Primeiramente, cabe explicar o que significa um "log" no contexto das urnas eletrônicas. Não é nada complicado: trata-se simplesmente de um conjunto de mensagens que descrevem

eventos que aconteceram na urna em questão, incluindo a data e horário de cada evento específico. Exemplos de registros desse tipo incluem o momento em que ela foi ligada, o estado da bateria então observado, o resultado das várias verificações que ela faz internamente (incluindo verificações de segurança, para identificar se o *software* nela carregado é legítimo), os momentos em que a votação foi iniciada e finalizada etc.

A título de exemplo: qualquer pessoa pode acessar os arquivos de log das urnas utilizadas nas eleições de 2022, já que são dados totalmente públicos, por meio do seguinte *site* https://resultados.tse.jus.br/oficial/app/index.html#/eleicao;e=e545/resultados. Para fins de ilustração, pode-se selecionar a cidade de São Paulo/SP, Zona 001, Seção 001, e escolher a opção "Log da Urna" (vide Figura B1).

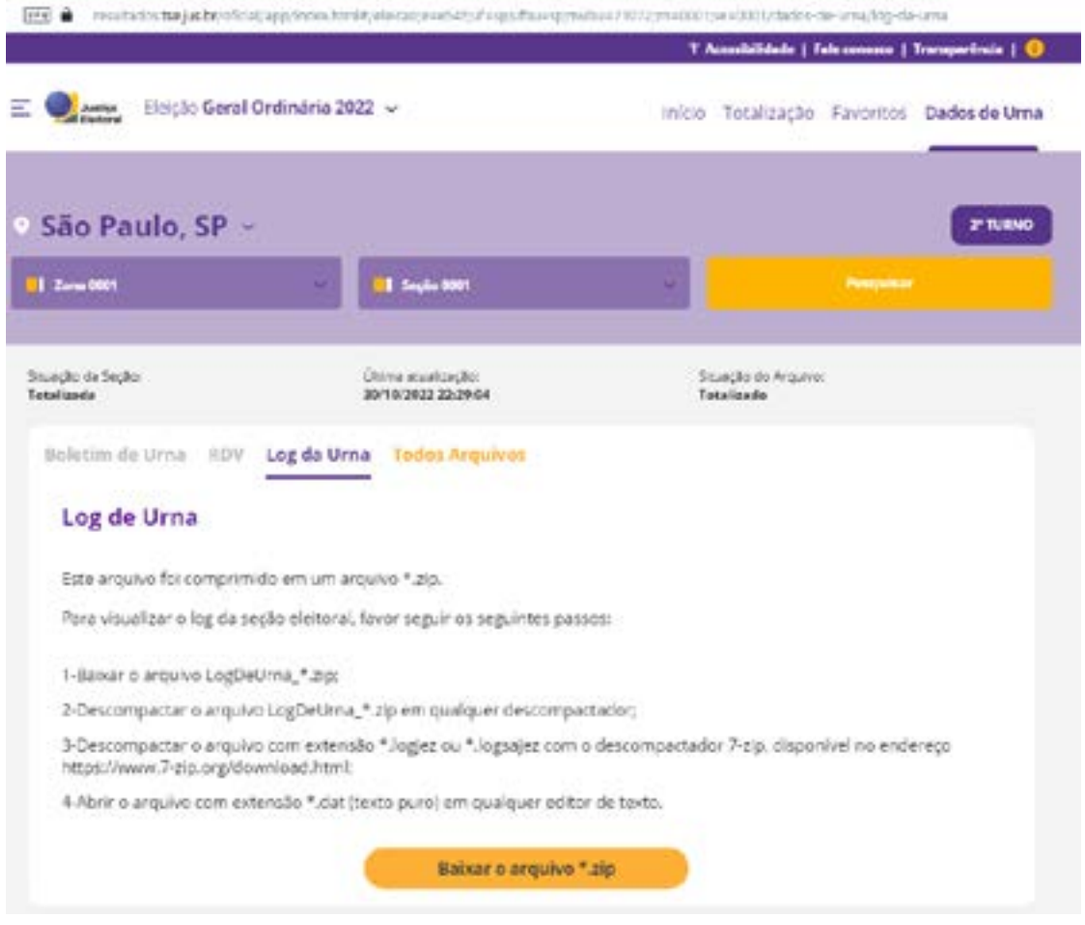


Figura B1 – Acessando o log da urna de São Paulo/SP, Zona 001, Seção 0001.

Fazendo isso, obtém-se um arquivo comprimido (extensão .zip) que, após aberto, permite acesso ao arquivo logd.dat. Esse é o arquivo de log, que nada mais é que um arquivo de texto que começa com as informações a seguir:

```
22/09/2022 11:02:54 INFO 67305985 LOGD Início das operações do logd
22/09/2022 11:02:54 INFO 67305985 LOGD Urna ligada em 22/09/2022 às 11:01:31
22/09/2022 11:02:54 INFO 67305985 SCUE Iniciando aplicação - Oficial - 1º turno
22/09/2022 11:02:54 INFO 67305985 SCUE Versão da aplicação: 8.26.0.0 - Onça-pintada
22/09/2022 11:02:56 INFO 67305985 SCUE Urna operando com bateria interna
22/09/2022 11:02:56 INFO 67305985 SCUE Bateria interna com carga parcial
```

O que o autor do Relatório Argentino percebeu é que, em algumas urnas, há "diferenças sutis entre os arquivos de 'log'", mostrando um exemplo. Daí o autor concluiu que "há, confirmadamente, ao menos dois *softwares* nas urnas, em diferentes modelos, não dependentes de determinado modelo". Logo de início, a conclusão pareceu um tanto estranha, porque é muito comum que um mesmo *software* possa registrar eventos diferentes em seu log, dependendo do que ele observa durante a execução. Um exemplo hipotético, mas ilustrativo: caso a bateria da urna esteja baixa, pode haver um alerta ao operador e um registro correspondente no log, de modo que os logs de urnas que estejam com a bateria baixa serão diferentes daqueles apresentados por urnas que não tenham esse problema durante sua inicialização. Tudo isso com **o mesmo *software***.

Apesar dessa estranheza na afirmação do Relatório Argentino, decidiu-se averiguar se ela tinha algum mérito. Para isso, a equipe de pesquisadores buscou identificar, no código-fonte da urna, especificamente o local onde as diferenças apontadas no relatório poderiam aparecer (as diferenças em questão são reproduzidas na Figura B2).

Figura B2 – Logs de urnas onde foram observados pontos de diferença no "Relatório Argentino"

O resultado foi que, novamente, o "Relatório Argentino" está equivocado: percebeu-se que o mesmo *software* (a saber, o único que foi disponibilizado à USP) é capaz de gerar trechos de log contendo ou não a linha adicional apontada, dependendo de como se deu a interação com o operador da urna durante a inicialização do sistema. O vídeo do procedimento experimental consta a seguir: https://youtu.be/Lrd9YZtP_RQ.

Mais especificamente: conforme é possível verificar nos logs fornecidos, eles se dão na aplicação SCUE. O SCUE é o "Sistema de Carga da Urna Eletrônica". Esta informação pode ser obtida no *site* do TSE: https://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/logistica-e-preparacao/ecossistema-da-urna. Este aplicativo é o responsável por carregar todo o *software* que roda na urna de uma mídia externa para a sua mídia interna, o que ocorre antes da eleição, durante a chamada "carga urna". O momento que determina se a linha adicional de log "Solicitação do número da seção" aparece ou não é apresentado na Figura B3, ao lado:

A equipe de investigadores pôde, então, constatar que a linha de log aparecer ou não depende de o operador da urna pressionar a tecla Confirma (assim gerando o log circulado em verde) ou pressionar a tecla Corrige (assim gerando o log circulado em vermelho). Após executar este experimento para os dois casos e extraindo os logs resultantes, foi possível reproduzir tais sequências de logs, usando o mesmo *software*. Dessa forma, ao contrário do que afirma o Relatório Argentino, as sequências distintas nos logs não representam indícios de existência de códigos-fonte distintos. Cabe enfatizar que este não é um dos

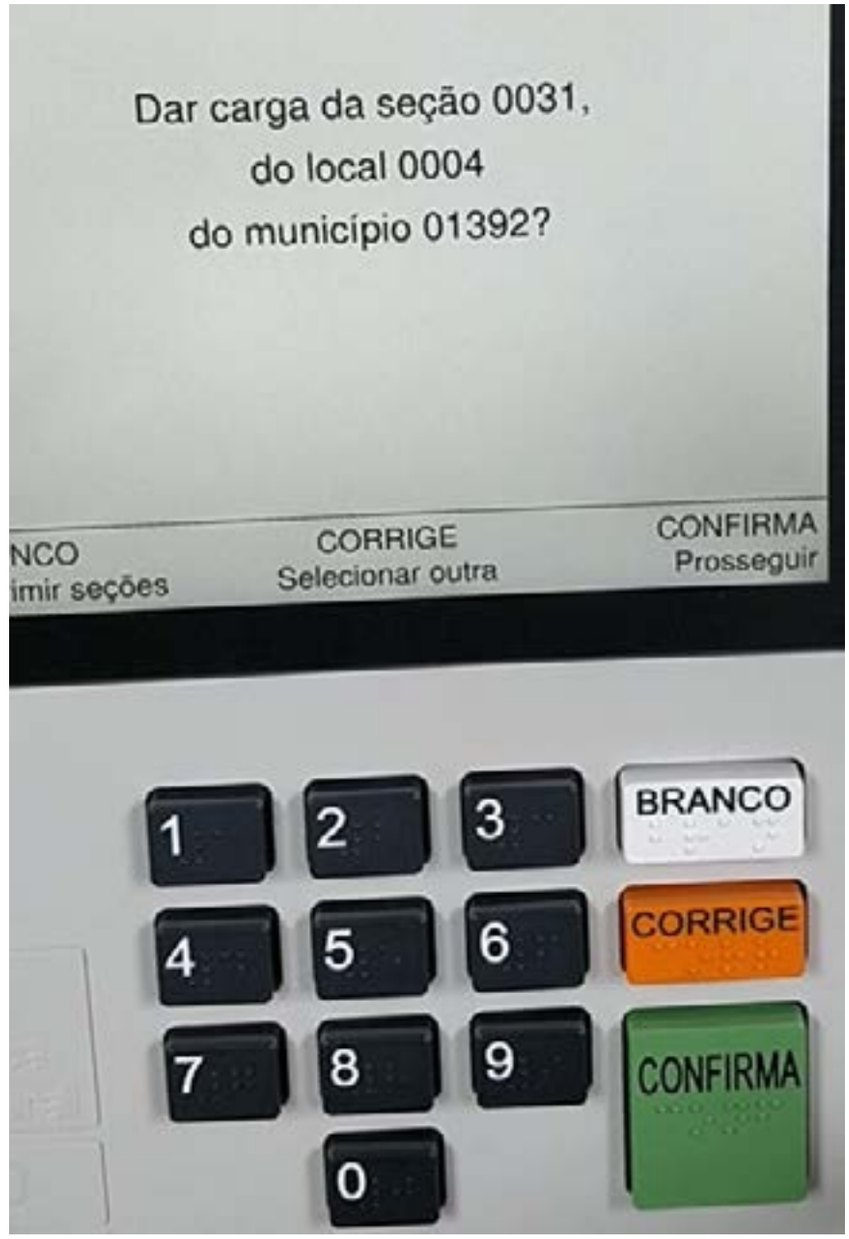


Figura B3 – Foto da urna eletrônica modelo 2020 à disposição dos investigadores na USP, mostrando o momento em que o SCUE está sendo executado.

únicos casos da urna em que logs são introduzidos na sequência condicionalmente por fatores de interação com o usuário. Dessa forma, como previamente mencionado, é aconselhada cautela em alegar indício de fraude com base em achado de sequências de logs distintas entre si.

Conclui-se, portanto, que estão totalmente equivocadas afirmações sensacionalistas como "há, confirmadamente, ao menos dois *softwares* nas urnas", que "Jamais poderia haver sequer uma diferença nesta sequência" e que "Nada mais explica essa diferença que não ao menos duas versões de *softwares*". Na realidade é muito fácil explicar essas diferenças analisando o código-fonte não havendo *a priori* razão alguma para assumir que a existência de códigos distintos seria a única explicação para isso (exceto, novamente, a tentativa de criar sensacionalismo).

Alegação C: Sobre a existência de uma "trava" na soma dos votos aos candidatos Lula e Bolsonaro

A afirmação da existência de uma "trava" sobre a soma do número de votos para os candidatos Lula e Bolsonaro é repetida em diversos pontos do Relatório Argentino, sendo ilustrada na Figura C1.

O autor do relatório argumenta então que "Este jamais seria um comportamento esperado", para se referir aos gráficos das urnas de modelos anteriores à UE2020. Entretanto, esse comportamento é na realidade perfeitamente esperado, tanto para as UE2020 quanto para os modelos anteriores: simplesmente, trata-se de uma consequência natural de haver um número máximo de eleitores aptos a votar em cada urna.

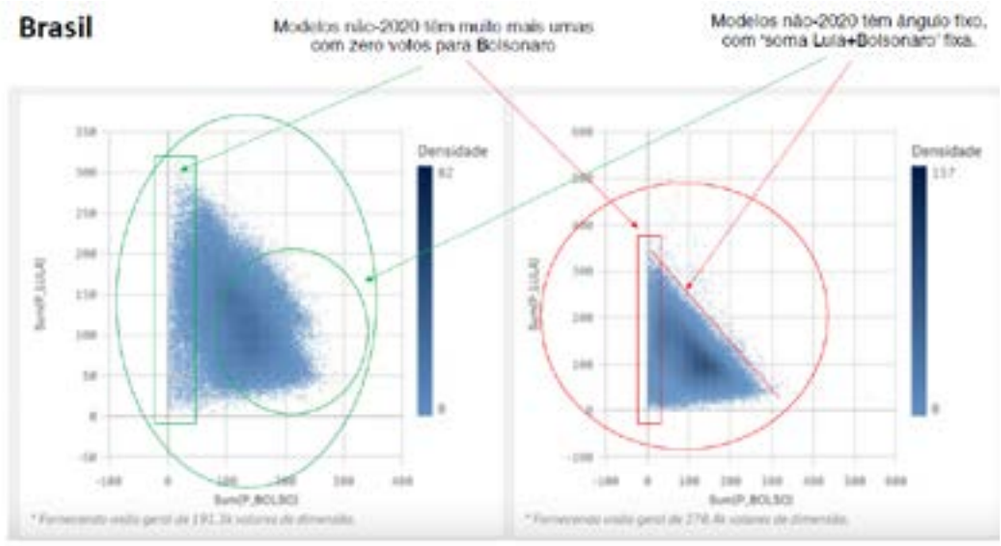


Figura C1 - Exemplo de suposta "trava" na soma de votos para Lula e Bolsonaro nos modelos não-2020 (direita), a qual não ocorreria nos modelos 2020 (esquerda). Fonte: "Relatório Argentino".

Para facilitar a compreensão deste ponto, considere um cenário simplificado, no qual o número máximo de eleitores em todas as urnas seja 400, e que haja apenas 2 candidatos, o primeiro recebendo X votos e o segundo obtendo Y votos. Nesse caso, qualquer resultado da soma de X+Y deve ser no máximo 400. Afinal, não pode haver mais votos do que o número de eleitores aptos a votar! Por outro lado, nem sempre a soma X+Y vai dar 400, pois alguns eleitores poderiam anular seus votos, ou não comparecer ao pleito. Logo, pode-se dizer que qualquer situação em que se observa $X+Y \leq 400$ estaria dentro do esperado. Ao amostrar di-

versas urnas, todas elas satisfazendo essa restrição inerente (ou, se preferir, "trava matemática"), o resultado é exatamente um triângulo como o mostrado no lado direito da Figura C1. Esse cenário simplificado, e alguns pontos representando possíveis resultados válidos de votação nesse cenário, são mostrados na Figura C2.2

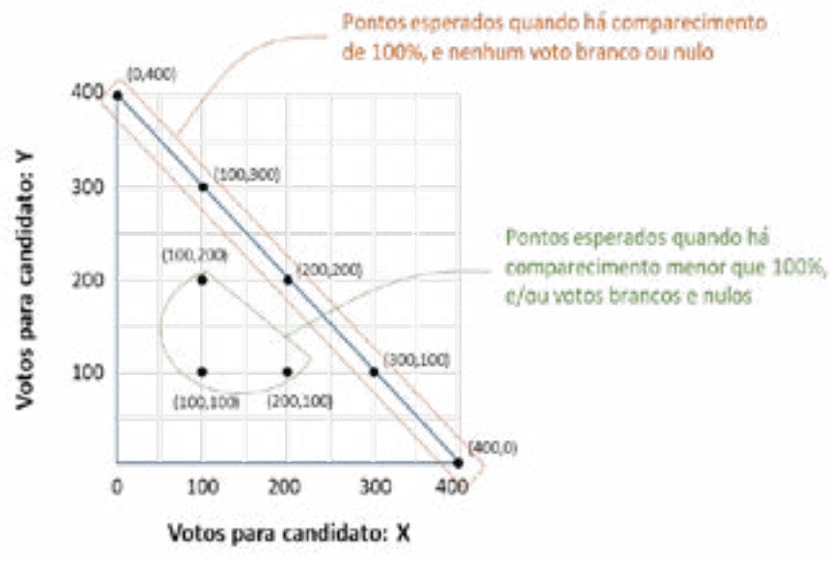


Figura C2 - Comportamento esperado para uma eleição com 2 candidatos e 400 eleitores por urna: forma-se naturalmente um gráfico de aparência triangular.

Como, mesmo no primeiro turno, os votos dos brasileiros concentraram-se essencialmente nos candidatos Lula e Bolsonaro, esse cenário simplificado com dois candidatos não é muito longe da realidade observada. Além disso, as urnas utilizadas nas eleições brasileiras costumam de fato ter um número máximo próximo de 400 eleitores, conforme mostra o gráfico da Figura C3 para as urnas efetivamente utilizadas nas eleições de 2022. A figura mostra também que há várias seções com um número menor de eleitores, embora números na faixa de 300 e 400 sejam mais comuns. Essa abordagem explica-se porque ela permite (1) reduzir o número de urnas utilizadas no pleito (mais eleitores por urna leva à necessidade de menos urnas), ao mesmo tempo que (2) evita-se a formação de longas filas (mais eleitores por urna aumenta a chance de formarem-se filas em horários de pico).

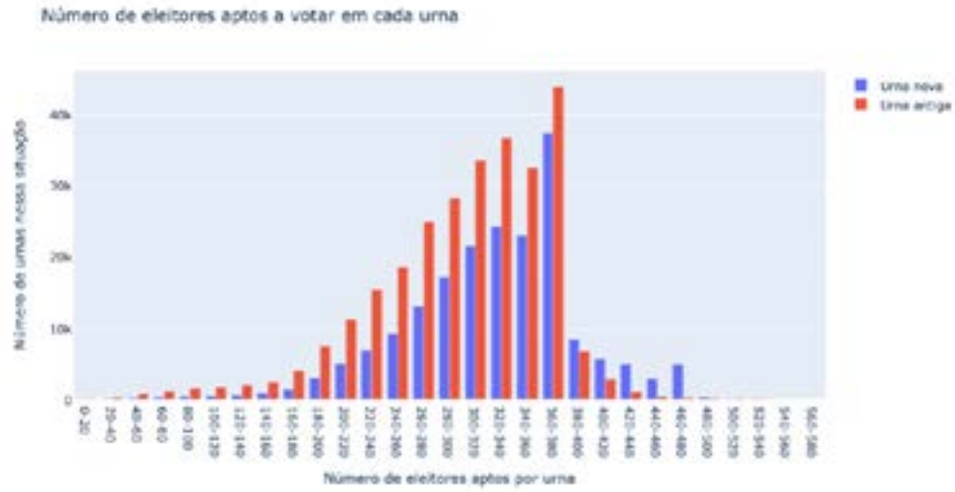


Figura C3 - Número de eleitores aptos a votar por modelo de urna, durante as eleições de 2022. Fonte: Autores com base nos dados disponíveis em https://dadosabertos.tse.jus.br/dataset/resultados-2022/resource/9f042e8b-ed41-4b18-a01b-e0613a68d90c

Logo, o que se esperaria observar para o gráfico criado a partir das amostragens feitas no Relatório Argentino para as UE anteriores a 2020 é exatamente o que foi observado: uma área triangular com uma zona limite concentrada na região próxima a 400!

Agora, o que explica então a "deformação" desse triângulo no gráfico da direita da Figura C1, que se refere às urnas 2020, escondendo o "ângulo fixo" observado nas urnas de modelos ante-

riores? Muito simples: observe novamente a Figura C3 e perceba que as UE2020 são as mais comumente usadas em seções nas quais o número de eleitores aptos supera a faixa dos 400, podendo chegar a números mais próximos de 500. Nesse cenário, espera-se que apareçam votos na região que fica após a linha que limita o número de eleitores a 400, conforme ilustra a Figura C4. Supondo que os votos nessa região mais externa se concentrem na área pontilhada mostrada à esquerda desta figura (uma área que, aproximadamente, dá um número similar de votos para os candidatos X e Y, algo estatisticamente esperado), pode-se observar algo muito similar ao perfil observado no "Relatório Argentino".

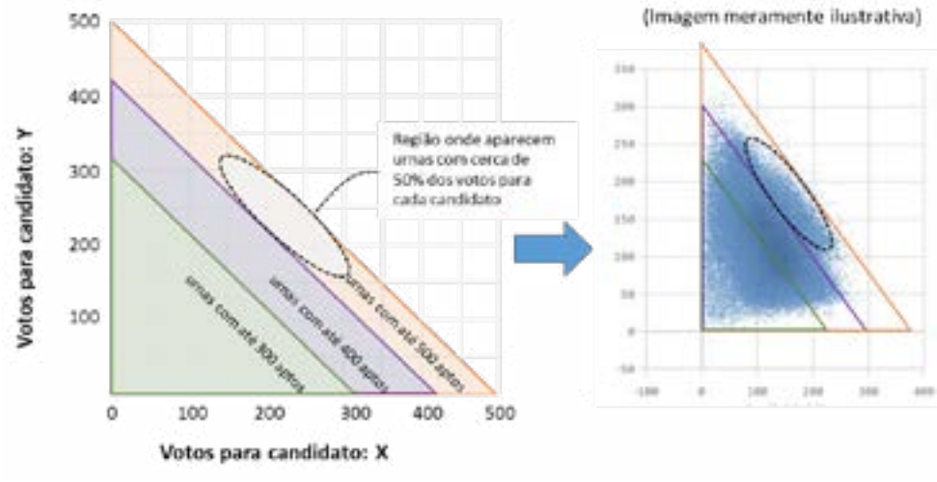


Figura C4 - Regiões onde se espera encontrar os resultados da votação para uma eleição com 2 candidatos, para 300, 400 e 500 eleitores aptos por urna (Esquerda). Supondo que os votos da região com mais eleitores aptos se concentrem na área pontilhada, o comportamento apresentado no gráfico do Relatório Argentino para as UE2020 é facilmente explicado. Nota: a imagem à direita é meramente ilustrativa, ou seja, os triângulos ali mostrados não necessariamente correspondem a urnas reais com 300, 400 ou 500 eleitores.

Novamente, ao contrário do que o Relatório Argentino afirma, não há qualquer estranheza em qualquer dos gráficos observados. Pelo contrário: usando apenas dados públicos, é fácil observar que os comportamentos obtidos, tanto para as urnas modelo 2020 como para modelos anteriores, levam exatamente a situações esperadas. Portanto, mais uma vez, o relatório equivoca-se ao fazer afirmações sensacionalistas como "Este jamais seria um comportamento esperado".

Conclusões

Após analisar tecnicamente o assim chamado "Relatório Argentino", as principais conclusões foram:

1. Alegação A: alega-se não haver documentação de auditoria recente para os modelos de urna anteriores a 2020, mas apenas para estas últimas.
    - Resultado da análise: não há qualquer embasamento para essa afirmação, dada a existência de análises de segurança bastante recentes tanto para as urnas modelo 2020 e 2015. Mesmo considerando que modelos mais antigos foram alvo de análises similares apenas no passado, a divisão entre "urnas modelos 2020" e "urnas de modelos anteriores" carece de critério técnico e, portanto, quaisquer conclusões tiradas a partir dessa comparação não devem ter qualquer relação com o modelo em si.
2. Alegação B: alega-se que as diferenças observadas em arquivos de log implicam a existência de códigos-fonte distintos sendo utilizados nas urnas eletrônicas brasileiras.

- Resultado da análise: embora potencialmente interessante como hipótese, a alegação se revela falsa. Foi possível reproduzir em laboratório o mesmo comportamento observado pelo autor do Relatório Argentino com o único código-fonte da urna eletrônica recebido do TSE pela USP, sem qualquer dificuldade.

3. Alegação C: alega-se haver uma "trava artificial" nos gráficos que mostram a soma dos votos aos candidatos Lula e Bolsonaro.

   - Resultado da análise: a alegação carece de qualquer fundamento. Os comportamentos observados, tanto para o gráfico das urnas modelo 2020 como para os gráficos de modelos anteriores, são facilmente explicáveis pela existência de número máximo de eleitores aptos a votar em cada urna, bem como pela distribuição desses valores máximos entre as urnas do modelo 2020 e para urnas de modelos anteriores.

Dadas essas observações e explicações, o que se conclui é que o Relatório Argentino não prima pelo rigor técnico, fazendo várias inferências infundadas e sensacionalistas. É difícil dizer se os erros (muitos dos quais podem ser considerados básicos) são causados por imperícia, pelo desejo deliberado de levar o leitor a erro, ou por uma combinação desses fatores.

Obviamente, essas observações não reduzem o potencial interesse em se realizar uma auditoria em urnas que pareçam suspeitas aos olhos de algum candidato, caso algum deles assim o deseje. Entretanto, sugere-se fortemente que eventuais pedidos dessa natureza, caso venham a fazer uso do Relatório Argentino como parte de sua fundamentação, não se apoiem em alegações como as aqui avaliadas, pois, ao partir de premissas falsas, a lógica decorrente é que as conclusões que dali sejam obtidas também sejam errôneas.

Anexo 2. Considerações sobre os logs das urnas eletrônicas brasileiras usadas nas eleições de 2022

14 de dezembro de 2022

LARC-PCS-EPUSP

Autores (em ordem alfabética)

- **Eduardo Lopes Cominetti**, Mestre e Aluno de Doutorado em Engenharia da Computação na Escola Politécnica da Universidade de São Paulo (USP)
- **Felipe Kenzo Shiraishi**, Engenheiro e Aluno de Mestrado na Escola Politécnica da Universidade de São Paulo (USP)
- **Leonardo Toshinobu Kimura**, Engenheiro e Aluno de Mestrado na Escola Politécnica da Universidade de São Paulo (USP)
- **Lucas Lago**, Mestre em Engenharia da Computação pela Escola Politécnica da Universidade de São Paulo (USP)
- **Marcos Antonio Simplicio Junior**, Professor Associado da Escola Politécnica da Universidade de São Paulo (USP)
- **Paulo Matias**, Professor Adjunto do Departamento de Computação da Universidade Federal de São Carlos (UFSCar)
- **Rafael Nobre Leite**, Engenheiro pela Universidade Federal de Itajubá (UNIFEI) e aluno de MBA em Ciência de Dados na Escola Superior de Agricultura Luiz de Queiroz da Universidade de São Paulo (USP)
- **Roberto Samarone dos Santos Araújo**, Professor Associado da Faculdade de Computação da Universidade Federal do Pará (UFPA)
- **Tiago Barbin Batalhão**, Doutor em Física pela Universidade Federal do ABC (UFABC)
- **Wilson Vicente Ruggiero**, Professor Titular da Escola Politécnica da Universidade de São Paulo (USP)

Resumo Executivo

O presente documento tem por objetivo esclarecer alguns pontos levantados em relatórios de autoria do Partido Liberal (PL) e do Instituto Voto Legal (IVL), nos quais são feitas diversas observações e alegações acerca dos logs das urnas eletrônicas utilizadas durante as eleições de 2022. Em suma, **o que é demonstrado neste Relatório é que as principais conclusões dos referidos documentos são infundadas, havendo ainda diversas alegações que carecem de rigor técnico**.

Mais detalhadamente, este documento se concentra em alegadas evidências que, segundo esses relatórios,

> "*comprovam que os arquivos Log de Urna são inválidos para todas as urnas eletrônicas de modelos antigos não 2020*" – vide (I) "Relatório Técnico – Logs Inválidos das Urnas Eletrônicas – Fiscalização das Eleições de 2022 no TSE. Relatório Preliminar, v 0.7 - 15/11/2022"[1]

ou que

> "*não há como realizar uma associação fiel do arquivo LOG com uma urna específica e, para além disso, também não há como relacionar tal arquivo com os demais elementos de auditoria de votos (BU e RDV) supostamente emitidos pelo mesmo equipamento*" – vide (II) "Representação Eleitoral para Verificação Extraordinária", apresentada pela Coligação Pelo Bem do Brasil (Partido Liberal, Republicanos e Progressistas), na p. 22.

Em particular, este Relatório se concentra nos seguintes aspectos:

- Primeiro: explicar o que é o erro no *software* das urnas que motivou as afirmações acima. Especificamente, analisa-se a razão pela qual os relatórios em questão respondem negativamente à pergunta

> "*Os arquivos LOG, obtidos no portal do TSE, contêm o valor correto do código de identificação da urna eletrônica, no campo documentado pelo TSE, em todas as suas linhas?*"

Em suma, **o presente documento mostra que <u>são corretas as observações</u> de que o "Código de identificação UE" não está presente nos logs das urnas de modelos anteriores ao UE2020**.

- Segundo: analisar as alegações no relatório que, em teoria, seriam depreendidas da observação anterior, as quais podem ser sumarizadas na frase:

> "*Nos arquivos LOG que não contêm o código de identificação da urna eletrônica correto, é impossível correlacionar univocamente esse arquivo LOG com o arquivo BU, invalidando a garantia de integridade do conteúdo do BU.*"

Demonstra-se aqui que essas <u>conclusões não têm qualquer fundamento técnico</u>. Na realidade, o que se comprova experimentalmente é que o "Código de identificação UE" não é o único (ou sequer o mais importante) produto gerado pelas urnas eletrônicas para vinculá-las aos resultados por elas produzidos, ou para permitir a verificação da integridade desses resultados. Assim, o que fica demonstrado é que **<u>qualquer pessoa</u> pode correlacionar um dado log com o Boletim de Urna correspondente, independentemente do modelo da urna e a despeito do problema relatado.**

- Terceiro: analisar, de forma não exaustiva, algumas das afirmações que aparecem em um ou mais dos relatórios em questão. O que se observa é que <u>várias afirmações são infundadas, por carecerem de rigor técnico</u>.

Este relatório tem teor técnico. Porém, ele também busca, na medida do possível, utilizar uma linguagem mais próxima do público em geral. Ao mesmo tempo, seguindo boas práticas científicas, as conclusões apresentadas não são meras opiniões, mas são demonstradas por meio de referências, exemplos e experimentos que podem ser executados por qualquer pessoa.

Introdução

O TSE e a USP firmaram o Convênio 14/2021, com a finalidade de permitir ao Laboratório de Arquitetura e Redes de Computadores (LARC), vinculado ao Departamento de Engenharia de Computação e Sistemas Digitais (PCS) da Escola Politécnica da Universidade de São Paulo (USP), planejar e executar testes de segurança sobre as urnas eletrônicas brasileiras. Como parte desse convênio, foram disponibilizadas para a Universidade de São Paulo: duas unidades do modelo UE2015 e três unidades do modelo UE2020; a documentação correspondente ao ecossistema das urnas; e os códigos-fontes e respectivos códigos compilados para realizar a carga das urnas para fins de testes.

Essa colaboração entre USP e TSE conta ainda com a parceria de pesquisadores em diferentes universidades no Brasil e no exterior (e.g., Universidade Federal de São Carlos – UFSCar, e Universidade Federal do Pará – UFPA). Esse conjunto de pesquisadores costuma elaborar sugestões diversas sobre estratégias para testar a segurança dos equipamentos, e também sobre inovações que poderiam contribuir com a segurança e transparência do processo eleitoral de forma geral.

Nesse contexto, tomamos conhecimento no dia 15/Novembro/2022, por meio do *site* "O Antagonista", do documento intitulado "Relatório Técnico - Logs Inválidos das Urnas Eletrônicas - Fiscalização das Eleições de 2022 no TSE. Relatório Preliminar, v0.7 - 15/11/2022"[1]. Esse documento tem como autores membros do Partido Liberal (os nomes listados são Valdemar da Costa Neto, Capitão Augusto e José Tadeu Candelária) e do Instituto Voto Legal (a saber, Carlos Rocha, Marcio Abreu e Flávio Gottardo de Oliveira). Posteriormente, no dia 22/Nov/2022, obtivemos acesso à "Representação Eleitoral para Verificação Extraordinária", documento de 224 páginas apresentado pela Coligação Pelo Bem do Brasil (Partido Liberal, Republicanos e Progressistas) e protocolado junto ao Colegiado do Tribunal Superior Eleitoral com o número 0601958-94.2022.6.00.0000. Finalmente, no dia 23/Nov/2022, tivemos acesso ao documento "Emenda à Inicial - Representação por Verificação Extraordinária", protocolada com o identificador 158427148. Por comodidade, o primeiro documento é aqui referenciado como "Relatório do PL/IVL-1"; o segundo, como "Relatório do PL/IVL-2"; e o terceiro, como "Relatório do PL/IVL-3". Ainda, quando a individualização desses documentos não for relevante para a discussão, o conjunto deles é simplesmente denominado "Relatórios do PL/IVL".

O que se pretende aqui é analisar, de maneira estritamente técnica e com base em evidências, referências, exemplos reais e experimentos (e não em meras opiniões ou impressões), os seguintes aspectos cobertos nesses relatórios:

- Explicar o que está sendo apontado como erro no *software* das urnas, que é o cerne da discussão nesses relatórios. Especificamente, analisa-se

a razão pela qual os relatórios em questão respondem negativamente à pergunta:

> *"Os arquivos LOG, obtidos no portal do TSE, contêm o valor correto do código de identificação da urna eletrônica, no campo documentado pelo TSE, em todas as suas linhas?"*

Em suma, **o presente documento mostra que são corretas as observações de que o "Código de identificação UE" não está presente nos logs das urnas de modelos anteriores ao UE2020:** no lugar dele, o que se observa é o valor "67305985". Destaca-se que **o log é o único documento gerado pela urna que apresenta esse problema, de modo que os documentos contendo os resultados da votação em si (boletim de urna e registro digital de votos) não são afetados**.

- Analisar as alegações no relatório que, em teoria, seriam depreendidas da observação anterior, as quais podem ser sumarizadas na seguinte frase extraída do Relatório do PL/IVL-2:

> *"Nos arquivos LOG que não contêm o código de identificação da urna eletrônica correto, é impossível correlacionar univocamente esse arquivo LOG com o arquivo BU, invalidando a garantia de integridade do conteúdo do BU."*

Demonstra-se aqui que essas conclusões não têm qualquer fundamento técnico. Na realidade, o que se demonstra experimentalmente é que o "Código de identificação UE" não é o único (ou sequer o mais importante) produto gerado pelas urnas eletrônicas para vincular o dispositivo aos resultados por ele produzidos, ou para permitir a verificação da integridade desses resultados. Assim, **o que se comprova é exatamente o oposto do que é afirmado no relatório: qualquer pessoa pode correlacionar um dado log com o Boletim de Urna correspondente, independentemente do modelo da urna e a despeito do problema observado.**

- Analisar, de forma não exaustiva, algumas das afirmações que aparecem em um ou mais dos relatórios em questão. O que se observa é que várias afirmações são infundadas, carecem de rigor técnico ou, ao menos, merecem alguns esclarecimentos adicionais para não serem erroneamente interpretadas.

Por outro lado, não faz parte dos objetivos deste documento aferir a segurança ou a auditabilidade de elementos que, embora componham o ecossistema da urna eletrônica brasileira, não tenham relação direta com os itens acima. Na realidade, fazer essa análise ampla é parte de um escopo mais geral, pois é exatamente o tema de colaboração vigente entre o TSE e universidades parceiras no Brasil para trazer melhorias ao processo eleitoral brasileiro.

A seguir, são apresentados os resultados das análises de cada um dos pontos que fazem parte do escopo deste relatório, bem como evidências que demonstram as conclusões aqui apresentadas.

A. O valor "67305985" nos logs de urnas de modelos anteriores ao UE2020

Primeiramente, cabe esclarecer o que é o "log" das urnas eletrônicas. Não é algo complicado: trata-se simplesmente de um

"diário de bordo", ou seja, um arquivo de texto que registra os eventos que aconteceram na urna em questão, com a data e horário de cada evento. Exemplos de registros desse tipo incluem: o momento em que a urna foi ligada; o estado da bateria então observado; o resultado das várias verificações que ela faz internamente (incluindo verificações de segurança, para identificar se o *software* nela carregado é legítimo); os momentos em que a votação foi iniciada e finalizada; as informações do local onde a urna foi utilizada (como código de município, zona eleitoral, local de votação e seção eleitoral); o código identificador da carga de *software* (também conhecido como "código de correspondência"). Esses arquivos são públicos, podendo ser obtidos diretamente no *site* Resultados do TSE (para consultas interativas, por Estado, zona e seção) ou, alternativamente, no Portal de Dados abertos do TSE (para obter conjuntos completos de dados, por Estado).[2,3] O Apêndice I deste documento mostra o passo a passo de como obter esses arquivos por meio do primeiro método.

Uma vez esclarecido esse ponto, podemos explicar o problema que foi apontado nos Relatórios do PL/IVL. De acordo com a documentação oficial do TSE, o arquivo de log deve seguir um formato similar ao mostrado na Listagem A1 a seguir:[4]

```
07/10/2018 16:38:21 INFO 1543882 LOGD Início das operações do logd 76607CDD3973A5AF
07/10/2018 16:38:21 INFO 1543882 LOGD Adicionando informação do log da FE AB3F33C2E41E03F6
07/10/2018 16:38:21 EXTERNO 1543882 LOGD Arquivo
154388212018100716382l-01.jez referente ao log da FE 52D44B463DC14B4E
07/10/2018 16:38:21 INFO 1543882 LOGD Fim da adição de informação do log da FE 143FA813CAB96612
07/10/2018 16:38:21 INFO 1543882 LOGD Copiando conteúdo da pasta logs 8C5E0BEE854CAB09
07/10/2018 16:38:21 INFO 1543882 LOGD Fim da cópia do conteúdo da pasta logs 543CB9DD6AA9E58D
07/10/2018 16:38:21 INFO 1543882 LOGD Iniciando log duplo 57DFB08637AE4281
07/10/2018 16:38:21 INFO 1543882 GAP Sincronismo de flash - Etapa Atualização de log:
OK F119F728CAECB090
```

Listagem A1. Exemplo de log de urna. Fonte: [4]

Perceba que o quarto campo de toda linha é um número repetido, "1543882", sublinhado no exemplo apresentado para facilitar a visualização. Esse é o código identificador da urna eletrônica, ou "ID_UE", que consiste essencialmente em um número de série daquela urna. Como qualquer identificador, esse número deve ser único por urna, de modo que o valor apresentado nos logs gerados por urnas distintas deve ser diferente. Entretanto, nas eleições de 2022, isso não ocorreu com as urnas de modelos UE2015, UE2013, UE2011, UE2010 e UE2009, ou seja, todos os modelos utilizados nessas eleições com exceção do modelo mais novo, denominado UE2020.[5] Especificamente, o que observam os Relatórios do PL/IVL é que, nessas urnas mais antigas, esse número é substituído pelo valor fixo "67305985" (que pode ser traduzido por "0x04030201", usando notação hexadecimal).[6]

Para ilustrar esse fato, podem-se comparar duas urnas, ambas usadas na zona eleitoral 0369 da cidade de Boituva/SP: uma na seção eleitoral 0050, que recebeu urnas do modelo UE2010, e outra na seção 0064, que recebeu urnas do modelo UE2020 (em caso de dúvida, a informação do modelo de urna pode ser obtida diretamente do próprio log da urna, buscando pelas palavras "Identificação do Modelo de Urna").

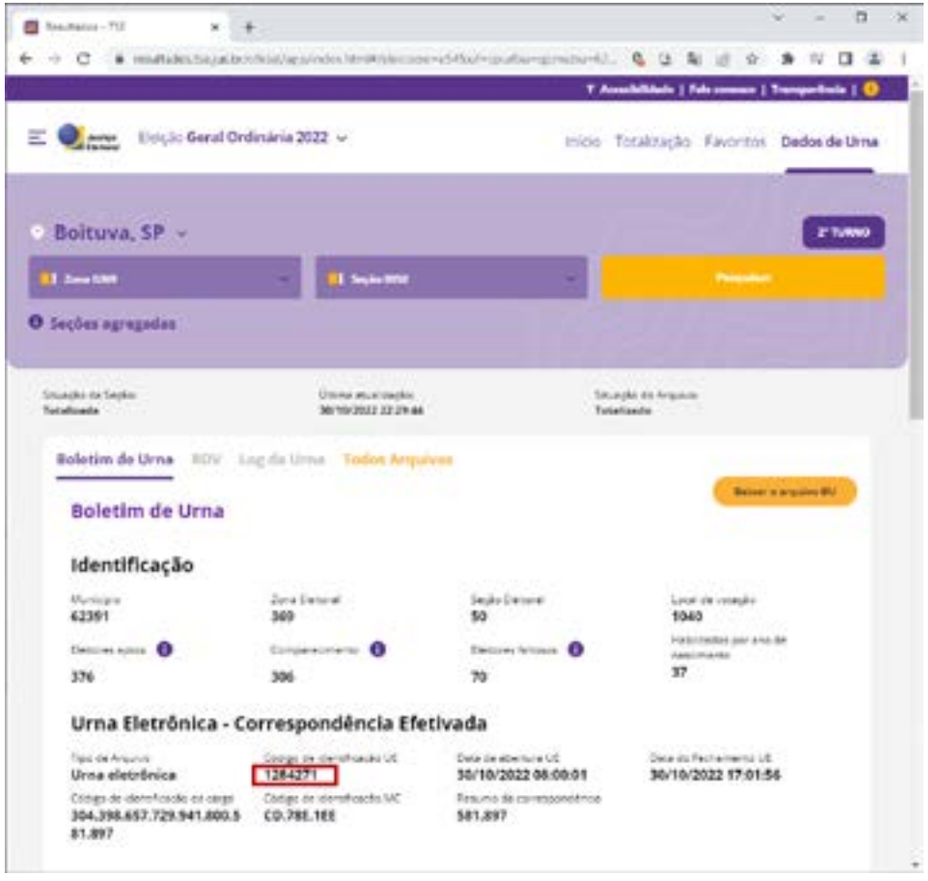


Figura A1 – O código de identificação (ID_UE) da urna eletrônica usada em Boituva/SP, na Zona 0369 e Seção 0050, é "1284271". Fonte: [2]

Conforme se observa na Figura A1, na seção 0050 foi utilizada a urna cujo identificador é "1284271". Já como mostra a Figura A2, a seção 0064 recebeu a urna cujo identificador é "2211541".

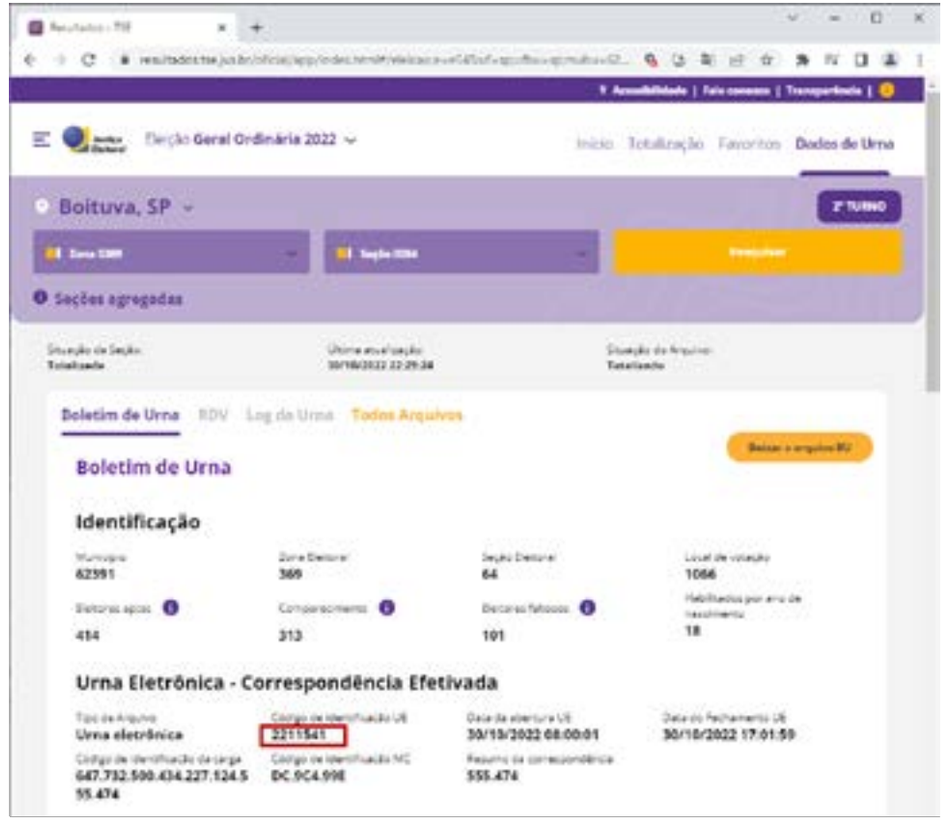


Figura A2 – O código de identificação (ID_UE) da urna eletrônica usada em Boituva/SP, na Zona 0369 e Seção 0064, é "2211541". Fonte: [2]

Ao analisar o log da urna da Seção 0064, não há problemas perceptíveis: o ID_UE "2211541" aparece em todas as linhas do log, como mostrado na Listagem A2 (por simplicidade, apenas as primeiras linhas são aqui reproduzidas):

```
22/09/2022 15:49:11 INFO 2211541 LOGD    Início das operações do logd          11FFFE578FBB9492
22/09/2022 15:49:11 INFO 2211541 LOGD    Urna ligada em 22/09/2022 às 15:48:40 963618CD7E54D3DD
22/09/2022 15:49:11 INFO 2211541 SCUE    Iniciando aplicação - Oficial - 1º turno    F 1 6 A 5 A B 6 D -
0DEC1C8
22/09/2022 15:49:11 INFO 2211541 SCUE    Versão da aplicação: 8.26.0.0 - Onça-pintada
1C32D1669E71254B
22/09/2022 15:49:13 INFO 2211541 SCUE    Urna operando com rede elétrica       493CE766074CF431
22/09/2022 15:49:13 INFO 2211541 SCUE    Bateria interna com carga parcial     15AA8CC8A7061DCF
```

Listagem A2. Trecho do arquivo de log da urna usada na zona eleitoral 0369 e seção eleitoral 0064 de Boituva/SP. Fonte: [2]

Em comparação, ao analisar o log da urna da Seção 0050, o que se observa são as linhas mostradas na Listagem A3, nas quais o ID_UE é simplesmente "67305985" (por simplicidade, apenas as primeiras linhas são aqui reproduzidas):

```
23/09/2022 16:45:16 INFO 67305985 LOGD Início das operações do logd          B5607DEC01E0B751
23/09/2022 16:45:16 INFO 67305985 LOGD Urna ligada em 23/09/2022 às 16:44:02 4DEA8601F2E19246
23/09/2022 16:45:16 INFO 67305985 SCUE Iniciando aplicação - Oficial - 1º turno 6A227592CC9F510C
23/09/2022 16:45:16 INFO 67305985 SCUE Versão da aplicação: 8.26.0.0 - Onça-pintada 683BF830370081A3
23/09/2022 16:45:18 INFO 67305985 SCUE Urna operando com rede elétrica 4A37B2F881A26CBD
23/09/2022 16:45:18 INFO 67305985 SCUE Bateria interna com carga plena 39ED112EDF908EB0
```

Listagem A3. Trecho do arquivo de log da urna usada na zona eleitoral 0369 e seção eleitoral 0050 de Boituva/SP. Fonte: [2]

Conforme já mencionado, o mesmo comportamento inesperado pode ser observado em todas as urnas dos modelos UE2015, UE2013, UE2011, UE2010 e UE2009, sejam elas usadas apenas no 1º turno, apenas no 2º turno, ou em ambos. Logo, de fato existe um erro na forma como o *software* faz a escrita do log para esses modelos de urna, que faz com que o ID_UE não esteja presente nos respectivos logs. Pode-se dizer, portanto, que nesse quesito específico, os Relatórios do PL/IVL estão corretos.

Contudo, para fins de clarificação, ressalta-se que o mesmo tipo de erro não foi observado nos outros arquivos gerados pela urna. Em particular, no Boletim de Urna (BU, que contém os votos totais obtidos por cada candidato), é possível identificar o código da urna e outras informações da seção de votação. O mesmo acontece no arquivo de Registro Digital de Votos (RDV, que contém os votos individuais que levam ao total apresentado no BU): as informações identificadoras da urna estão bastante explícitas. De fato, as Listagens A4 e A5 a seguir mostram esses dados extraídos do BU e do RDV da mesma zona e seção apresentadas na Figura A1. O Apêndice II mostra um passo a passo que permite a qualquer pessoa extrair essas informações dos arquivos de BU e RDV disponibilizados pelo TSE.

```
. urna:
. . correspondenciaResultado:
. . . carga:
. . . . codigoCarga = 30439865772994180058 1897
. . . . dataHoraCarga = 20220923T164700
. . . . numeroInternoUrna = 1284271
. . . . numeroSerieFC = cd78e1ee
. . . identificacao = ('identificacaoSecaoEleitoral', {'municipioZona': {'municipio': 62391, 'zona': 369},
'local': 1, 'secao': 50})
. . numeroSerieFV = 48ff9a84
. . tipoArquivo = votacaoUE
. . tipoUrna = secao
. . versaoVotacao = 8.26.0.0 - Onça-pintada
```

Listagem A4. Trecho do Boletim de Urna de Boituva/SP, com o número interno da urna e outras informações identificadoras (como município e zona). Fonte: [2]

```
. urna:
. . correspondenciaResultado:
. . . carga:
. . . . codigoCarga = 30439865772994180058 1897
. . . . dataHoraCarga = 20220923T164700
. . . . numeroInternoUrna = 1284271
. . . . numeroSerieFC = cd78e1ee
. . . identificacao (identificacaoSecaoEleitoral):
. . . . local = 1
. . . . municipioZona:
. . . . . municipio = 62391
. . . . . zona = 369
. . . . secao = 50
. . numeroSerieFV = 48ff9a84
. . tipoArquivo = votacaoUE
. . tipoUrna = secao
. . versaoVotacao = 8.26.0.0 - Onça-pintada
```

Listagem A5. Trecho do Registro Digital de Votos de Boituva/SP, com o número interno da urna e outras informações identificadoras (como município e zona). Fonte: [2]

1B. Sobre a impossibilidade de correlacionar cada Log de Urna com o Boletim de Urna correspondente, devido ao erro observado

Uma vez confirmada a observação sobre a ausência do ID_UE nos logs das urnas de modelos anteriores ao UE2020, passamos a analisar as conclusões dos Relatórios do PL/IVL sobre esse fato. Todos esses relatórios são unânimes em alegar que o erro observado impede a verificação da correspondência entre um arquivo de log e as urnas eletrônicas que os geraram. A título de exemplo, essa afirmação aparece no Relatório do PV/IVL-1 como:

> *"Nos arquivos Log de Urna que não contêm o código de identificação da urna eletrônica correto, é impossível correlacionar univocamente esse log com o Boletim de Urna, invalidando a possibilidade de auditoria".*

Também aparece no Relatório do PV/IVL-2 em frases como:

> *"Não há como realizar uma associação fiel do arquivo LOG com uma urna específica e, para além disso, também não há como relacionar tal arquivo com os demais elementos de auditoria de votos (BU e RDV) supostamente emitidos pelo mesmo equipamento".*

Finalmente, a alegação é reforçada no Relatório do PV/IVL-3, em afirmações como:

> *"O código de identificação da urna eletrônica, lido diretamente do hardware do equipamento, e exibido no registro de cada atividade, em cada linha do LOG, é essencial 'para vincular cada atividade à urna física (hardware) que realizou a atividade, e, assim, validar o registro em cada linha do LOG, para fins de auditoria de funcionamento da urna eletrônica. Outros dados inseridos manualmente, por operadores humanos, tais como os códigos do município, da zona eleitoral, do local de votação e da seção eleitoral, são mutáveis e não permitem assegurar a necessária vinculação ao hardware físico da urna, no registro de cada atividade, em cada linha do LOG".*

Dessa forma, pode-se considerar que a principal alegação técnica apresentada nos Relatórios do PL/IVL é a de que, supostamente, seria impossível saber a qual urna corresponderia um log cujo ID_UE informado seja 67305985, dado o grande número de urnas que poderia estar por trás desse identificador. **Essa afirma-**

ção, entretanto, não tem fundamento. A razão é que o ID_UE não é o único (ou sequer o principal) identificador que liga de forma unívoca um arquivo gerado durante a votação (inclusive logs) à urna eletrônica responsável pela sua geração. Conforme exposto na Seção A, a própria combinação {código de município, zona eleitoral, local de votação e seção eleitoral} pode, ao menos em princípio, ser usada como um identificador para a urna eletrônica. Qualquer pessoa pode verificar esse fato: basta seguir o procedimento descrito no Apêndice I para encontrar esses dados identificadores diretamente no arquivo de log, qualquer que seja o modelo de urna. Consequentemente, qualquer pessoa pode ir além e realizar a tarefa supostamente "impossível" de descobrir o ID_UE dado apenas um log de uma urna de modelo anterior ao UE2020, por meio do seguinte procedimento:

1. Peça para alguém te enviar um log qualquer obtido do site Resultados do TSE,[2] sem te dizer qual a zona e seção escolhida, ou qualquer outra informação. Para isso, basta que ele siga os passos mostrados nas Figuras Ap1 a Ap7 do Apêndice I.

2. Em seguida, descubra a zona e seção buscando por essa informação diretamente no log, e realize uma consulta pelo BU correspondente também no site Resultados do TSE.[2] Para isso, basta seguir os passos mostrados nas Figuras Ap8 a Ap11 do Apêndice I, acrescentando o passo de buscar o nome do Município a partir do seu código numérico mostrado no log – essa informação é necessária no passo da Figura Ap11. Como a lista de municípios é razoavelmente estática, provavelmente a forma mais fácil de executar esse passo extra é consultando a planilha (relativa ao ano de 2020) disponível no site do TSE.[7]

3. E isso conclui o experimento: com um simples cruzamento de dados, pode-se realizar a "impossível" tarefa de correlacionar o log de uma urna qualquer com o restante dos documentos gerados por ela. Em particular, pode-se obter o ID_UE da urna a partir do seu BU.

Agora, pode-se argumentar que as informações relativas a zona e seção não podem ser consideradas um "identificador forte" das urnas, por serem fornecidas por usuários humanos e, portanto, serem potencialmente sujeitas a manipulação durante a carga do *software* na urna. Essa é exatamente a alegação feita no Relatório do PL/IVL-3, no qual se afirma que:

> "*Outros dados inseridos manualmente, por operadores humanos, tais como os códigos do município, da zona eleitoral, do local de votação e da seção eleitoral, são mutáveis e não permitem assegurar a necessária vinculação ao hardware físico da urna*".

Mesmo assumindo, para fins de argumentação, que essa alegação seja correta, bastaria então verificar outro identificador da urna mencionado também na Seção A: o código identificador da carga de *software* (também conhecido como "código de correspondência"). Afinal, esse identificador não é gerado por humanos, mas sim pelo *software* da urna (especificamente, pelo *Software* de Carga da Urna Eletrônica – SCUE).

Para verificar que qualquer pessoa pode usar esse identificador para ligar um log qualquer à urna correspondente, basta seguir novamente o passo a passo do Apêndice I. Isso permite obter o código de carga da urna a partir do log. De fato, as Listagens A6 e A7, a seguir, mostram os códigos de carga obtidos a partir dos logs das duas urnas de Boituva/SP usadas nos exemplos até aqui:

```
23/09/2022 16:48:42 INFO 67305985 SCUE Município: 62391 568DFE4AA16F17C9
23/09/2022 16:48:42 INFO 67305985 SCUE Zona Eleitoral: 0369 05C6F1F89666166A
23/09/2022 16:48:42 INFO 67305985 SCUE Local de Votação: 1040 73F6C0F6D54C0658
23/09/2022 16:48:42 INFO 67305985 SCUE Seção Eleitoral: 0050 A6B65CE8F46C472E
23/09/2022 16:49:03 INFO 67305985 SCUE Imprimindo extrato de carga DF7267B0A672785A
23/09/2022 16:49:07 INFO 67305985 SCUE Confirmação do extrato de carga 31D25FFB943A4CB0
23/09/2022 16:49:07 INFO 67305985 LOGD Iniciando cópia de Log da ME para MI 6BF3610F1941A46C
23/09/2022 16:49:07 INFO 67305985 LOGD Cópia de Log da ME para MI realizada com sucesso. 57FBE8A-63828C3DC
23/09/2022 16:49:08 INFO 67305985 SCUE Código de carga 304.398.657.729.941.800.581.897 gravado na tabela de correspondência D443F2BF06E63C0D
```

Listagem B1. Trecho do arquivo de log da urna usada na zona eleitoral 0369 e seção eleitoral 0050 de Boituva/SP. Fonte: [2]

```
22/09/2022 15:49:15 INFO 2211541 SCUE Município: 62391 5222668ED4E8D5B2
22/09/2022 15:49:15 INFO 2211541 SCUE Zona Eleitoral: 0369 AC552C405A7060A4
22/09/2022 15:49:15 INFO 2211541 SCUE Local de Votação: 1066 52F8B78300C30F69
22/09/2022 15:49:15 INFO 2211541 SCUE Seção Eleitoral: 0064 FC5C415ACA03DAA0
22/09/2022 15:49:23 INFO 2211541 SCUE Imprimindo extrato de carga 88A6F46FB6E8C08F
22/09/2022 15:49:26 INFO 2211541 SCUE Confirmação do extrato de carga FA889E04064BAF55
22/09/2022 15:49:26 INFO 2211541 LOGD Iniciando cópia de Log da ME para MI 92044A8834B5F024
22/09/2022 15:49:26 INFO 2211541 LOGD Cópia de Log da ME para MI realizada com sucesso. B945D-F79999B5363
22/09/2022 15:49:26 INFO 2211541 SCUE Código de carga 647.732.500.434.227.124.555.474 gravado na tabela de correspondência 0DC650F453A52CBB
```

Listagem B2. Trecho do arquivo de log da urna usada na zona eleitoral 0369 e seção eleitoral 0064 de Boituva/SP. Fonte: [2]

A execução do passo seguinte, de obter o ID_UE, torna-se então um pouco mais trabalhosa do que no caso em que a trinca {município, zona, seção} é usada como identificador da urna, mas novamente é bem longe de impossível. Especificamente, os dados necessários para fazer o respectivo cruzamento encontram-se no conjunto de dados "Resultados – 2022 – Correspondências esperadas e efetivadas – 2º turno":[8] essa página tem as "correspondências" esperadas de todos os Estados do Brasil, ou seja, arquivos de texto no formato CSV (valores separados por ponto e vírgula) contendo, entre outras informações, os códigos identificadores de carga de *software* e ID_UE das urnas, separados por Estado. Para manipular esses arquivos, o ideal seria usar ferramentas de processamento de dados. Porém, como nosso interesse é apenas realizar a (perfeitamente possível) tarefa de descobrir o ID_UE da urna com código de carga "304.398.657.729.941.800.581.897" (modelo UE2010, da Seção 0050), além de confirmar que a urna com ID_UE 2211541 (modelo UE2020, da Seção 0064) tem o código de carga "647.732.500.434.227.124.555.474", podemos usar simplesmente um *software* de edição de texto que suporta arquivos grandes – por exemplo, o Notepad++.[9] Especificamente, qualquer pessoa pode fazer o seguinte:

1. Fazer o *download* dos arquivos de correspondência do 2º turno para todo o Estado de São Paulo a partir do *site* "Resultados – 2022 – Correspondências esperadas e efetivadas – 2º turno", previamente mencionado:[8] Se preferir, isso pode ser feito diretamente pelo link https://cdn.tse.jus.br/estatistica/sead/eleicoes/eleicoes2022/correspefet/CEFT_2t_SP_311020221100.zip.[10]
2. Descompactar o arquivo usando o aplicativo de sua preferência (e.g., o 7zip).[11]
3. Abrir o arquivo contendo as urnas efetivamente utilizadas no pleito, nomeado "csec_2t_SP_301020221145.csv", usando o Notepad++.
4. Buscar, usando o comando Ctrl+F, o código de carga da urna desejada, removendo os pontos entre os dígitos. Ou seja, para encontrar as urnas

das Seções 0050 e 0064, faça a busca por "304398657729941800581897" e por "64773250043422712455547 4", respectivamente.

5. Observe o resultado, reproduzido na Figura B1: você deve encontrar as informações das urnas buscadas nas linhas 7628 e 7636. Como seria de se esperar, o ID_UE da urna da seção 0050 é 1284271 (veja informação indicada pela seta), enquanto o ID_UE da urna da seção 0064 é 2211541 (como já era possível saber pelo seu log).
6. Pronto! Mais uma tarefa "impossível" realizada com sucesso.

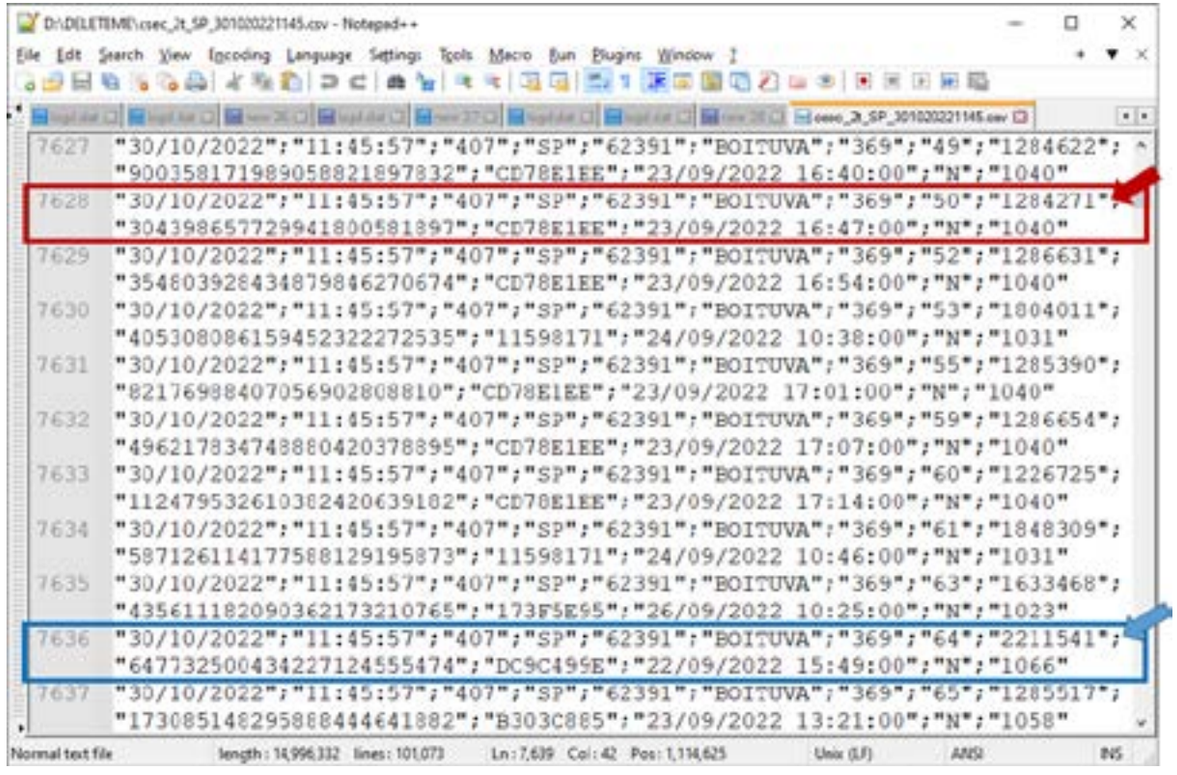


Figura B1 – Busca por urnas pelo código de carga, usando o arquivo de correspondências do Estado de São Paulo. Fonte: [8]

B.1. Mas e a integridade desses logs...?

Considerando os procedimentos mostrados até aqui, deve estar mais claro que qualquer pessoa pode recuperar o ID_UE de qualquer urna a partir do seu arquivo de log. Isso vale até mesmo para aquelas urnas afetadas pelo erro apontado pelos Relatórios do PL/IVL. Porém, o leitor mais cético (ou familiarizado com a área de segurança) deve estar desconfiado de uma questão: mas

como saber se o arquivo de log não foi alterado?! Afinal, uma auditoria deve considerar a possibilidade de que a integridade dos dados tenha sido comprometida!

De fato, o leitor está correto em fazer essa pergunta. Na realidade, ele está tão correto que, embora talvez não tenha notado, em todas as Listagens apresentadas até aqui os logs foram ligeiramente modificados: nos arquivos de log originais, os campos são separados por um caractere de tabulação, os quais foram aqui substituídos por caracteres de espaço para facilitar a visualização. Essa modificação foi feita para ambas as urnas analisadas em nossos exemplos, dos modelos UE2020 e UE2010, o que deve deixar claro que nenhum dos arquivos de log está imune a esse tipo de alteração por um simples editor de texto. Mais precisamente, qualquer pessoa pode acessar o log de uma urna qualquer (UE2020 ou não) e substituir o identificador de UE, as informações de zona, seção e município, o código de carga, ou qualquer outra informação, e então salvar o arquivo modificado com o mesmo nome do arquivo original. O resultado é um arquivo de log aparentemente legítimo, mas cujo conteúdo não corresponde à realidade. Não poderia ser diferente: o log é apenas um arquivo de texto, de fácil modificação usando um editor de texto simples, como ilustra o passo a passo no Apêndice III.

E é agora que vem a pergunta importante: o que impede então esse "ataque de modificação" (ou "fraude por editor de texto", se preferir)? Certamente não é o famigerado ID_UE, que pode ser igualmente modificado. A resposta é muito simples: **a integridade dos logs da urna, assim como de todos os outros resultados por ela gerados, é protegida pela assinatura digital daquela urna, gerada usando uma chave de assinatura única por urna**. Essa chave de assinatura (também chamada de "chave privada") é protegida por um *hardware* de segurança, enquanto a chave de verificação (também conhecida como "chave pública") correspondente faz parte dos arquivos disponibilizados para auditoria dos resultados da eleição na página de dados abertos.[12] Como resultado, qualquer tentativa de modificar o log da urna (ou outros arquivos ainda mais importantes, como BU e RDV), invalidaria a assinatura digital correspondente, revelando a falsificação daquele arquivo. Como apenas a urna consegue gerar assinaturas válidas para os dados que ela produz, saber operar um editor de texto está longe de ser suficiente para realizar qualquer alteração nos arquivos. A única forma de realmente fazê-lo seria extrair a chave privada da urna alvo. Mas como? A verdade é que essa é uma tarefa extremamente desafiadora: a chave privada de cada urna é única e armazenada em um componente de *hardware* dedicado, protegido por uma grossa camada de resina, conhecido como Módulo de Segurança Embarcado (MSE) – vide o artigo científico "Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo T-DRE", publicado no Workshop de Tecnologia Eleitoral do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2019).[13] Portanto, **chegamos ao identificador mais importante das urnas eletrônicas atualmente utilizadas: sua chave pública, que está matematicamente vinculada à chave privada protegida pelo hardware da urna**, permitindo a verificação das assinaturas geradas pelas urnas sem revelar o valor da chave de assinatura.

É essa verificação, e não a presença/ausência do ID_UE no conteúdo dos arquivos, que de fato permite o vínculo forte entre uma urna específica e os arquivos por ela produzidos, incluindo seu log. E como verificar essas assinaturas? Primeiramente, os arquivos de assinatura estão publicamente disponíveis por meio do *site* de dados abertos do TSE:[12] são os arquivos com extensão ".vscmr" e ".vscsa", que podem ser obtidos diretamente (junto com logs, boletins de urna, registros digitais de votos, entre outros documentos) na página "Resultados 2022 – Arquivos transmitidos para totalização".[14] Uma vez de posse desses arquivos, é possível extrair o certificado digital da urna eletrônica, que contém a chave pública da urna (e, portanto, é único por dispositivo). Como ilustra a Figura B2 para a urna usada na Zona 0369 e Seção 0050 de Boituva/SP, é interessante notar que o campo "Common Name" desse certificado contém também o ID_UE da urna, mesmo nos modelos anteriores a UE2020. O certificado constituindo-se, portanto, em ainda outra forma de vincular os logs e demais arquivos produzidos pela urna ao seu ID_UE. O certificado é emitido pelo próprio TSE antes das eleições e, essencialmente, habilita a urna a ser utilizada nos pleitos, ao prover um meio para que assinaturas digitais geradas pelo equipamento em questão sejam verificadas. Uma vez validado esse certificado, o passo seguinte é verificar as assinaturas feitas pelo MSE da urna em si. Essas assinaturas são calculadas usando algoritmos padronizados, a saber: padrão ECDSA/P521 nas urnas mais antigas, dos modelos UE2009 até UE2015;[15, 16] e padrão EdDSA/E521 nas urnas de modelo UE2020.[16]

```
C:\Users\Toshi\Downloads\testes_bu_rdv>openssl x509 -text -noout -in cert.der
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 555051 (0x8782b)
        Signature Algorithm: ecdsa-with-SHA512
        Issuer: CN = AC URNA, ST = DF, C = BR, emailAddress = acurna@tse.jus.br, O = TSE, OU = STI, L = Brasilia
        Validity
            Not Before: Jun  5 14:55:09 2012 GMT
            Not After : Feb 12 14:55:09 2026 GMT
        Subject: CN = uea=01284271, ST = DF, C = BR, O = TSE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (521 bit)
                pub:
                    04:01:5b:6e:8c:7e:6a:03:a1:4d:e0:ed:65:ea:5b:
                    12:35:a5:7d:ad:92:81:c3:95:e8:ca:99:47:ec:bf:
                    78:6b:38:ba:57:e9:49:f2:9f:b1:b5:72:0b:df:8a:
                    55:7a:c8:a2:17:25:88:f1:78:c3:2b:54:09:a9:09:
                    fd:c8:27:e2:6a:60:71:00:a1:ea:29:15:5e:34:b0:
                    e0:72:23:3d:d0:8d:0f:56:3a:6e:a8:9c:b6:6a:64:
                    b2:8c:88:b7:73:87:26:7f:43:99:71:e6:fb:8e:be:
                    ad:7f:24:cd:61:7c:a9:1f:dd:7d:4c:7b:d6:7d:d5:
                    f4:d9:80:37:34:2a:d7:2d:52:c6:19:c1:73
                ASN1 OID: secp521r1
                NIST CURVE: P-521
```

Figura B2. Trecho do certificado do hardware da urna usada na zona eleitoral 0369 e seção eleitoral 0050 de Boituva/SP, de modelo UE2010. Observe que o ID_UE está presente no campo "Common Name". Fonte: [2]

O Apêndice IV deste documento mostra o passo a passo de como instalar e utilizar um verificador de assinaturas desenvolvido pelos autores deste Relatório e disponibilizado publicamente via GitHub.[35] Esse pequeno verificador foi criado a partir de ferramentas abertas, exatamente para permitir que quaisquer pessoas, em particular aquelas com algum conhecimento técnico de computação, possam fazer essa verificação e analisar o seu conteúdo. Já adiantando o resultado que deve ser obtido: **testamos todos os arquivos de assinatura disponibilizados no *site* do TSE,[14] processo que demorou cerca de 4 horas em um computador pessoal, e nenhuma das verificações retornou erro**.

Por fim, cabe notar que, mesmo que não existissem essas assinaturas ou um programa de fácil uso para verificá-las, a validação dos logs ainda poderia ser feita acessando fisicamente as urnas em questão. Por exemplo, seria possível amostrar algumas urnas para as quais exista alguma dúvida sobre a integridade do log, e então solicitar que essa urna gere novamente os arquivos que foram enviados ao TSE. Esse procedimento, de gerar mais de uma vez os mesmos resultados, não é estranho no sistema eleitoral brasileiro: afinal, no próprio dia da eleição, isso pode ser feito para fins de contingência, ou seja, em caso de problemas no envio de resultados para o processo de totalização (e.g., a falha na leitura de uma mídia de resultados). Portanto, **novamente não se justifica a alegação de que seria impossível vincular um log a uma urna, dado que isso sempre pode ser feito acessando a urna fisicamente, em uma auditoria.**

B.2. As incorreções nos Relatórios do PL/IVL sobre este ponto

Neste ponto, deve estar claro para o leitor que:

1. Se for assumido que certo *arquivo de log* não foi modificado, há mais de um identificador dentro desse mesmo arquivo que permite ligá-lo à urna correspondente de forma confiável. Logo, o erro que faz com que um dos identificadores das urnas, o ID_UE, esteja ausente nos logs em todas as urnas modelo UE2015, UE2013, UE2011, UE2010 e UE2009 não impede a ligação de um log com a urna correspondente, nem interfere nos resultados apurados pela urna.

2. Se for assumido que o *arquivo de log pode ter sido modificado*, então a presença do ID_UE no log (nas urnas UE2020) ou sua ausência (nas urnas de outros modelos) é simplesmente irrelevante para permitir a ligação entre aquele log e a urna. O que importa nesse caso é a validade da assinatura digital produzida pela urna, usando sua chave de assinatura (única por urna eletrônica).

Lendo os Relatórios do PL/IVL, não fica claro se os seus autores assumem ou não a integridade dos logs quando tentam avaliar o impacto do problema identificado nas urnas anteriores à UE2020. Entretanto, independentemente da hipótese adotada, **a conclusão de que seria possível auditar os logs de urnas UE2020 e não seria possível fazê-lo para outros modelos carece de qualquer fundamentação técnica**. Afinal, em ambos os cenários, **a presença ou ausência do ID_UE nos logs é pouco ou nada relevante na prática**. Na realidade, esse código provavelmente teria

maior relevância se fosse o único identificador presente nos logs, ou se essa fosse a única informação assinada digitalmente pelas urnas eletrônicas. Porém, nenhuma dessas condições se verifica no sistema eleitoral brasileiro.

Isso posto, parece que o principal argumento técnico dado pelos Relatórios do PL/IVL para uma alegada importância do ID_UE nos logs vai no sentido do que é afirmado no Relatório do PL/IVL-3:

> "*O código de identificação da urna eletrônica, lido diretamente do hardware do equipamento, e exibido no registro de cada atividade, em cada linha do LOG, é essencial 'para vincular cada atividade à urna física (hardware) que realizou a atividade, e, assim, validar o registro em cada linha do LOG, para fins de auditoria de funcionamento da urna eletrônica"* (grifo nosso).

Portanto, cabe esclarecer os erros dos dois principais argumentos nessa frase:

- Leitura direta do hardware: à primeira vista, pode parecer que um identificador extraído de um hardware é mais "forte" do que um identificador inserido por humanos (como zona e seção) ou gerado pelo software da urna (como o código de carga da urna). Afinal, até mesmo no presente relatório fizemos questão de reforçar a importância de se proteger a chave privada da urna por meio de hardware dedicado, uma vez que o vazamento dessa chave permitiria gerar assinaturas digitais válidas para dados falsos (não apenas log, mas também Boletim de Urna e RDV!). Porém, existe uma diferença fundamental entre o ID_UE e a chave privada da urna eletrônica: o ID_UE, após ser lido do hardware, é registrado às claras no log, fora do ambiente protegido pelo módulo de segurança da urna, algo que não acontece com a chave privada. Portanto, após o ID_UE ser escrito no log, é muito simples modificar seu valor ou copiá-lo para outro arquivo, bastando para isso usar um editor de texto. Já a chave privada é usada para gerar dados dela derivados: a assinatura digital, que é única por arquivo assinado e prova que aquele arquivo foi de fato gerado pelo hardware da urna. Talvez esse ponto (que definitivamente não é um mero detalhe) fique mais fácil de ser compreendido ao se comparar duas tecnologias de cartão de crédito: aquelas que usam apenas tarja magnética e aquelas dotadas de cartões inteligentes (o "chip" ou "smart card"). Nos cartões do primeiro tipo, mais antigos, as informações de identificação única do cartão de crédito ficavam todas na tarja magnética. Uma vez lida essa informação, nada impedia o leitor de copiá-las para outro cartão, criando um "clone" idêntico ao original: afinal, as informações até então protegidas pela tarja magnética são registradas às claras fora daquele ambiente, podendo ser copiadas e até mesmo alteradas facilmente (embora a alteração provavelmente não seria o objetivo de uma clonagem). Por outro lado, o risco de clonagem desse tipo é muito mais baixo nos cartões com chip, mais modernos, que usam assinaturas digitais durante a sua operação (para detalhes técnicos sobre a operação e segurança desses cartões, sugere-se a leitura da especificação).[17] A razão é exatamente que os smart cards protegem a chave de assinatura utilizada, prevenindo sua leitura por atacantes: a única coisa que sai do smart card são informações derivadas das chaves por ele protegidas. Obviamente, isso não impede a "clonagem" do número do cartão usado para compras na Internet (exatamente porque esse número, gravado no "hardware" do cartão, é apresentado às claras durante a compra!). Porém, a clonagem em compras físicas, realizada simplesmente por uma leitora do cartão, é tida como inviável (vide, por exemplo, a discussão da Febraban sobre esse

ponto).[18] Como os requisitos de segurança entre urnas eletrônicas e cartões de crédito são bem diferentes, não é cabível qualquer comparação direta entre eles. Todavia, essa comparação ilustra a baixa relevância do ID_UE ser "lido diretamente do hardware". Além disso, ela mostra a alta relevância das assinaturas digitais realizadas com a chave de assinatura das urnas, contrariamente ao que afirmam os Relatórios do PL/IVL.

- Registro em cada linha do log: em uma análise superficial, pode-se dizer que o registro do ID_UE em cada linha do log de alguma forma traz mais confiança às suas linhas individuais. Esse argumento, entretanto, não faz qualquer sentido. Afinal, com um simples editor de texto seria possível substituir todas as ocorrências de ID_UE com esforço mínimo: bastaria usar o comando de substituição (Ctrl+H, no caso do Notepad++) no log de uma urna para substituir um valor qualquer por outro no documento inteiro. Isso permite substituir o ID_UE, o identificador de carga, a zona e a seção etc., com essencialmente o mesmo esforço. Portanto, conforme discutido no início desta seção: no cenário em que se considera que o log possa ter sido alterado, apenas a assinatura digital pode ser considerada um identificador confiável; no cenário em que não se considera a hipótese de o log ter sido alterado, qualquer identificador único da urna, seja ele repetido ou não nas linhas do log, tem relevância similar.

Esses exemplos ilustram a **carência de rigor técnico nas colocações feitas pelos Relatórios do PL/IVL ao tentar dar uma importância indevida ao ID_UE**. Obviamente, isso não significa que o erro identificado naqueles documentos deva ser ignorado. Pelo contrário: ele deve ser corrigido, até mesmo para facilitar a leitura dos arquivos de log e a sua correlação com outros produtos da urna. O que deve ficar claro das colocações aqui apresentadas é que, ao contrário do que alegam esses relatórios, **o erro relativo à escrita do ID_UE nos logs das urnas anteriores à UE2020 não impede em momento algum que seja feita a correlação entre log e os resultados da urna correspondente**.

B.3. As reais causas do erro observado: conclusões após análise do código fonte da urna

Um dos argumentos que têm sido usados para tentar conferir maior impacto ao problema observado nos Relatórios do PL/IVL é que a constatação de que houve um erro de programação no *software* da urna eletrônica pode significar a existência de outros erros. Embora essa afirmação não esteja incorreta, ela ignora um fato: **todo e qualquer software minimamente complexo tem falhas** (ou *bugs*, no jargão técnico). Logo, **a mera existência de uma falha não significa que o sistema todo (ou seus resultados) devem ser simplesmente descartados**, pois fazê-lo equivaleria a dizer que um pequeno risco na porta de um carro pode ser considerado razão suficiente para enquadrá-lo em um caso de "perda total" do veículo. Em outras palavras, **o que importa não é a existência de um erro em um sistema, mas sim seus reais efeitos.** A menos que esses efeitos sejam graves, não há motivos para descartar o sistema como um todo ou os resultados por ele produzidos.

Como demonstrado ao longo desta seção, entretanto, não se observa *a priori* qualquer razão para se dizer que o erro na escrita do ID_UE nos logs das urnas seja de fato capaz de invalidar o resultado produzido pelas urnas afetadas. Afinal, o erro sequer im-

possibilita a ligação entre o log da urna e os outros documentos por ela produzidos, argumento principal dos Relatórios do PL/IVL.

A despeito disso, ainda assim é razoável que se considere relevante verificar mais a fundo a causa da falha em questão, para então entender as suas reais consequências. Exatamente por isso, nesta seção explica-se o que aconteceu no *software* da urna que levou ao problema observado no ID_UE das urnas de modelos anteriores à UE2020. Como a USP, entre outras Instituições de Ensino Superior, tem uma cópia do código-fonte das urnas eletrônicas, isso pode ser feito de forma independente do TSE, nas dependências do LARC. Por outro lado, como esse código ainda não foi colocado em domínio público, a discussão não mostra os detalhes do erro, mas uma abstração capaz de explicar o problema ocorrido.

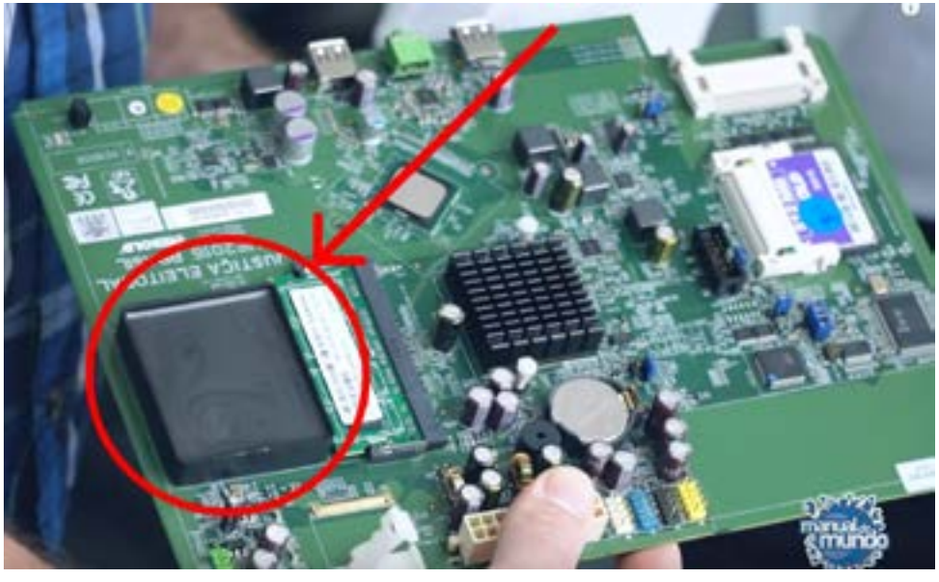


Figura B3. Foto da placa-mãe de uma urna 2015, representante do conjunto Urnas Pré-modelo 2020, com foco na região em que se situa o hardware de segurança dedicado. Fonte: imagem extraída e adaptada do vídeo "Como Funciona a Urna Eletrônica"[19]

Para compreender a causa do problema, é útil explicar primeiramente as diferenças existentes nas formas como cada versão de urna obtém o valor do ID_UE para então escrevê-lo no log. A seguir, identificam-se conjuntos de versões de urnas por similaridades na forma como elas obtêm o seu ID:

- Urnas pré-UE2009: Reúne as urnas de modelo anterior à urna de modelo UE2009. A característica em comum entre elas é o fato de obterem o ID_UE a partir de uma posição fixa da memória. Nenhuma urna desta categoria foi utilizada nas eleições de 2022.
- Urnas pós-UE2009/pré-UE2020: Reúne as urnas modelo UE2009, UE2010, UE2011, UE2013 e UE2015. Estas urnas já possuem o hardware de segurança dedicado (vide Figura B3) e foram usadas no passado em pleitos que envolviam urnas pré-modelo UE2009.
- Urna UE2020: Apenas um modelo de urna pertence a esta categoria, a UE2020. Também possui um hardware de segurança dedicado e foi introduzida nas eleições de 2022.

Apesar de nenhuma urna da categoria *pré-UE2009* ter sido utilizada nestas eleições, é importante explicar o seu modo de obtenção do ID_UE para facilitar o entendimento do erro observado nos logs. Como não havia um *hardware* de segurança dedicado nessa categoria de urna, o que se fazia para obter tal informação era armazenar o ID_UE em uma posição fixa da memória. Quando o sistema da urna quisesse ter acesso a essa informação para, por exemplo, inseri-la no arquivo de log, fazia-se uma leitura dessa posição fixa da memória.

A partir do momento em que as urnas passaram a contar com um *hardware* de segurança dedicado, surge a categoria das urnas pós-UE2009/pré-UE2020. A informação do ID_UE passou a ser armazenada no interior do *hardware* de segurança como um número de série. Para acessar recursos e acionar as funcionalidades deste *hardware* de segurança, o sistema operacional da urna envia comandos específicos e recebe respostas de forma muito semelhante a como um sistema operacional obtém informações de seus periféricos, como um mouse ou um teclado.

Para a urna de modelo UE2020, o mecanismo de obtenção do ID_UE é idêntico ao das urnas *pós-UE2009/pré-UE2020*.

Figura B4. Diagrama ilustrando como cada uma das famílias de modelo de urna apresentadas deveria operar para obter o ID_UE corretamente. Fonte: autoria própria

A USP, em função do convênio com o TSE, tem recebido diversas versões do código-fonte. Uma das versões recebidas corresponde a uma versão anterior ao início das suas adaptações para lidar com as urnas UE2020. Ao analisar esta versão do código, verificou-se que as urnas *pós-UE2009/pré-UE2020* requisitavam corretamente a informação de ID do *hardware* de segurança. Em compensação, ao analisar a versão mais recente do código-fonte recebido (Onça Pintada, usada nas eleições de 2022), verificou-se que o programa de gravação de log (denominado *logd*) dessas urnas não mais obtinha o ID_UE da forma correta, mas acessava uma posição fixa de memória, tal como era feito nas urnas *pré-UE2009*. Dessa forma, foi possível identificar a causa do problema: como não se grava mais o ID_UE das urnas nesta posição fixa de memória desde as urnas *pré-UE2009*, a informação obtida pelo *logd* ao ler essa posição de memória produziu um valor arbitrário, que no caso coincide com o número 0x04030201 (67305985). Quando foi verificada a forma como o *logd* trata a obtenção do ID_UE das urnas modelo UE2020, percebeu-se que ele o faz da forma correta, enviando requisições ao *hardware* de segurança. Esse ponto é ilustrado nas Figuras B4 e B5.

Figura B5. Diagrama ilustrando como o erro do software faz cada família de modelos de urnas funcionar. O erro no ID_UE mostrado nos arquivos de log ocorre porque as urnas pós-UE2009/pré-UE2020 utilizam um método obsoleto para obter esse identificador, em vez de requisitar esta informação do hardware de segurança dedicado.
Fonte: autoria própria

Cabe enfatizar que esse erro não é evidência de que haveria dois códigos-fontes nas urnas utilizadas nas eleições de 2022. Afinal, **o mesmo código-fonte** testa em que tipo de urna ele está sendo executado e age segundo o modelo de urna em questão. Além disso, **o mesmo erro não foi observado em outros programas que compõem o ecossistema da urna**, como, por exemplo, aqueles responsáveis pela escrita do BU e RDV, como já observado experimentalmente ao final da Seção A. No entanto, esse problema revela ao menos duas outras implicações:

- A base de código evoluiu de uma versão funcional para outra envolvendo uma estratégia obsoleta para obtenção do ID_UE, fazendo com que as urnas *pós-UE2009/pré-UE2020* deixassem de obter esse valor de forma correta na porção do código que lida com o log. Ou seja, como a versão anterior desse mesmo código realizava esta função corretamente, houve uma falha no processo de revisão de código do TSE. Cabe, portanto, a recomendação de que o TSE reforce seus processos internos de revisão e testes de código. Em particular, embora o código atual já inclua diversos testes automatizados, cabe um esforço para expandir essa base, considerando como escopo tanto os arquivos de log (onde houve a falha) como o restante do código (para se precaver de eventuais falhas futuras).

- O fato de o levantamento feito nos Relatórios do PL/IVL ter apontado que todas as urnas *pós-UE2009/pré-UE2020* apresentaram o mesmo erro revela que nenhuma delas conseguiu obter um ID escrito em uma posição de memória fixa tal como as urnas *pré-UE2009* faziam. Isso é um indicativo de que, como seria esperado, não foram utilizadas indevidamente urnas de modelos desprovidos de módulo de segurança (i.e., pré-UE2009) nas eleições de 2022.

C. Miscelânea

Nesta seção, são incluídas algumas discussões com o objetivo de clarificar, discutir ou refutar algumas das afirmações encontradas nos Relatórios do PL/IVL. Os pontos aqui apresentados não cobrem a totalidade de argumentos problemáticos ali observados, mas concentram-se em alguns itens considerados particularmente relevantes.

C.1. Log e outros elementos de auditoria da urna eletrônica

No Relatório do PL/IVL-3, ao analisar a afirmação

> "*A urna só assina o seu log e a assinatura é suficiente para garantir com segurança criptográfica que o log veio daquela urna de fato*",

publicada em reportagem da *Folha de S. Paulo*, alega-se que

> "*A afirmação na matéria está errada, porque o LOG é o* único instrumento reconhecido*, na documentação fornecida pelo TSE, como elemento essencial para auditoria de funcionamento da urna eletrônica, pelos partidos políticos e entidades fiscalizadoras*" (grifo nosso).

O Relatório do PL/IVL-3 não deixa clara qual seria a referida "documentação fornecida pelo TSE", então é difícil saber a fonte para essa alegação. Entretanto, ela não parece condizente com a realidade, uma vez que diversas documentações oficiais do TSE costumam mencionar "assinaturas digitais" como um mecanismo importante para que se possa realizar a auditoria do processo eleitoral (a título de exemplo, vide orientações de auditoria do TSE).[20] Além disso, como demonstrado e discutido na Seção B do presente documento, as assinaturas digitais feitas sobre os resultados produzidos pelas urnas, incluindo logs, são sim um elemento extremamente importante para auditoria de funcionamento das urnas eletrônicas: sem essas assinaturas, o próprio log perderia seu valor!

Enquanto seria perfeitamente razoável afirmar que o processo eleitoral brasileiro poderia incluir ainda mais mecanismos para permitir a auditoria completa dos seus resultados, é inadequado afirmar que as assinaturas digitais dos dados produzidos não têm relevância para fins de auditoria – tal afirmação carece de qualquer fundamentação técnica.

C.2. Alegações de violação de sigilo nos logs

No relatório PL/IVL-2, existem diversas afirmações que usam a expressão

> "*violação do sigilo do ato de votar*".

Essas afirmações são exemplificadas com linhas de log como as mostradas na Listagem C1 a seguir (correspondente ao Município de Guaíra/PR, Zona 0090 Seção 0088).

```
02/10/2022 11:11:22 INFO 67305985 VOTA Voto confirmado para [Deputado Estadual]   BB8551D74BE-3CAEC
02/10/2022 11:11:30 INFO 67305985 VOTA Tecla indevida pressionada 0A7FF01CF406245C
02/10/2022 11:11:42 INFO 67305985 VOTA Voto confirmado para [Senador] 4F07F392DFC87582
02/10/2022 11:11:51 ERRO 67305985 VOTA N3api17CMessageExceptionE - (Código (12)) CMessageException - CScreenMT::Write - erro na escrita de texto 12: 0 (1,2) [NOME_SUPRIMIDO_NESTE_EXEMPLO] 6E9C2420274AAD30
02/10/2022 11:17:10 INFO 67305985 INITJE Urna desligada pela chave          7EB98A5A42921948
02/10/2022 11:17:18 INFO 67305985 LOGD Fechando o arquivo de Log           B06D60198EFF1C85
02/10/2022 11:19:06 INFO 67305985 LOGD Início das operações do logd        CFC1CCD5D33B4EEC
02/10/2022 11:19:06 INFO 67305985 LOGD Urna ligada em 02/10/2022 às 11:18:19   D56AD-F7BB4EE0133
```

Listagem C1. Trecho de arquivo de log da urna usada no município de Guaíra/PR, zona 0090 seção: 0088.
Fonte: adaptado de [2]

O que é possível observar é que o log contém de fato um dado pessoal (nome do eleitor, aqui substituído por "NOME_SUPRIMIDO_NESTE_EXEMPLO" por não se observar

qualquer benefício em listá-lo aqui explicitamente). Conforme pode-se depreender da leitura do log, esse nome é mostrado após uma falha no *software* da urna que força o mesário a realizar o seu desligamento manualmente. Porém, não é possível observar, em lugar algum, quaisquer informações que poderiam levar a inferir qual seria o voto do eleitor. Em outras palavras, o que é possível descobrir com isso é a informação temporal de quando o voto estava sendo realizado pelo eleitor, e nada mais do que isso. Em particular, não é possível, de forma alguma, identificar *em quem* o eleitor votou, ou mesmo se ele anulou o voto – apenas sabe-se que ele votou e em qual horário. Curiosamente, essa informação não é muito diferente daquela obtida ao acompanhar ao vivo o momento em que algumas pessoas famosas votam, situação rotineiramente capturada por emissoras de rádio e televisão, sem qualquer alarde.

A propósito, essa questão sobre nomes no log é igualmente irrelevante para o sigilo do voto se a urna eletrônica tiver de alguma forma "congelado" em razão do erro, mantendo o voto do eleitor na tela em vez de exibir uma mensagem de erro. Nesse cenário, o que se poderia esperar é que o mesário desligasse a urna pela parte traseira (exposta pela cabina de votação, conforme mostra a Figura C1), sem acessar a tela em si, de modo a preservar o sigilo do voto ali mostrado.[36] Porém, caso o mesário acessasse a tela por algum motivo, ele seria capaz de vincular o voto ali visualizado ao eleitor correspondente pelo simples fato de ter recebido o documento de identificação desse eleitor logo antes de habilitá-lo a votar (ou seja, sem acessar qualquer arquivo de log!). Portanto, misturar essa questão procedimental, de como tratar corretamente um eventual travamento de tela, com a existência de nomes nos logs, também não teria qualquer cabimento.

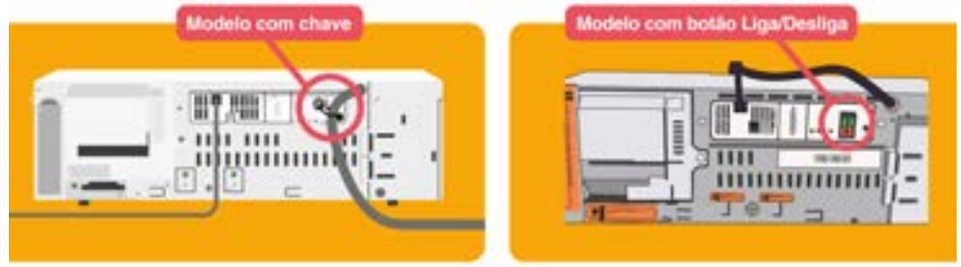


Figura C1. Imagem traseira dos modelos de urnas eletrônicas usadas nas Eleições de 2022, com destaque para os mecanismos de desligamento das urnas (expostos na parte traseira da urna, que fica exposta para o mesário).
Fonte: [36]

Isso posto, não fica clara a razão pela qual os Relatórios do PL/IVL discutem esse caso como de alta relevância. **Esse ponto seria relevante apenas se o sigilo do voto, não do "ato de votar", fosse violado**. Por outro lado, como os próprios Relatórios do PL/IVL não parecem afirmar que o sigilo do voto do eleitor teria de alguma forma sido violado nessas ocasiões, cabe apenas a clarificação aqui realizada, pois aparentemente essa foi a interpretação (errônea) dada por algumas pessoas.[21]

C.3. Sobre o uso de ICP Brasil

No Relatório PL/IVL-3, é afirmado o seguinte:

> *"A assinatura digital proprietária do TSE é um instrumento interno aos seus técnicos, que não foi disponibilizado para a auditoria de funcionamento da urna eletrônica. A assinatura digital interna utilizada pelo TSE não foi realizada com um certificado digital ICP-Brasil, que é a única*

forma definida em lei, para garantir a presunção legal de veracidade de documentos eletrônicos. O TSE informou, na reunião com as entidades fiscalizadoras em 01/08/2022, que não utiliza um certificado digital da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) para a assinatura digital dos documentos eletrônicos gerados pela urna eletrônica. A instalação de um certificado digital ICP-Brasil, em cada urna eletrônica, é a única forma definida na legislação para garantir a presunção legal de veracidade dos documentos eletrônicos gerados pela urna eletrônica. Havendo evidência de que o TSE não utiliza certificados digitais ICP-Brasil nas urnas eletrônicas, não cumprindo o requisito estabelecido de presunção legal de veracidade dos documentos eletrônicos emitidos pelas urnas, ficam prejudicados os instrumentos necessários para assegurar a validade dos atos administrativos decorrentes da votação, que devem atender ao disposto no Art. 10 § 1º da Medida Provisória 2.200-2/2001. Sem a assinatura eletrônica qualificada, com um certificado digital da ICP-Brasil, os documentos gerados pela urna eletrônica, incluindo a zerésima, o Registro Digital do Voto (RDV), o Boletim de Urna (BU) e o Log de Urnas (LOG), não têm a garantia da presunção legal de que o seu conteúdo é legítimo e verdadeiro, conforme definida em lei."

O primeiro ponto a se ressaltar aqui é que **a afirmação de que "A assinatura digital proprietária do TSE é um instrumento interno aos seus técnicos" parece carecer de fundamentação técnica**. A razão é que, como discutido na Seção B do presente relatório, as assinaturas feitas pelo *hardware* da urna eletrônica usam algoritmos padronizados internacionalmente, a saber: o padrão ECDSA/P521 nas urnas mais antigas, dos modelos UE2009 até UE2015;[13, 15, 16] e o padrão EdDSA/E521 nas urnas de modelo UE2020.[16, 22] Ainda, ao analisar o certificado extraído do arquivo ".vscmr" disponível no Portal de Dados Abertos do TSE para a urna usada na Zona 0369 e Seção 0050 de Boituva/SP, o que se obtém como resultado é o mostrado na Figura C2, que revela exatamente os algoritmos esperados.[12] Cabe notar que esse certificado foi lido com um aplicativo aberto e amplamente usado para esse propósito, o OpenSSL.[23] Logo, seria incorreto chamar esses algoritmos ou certificados de soluções proprietárias do TSE.

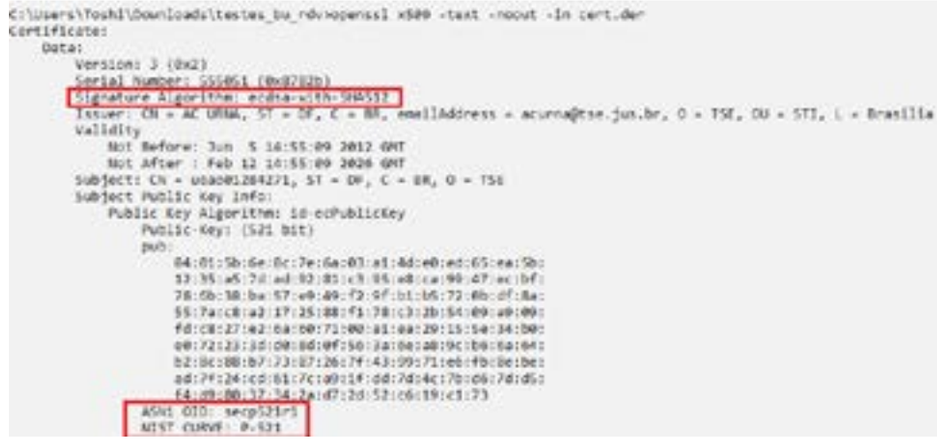


Figura C2. Trecho do certificado do hardware da urna usada na zona eleitoral 0369 e seção eleitoral 0050 de Boituva/SP. Observe o uso de algoritmos padrão para a assinatura, ECDSA/P521. Fonte: [2]

O segundo ponto, mais longamente discutido na afirmação, é de que as urnas brasileiras não usam certificados digitais ICP-Brasil. **Embora seja fato que as assinaturas feitas pelas urnas não estejam ancoradas na ICP-Brasil, do ponto de vista técnico esse fato é completamente irrelevante para garantir a confiança do processo eleitoral, ou dos resultados produzidos pelas urnas eletrônicas**.

Para compreender essa afirmação, faz-se necessário entender o que é uma Infraestrutura de Chaves Públicas (ICP) – ao leitor interessado, sugere-se o curso da UNIVESP sobre Segurança da Informação (em particular, a Videoaula 04).[24] Desde que surgiu o conceito de assinatura digital, com uso de chaves privadas de assinatura e chaves públicas de verificação, percebeu-se um desafio: como associar uma chave pública, que tem uma aparência um tanto aleatória, com a identidade de seu dono? Afinal, sem essa associação, é inviável saber se uma chave pública apresentada por alguém afirmando ser a entidade X de fato pertence a essa entidade: o risco nesse caso é que aquela chave pública pode pertencer a uma entidade Y, tentando se passar por X!

O que muitos sistemas decidiram fazer para solucionar esse problema foi criar uma espécie de "cartório digital", denominado Autoridade Certificadora (AC). Essencialmente, uma AC é responsável por emitir os chamados Certificados Digitais, documentos assinados pela AC e que contêm uma chave pública juntamente com o conjunto de informações necessárias para identificar o dono dessa chave. Uma vez verificada a assinatura da AC sobre o certificado, pode-se ter confiança no vínculo entre a chave pública e seu dono, assumindo: (1) que a chave pública da AC em si seja conhecida por quem deseja verificar o certificado por ela assinado (por exemplo, porque veio pré-carregada com o *software* de verificação); e (2) que a AC é honesta, no sentido de que não emitiria um certificado falso.

Nesse contexto, uma ICP é essencialmente uma forma pela qual as ACs comumente se organizam para poder fazer a emissão de certificados digitais de forma segura e eficiente. Para isso, estabelece-se uma cadeia de confiança em vários níveis, como ilustra a Figura C2. No nível mais elevado, existe uma AC raiz. Essa AC atua como a base de confiança do sistema e, portanto, não precisa ser certificada por outra entidade (a própria AC raiz emite seu certificado, autoassinado). Abaixo da AC raiz, existem as AC intermediárias, cujos certificados digitais são assinados pela AC raiz ou por outras AC intermediárias. Finalmente, no último nível existem os usuários finais, que possuem seus certificados digitais assinados por AC intermediárias. O certificado digital de uma entidade qualquer é, então, considerado válido se ele tiver sido corretamente assinado por todas as ACs na cadeia de autoridades entre ele e a AC raiz correspondente.

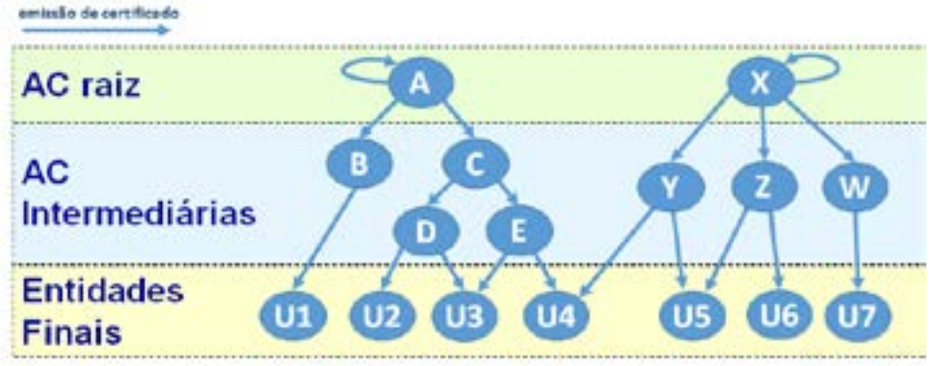


Figura C2. Visão geral da cadeia de confiança estabelecida em sistemas baseados em uma Infraestrutura de Chaves Públicas (ICP). Fonte: autores.

A decisão de organizar as ICP em múltiplos níveis é resultado do custo crescente de preservar a segurança dos certificados de AC em função do seu nível de confiança: certificados de AC raiz geralmente são mantidos em computadores sem qualquer conexão externa, com proteções físicas contra acessos não autorizados e desastres naturais. Consequentemente, o custo de ter um

certificado digital assinado por uma AC raiz é bastante superior ao custo de um certificado assinado por uma AC intermediária, que comumente permanece conectada à Internet para atender a solicitações de um grande volume de usuários. É também interessante notar que existem múltiplas AC raiz e AC intermediárias consideradas confiáveis no mundo. Uma delas, de uso razoavelmente restrito ao território nacional brasileiro, é a AC raiz da ICP-Brasil.[25]

Uma vez esclarecido o que é uma ICP, podemos discutir o caso específico do sistema eleitoral brasileiro: nele, o certificado digital de cada urna eletrônica é assinado pela AC do TSE, a qual é tratada, para fins eleitorais, como uma AC raiz. Portanto, a forma mais simples de integrar a cadeia de certificados das urnas à hierarquia da ICP-Brasil seria transformar a AC do TSE em uma AC intermediária, por exemplo, logo abaixo da AC raiz da ICP-Brasil. Dessa maneira, todos os certificados assinados pela AC do TSE também se encontrariam na cadeia de confiança da ICP-Brasil. Do ponto de vista técnico, entretanto, esse cenário não seria muito diferente do atual, dado que a AC (agora intermediária) do TSE continuaria sendo a responsável de fato pela geração de certificados das urnas. Já se a AC do TSE for substituída por uma AC que já esteja sob a égide da ICP-Brasil, chega-se ao proverbial caso de se "trocar seis por meia dúzia": afinal, ter-se-ia novamente o cenário em que deve haver uma AC que precisa se incumbir de emitir certificados digitais para as urnas eletrônicas brasileiras.

Ao mesmo tempo que a adoção de certificados ICP-Brasil no processo eleitoral não apresenta benefícios técnicos palpáveis, a discussão sobre sua necessidade parece um tanto seletiva, considerando que a quase totalidade dos *sites* e sistemas de empresas no Brasil não utiliza a ICP-Brasil como AC raiz. Como exemplo, o próprio *site* do Banco do Brasil utiliza a AC raiz USERTrust RSA Certification Authority, dos Estados Unidos (vide Figura C3), enquanto a Caixa Econômica Federal utiliza a AC raiz GlobalSign Root CA, da Bélgica (vide Figura C4). Não obstante, dados coletados e processados por esses sites e sistemas subjacentes, até onde se pode imaginar, possuem validade legal. Logo, não fica claro, ao menos do ponto de vista técnico, a razão pela qual seria necessário ou mesmo relevante o uso de certificados ICP-Brasil nas urnas eletrônicas.

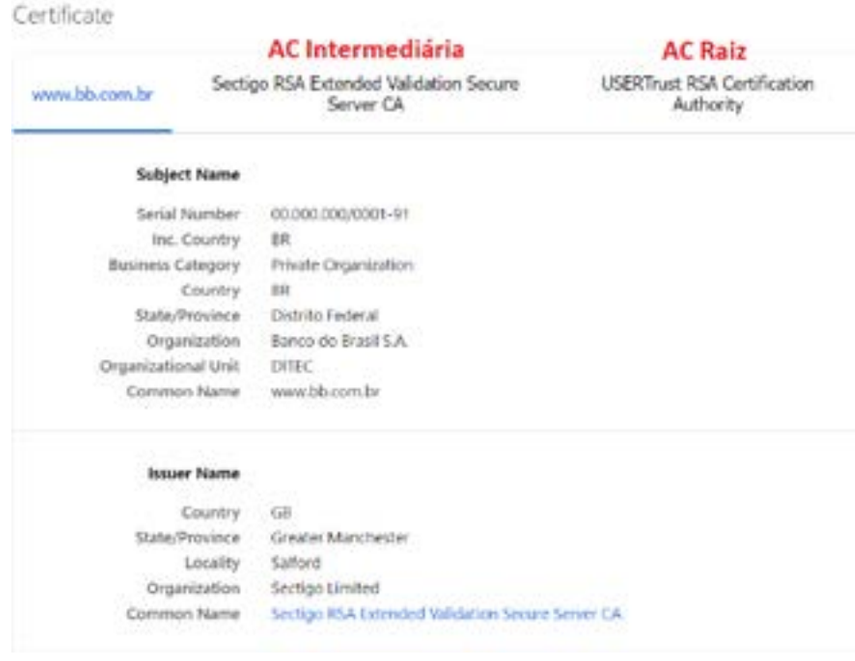


Figura C3. Certificado digital do Banco do Brasil, destacando AC intermediária e AC raiz. Fonte: [26]

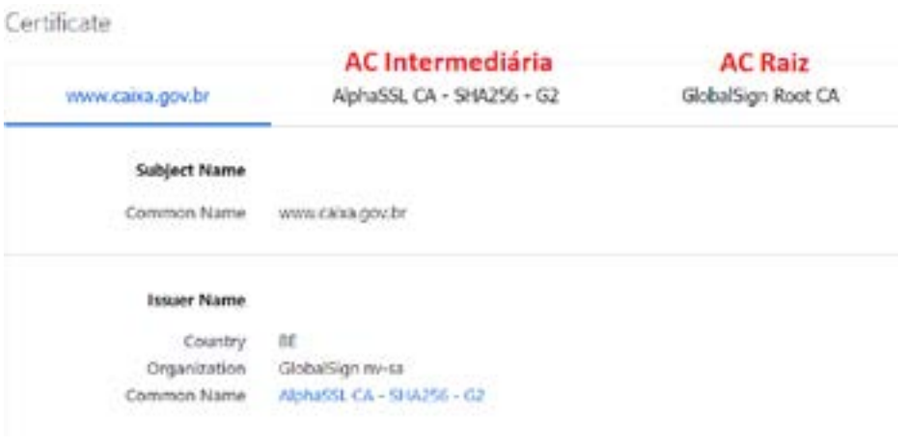


Figura C4. Certificado digital da Caixa, destacando AC intermediária e AC raiz. Fonte: [27]

Considerando todos esses aspectos, uma solução que provavelmente seria mais razoável de se propor para aumentar a confiabilidade dos certificados emitidos pelo TSE para as urnas seria a criação de um log transparente, como propõe a iniciativa conhecida como *Certificate Transparency*.[28] Essencialmente, o objetivo dessa iniciativa é dar rastreabilidade a todos os certificados digitais emitidos por uma AC, visando a uma maior garantia da correta geração desses certificados (no caso em pauta, dos certificados das urnas eletrônicas). De fato, o projeto *Certificate Transparency* foi criado pela Google com o exato objetivo de evitar a criação de certificados espúrios ou não autorizados, depois de casos como o da AC holandesa Diginotar.[29] Em um cenário eleitoral dotado de um log transparente, todo certificado de urna criado seria inserido em uma estrutura que aceita apenas a adição de elementos, e que pode ser monitorada e verificada de maneira simples por entidades diversas (e.g., Ministério Público Federal, Polícia Federal, Ordem dos Advogados do Brasil, partidos políticos, entre outras). Essas entidades podem, então, assegurar que nenhum certificado foi gerado após as eleições, ou modificado após a sua criação. Entretanto, cabe ressaltar que qualquer AC (incluindo a atualmente gerida pelo TSE) pode utilizar um sistema de logs transparentes para seus certificados – como fazem USERTrust e GlobalSign, que incluem o campo "Embedded SCTs" nos certificados por elas emitidos. Assim, novamente **soam tecnicamente incompreensíveis as afirmações de que ter as urnas eletrônicas brasileiras sob a égide da ICP-Brasil seria de alguma forma uma evolução do sistema**.

C.4. Sobre a distribuição de urnas de diferentes modelos nas eleições

No Relatório do PL/IVL-2, é afirmado que

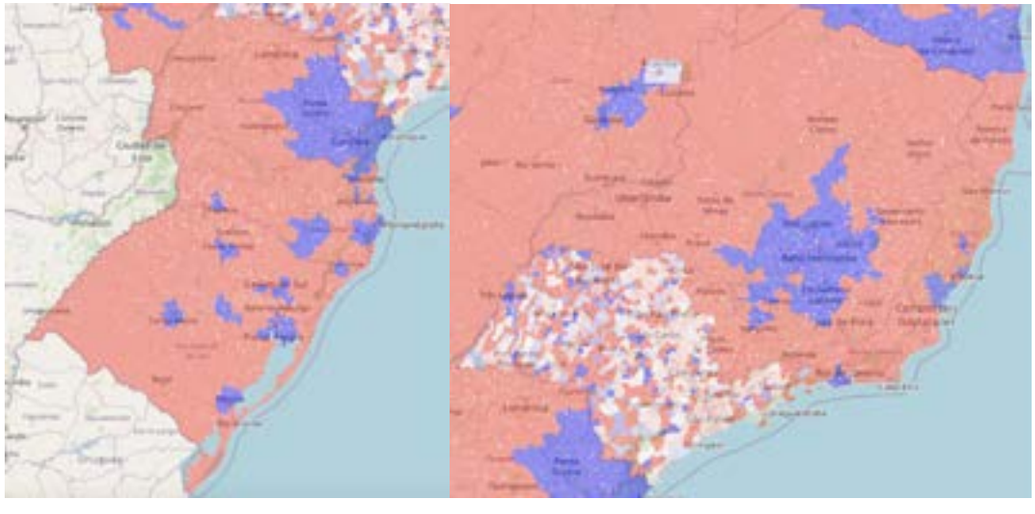
> *"Urnas eletrônicas do modelo UE2020 [teriam sido] distribuídas aparentemente de forma proporcional e equitativa pelo país pela própria Justiça Eleitoral".*

É fato que todas as Unidades da Federação receberam uma mistura de urnas UE2020 e outras dos modelos antigos. Mais especificamente, essa afirmação pode ser apurada usando dados disponíveis no Portal de Dados Abertos do TSE:[30] os próprios logs contêm os modelos de urna para cada município, zona e seção, bastando procurar neles pelo texto "Identificação do Modelo de Urna". Compilados esses dados, pode-se observar que o percentual de urnas UE2020 variou de um mínimo de 35,9% em Alagoas até um máximo de 81,3% em Roraima.

Por outro lado, dentro de cada Unidade da Federação, a distribuição das urnas não foi feita de forma proporcional e equitativa. Na maioria dos casos (as principais exceções sendo SP, DF e RR), as urnas novas ficaram concentradas próximas das capitais ou cidades de grande porte. O caso do RJ é bastante ilustrativo: entre 92 municípios, 4 deles (Rio de Janeiro, Mesquita, Nilópolis e Nova Iguaçu) usaram exclusivamente as urnas do modelo UE2020, enquanto os demais 88 municípios usaram exclusivamente as urnas de modelos anteriores. Outro caso ilustrativo é o AM, onde apenas o município de Manaus recebeu as urnas novas, do modelo UE2020.

Esse ponto é ilustrado no conjunto de imagens mostrado na Figura C5, em que é possível observar como as urnas eletrônicas ficaram distribuídas no território nacional. Nessa figura, para facilitar a visualização, é usada uma escala de cor para cada município: vermelho indica apenas urnas de modelos mais antigos, anteriores à UE2020; azul indica apenas urnas novas, do modelo UE2020; já cores intermediárias entre esses dois extremos indicam que houve uma mistura de urnas novas e antigas. Perceba que na grande maioria dos municípios não houve mistura de urnas, ou seja, as cidades receberam exclusivamente urnas UE2020 ou exclusivamente urnas dos modelos anteriores. As principais exceções são SP, DF e RR, onde se vê uma distribuição um pouco mais uniforme, embora não perfeitamente uniforme (por exemplo, há grupos de municípios vizinhos utilizando o mesmo tipo de urna).

Uma análise ainda mais detalhada da distribuição dos modelos de urnas pode ser encontrada em outras fontes públicas.[31] **Portanto, não tem sustentação a alegação de que haveria uma distribuição "proporcional e equitativa" das urnas dos modelos UE2020 e anteriores pelo País**: a própria análise dos logs das urnas, ponto focal dos Relatórios do PL/IVL, pode ser utilizada para verificar esse fato.



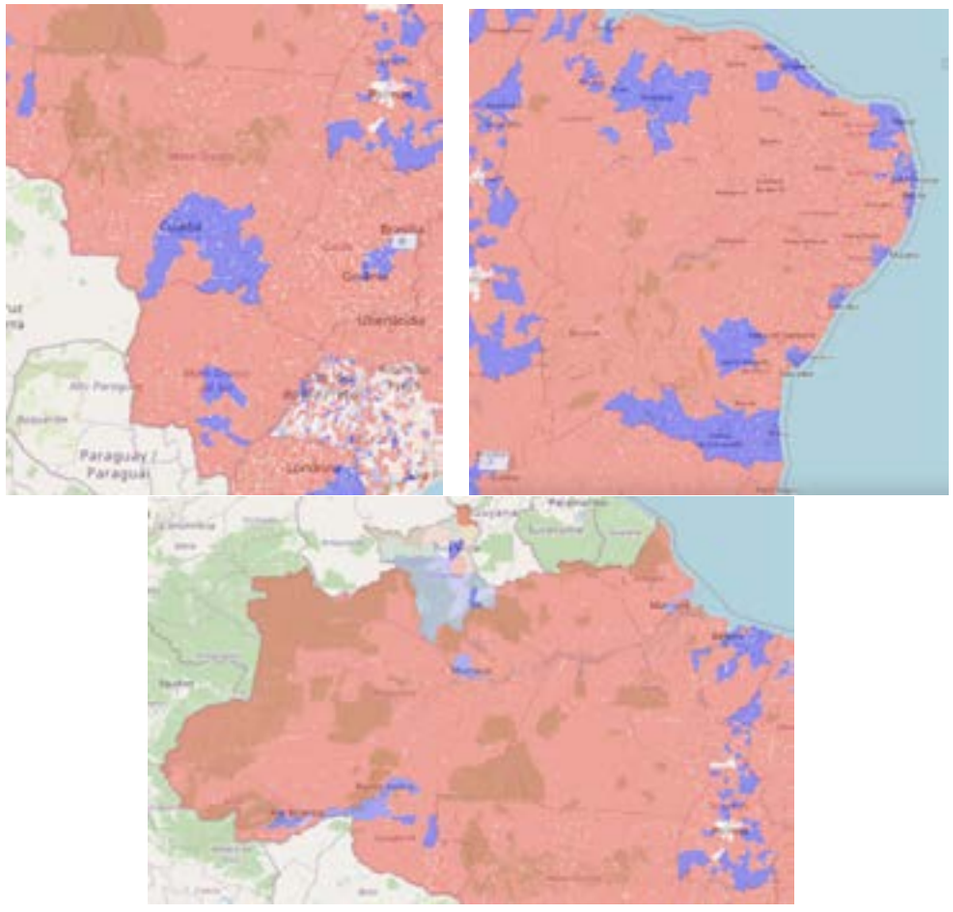


Figura C5. Distribuição de Urnas Eletrônicas no território brasileiro. É adotada uma escala de cor entre vermelho (urnas antigas, anteriores ao modelo UE2020) e AZUL (urnas novas, do modelo UE2020) para indicar a prevalência de cada modelo de urna nas cidades em questão, dependendo da proporção. Nota-se que a maioria das cidades contaram com apenas um modelo de urna, enquanto as combinação de diferentes modelos (indicada por coloração intermediária entre azul e vermelho) ocorreu principalmente em SP, DF e RR.

Conclusões

Conforme demonstrado neste documento, o principal (e talvez único) mérito dos Relatórios do PL/IVL consiste em ter trazido a público um erro que de fato foi observado nos logs de urnas utilizadas nas eleições de 2022, sem que isso tenha afetado outros arquivos (e.g., Boletim de Urna). Especificamente, esse erro de *software* levou as urnas eletrônicas dos modelos UE2015, UE2013, UE2011, UE2010 e UE2009 a gerarem logs nos quais o campo onde deveria estar o código de identificação da urna eletrônica (ID_UE) é preenchido com um número fixo, "67305985". Apesar do baixo impacto, logicamente trata-se de um problema que deve ser corrigido, e a análise do código-fonte indica que isso pode ser feito com reduzido esforço.

Por outro lado, **carecem de qualquer fundamentação técnica as inferências feitas pelos autores dos Relatórios do PL/IVL a partir da observação desse erro**, em especial a alegada impossibilidade de ligar arquivos de log de urnas dos modelos afetados aos outros documentos gerados por aquelas urnas. Contrariamente a essa afirmação, e conforme aqui demonstrado por meio de experimentos, referências e exemplos, **qualquer pessoa pode correlacionar um dado log com o Boletim de Urna correspondente, independentemente do modelo da urna e a despeito do problema observado**. Mais precisamente, assumindo-se que o log não tenha sido modificado, essa correlação pode ser feita por meio de outros identificadores presentes no próprio arquivo de log, como o código de carga da urna e as informações de município, zona e seção. Já a hipótese de modificação dos arquivos

de log pode ser descartada por meio da verificação da assinatura digital da urna sobre esse arquivo de log, tirando proveito do fato de que cada urna eletrônica tem uma chave de assinatura única, protegida por *hardware*. Dessa forma, demonstra-se aqui que o identificador mais robusto das urnas eletrônicas brasileiras não é o ID_UE, mas sim a assinatura digital feita pelo equipamento (cujo certificado correspondente também contém o ID_UE), que pode ser verificada com a ferramenta disponibilizada em Verificador de Assinaturas de Resultados das Urnas Eletrônicas,[35] ou até mesmo reproduzida com algum esforço de desenvolvimento. Todas essas observações contradizem frontalmente as principais alegações feitas nos Relatórios do PL/IVL.

Outras afirmações cuja fundamentação técnica é similarmente falha (como a necessidade de inserção dos certificados das urnas eletrônicas na ICP-Brasil), ou de teor potencialmente enganador (como o "sigilo do ato de votar", que não preserva qualquer relação com o "sigilo do voto", este último protegido por lei), foram igualmente analisadas na tentativa de esclarecer a população interessada.

De posse das informações e ferramentas aqui fornecidas, o que se espera é que mesmo leitores não técnicos possam aferir, por si próprios, essas conclusões. Afinal, acreditamos que esclarecer assuntos técnicos para a população geral é uma das contribuições que universidades públicas podem dar à sociedade brasileira. Até por essa razão, tentamos ilustrar cada ponto aqui abordado com evidências, exemplos reais e experimentos que podem ser realizados por qualquer pessoa, com maior ou menor grau de dificuldade. Por outro lado, como este é um trabalho em andamento, estamos e sempre estaremos dispostos a discutir os pontos abordados e estender as análises realizadas, além de fazer correções necessárias quando considerado cabível.

APÊNDICES AO ANEXO 2

Anexo 2 – Apêndice I

Passo a passo para realizar a "impossível" tarefa de verificar a correspondência entre logs de urnas e as urnas correspondentes. Siga o que pedem as figuras.

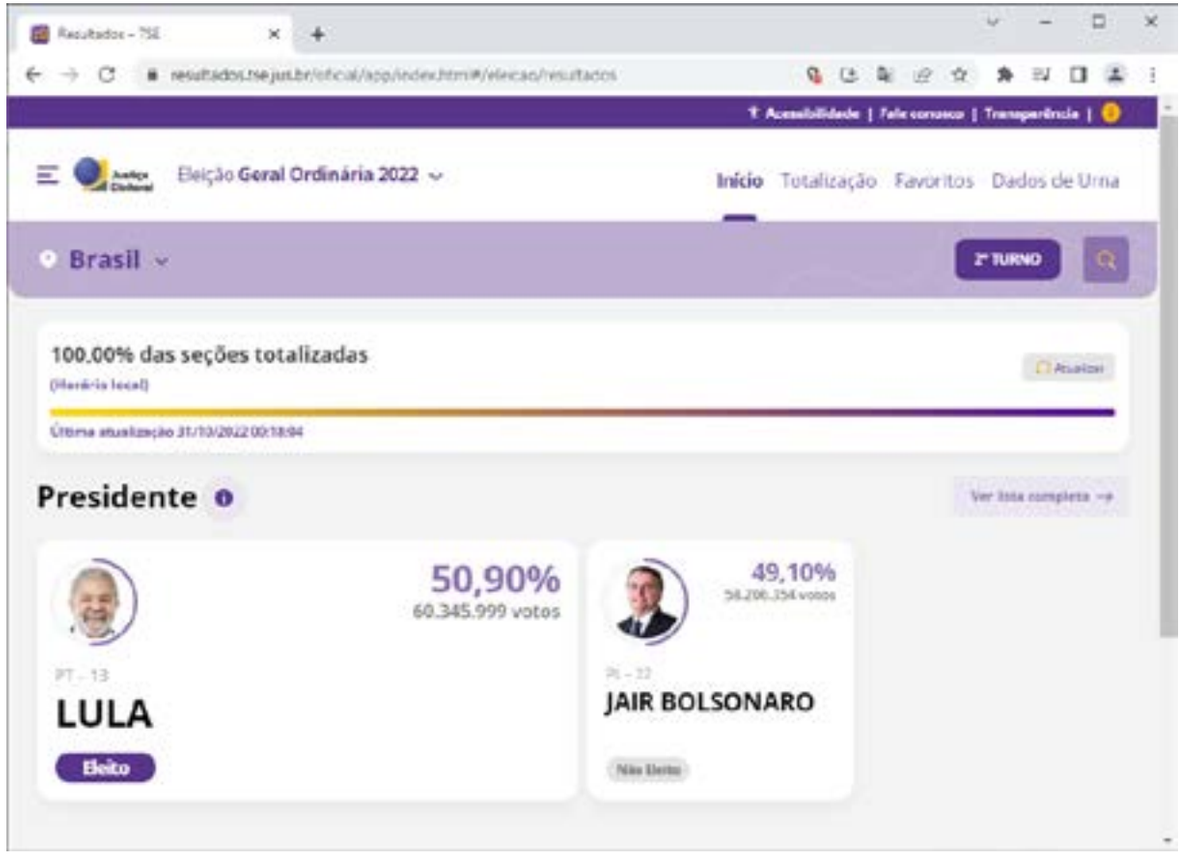


Figura ApI.1. Comece acessando [2]

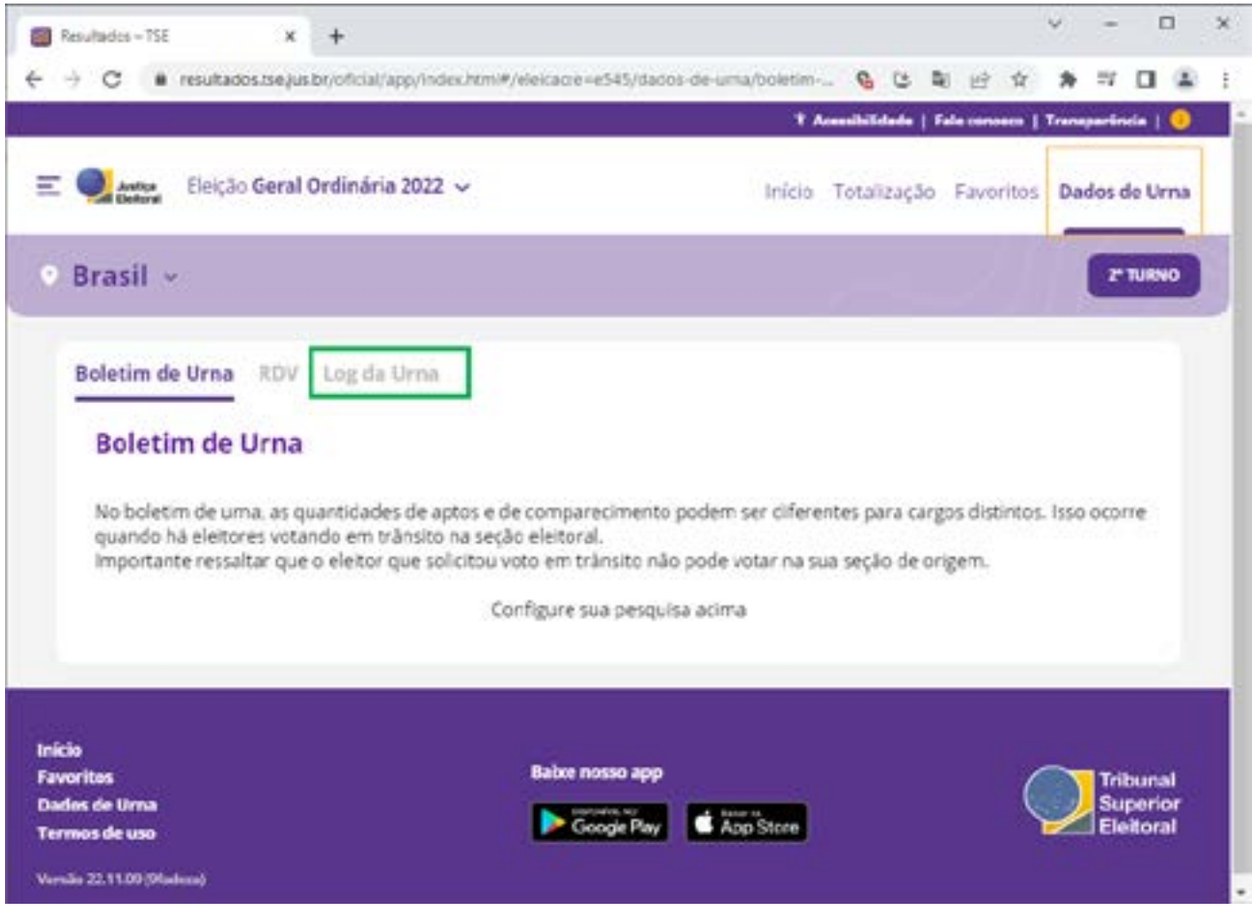


Figura ApI.2. Clique em Dados de Urna (botão no alto à direita), e em seguida em "Log da urna" (botão em destaque na figura)

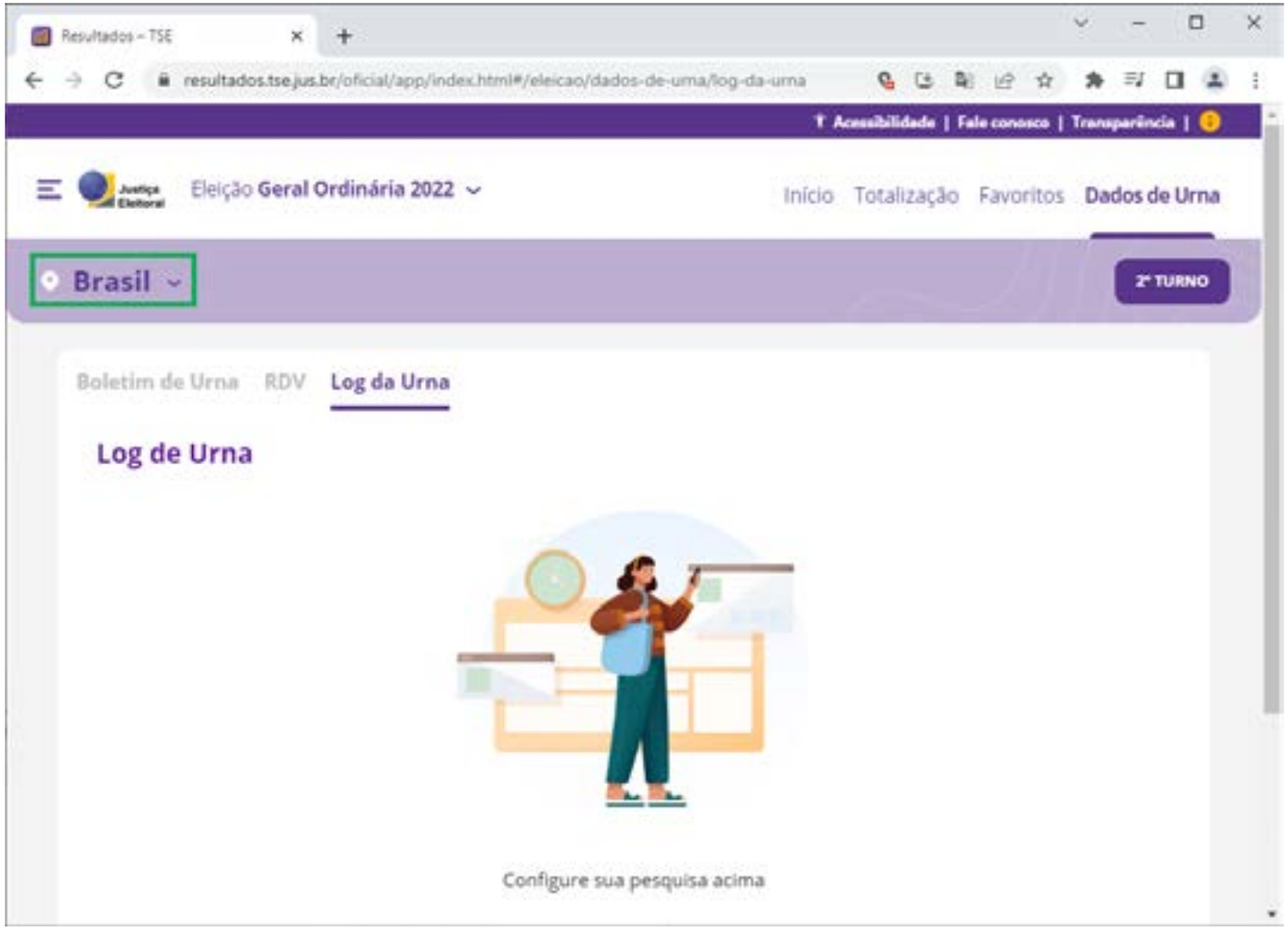


Figura ApI.3. No alto à esquerda, clique em "Brasil" para poder acessar os dados de um local específico do país

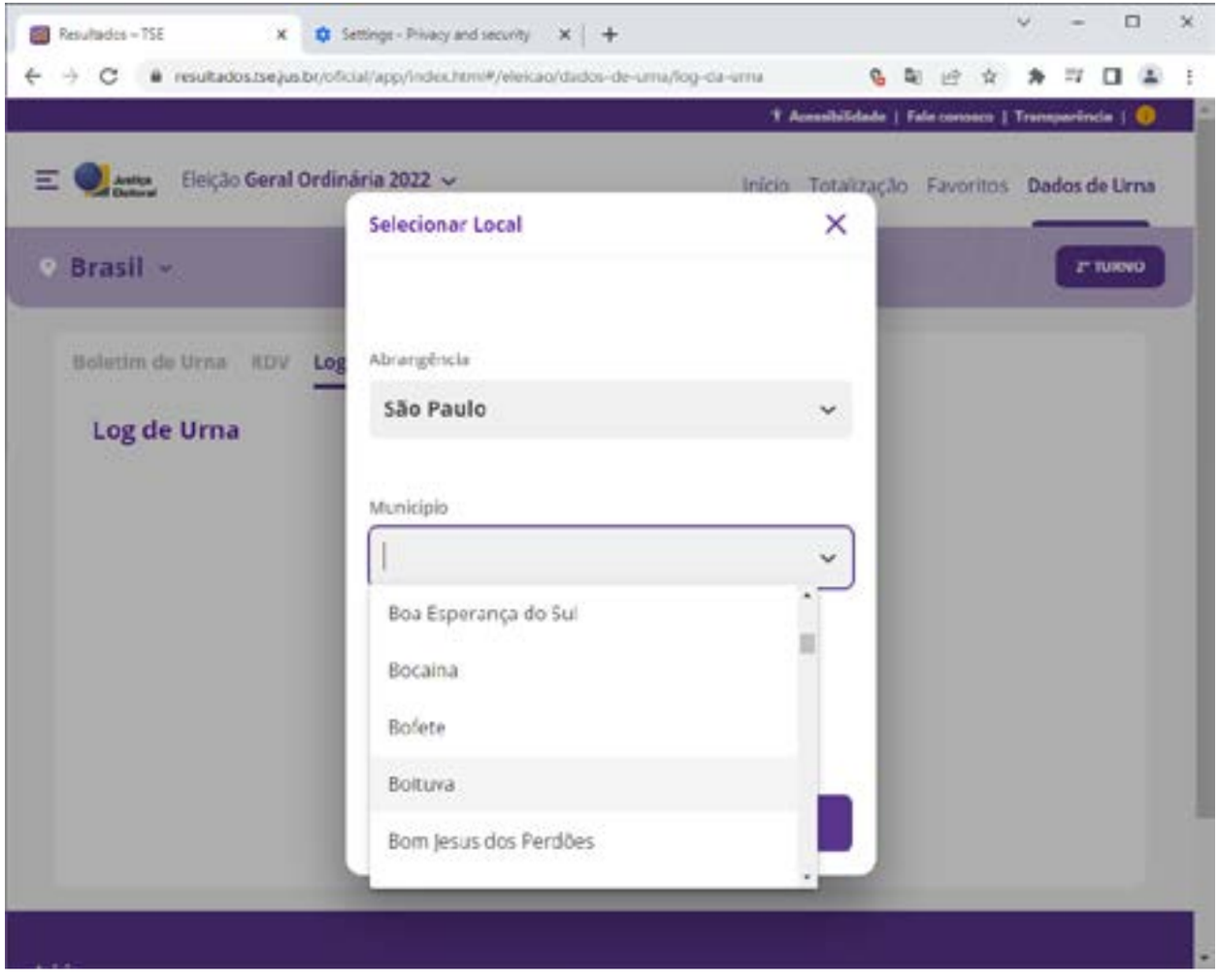


Figura ApI.4. Selecione um Estado e cidade. No exemplo da figura, é selecionada a cidade de Boituva, no Estado de São Paulo.

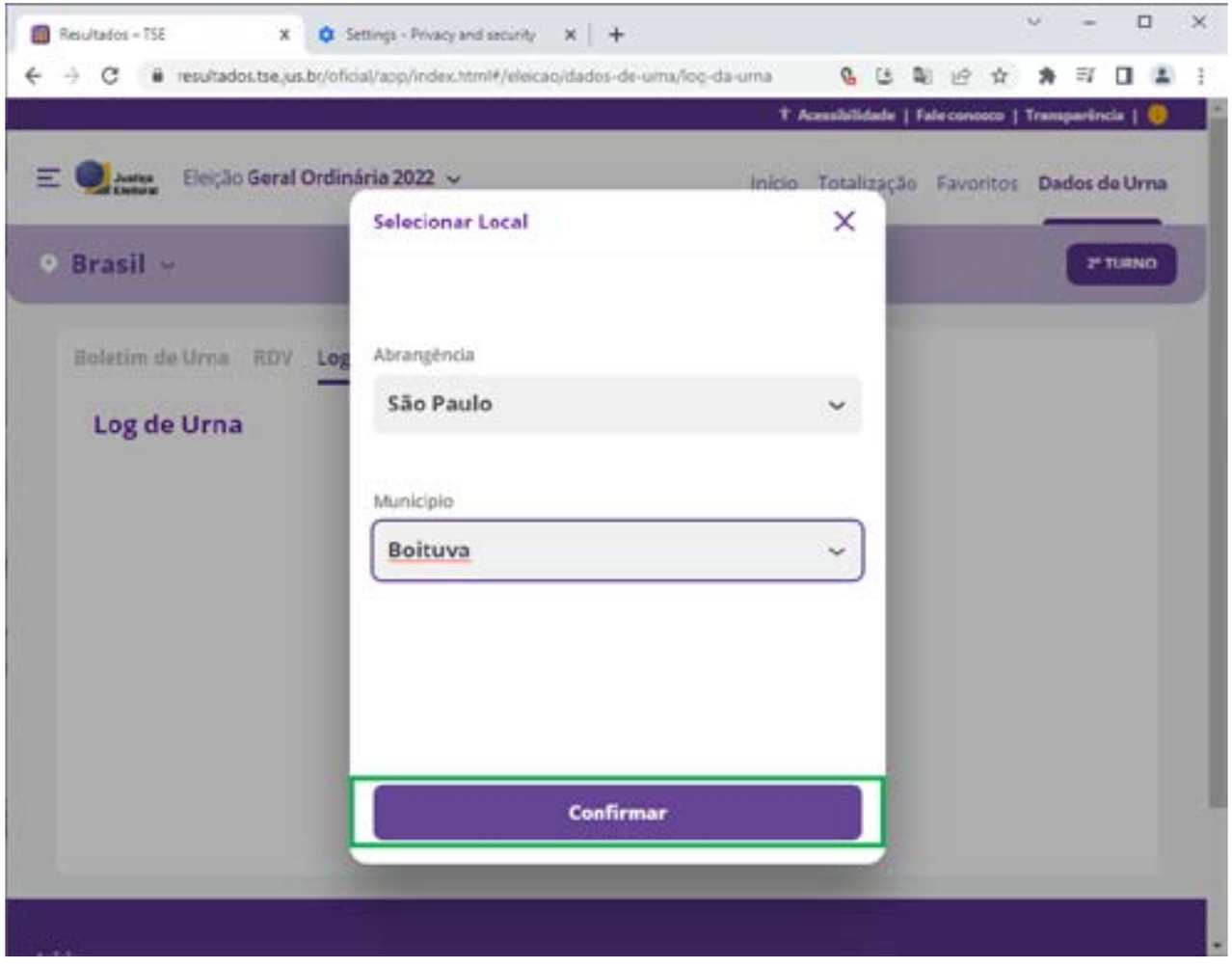


Figura ApI.5. Clique então no Botão Confirmar.

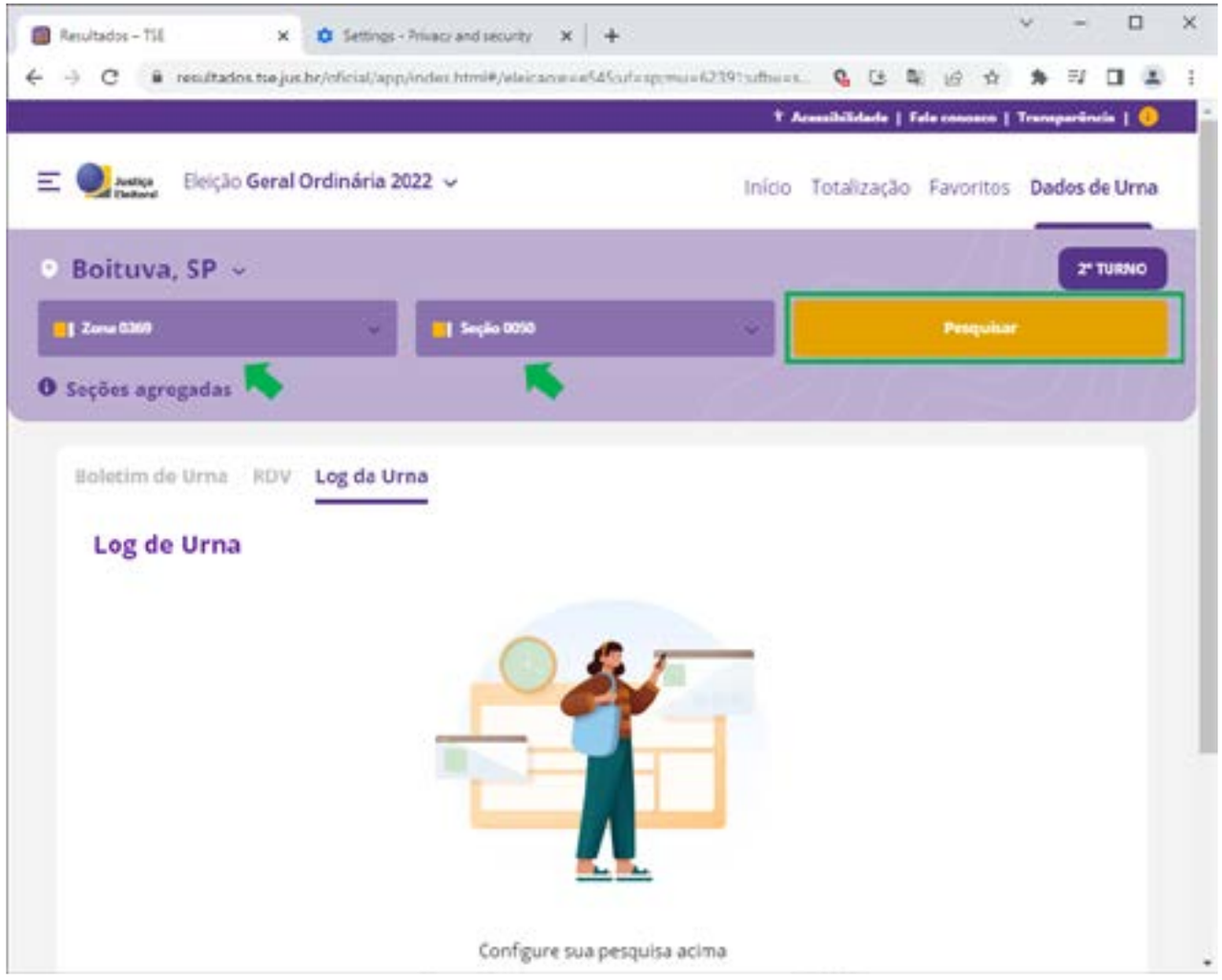


Figura ApI.6. Selecione então uma Zona e Seção. Clique então no botão Pesquisar.

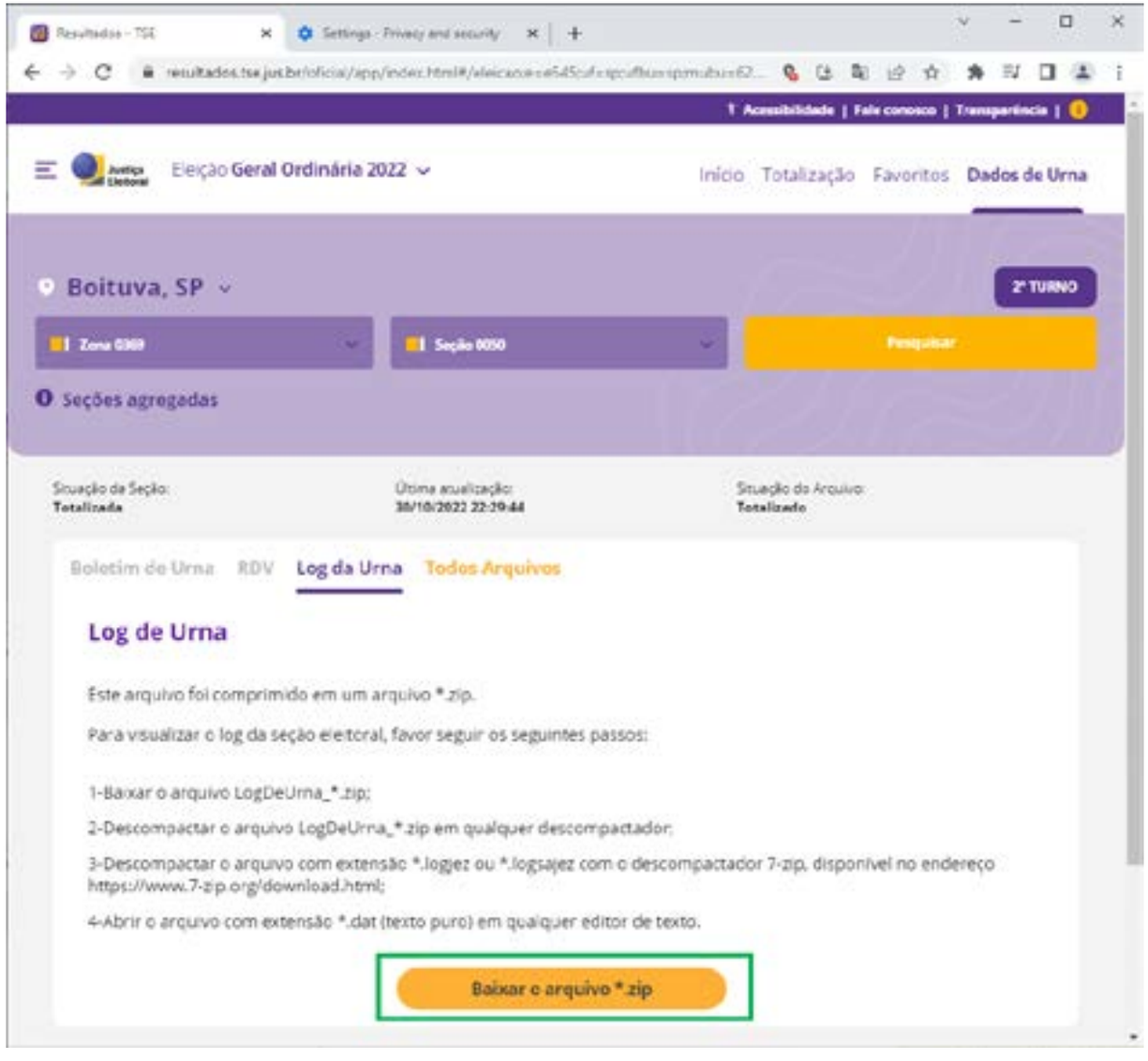


Figura ApI.7. Faça então o download do arquivo de log, comprimido no formato .zip

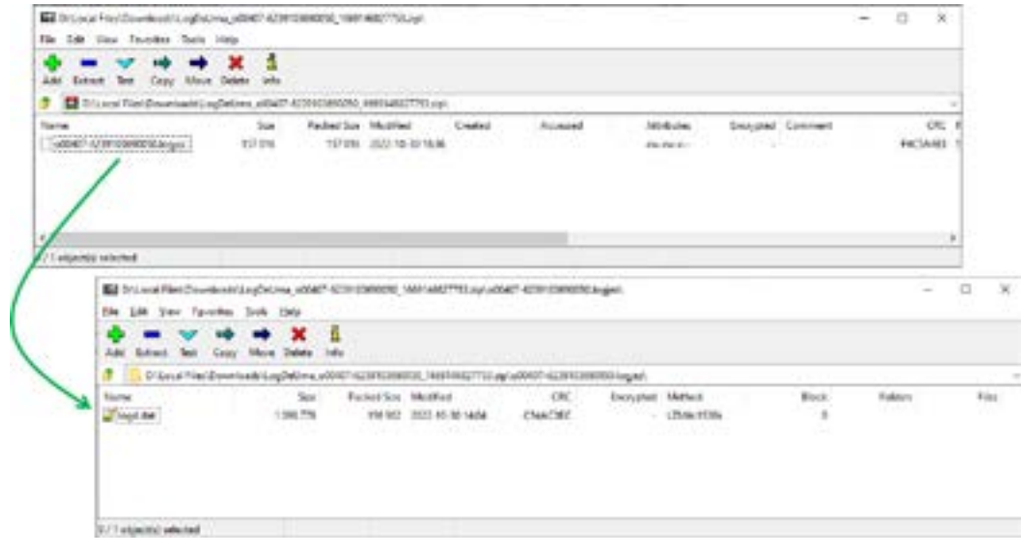


Figura ApI.8. Abra então o arquivo usando o aplicativo de descompactação de sua preferência, como o 7zip ([11]): dentro do arquivo .zip você encontrará um arquivo .logjez, que também pode ser aberto com o mesmo aplicativo de descompactação para dar acesso ao arquivo log.dat.

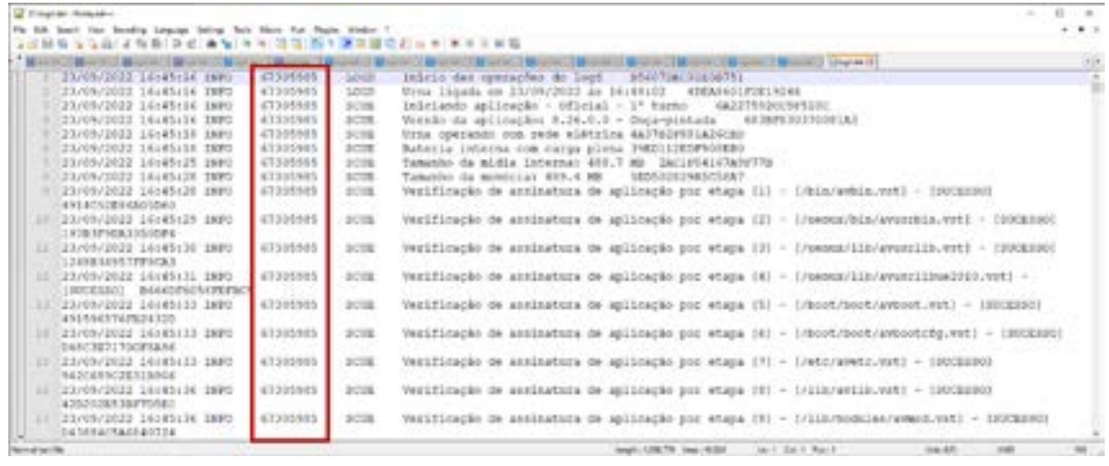


Figura ApI.9. Finalmente, use um editor de texto como o Notepad++ ([9]) para abrir o arquivo log.dat. Você verá diversas linhas no arquivo de log. Se for uma urna de modelo diferente de 2020, você verá o número "67305985" na quarta coluna do arquivo, onde deveria estar o código de identificação da urna eletrônica (UE).
Este é o problema apontado pelo Relatório do PL/IVL.

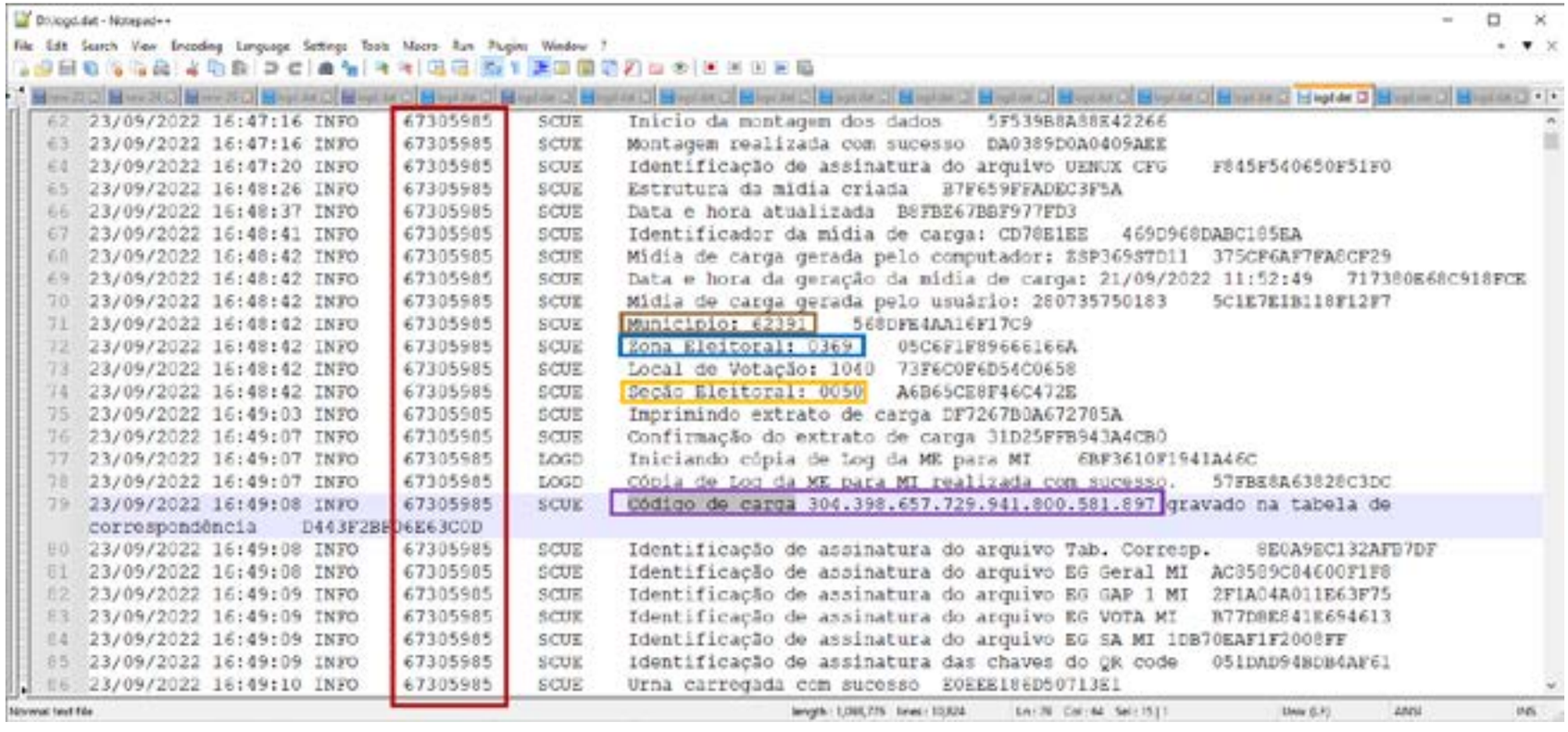


Figura ApI.10. Agora, procure dentro do arquivo (por exemplo, usando o atalho Ctrl+F) pelo texto "Código de carga". Esse é um número único relativo a cada urna e, portanto, que a identifica a despeito da ausência do identificador da UE no arquivo. Mais do que isso, logo acima do código de carga você consegue obter os identificadores do Município, Zona Eleitoral e Seção Eleitoral da Urna, outra combinação única por urna e que, portanto, pode ligá-la a seu Boletim de Urna e RDV.

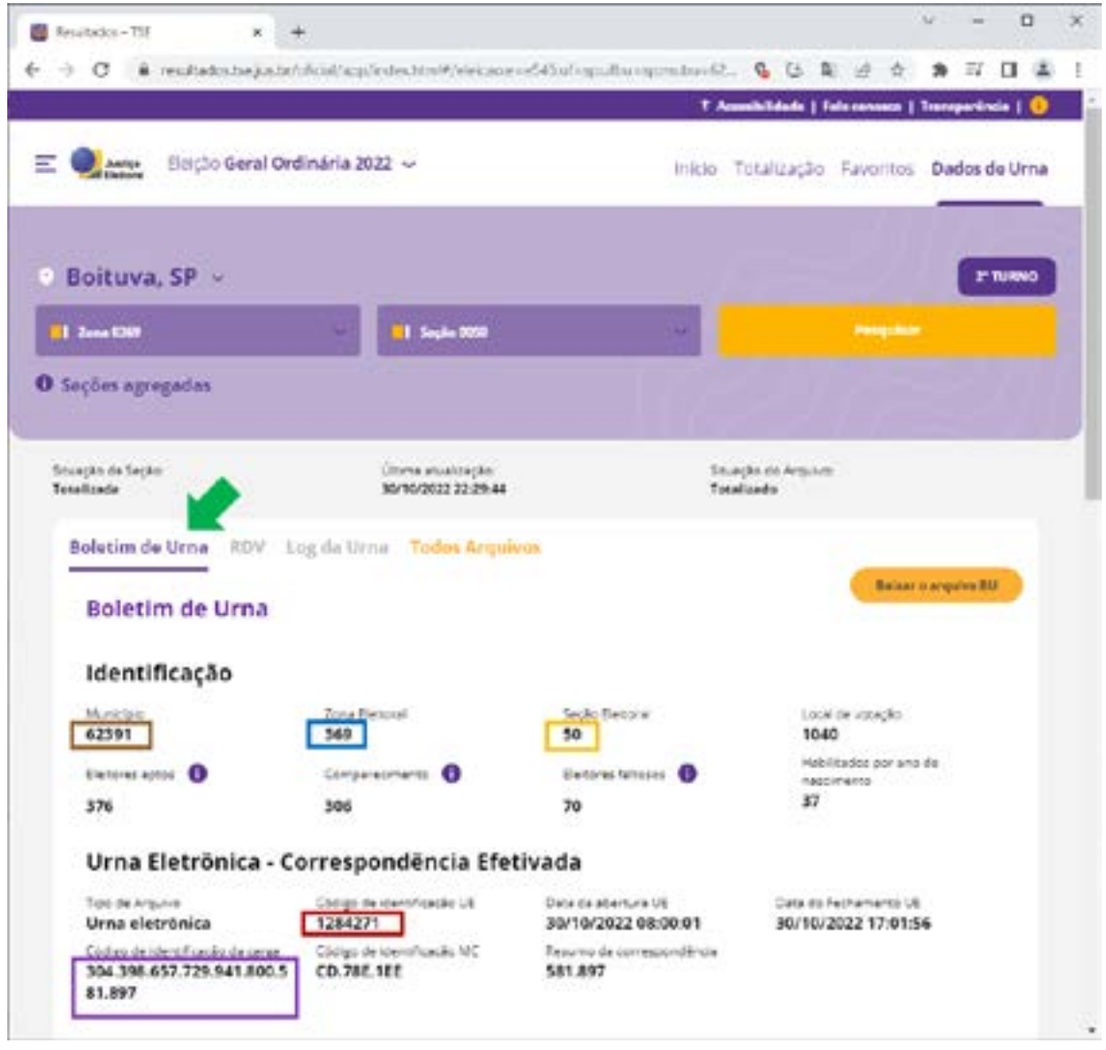
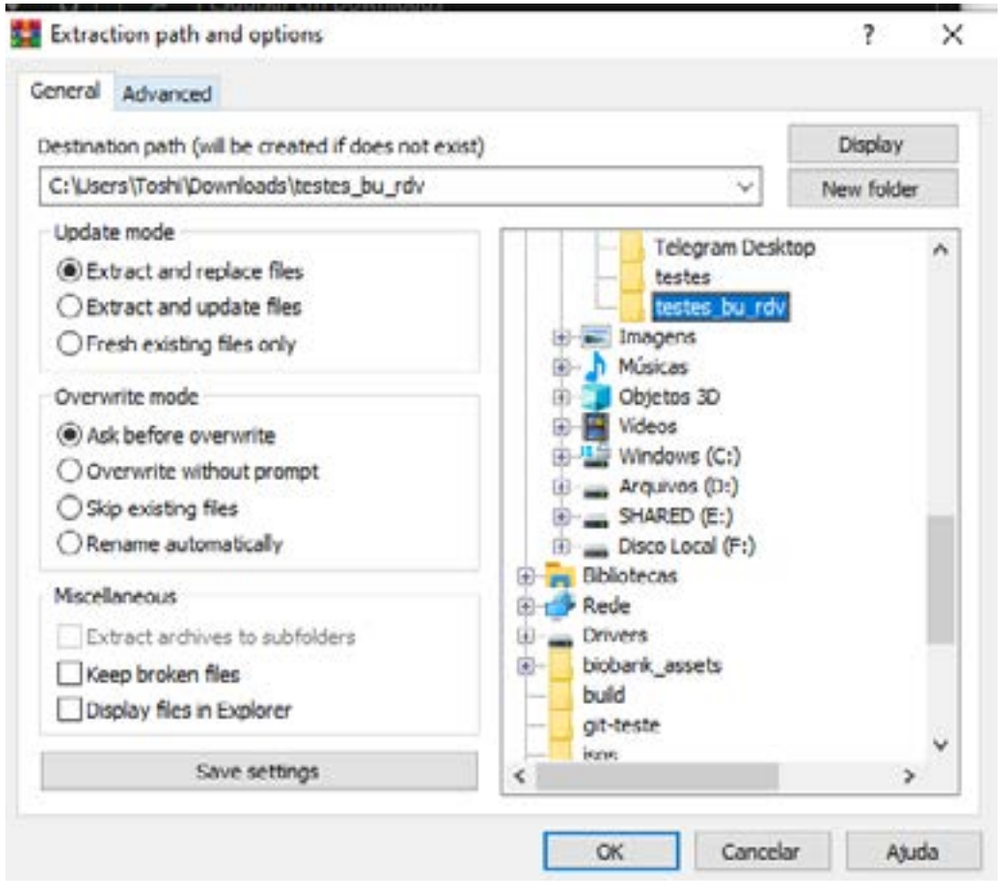


Figura ApI.11. Para conferir que a ligação entre o log e os dados da urna estão corretos, você pode clicar em "Boletim de Urna" (indicado pela seta na figura) e verificar a correspondência de todos os campos destacados na Figura ApI.10, exceto o campo "Código de identificação UE" (onde se encontra o problema).
Pronto, pode ser um pouco trabalhoso, mas bem longe de "impossível"...

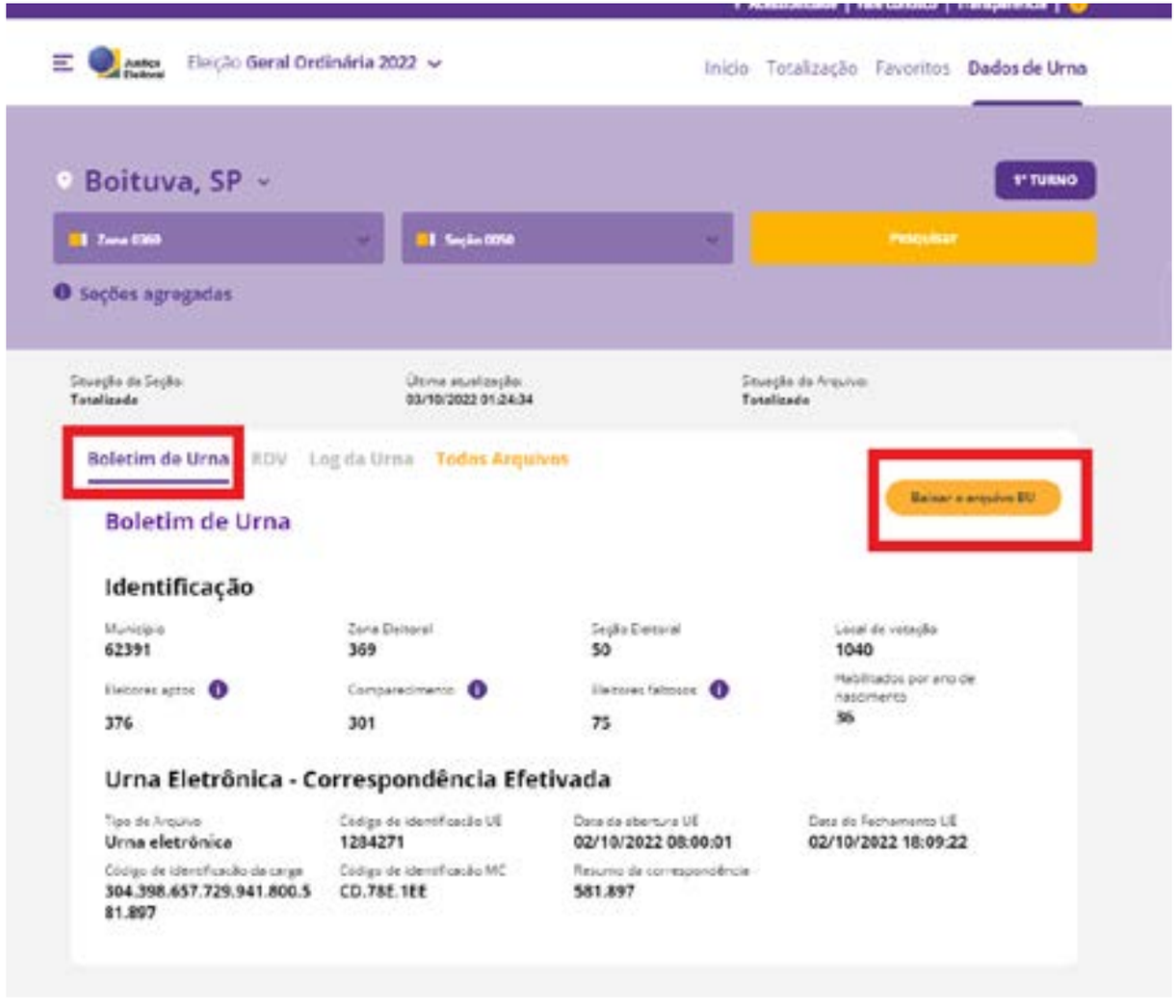
Anexo 2 – Apêndice II

Como encontrar o código de identificação da urna no BU e no RDV

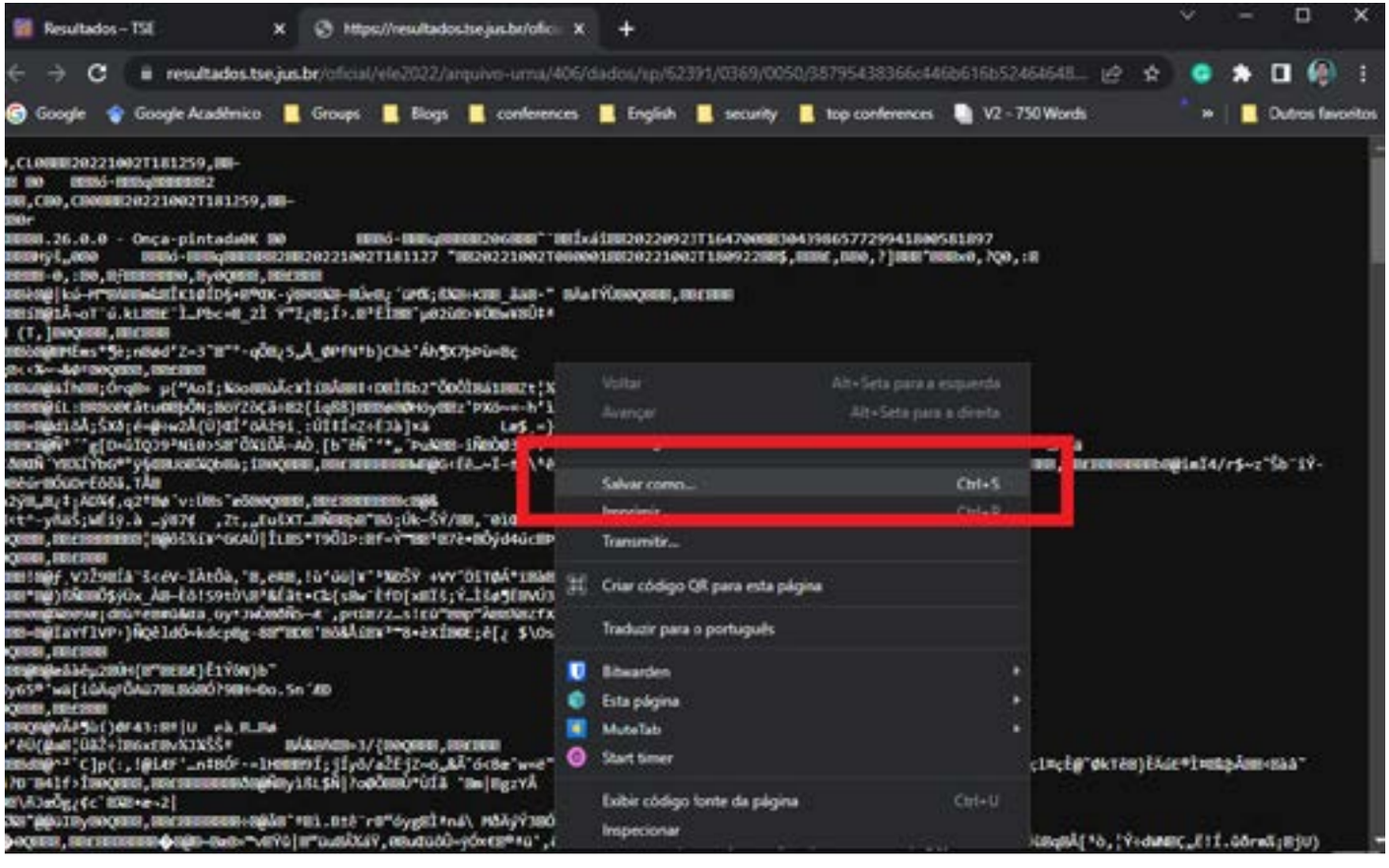
ApII.1. Comece acessando o site oficial do TSE para baixar a especificação dos arquivos de BU e RDV e os scripts (bu_dump.py e rdv_dump.py) que utilizaremos posteriormente. Tudo é baixado como um único arquivo no formato .zip. Fonte: [4]



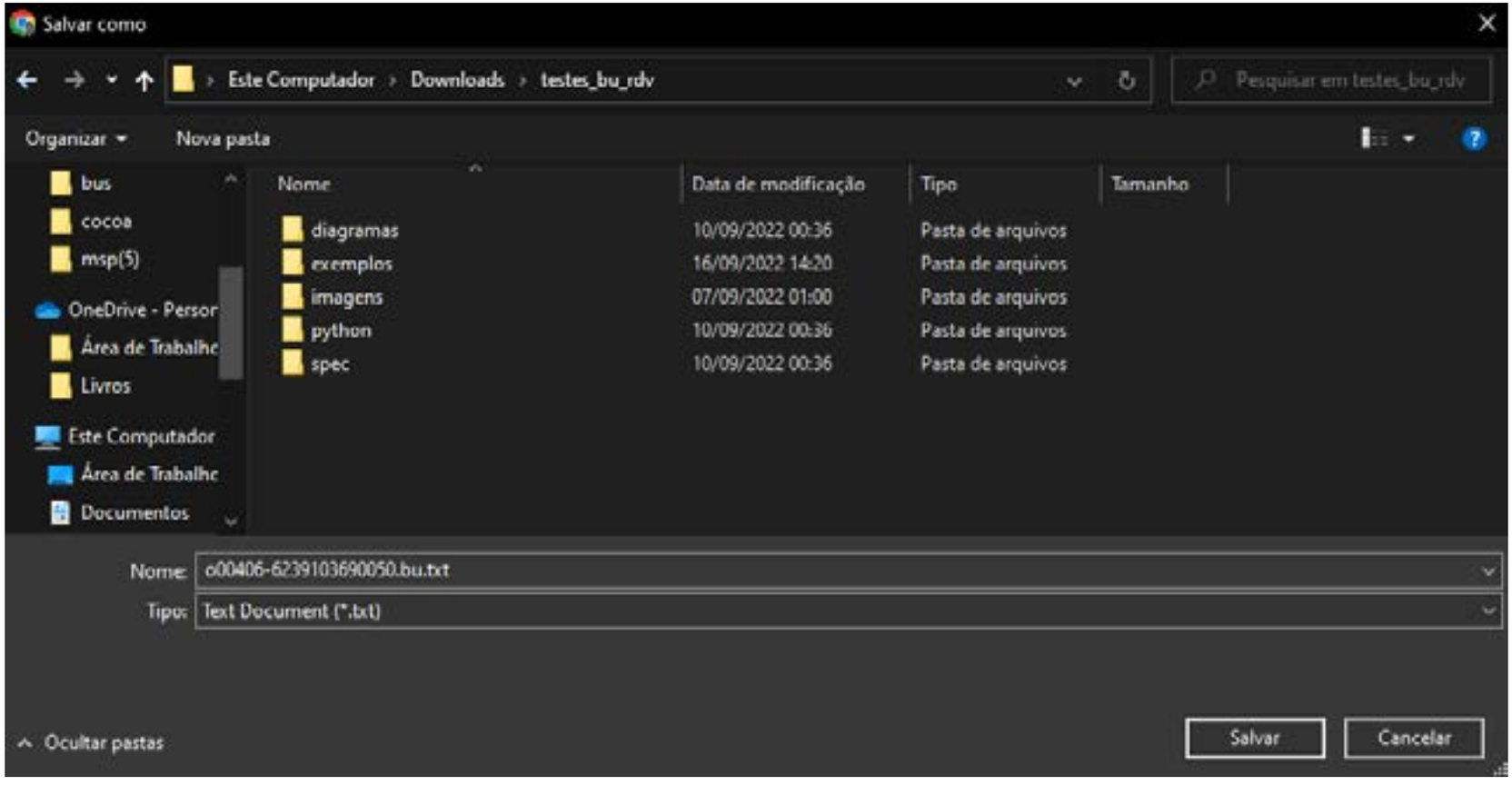
ApII.2. Descompacte o arquivo com o aplicativo de sua preferência (e.g., 7zip [11]) em uma nova pasta. No nosso exemplo, criamos uma pasta chamada "testes_bu_rdv"



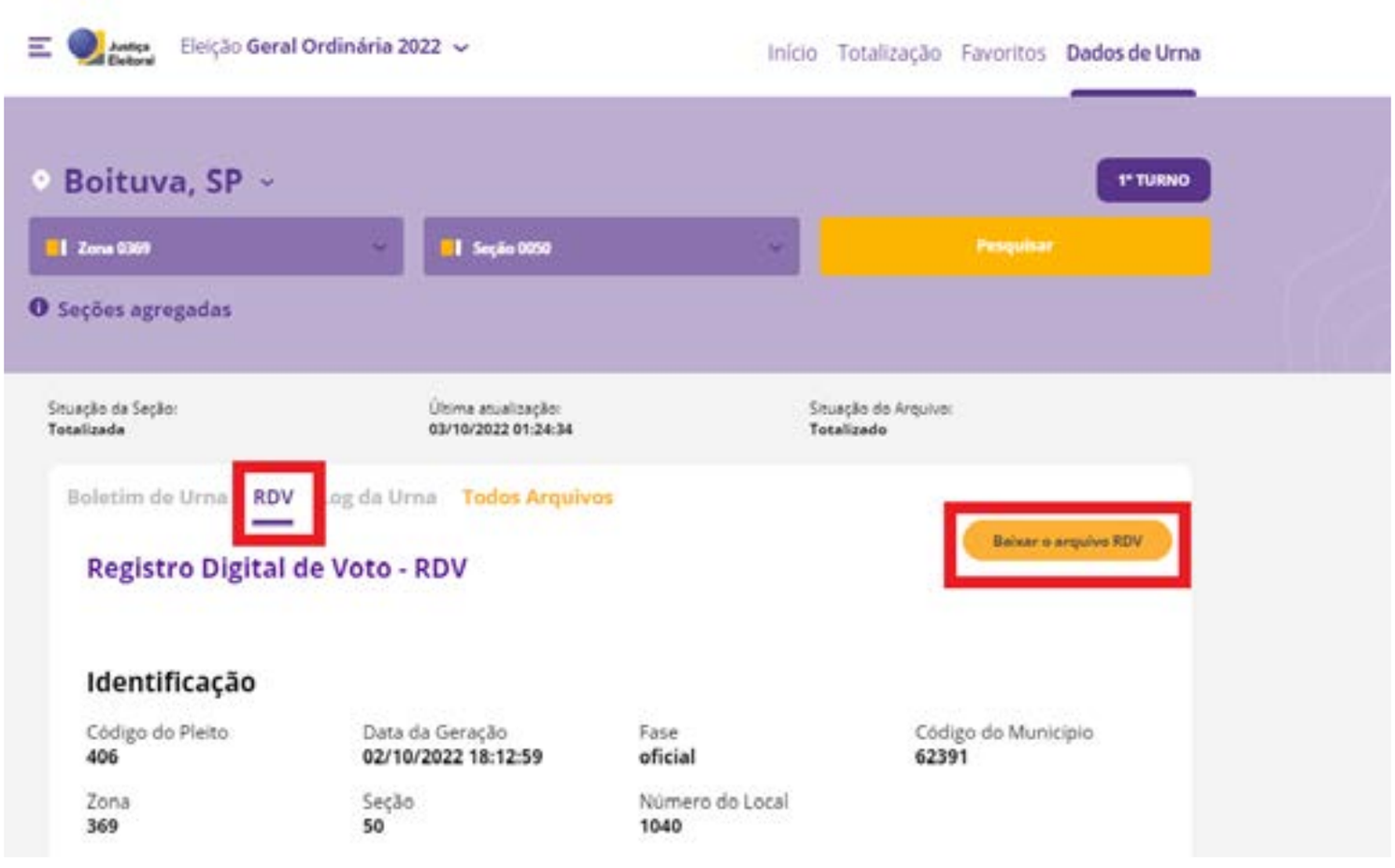
ApII.3. Acesse o site https://resultados.tse.jus.br/ e selecione a cidade/zona/seção de interesse (ver Apêndice I). Selecione a aba de Boletim de Urna e clique em "Baixar o arquivo BU"



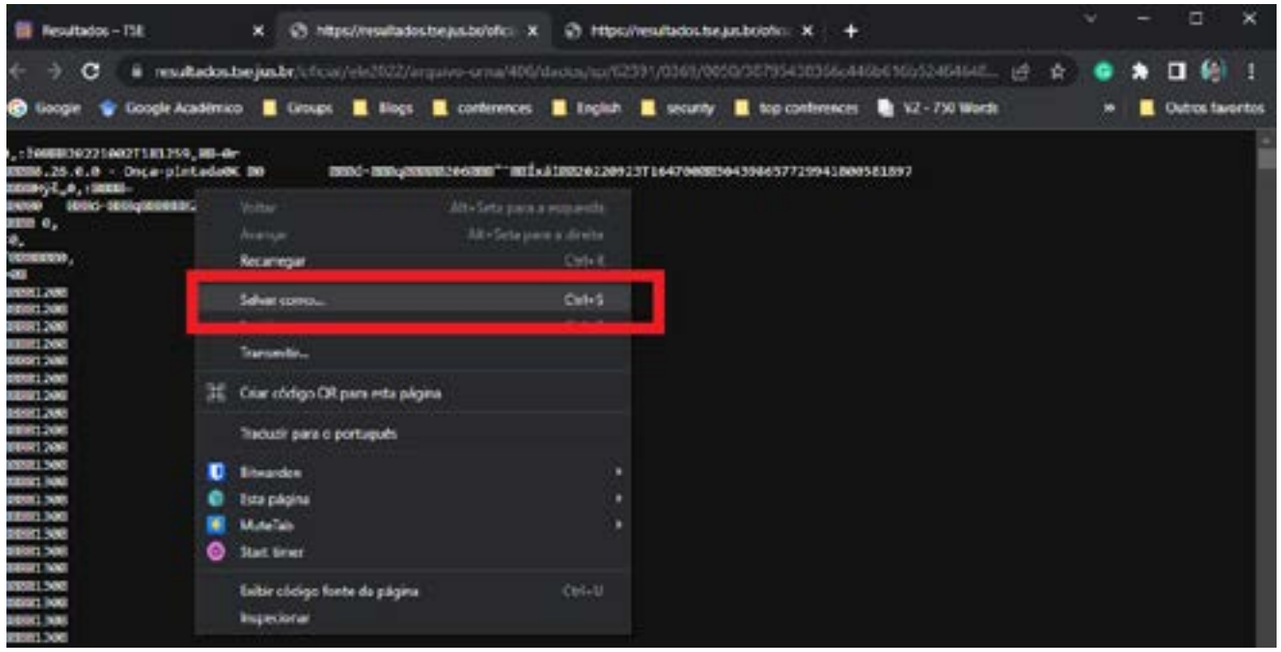
ApII.4. Será aberta uma nova aba com as informações do BU. Podemos salvar essas informações clicando com o botão direito do mouse e selecionando "salvar como..."



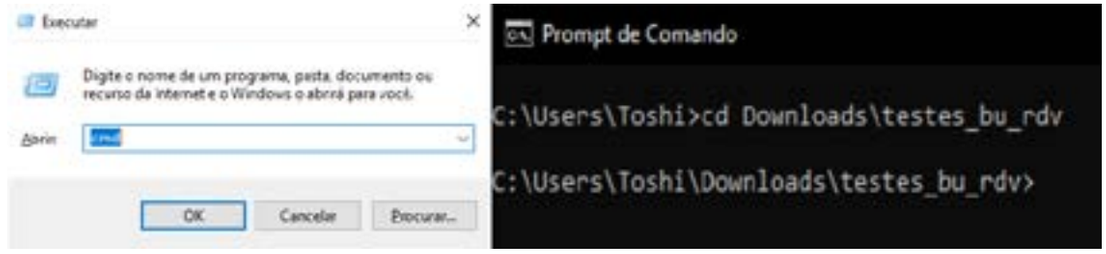
ApII.5. Selecione a mesma pasta criada no passo da Figura ApII.2 (no nosso caso, "testes_bu_rdv") e clique em "salvar".



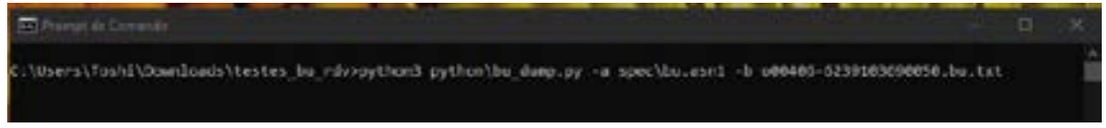
ApII.6. Agora, vamos fazer a mesma coisa com o RDV. Volte para a página de resultados, selecione a aba RDV e clique em "Baixar o arquivo RDV"



ApII.7. Na nova aba que se abre, clique em "salvar como" e salve na mesma pasta criada anteriormente



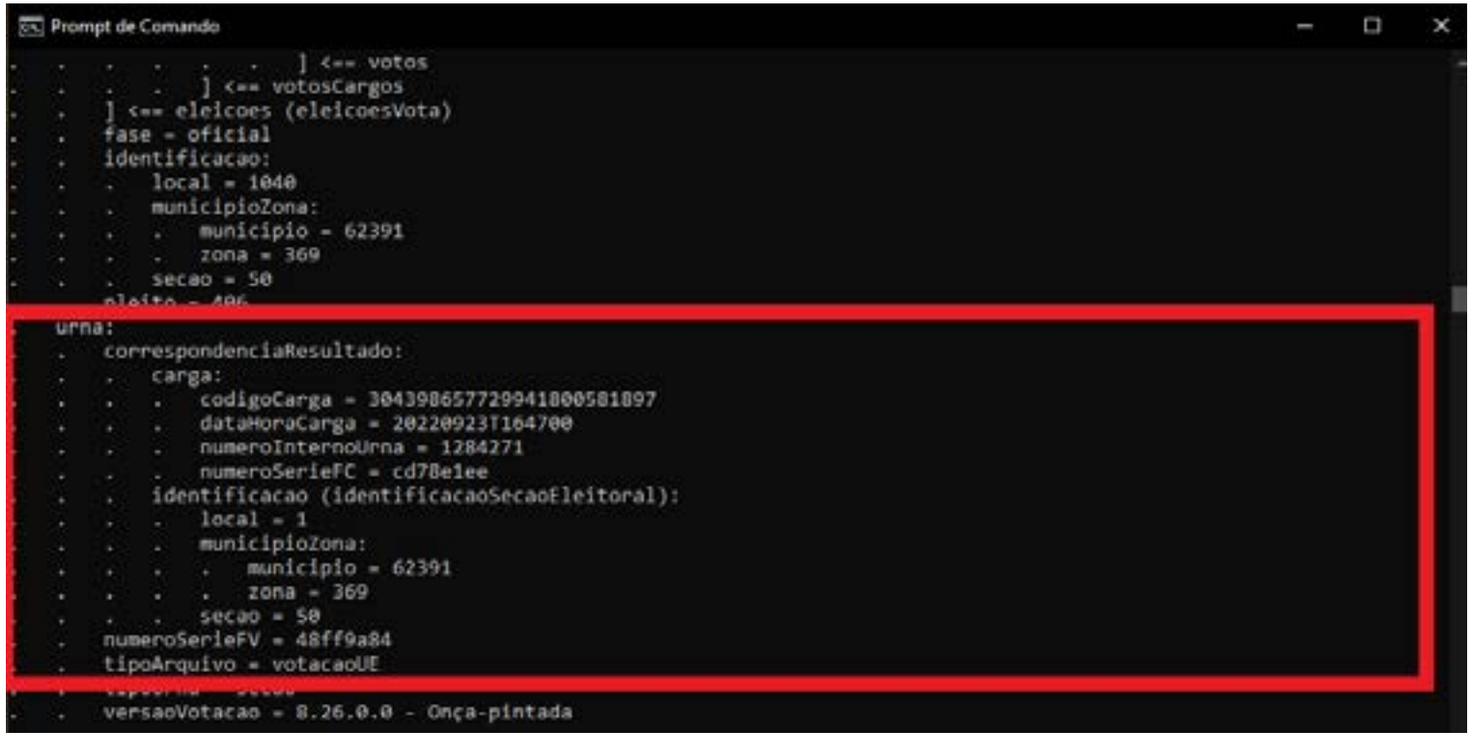
ApII.8. Agora, vamos ler os arquivos obtidos. Usando o Windows, abra um prompt de comando (windows+r, e digite "cmd") e vá até o diretório onde vc baixou todos os arquivos



ApII.9. Finalmente, execute o programa bu_dump.py através da linha de comando (como exemplificado na figura). A estrutura do comando é "python3 bu_dump.py -a <arquivo ASN1 de modelo> -b <arquivo BU>". Para isso, você precisará ter o python3 instalado em seu computador ([32]).

ApII.10. Ao clicar em <ENTER>, você conseguirá ver todas as informações contidas no BU. No final da impressão, você poderá observar as informações identificadoras da urna eletrônica

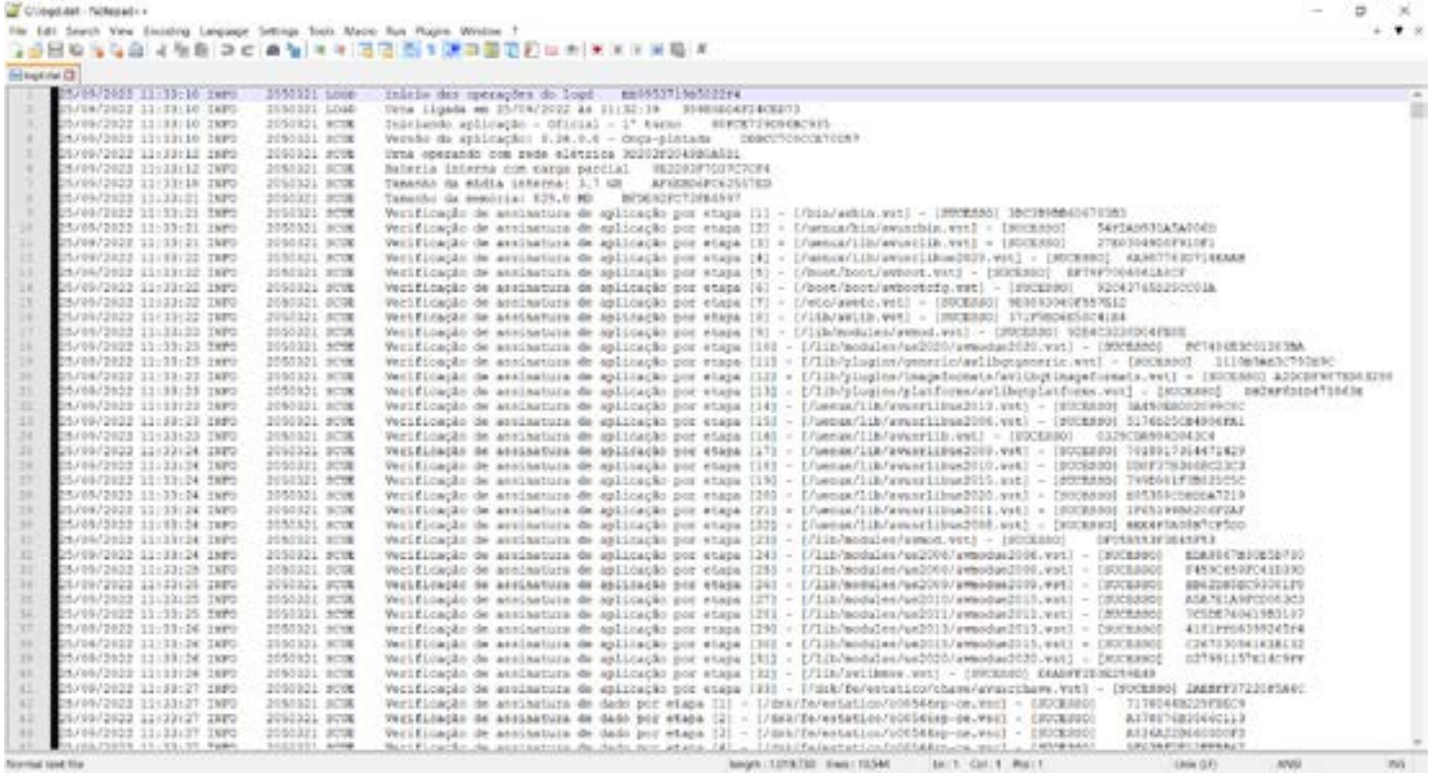
ApII.11. Podemos agora fazer a mesma coisa com o RDV. Dessa vez, a estrutura de comando é "python3 rdv_dump.py -a <arquivo ASN1 de modelo> -r <arquivo RDV>"



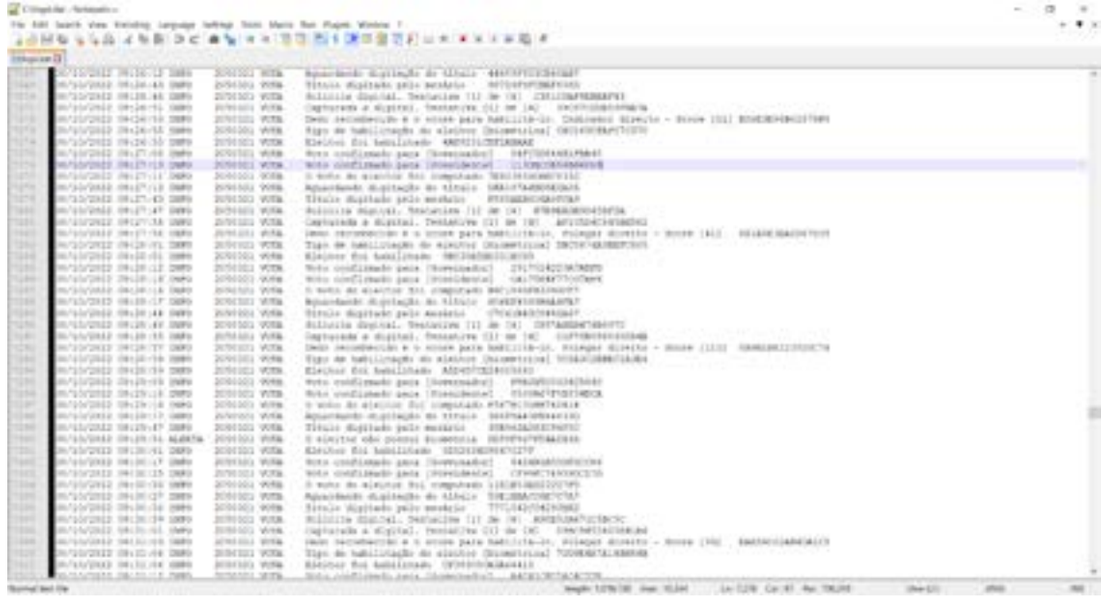
ApII.12. Ao clicar em <ENTER>, podemos ver todas as informações do RDV. Novamente, no final do arquivo, podemos visualizar as informações correspondentes à urna eletrônica

Anexo 2 – Apêndice III

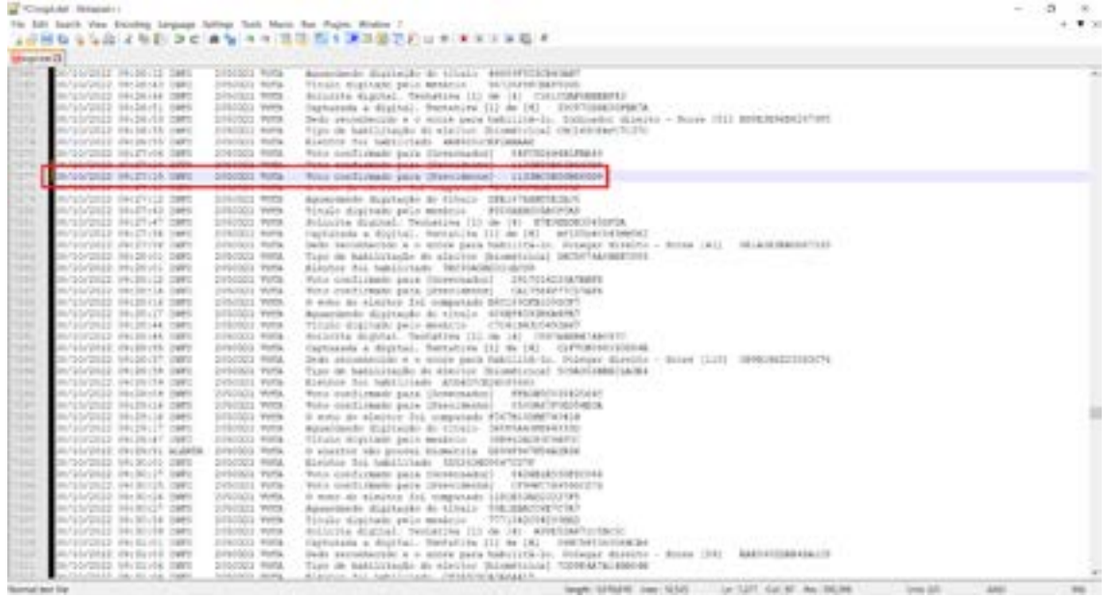
Modificação de log da urna eletrônica: desmentindo que ID_UE tem alguma relevância quando comparado com assinatura digital



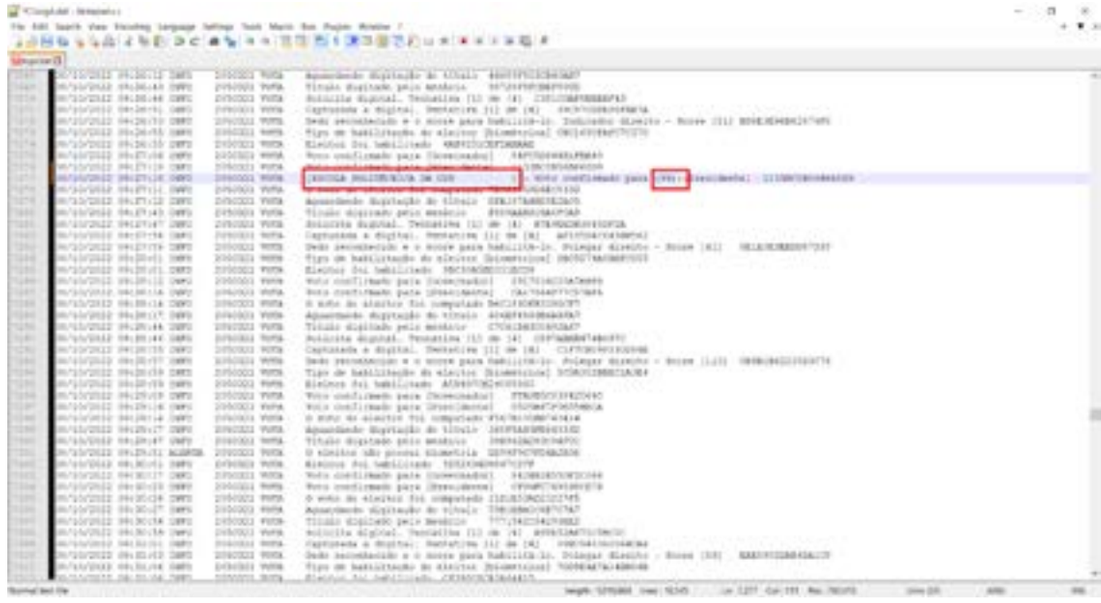
ApIII.1. Obtenha o log que se deseja modificar e abra-o com um editor de texto qualquer. Neste exemplo, o Notepad++ ([9]) foi utilizado.



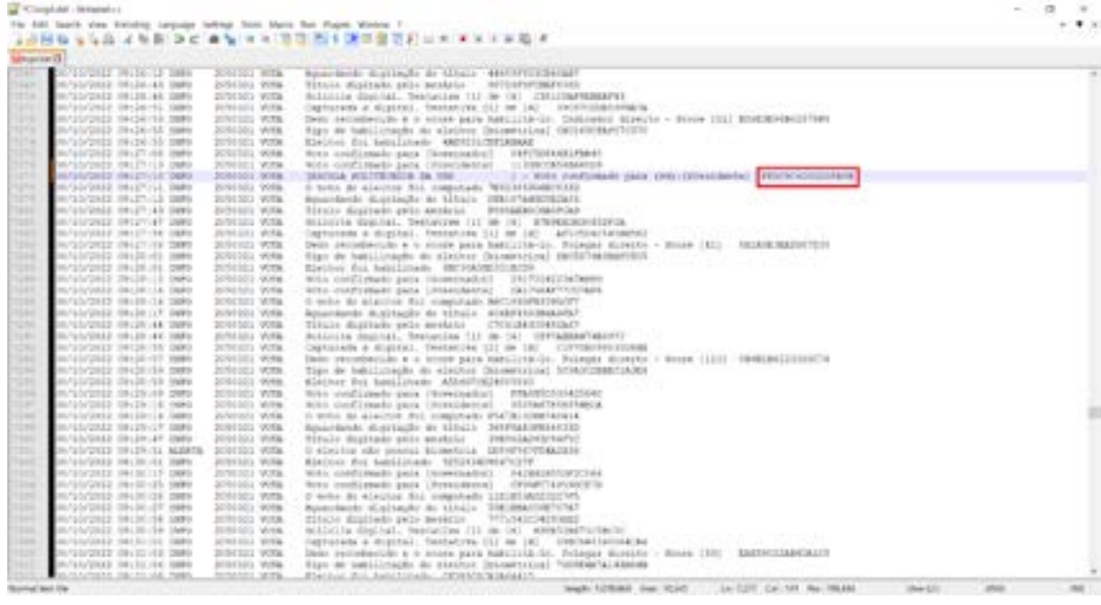
ApIII.2. Navegue até o ponto que se deseja realizar a modificação.



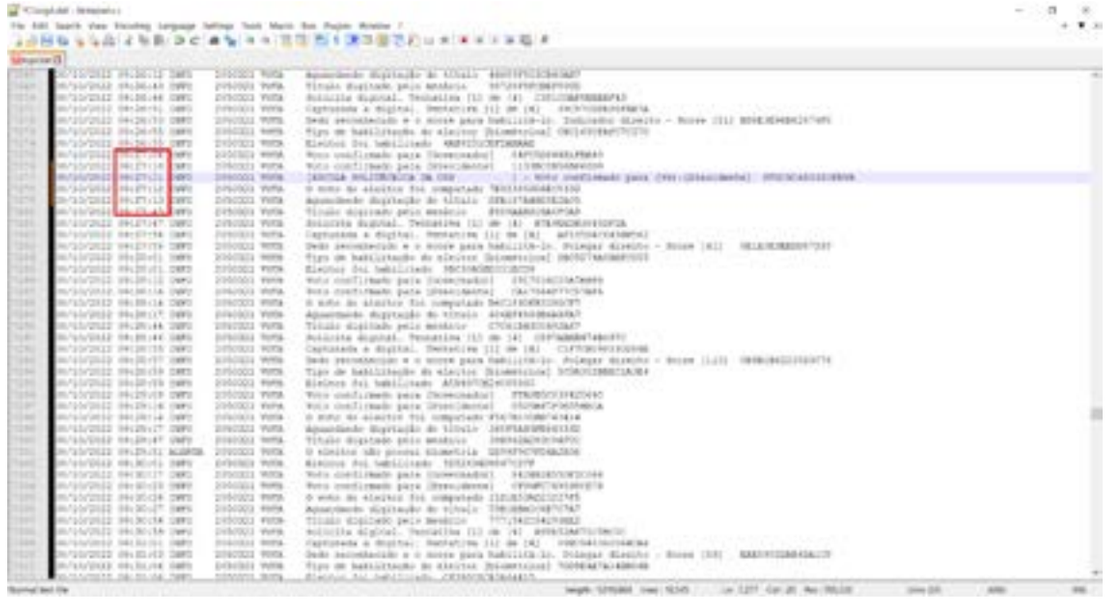
ApIII.3. Copie uma linha do log e a insira na sequência. Este processo é feito para facilitar a modificação, já que o formato da linha, incluindo o ID_UE da urna, já é copiado.



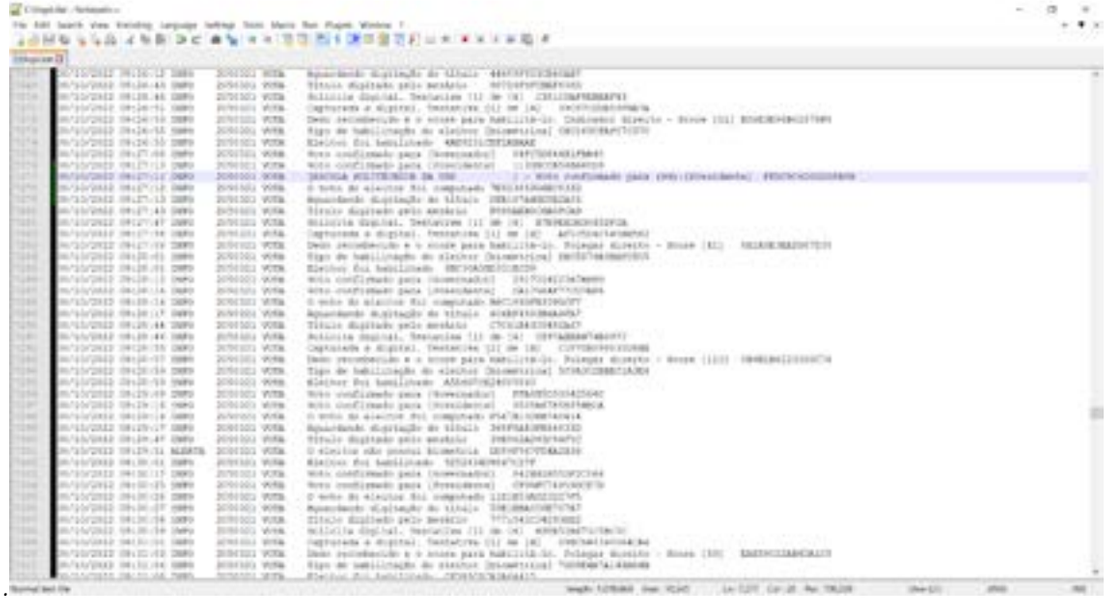
ApIII.4. Modifique a linha como desejado. Neste exemplo, buscou-se criar uma incerteza quanto ao sigilo do voto de um determinado eleitor.



ApIII.5. Altere o valor do campo hexadecimal de 8 bytes para um valor aleatório. Neste exemplo, o valor aleatório foi "FFDC9C6D3320FB8B". Nota: esse campo é um SipHash ([33]), um mecanismo de autenticação "para uso exclusivo do software e da Justiça Eleitoral e não pode ser validado por terceiros" (vide [34]). Logo, embora essa alteração possa ser percebida pelo TSE, o mesmo não ocorrerá com um auditor (que precisaria da assinatura digital do log para notá-la).



ApIII.6. Faça ajustes necessários no campo de hora, a fim de tornar a sequência de eventos temporalmente crível

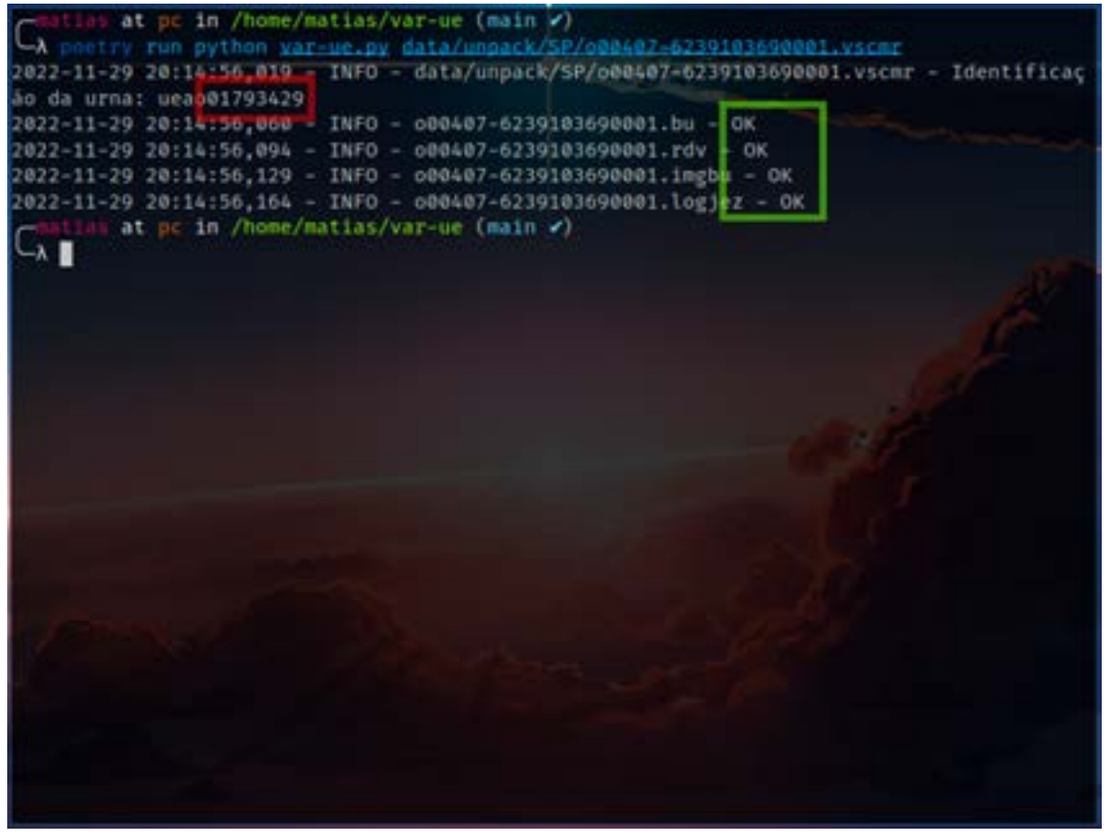


ApIII.7. Salve o arquivo e pronto: agora você tem um log de urna, com seu ID_UE correto, que sugere que o sigilo de voto de um eleitor foi quebrado. Se a correção do ID_UE fosse de alguma forma útil para aferir a autenticidade do log, como sugerem os Relatórios do PL/IVL, você teria acabado de "hackear a urna". Porém, como é falsa a premissa de que o ID_UE é essencial (ou mesmo útil) para conferir autenticidade aos logs, o máximo que esse "ataque" seria capaz de fazer seria criar comoção sem qualquer fundamento técnico…

Anexo 2 – Apêndice IV

VAR UE – Verificando as Assinaturas de Resultados da Urna Eletrônica

ApIV.1. Instalação da ferramenta – clone o repositório e utilize o Poetry para gerar um virtualenv. Instruções mais detalhadas podem ser encontradas em [35].



ApIV.2. Passe à ferramenta VAR UE um ou mais arquivos com extensão .vscmr ou .vscsa, ou um diretório contendo esses arquivos. Para cada arquivo, a ferramenta recupera o ID_UE (em vermelho) do campo Common Name do próprio certificado digital da urna! As mensagens de "OK" (em verde) indicam que as assinaturas são válidas.
Se encontrar qualquer assinatura inválida, a ferramenta aborta a execução e exibe uma mensagem de erro. Testamos todos os arquivos de assinatura disponibilizados no site do TSE, processo que demorou cerca de 4 horas, e nenhuma das verificações retornou erro.

Anexo 2 – Referências

[1] DANTAS, C. Exclusivo: PL vai pedir anulação das eleições de 2022. O Antagonista, 2022. Disponível em: https://oantagonista.uol.com.br/brasil/exclusivo-pl-vai-pedir-anulacao-das-eleicoes-de-2022/. Acesso em: 28 nov. 2022.

[2] TRIBUNAL SUPERIOR ELEITORAL. Resultados do TSE. 2022. Disponível em: https://resultados.tse.jus.br/oficial/app/index.html#/eleicao/resultados. Acesso em: 28 nov. 2022.

[3] TRIBUNAL SUPERIOR ELEITORAL. Resultados 2022 - arquivos transmitidos para totalização. 2022. Disponível em: https://dadosabertos.tse.jus.br/dataset/resultados-2022-arquivos-transmitidos-para-totalizacao. Acesso em: 28 nov. 2022.

[4] TRIBUNAL SUPERIOR ELEITORAL. Documentação técnica do software da urna eletrônica - eleições 2022. 2022. Disponível em: https://www.tse.jus.br/eleicoes/eleicoes-2022/documentacao-tecnica-do-software-da-urna-eletronica. Acesso em: 28 nov. 2022.

[5] TRIBUNAL SUPERIOR ELEITORAL. Conheça os seis modelos de urnas eletrônicas das eleições 2022. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Setembro/conheca-os-seis-modelos-de-urnas-eletronicas-das-eleicoes-2022. Acesso em: 28 nov. 2022.

[6] WIKIPEDIA. Sistema de numeração hexadecimal. 2022. Disponível em: https://pt.wikipedia.org/wiki/Sistema_de_numera%C3%A7%C3%A3o_hexadecimal. Acesso em: 28 nov. 2022.

[7] TRIBUNAL SUPERIOR ELEITORAL. Dados consolidados eleitorado 2020. 2020. Disponível em: https://www.tse.jus.br/eleicoes/eleicoes-2020/prestacao-de-contas/arquivos/dados-consolidados-do-eleitorado-2020. Acesso em: 28 nov. 2022.

[8] TRIBUNAL SUPERIOR ELEITORAL. Resultados – 2022 – correspondências esperadas e efetivadas – 2º turno. 2022. Disponível em: https://dadosabertos.tse.jus.br/dataset/resultados-2022-correspondencias-esperadas-e-efetivadas-2-turno. Acesso em: 28 nov. 2022.

[9] HO, D. Notepad++ download. Notepad++, 2022. Disponível em: https://notepad-plus-plus.org/downloads/. Acesso em: 28 nov. 2022.

[10] TRIBUNAL SUPERIOR ELEITORAL. Arquivos de correspondência do 2o turno para o estado de São Paulo. 2022. Disponível em: https://cdn.tse.jus.br/estatistica/sead/eleicoes/eleicoes2022/correspefet/CEFT_2t_SP_311020221100.zip. Acesso em: 28 nov. 2022.

[11] PAVLOV, I. 7-zip download. 7-Zip, 2022. Disponível em: https://www.7-zip.org/download.html. Acesso em: 28 nov. 2022.

[12] TRIBUNAL SUPERIOR ELEITORAL. Arquivos disponibilizados para auditoria dos resultados da eleição. 2022. Disponível em: https://dadosabertos.tse.jus.br/gl/dataset/. Acesso em: 28 nov. 2022.

[13] MONTEIRO, J.; LIMA, S.; RODRIGUES, R.; ALVAREZ, P.; MENESES, M.; MENDONÇA, F.; COIMBRA, R. Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo T-DRE. In: SBC. Anais do IV Workshop de Tecnologia Eleitoral. São Paulo, SP, 2019. p. 1–12. Disponível em: https://sbseg2019.ime.usp.br/anais/197131.pdf. Acesso em: 28 nov. 2022.

[14] TRIBUNAL SUPERIOR ELEITORAL. Resultados 2022 – arquivos transmitidos para totalização. 2022. Disponível em: https://dadosabertos.tse.jus.br/gl/dataset/resultados-2022-arquivos-transmitidos-para-totalizacao. Acesso em: 28 nov. 2022.

[15] NIST. FIPS 186-4: Digital Signature Standard (DSS). Gaithersburg, MD, 2013. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf. Acesso em: 28 nov. 2022.

[16] NIST. FIPS 186-5: Digital Signature Standard (DSS) – Draft. Gaithersburg, MD, 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf. Acesso em: 28 nov. 2022.

[17] EMVCO, L. EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management. 2011. Disponível em: https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf. Acesso em: 28 nov. 2022.

[18] FEBRABAN. FEBRABAN alerta para golpes envolvendo cartões de crédito e débito. 2019. Disponível em: https://portal.febraban.org.br/noticia/3259/pt-br/. Acesso em: 28 nov. 2022.

[19] MANUAL DO MUNDO. Como funciona uma urna eletrônica. 2018. Disponível em: https://www.youtube.com/watch?v=4wrMLzqgKEI. Acesso em: 28 nov. 2022.

[20] TRIBUNAL SUPERIOR ELEITORAL. Como realizar auditoria. 2022. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/como-realizar-auditoria. Acesso em: 28 nov. 2022.

[21] CERIMEDO, F. Alegação de violação de sigilo dos votos. Twitter, 2022. Disponível em: https://twitter.com/FercerimedoBR/status/1592505676261384197. Acesso em: 28 nov. 2022.

[22] TRIBUNAL SUPERIOR ELEITORAL. Anexo IV – Especificações Técnicas – Segurança – URNA ELETRÔNICA – UE2022. 2021. Disponível em: https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/arquivos-edital-1-2021/1-22-anexo-iv-especificacoes-tecnicas-seguranca/@@download/file/Anexo_IV___Especificacoes_Tecnicas___Seguranca.pdf. Acesso em: 28 nov. 2022.

[23] THE OPENSSL PROJECT. OpenSSL – Open Source Toolkit for the Transport Layer Security (TLS) . 2022. Disponível em: https://www.openssl.org/. Acesso em: 28 nov. 2022.

[24] UNIVESP. Segurança da informação – aula 04 – algoritmos assimétricos e certificação digital. 2018. Disponível em: https://www.youtube.com/watch?v=4xv0RD8T1qA. Acesso em: 28 nov. 2022.

[25] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Repositório AC-Raiz. 2022. Disponível em: https://www.gov.br/iti/pt-br/assuntos/repositorio/repositorio-ac-raiz. Acesso em: 28 nov. 2022.

[26] BANCO DO BRASIL. Site – Banco do Brasil. 2022. Disponível em: https://www.bb.com.br/site. Acesso em: 28 nov. 2022.

[27] CAIXA. Site – Caixa. 2022. Disponível em: https://www.caixa.gov.br/Paginas/home-caixa.aspx. Acesso em: 28 nov. 2022.

[28] CERTIFICATE TRANSPARENCY. Certificate Transparency (CT). 2022. Disponível em: https://certificate.transparency.dev/. Acesso em: 28 nov. 2022.

[29] WIKIPEDIA. DigiNotar. 2022. Disponível em: https://en.wikipedia.org/wiki/DigiNotar. Acesso em: 28 nov. 2022.

[30] TRIBUNAL SUPERIOR ELEITORAL. Portal de Dados Abertos do TSE. 2022. Disponível em: https://dadosabertos.tse.jus.br/. Acesso em: 28 nov. 2022.

[31] LEITE, R. N. Eleições 2022. 2022. Disponível em: https://rafnleite.github.io/relatorio_eleicoes.html. Acesso em: 28 nov. 2022.

[32] PYTHON SOFTWARE FOUNDATION. Python. 2022. Disponível em: https://www.python.org/. Acesso em: 28 nov. 2022.

[33] AUMASSON, J.-P.; BERNSTEIN, D. J. Siphash: a fast short-input PRF. In: SPRINGER. International Conference on Cryptology in India. 2012. p. 489–508. Disponível em: https://github.com/veorq/SipHash. Acesso em: 28 nov. 2022.

[34] TRIBUNAL SUPERIOR ELEITORAL. Formato dos arquivos de log. 2022. Disponível em: https://www.tse.jus.br/eleicoes/eleicoes-2022/arquivos/formato-dos-arquivos-de-log-17-9-22. Acesso em: 28 nov. 2022.

[35] EPIC LEET TEAM. VAR UE: Verificador de Assinaturas de Resultados das Urnas Eletrônicas. Disponível em: https://github.com/epicleet/var-ue. Acesso em: 29 nov. 2022.

[36] TSE, Manual do Mesário – Eleições 2022. Disponível: https://static.tre-al.jus.br/portal/eleitor/mesarios/tre-al-manual-do-mesario-tse-versao-web-2022.pdf Acesso em: 30 nov. 2022.

UNIVERSIDADE DE SÃO PAULO

Missão de Observação Eleitoral 2022

Este Relatório analisa as eleições de 2022, tendo por base a disputa presidencial, contextualizando o período pré e pós-eleitoral, e não apenas os dias em que foram realizadas as votações em 1º e 2º turnos. Tal enfoque amplia a ótica de análise, a fim de que se possa compreender a dinâmica do processo, e não apenas fatos isolados, servindo para informar *urbi et orbe* ("para a cidade e o mundo") o que se passou nas eleições presidenciais de 2022, sendo um Relatório *independente*, a ser apresentado ao *Presidente do TSE* e *às Chefias dos Poderes da República* (Resolução TSE 23.678/21, art. 24, §3º). Foram observados, em especial, aspectos referentes à segurança das urnas eletrônicas e o âmbito jurídico da eleição presidencial de 2022, contendo, ao final, algumas recomendações para o aperfeiçoamento do sistema.