Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

A confiança em sistemas de votação eletrônica: uma análise quantitativa da aceitação das urnas eletrônicas no Brasil e seus efeitos moderadores

Celio Castro Wermelinger

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. João Mello da Silva

Coorientador
Prof. Dr. Ari Melo Mariano

Brasília
2024

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

CW489c

Castro Wermelinger, Celio
A confiança em sistemas de votação eletrônica: uma análise quantitativa da aceitação das urnas eletrônicas no Brasil e seus efeitos moderadores / Celio Castro Wermelinger; orientador João Mello da Silva; co-orientador Ari Melo Mariano. -- Brasília, 2024.
209 p.

Dissertação(Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2024.

1. Voto eletrônico. 2. Urna eletrônica. 3. Voto impresso. 4. UTAUT. 5. PLS-SEM. I. Mello da Silva, João, orient. II. Melo Mariano, Ari, co-orient. III. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

A confiança em sistemas de votação eletrônica: uma análise quantitativa da aceitação das urnas eletrônicas no Brasil e seus efeitos moderadores

Celio Castro Wermelinger

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. João Mello da Silva (Orientador)
CIC/UnB

Prof. Dr. Wilson Vicente Ruggiero
Universidade de São Paulo

Prof. Dr. Marcos Antonio Simplicio Junior
Universidade de São Paulo

Prof.a Dr.a Edna Dias Canedo
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 29 de novembro de 2024

Dedicatória

Dedico este trabalho aos servidores e colaboradores da Justiça Eleitoral, que trabalham arduamente no intuito de garantir a confiança do processo eletrônico de votação do Brasil.

Agradecimentos

Esta dissertação foi elaborada no curso de Mestrado Profissional do Programa de Pós-Graduação em Computação Aplicada, do Departamento de Ciência da Computação, da Universidade de Brasília. A esta instituição, na figura de seus valorosos professores, agradeço a oportunidade e os meios a mim disponibilizados para realização da pesquisa.

Ao Professor Doutor João Mello da Silva, meu orientador, por todos os ensinamentos, pelo incondicional apoio, pela parceria, dedicação, paciência e, especialmente, pela motivação.

Igualmente, gratidão ao Professor Doutor Ari Melo Mariano, meu coorientador, pela disponibilidade, pelo aprendizado, o aconselhamento assertivo e o auxílio na definição do tema do trabalho e na realização da pesquisa.

Aos amigos do Tribunal Superior Eleitoral pelos anos de trabalho, parcerias, discussões e desafios enfrentados em conjunto para a realização de eleições livres, limpas e justas no Brasil.

Ao meus pais que, desde cedo, me ensinaram o valor da educação para compreender o mundo, respeitar as pessoas e construir uma carreira profissional.

À minha esposa e aos nossos filhos que tiveram paciência e compreensão pela ausencia nas mais variadas ocasiões durante a realização do curso.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Os sistemas de informação são utilizados em vários ramos do conhecimento. No contexto eleitoral, em geral, seu uso tem o intuito de melhorar a gestão, agilizar procedimentos, reduzir fraudes e aumentar a segurança do processo de votação. No caso brasileiro, a adoção da urna eletrônica visou combater o histórico de fraudes da votação manual. Desde 1996, a confiança nos equipamentos de votação é motivo de questionamentos e debates. Nesse sentido, esta pesquisa aplicada, com abordagem quantitativa e qualitativa, teve por objetivo propor etapas para melhorar a aceitação da urna eletrônica no Brasil, a partir da identificação das propriedades formadoras da confiança em sistemas de votação eletrônica. Para tanto, foi levantado o estado da arte de publicações acerca da votação eletrônica nas bases *Web of Science* (WoS) e *Scopus*, desde 1996, e utilizado o modelo *Unified Theory of Acceptance and Use of Technology* (UTAUT), para avaliar a aceitação das urnas eletrônica no Brasil, e o método de equações estruturadas *Partial Least Squares - Structural Equation Modeling* (PLS-SEM) para analisar os resultados. A partir das 1.851 respostas à pesquisa eletrônica, o modelo proposto teve potencial explicativo de 0,848 sobre a Intenção de Uso da urna eletrônica e de 0,588 sobre a Intenção de Mudança para incluir a impressão do voto. Dentre as variáveis, a Confiança Global, construto de segunda ordem resultante da união da Percepção de Segurança e da Confiança na Tecnologia, e a Expectativa de Performance impactaram tanto a Intenção de Uso, em 43,7% e 33,3%, quanto a Intenção de Mudança, em 68,8% e 7,3%, respectivamente. Em relação aos efeitos moderadores, o gênero impactou as variáveis Confiança Global, Expectativa de Performance e Influência Social. A idade influênciou a Confiança Global e a Expectativa de Esforço, assim como a escolaridade afetou a Expectativa de Performance, e a orientação política impactou a Confiança Global, a Expectativa de Esforço e a Influência Social. Ao final, a partir da análise da relação de importância vs. Desempenho, *Importance-Performance Map Analysis* (IPMA) das variáveis do modelo, foram propostas iniciativas visando aumentar a confiança no processo eletrônico de votação do país.

Palavras-chave: Voto eletrônico, Urna eletrônica, Voto impresso, UTAUT, PLS-SEM, IPMA, Brasil

Abstract

Information systems are used in various branches of knowledge. In the electoral context, in general, its use is intended to improve management, streamline procedures, reduce fraud and increase the security of the voting process. In the Brazilian case, the adoption of electronic voting machines aims to combat the history of manual voting fraud. Since 1996, confidence in voting has been a reason for questioning and debate. In this sense, this applied research, with a quantitative and qualitative approach, aimed to propose steps to improve the acceptance of electronic voting machines in Brazil, based on the identification of trust-forming properties in electronic voting systems. To this end, the state of the art of publications on electronic voting was surveyed in the Web of Science (WoS) and Scopus databases, since 1996, and the Unified Theory of Acceptance and Use of Technology (UTAUT) model was used to evaluate the acceptance of electronic voting machines in the Brazil, and the structured equation method Partial Least Squares - Structural Equation Modeling (PLS-SEM) to analyze the results. From the 1,851 responses to the electronic survey, the proposed model had an explanatory potential of 0.848 on the Intention to Use the voting machine and 0.588 on the Intention to Change to include printed votes. Among the variables, Global Trust, a second-order construct resulting from the union of Security Perception and Trust in technology, and Performance Expectation impacted both the Intention to Use, at 43.7% and 33.3%, as for Intention to Change, at 68.8% and 7.3%, respectively. Regarding moderating effects, gender impacted the variables Global Trust, Performance Expectation and Social Influence. Age influenced Global Trust and Effort Expectancy, just as education affected Performance Expectancy, and political orientation impacted Global Trust, Effort Expectancy and Social Influence. In the end, based on the analysis Importance-Performance Map Analysis (IPMA) of the model variables, initiatives were proposed to increase confidence in the country's electronic voting process.

Keywords: *e-voting, Voting machine, Printed vote, UTAUT, PLS-SEM, IPMA, Brazil*

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ACM *Association for Computing Machinery.*

AVE *Average Variance Extracted.*

BPMN *Business Process Model and Notation.*

BU Boletim de urna.

CB-SEM *Covariance Based.*

CISA *Cybersecurity and Infrastructure Security Agency.*

CNT Confederação Nacional dos Transportes.

D-S *Dempster–Shafer.*

DRE *Direct Recording Eletronic.*

E2E *End-to-End.*

ERP *Enterprise Resource Planning.*

HAVA *Help America Vote Act.*

HT *Hough transform.*

IBE *Identity-Based Encryption.*

IDEA *International Institute for Democracy and Electoral Assistance.*

IDT *innovation Difusion Theory.*

IEEE *Institute of Electrical and Electronic Engineers.*

IoT Internet of Things.

IPMA *Importance-Performance Map Analysis.*

k-TAA *k-Times Anonymous Authentication.*

MM *Motivational Model.*

MPCU *Model of Personal Computer Utilization.*

NAAL Avaliação Nacional de Alfabetização de Adultos.

NFC *Near Field Communication.*

PEI *Perceptions of Electoral Integrity.*

PLS-SEM *Partial Least Squares - Structural Equation Modeling.*

RDV Registro Digital do Voto.

RFID *Radio Frequency Identification.*

SCT *Social Cognitive Theory.*

SEM *Structural Equation Modeling.*

TAM *Technology Acceptance Model.*

TAM/TPB *Combined TAM and TPB.*

Temac Teoria do Enfoque Meta Analítico.

TPB *Theory of Planned Behavior*.

TPS Testes Públicos de Segurança dos Sistemas Eleitorais.

TRA *Theory of Reasoned Action.*

TRE Tribunal Regional Eleitoral.

TSE Tribunal Superior Eleitoral.

UTAUT *Unified Theory of Acceptance and Use of Technology.*

VIF *Variance Inflation Factor*.

VVPAT *Voter Verifiable Paper Audit Trail.*

VVSG *Voluntary Voting System Guidelines.*

WoS *Web of Science.*

ZKP *Zero Knowledge Proof.*

Capítulo 1

Introdução

Os sistemas de informação destinam-se a fornecer conhecimento, notícias, fatos, dados, aprendizagem e conhecimento necessários à condução de um negócio [1]. Atualmente, são protagonistas na economia global em virtude de serem capazes de armazenar, processar e fornecer informações com precisão [2]. Ainda, além da tecnologia, incluem também pessoas e organizações[3].

Neste cenário, os sistemas de informação são implementados com o propósito de melhorar a eficácia e eficiência de uma organização [3]. Em função da alta competitividade e da imprevisibilidade dos mercados, a tecnologia da informação é uma das ferramentas que as organizações utilizam para se manterem ativas e atualizadas. Dessa forma, o sucesso de uma organização está relacionado a sua habilidade de implementar, dominar e valorizar conhecimentos tecnológicos [4].

Os sistemas de informação, há tempos, são utilizados em diversos campos de conhecimento tais como engenharia espacial, distribuição de energia, comunicação, medicina, entre outros. O meio militar foi um impulsionador, considerando que a introdução de equipamentos e armas mais sofisticados e complexos exigiam mais confiabilidade em sua operação [5].

Umas das preocupações relacionadas a sua utilização diz respeito a verificação do cumprimento dos requisitos funcionais e não funcionais esperados. Em alguns contextos, os sistemas de informação devem ser especializados e atender a um conjunto de propriedades específicas. Uma dessas aplicações é a votação eletrônica, que possui um conjunto muito distinto de requisitos [6] visando garantir a lisura na realização de eleições.

De maneira suscinta, [7] define seis princípios a serem adotados pelos sistemas de votação, são eles:

1. Apenas eleitores aptos devem votar;
2. Cada eleitor vota apenas uma vez;

3. Ninguém deve ser capaz de conhecer o conteúdo do voto, a não ser o próprio eleitor;
4. Não deve ser possível duplicar votos;
5. Qualquer tentativa de alteração de voto deve ser detectada;
6. Eleitores devem poder verificar que seu voto foi contado.

Em países democráticos, eleições tem papel fundamental na escolha de seus governantes [8]. No intuito de aprimorar a segurança do processo e reduzir fraudes, melhorar a gestão e performance e/ou aumentar a participação do eleitorado [9], os sistemas de informação são peças importantes do processo eleitoral de vários países, incluindo o Brasil.

Segundo o *International Institute for Democracy and Electoral Assistance* (IDEA), a votação eletrônica refere-se à emissão, contagem e tabulação de votos, com o uso de sistemas eletrônicos [8]. Por serem ferramenta central do processo eleitoral, sistemas de votação eletrônica estão relacionados à garantia da democracia. Nesse contexto, a proteção à democracia contempla proporcionar eleições que reflitam com precisão as intenções dos eleitores e garantam a confiança do público [10].

Assim, uma das tarefas mais importantes e desafiadoras de um governo democrático é o planejamento e a execução das eleições que definem seu sucessor. Resultados duvidosos, tecnologia deficiente e métodos engenhosos de fraude são observados ao longo da história eleitoral [11].

No Brasil, a fraude foi uma constante nas eleições durante a sua história. Além de ferramenta de coação dos eleitores, as fraudes eram utilizadas como parte da estratégia de embate entre os grupos políticos e envolviam o eleitor, o voto e o candidato [12].

Esse cenário começou a mudar a partir da criação da Justiça Eleitoral. Desde então, o combate às fraudes foi melhor estruturado e evoluiu para a informatização do processo eleitoral, no intuito de diminuir ao máximo a intervenção humana, principal causa dos erros intencionais ou não [12].

Cabe ressaltar que diferentes graus de participação humana estarão presentes nas variadas etapas do processo eleitoral. A questão principal são os controles que podem ser aplicados para garantir a correta realização das atividades previstas.

Maior expoente da votação informatizada do Brasil, a urna eletrônica é parte de um processo mais amplo, que envolve várias funções como gestão do cadastro de eleitores, bem como várias etapas de preparação e apuração dos votos [13].

Apesar da constante evolução dos mecanismos de segurança e auditoria do processo eletrônico de votação do Brasil [14][15], desde o início da informatização, pairam questionamentos e dúvidas sobre a confiança do processo eleitoral, em especial quanto às urnas eletrônicas [16][17][18][19].

Essa incerteza não ronda apenas a votação eletrônica. A desconfiança é uma das barreiras mais importantes à adoção de serviços eletrônicos, especialmente quando estão envolvidas informações pessoais ou financeiras [20]. Estudos sugerem que serviços públicos eficazes são influenciados pela confiança dos cidadãos relativamente à proteção e à privacidade de dados [21].

Sem uma definição única [22], a confiança pode ser caracterizada como a medida em que uma parte está disposta a depender da outra numa determinada situação com um sentimento de relativa segurança, mesmo que sejam possíveis consequências negativas [23]. Ainda segundo esses autores, esta definição reconhece que a confiança não pode existir sem risco, vez que é a presença das "consequências negativas" a motivação para que se construa a confiança ou a falta dela.

Muitos países, em vários continentes, tiveram iniciativas para utilização da votação eletrônica, sendo algumas bem sucedidas e sustentáveis, como Brasil, Índia e Estônia, e outras canceladas ou apenas parcialmente implementadas, como Alemanha, Holanda e Suíça [8].

Dessa forma, é compreensível a existência de questionamentos sobre as urnas eletrônicas no Brasil e há espaço demonstrar os mecanismos existentes atualmente que visam dar confiança ao processo eleitoral do país, além de propor iniciativas para aumentar a confiança nesses equipamentos, embasadas na análise dos critérios que afetam sua aceitação pela população.

1.1 Problema de pesquisa

Apesar de propiciar o aumento da segurança e da prevenção de fraudes, por reduzir a participação humana, a votação eletrônica também encontra desafios, tais como definem os autores de [24]:

1. falta de transparência e compreensão do sistema;
2. falta de padrões amplamente aceitos;
3. risco de fraude e manipulação por pessoas privilegiadas ou hackers;
4. aumento dos custos da infraestrutura de votação.

Verifica-se assim que os sistemas de votação eletrônica necessitam atender requisitos e funcionalidades capazes de demonstrar que os benefícios propiciados pelo uso da tecnologia superam os riscos envolvidos. Dentre estes, destacam-se a segurança, acurácia, garantia da privacidade, verificabilidade, auditabilidade e transparência, entre outros [25].

De acordo com a Justiça Eleitoral [13], a informatização do voto no Brasil é resultado dos esforços para possibilitar ao cidadão os meios necessários à plena manifestação da vontade popular, conferindo segurança, celeridade e confiabilidade ao processo eleitoral.

Nesse processo eletrônico de votação, apesar de ser apenas um dos componentes, o Tribunal Superior Eleitoral defende que a urna eletrônica tornou-se símbolo de democracia e transparência [13]. Contudo, visando eliminar vulnerabilidades que permitiam fraudes eleitorais, ainda antes da adoção do equipamento de votação, houve a digitalização do cadastro de eleitores e dos resultados dos boletins de urna, bem como a totalização eletrônica de todos os votos do país [26].

Porém, há questionamentos sobre a segurança do sistema, em que pese o reconhecimento das vantagens do uso tecnologia para a votação, tais como: (i) a maior precisão dos eleitores para escolher seus candidatos, a partir da exibição das fotos na tela da urna eletrônica; (ii) a redução da ambiguidade da interpretação do registro manual dos números pelo eleitor; e (iii) a agilidade na totalização dos resultados [18].

Em síntese, o processo eletrônico de votação no Brasil recebe críticas quanto à autenticação do eleitor, à segurança da urna eletrônica, à falta de um registro físico do voto e à confiança estar concentrada nas autoridades eleitorais [18].

Desses pontos de desaprovação, vale destacar o registro físico do voto, ou voto impresso. Motivo de intensos debates, sua adoção nas eleições brasileiras encontra idas e vindas desde as Eleições de 2002. Os apoiadores da impressão do voto defendem que seria uma medida eficaz para combater a necessidade de avaliar o hardware e software da urna eletrônica para gerar confiança nos resultados.

Esse cenário de questionamentos à confiança do processo eletrônico de votação, em especial da urna eletrônica, motiva pesquisar os fatores que influenciam a aceitação do equipamento de votação e pode auxiliar na proposição de medidas que aumentem a confiança na sua utilização e, por consequência, no processo como um todo.

A aceitação do uso de tecnologias é objeto de estudo na Academia desde os anos de 1970. Esses estudos resultaram na proposição de vários modelos que procuram explicar a adoção de tecnologia do ponto de vista do indivíduo [4].

Dentre os modelos existentes, os autores de [27] propuseram o *Unified Theory of Acceptance and Use of Technology (UTAUT)*, o qual sugere que a intenção de uso de uma tecnologia é definida pela expectativa de desempenho, expectativa de esforço, influência social e condições facilitadoras que ela traz, além de ter como variáveis moderadoras o gênero, idade, experiência e voluntariedade de uso dos indivíduos.

Os estudos indicam registros da aplicação do modelo UTAUT em outros países para avaliar a aceitação da tecnologia no cenário eleitoral. Na Coréia do Sul [28], foram avaliadas relações causais entre fatores que influenciam a aceitação de um sistema de votação

em um teste para uma primeira experiência do país com voto eletrônico. No Vietnã [29], o modelo foi utilizado para esclarecer o comportamento do usuário ao utilizar um serviço de votação remota. Em Gana [30], as variáveis do modelo foram utilizadas para pesquisar a confiança dos cidadãos na adoção de um sistema de votação eletrônica. No Chile [31], avaliou-se a aceitação da votação pela internet por estudantes de uma universidade local. Nos Estados Unidos [32], foram avaliados os fatores que afetam a intenção de votação online, dividindo-se os entrevistados entre jovens (18 a 25 anos) e idosos (acima de 60 anos). Na Índia [33], ampliou-se o modelo para avaliar a aceitação das urnas eletrônicas em uso no país.

Nesse cenário, é de grande valia examinar a aceitação das urnas eletrônicas pelos eleitores brasileiros para identificar quais variáveis mais impactam na confiança do uso desses equipamentos, bem como no interesse da adoção do voto impresso.

Considerando esse contexto, define-se a questão de pesquisa deste estudo: **Quais fatores influenciam a aceitação da urna eletrônica e o interesse em imprimir o voto nas eleições brasileiras?**

1.2 Justificativa

Considerando a tradição brasileira de realizar eleições desde 1532 [13], a confiança do processo eleitoral é fator de interesse da sociedade. O combate às fraudes, que há muito permeiam as eleições, motivou a informatização do processo eleitoral do país [12]. Dessa forma, ações que visem aumentar a confiança no processo eletrônico de votação do Brasil são bem recebidas e importantes para o país.

Desde a informatização, as fraudes foram reduzidas a tal ponto que não se tem registro de eventos que tenham comprometido nenhum pleito. Contudo, a base eletrônica do processo de votação torna mais difícil seu entendimento pela população e pode gerar desconfiança. Seja uma dúvida legítima ou resultado de uma manipulação, como as recentes *fake news*, quanto mais informações disponíveis menor o espaço para desinformação e questionamentos.

Por isso, aplicar um modelo reconhecido e aceito pela comunidade acadêmica como o UTAUT, para avaliar a aceitação do uso das urnas eletrônicas no contexto eleitoral brasileiro, além de ampliar o campo de aplicação do modelo teórico, auxilia a identificar os fatores que influenciam a confiança da população nos equipamentos, bem como quais ações podem ser tomadas para aumentar a confiabilidade.

Do ponto de vista da Justiça Eleitoral, conhecer os fatores que influenciam a confiança das urnas eletrônicas, bem como receber propostas para direcionar os recursos e esforços no sentido de aprimorar os níveis de confiança, é de extrema relevância para cumprir sua

missão, qual seja: "*Promover a cidadania e garantir a legitimidade do processo eleitoral e a efetiva prestação jurisdicional, a fim de fortalecer a democracia*" [34].

1.3 Objetivos

1.3.1 Objetivo Geral

Este trabalho tem por objetivo propor etapas para melhorar a aceitação da urna eletrônica no Brasil, a partir da identificação das propriedades formadoras da confiança em sistemas de votação eletrônica.

1.3.2 Objetivos Específicos

Para se atingir o objetivo geral, esse trabalho compreende os seguintes objetivos específicos:

1. Levantar as principais abordagens e a evolução das pesquisas recentes sobre a votação eletrônica.
2. Identificar fatores que influenciam a confiança em sistemas eletrônicos de votação.
3. Descrever o processo eletrônico de votação brasileiro.
4. Analisar as variáveis que impactam na aceitação da urna eletrônica no Brasil.
5. Avaliar a relação de importância e desempenho das variáveis que impactam na aceitação da urna eletrônica no Brasil.

1.4 Estrutura do Trabalho

Este trabalho tem o total de oito capítulos, sendo que o primeiro foi esta introdução. O conteúdo dos demais é descrito a seguir:

- **Capítulo 2:** apresenta a revisão bibliográfica, realizada com o auxílio da Teoria do Enfoque Meta Analítico (Temac) para levantar as publicações e informações mais relevantes sobre a votação eletrônica. Com a utilização de índices bibliométricos, são apresentadas informações da preparação da pesquisa, da evolução das publicações sobre o tema ao longo dos anos e das publicações mais relevantes.
- **Capítulo 3:** apresenta a revisão da literatura a respeito da evolução das eleições, das tecnologias eleitorais e dos requisitos dos sistemas eletrônicos de votação, bem como dos fatores que influenciam a confiança na votação eletrônica.

- **Capítulo 4:** descreve o processo eletrônico de votação brasileiro, apresentando sua estrutura, funções e processo.
- **Capítulo 5:** detalha o modelo lógico e as hipóteses adaptadas do modelo original e aborda a aceitação das urnas eletrônicas no Brasil.
- **Capítulo 6:** aborda a metodologia de pesquisa utilizada, apresentando o tipo, dados do local e objeto da pesquisa.
- **Capítulo 7:** fornece as informações das análises e resultados obtidos com a aplicação da pesquisa.
- **Capítulo 8:** apresenta as considerações finais e as sugestões para trabalhos futuros.

Capítulo 2

Revisão do Estado da Arte

Nesse estudo foi utilizada a abordagem Temac proposta por [35]. A metodologia é composta por três etapas:

1. **Preparação da pesquisa**: realizada previamente, busca-se definir o descritor (*string*) ou palavra-chave mais adequada e estabelecer o período de tempo, as bases de dados e as áreas do conhecimento a serem utilizadas na pesquisa;
2. **Apresentação e inter-relação dos dados**: a partir dos resultados encontrados, há inúmeras opções de informações a serem exibidas tais como períodos que mais publicam sobre o tema, evolução ano a ano, documentos mais citados, autores que mais publicaram versus autores que mais foram citados, universidades e países que mais publicaram e a frequência de palavras chaves;
3. **Detalhamento, modelo integrador e validação por evidências**: de posse das informações levantadas, a análise é aprofundada visando uma melhor compreensão sobre o tema pesquisado.

O software bibliométrico *VOSViewer* foi utilizado como ferramenta para criar os mapas de calor e viabilizar análise das redes de ocorrência de palavras, citação e cocitação e acoplamento bibliográfico dos dados encontrados na literatura científica relacionada. As informações utilizadas para criação dos mapas foram extraídas das bases de pesquisa *Web of Science (WoS)* e *Scopus*.

2.1 Preparação da Pesquisa

2.1.1 Bases de dados utilizadas

Nesse estudo, foram utilizadas as bases de publicações científicas *WoS* e *Scopus*, em função de serem bem conceituadas nas diversas comunidades acadêmicas internacionais, possuírem grande quantidade, representatividade e qualidade dos documentos registrados [35].

As bases *Institute of Electrical and Electronic Engineers* (IEEE) e *Google Scholar* tiveram sua utilização avaliadas mas foram descartadas. A primeira, *IEEE*, porque os artigos relacionados ao tema estavam contemplados na *WoS* e *Scopus* e a segunda, por problemas na indexação das publicações.

2.1.2 Termo de pesquisa

A pesquisa foi realizada procurando-se a *string* (*"e-voting" or "voting machine"*) no título, resumo ou palavras-chave dos documentos contidos nas referidas plataformas de publicações científicas.

Importante destacar que originalmente o termo *"e-voting"* refería-se a votação eletrônica de maneira ampla. Porém, com o crescimento da internet, começa a ganhar mais relevância a utilização do termo para soluções de votação *online*, uma espécie do gênero votação eletrônica. Em que pese esse indicativo de restrição à amplitude do termo, ele foi considerado ainda representativo para a essa pesquisa. Adicionalmente, o termo *"voting machine"* refere-se aos equipamentos utilizados nas votações, uma outra abordagem para contemplar o voto eletrônico. Ao utilizar o conector *"or"*, os resultados foram somados, aumentando a cobertura do tema.

Considerando a adoção da votação eletrônica no Brasil em 1996, utilizou-se essa referência para início do período de tempo da pesquisa, cobrindo até abril de 2023. Assim, a pesquisa contemplou a produção científica sobre o tema durante todo o período de utilização das urnas eletrônicas no país. Adicionalmente, a pesquisa restringiu-se a publicações realizadas na lingua inglesa ou portuguesa.

Como resultado, foram encontrados 1.133 registros na *WoS* e 3.806 na Scopus. A pesquisa abrangeu artigos, conferências, *preceeding papers*, *reviews* e capítulos de livros sem delimitar as áreas de conhecimento, de modo a atingir uma ampla cobertura do assunto pesquisado.

2.2 Apresentação dos dados e interrelações

Existem inúmeras maneiras de apresentar os dados e suas interrelações obtidos na pesquisa. Entretanto, alguns resultados que se repetem nas pesquisas de enfoque meta-analítico e, por isso, são esperados por pesquisadores e editores em geral [35]. Esses resultados são apresentados a seguir.

2.2.1 Registro mais antigo

Publicado em 1998, na revista *Proceedings 14th Annual Computer Security Applications Conference*, com o título *"Anonymous secure e-voting over a network"*, [36] é o artigo mais longevo encontrado na *WoS*. Tratava-se de uma proposta inovadora à época de dois novos esquemas de votação eletrônica que protegem a privacidade dos eleitores e evitam o voto duplo pelo eleitor. Os esquemas eram baseados no algoritmo de assinatura digital ElGamal e não exigiam nenhum canal de votação especial, podendo ser implementados em redes existentes, como a Internet.

Na *Scopus*, foram encontrados 4 artigos no ano de 1996, a Tabela 2.1 a seguir apresenta os detalhes dessas publicações.

Título	**Assunto**
Optimal batch service of a polling system under partial information [37]	O artigo propunha uma solução para o escalonamento ótimo de um servidor batch de capacidade infinita em uma rede de filas em anel com N nós, onde o controlador apenas observava o comprimento da fila em que o servidor estava localizado. A solução proposta envolvia políticas de escalonamento limiar e provava a otimalidade e monotonicidade dessas políticas. O critério de custo incluia custos lineares de manutenção, custos fixos de despachar e recompensas de serviços lineares. O artigo era motivado por vários sistemas, incluindo sistemas de informação, sistemas de votação, sistemas de transporte e sistemas de veículos guiados automaticamente com estações dispostas em um anel.

Continua na próxima página

Tabela 2.1 – continuação da página anterior

Título	Assunto
An implementable secure voting scheme [38]	O trabalho apresentava um esquema de votação eletrônica para garantir a privacidade das cédulas utilizando polinômios. Cada cédula era representada como um erro introduzido aleatoriamente em uma sequência de valores obtidos a partir desses polinômios. A contagem das cédulas equivalia a detectar esses erros, interpretá-los e torná-los públicos. O esquema permitia qualquer comportamento do eleitor, ao contrário de outros esquemas que usavam canais anônimos, os quais normalmente não permitiam que os eleitores se abstivessem. O artigo descrevia as diferentes fases de votação junto com os algoritmos que as controlavam. A segurança do esquema era baseada principalmente na integridade dos algoritmos utilizados na votação. O esquema atendia a todos os requisitos da definição de esquema seguro fornecida no documento e podia ser implementado em qualquer protocolo confiável da camada de transporte, por exemplo o *Transmission Control Protocol* da Internet.
Deriving consensus in multiagent systems [39]	O artigo discutia pesquisas sobre como criar ambientes em que agentes automatizados podiam trabalhar juntos de forma eficaz. O foco estava em como os agentes podiam chegar a um consenso sem revelar todas as suas preferências ou gerar alternativas antes do processo de votação. O artigo também discutia a importância de projetar sistemas de solução de problemas que pudessem lidar efetivamente com domínios difíceis, incluindo aqueles em que a distribuição era uma característica inata do próprio sistema.

Continua na próxima página

Tabela 2.1 – continuação da página anterior	
Título	**Assunto**
A collision-free secret ballot protocol for computerized general elections [40]	O artigo discutia vários esquemas de votação criptográfica propostos por diferentes pesquisadores. O objetivo desses esquemas era garantir que todas as cédulas dos eleitores elegíveis fossem contadas corretamente e que o resultado da eleição não pudesse ser manipulado pela autoridade eleitoral. No entanto, cada esquema tinha suas próprias limitações e desafios. Alguns esquemas preservavam a privacidade dos eleitores, mas não eram verificáveis, enquanto outros eram mais adequados para eleições em grande escala, mas exigiam que todos os eleitores registrados votassem. No geral, o artigo fornecia uma visão geral dos desafios e limitações dos esquemas de votação criptográfica e destacava a necessidade de mais pesquisas nessa área.

Tabela 2.1: Artigos de 1996 - *Scopus* (Fonte própia)

Conhecidas as publicações mais antigas, apresenta-se agora a evolução das publicações sobre o tema da pesquisa ao longo dos anos.

2.2.2 Evolução do tema ano a ano

Em relação à evolução da quantidade de publicações, a Figura 2.1, apresenta o número de publicações na *WoS*, desde 1998. Verifica-se um aumento no número de publicações a partir do ano de 2003, atingindo-se o maior número em 2019. Considerando todo o período, obtém-se uma média de 45 publicações por ano, com uma clara tendência de crescimento.

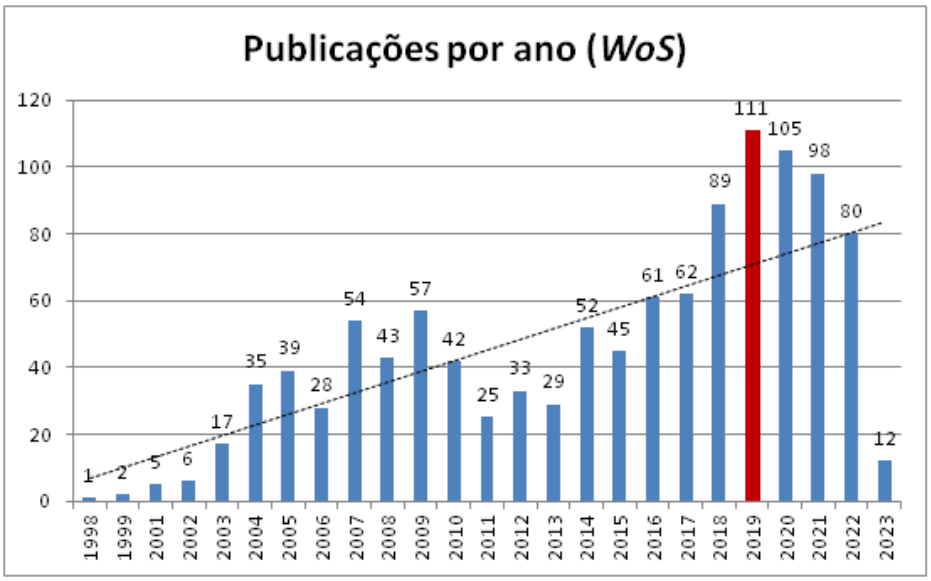

Figura 2.1: Evolução das publicações – *WoS* (Fonte própria)

A base da *Scopus*, a Figura 2.2, registra as primeiras publicações no ano de 1996.

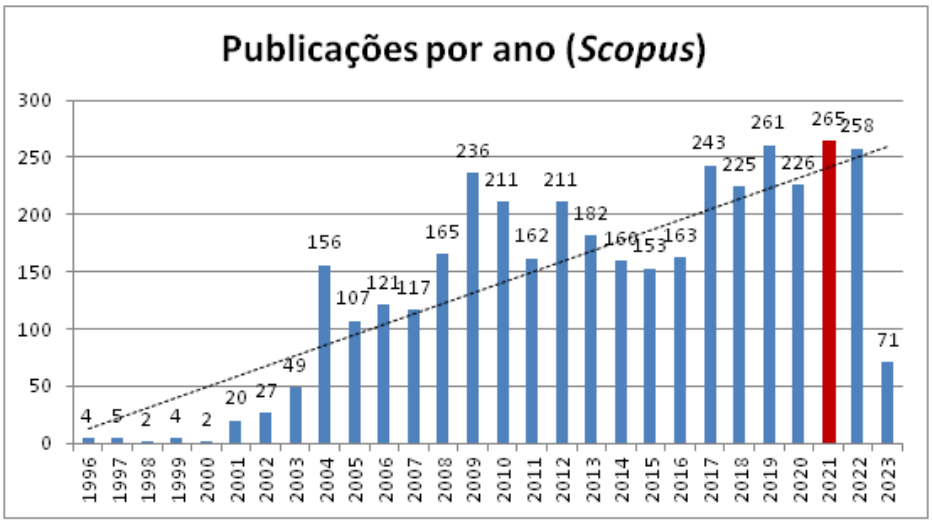

Figura 2.2: Evolução das publicações – *Scopus* (Fonte própria)

Nesta plataforma, o aumento no número de publicações acontece a partir de 2001, com o pico em 2021 e média de 135 publicações por ano, também com uma clara tendência de crescimento.

2.2.3 Autores e artigos mais citados

Quanto aos autores, os mais citados constam da Tabela 2.2. Há significativa diferença entre os resultados encontrados nas bases de pesquisa. Na *WoS*, destacam-se Hao, F. e

Shahandashti, S. F. com mais de 200 citações. Por outro lado, na *Scopus*, Ryan, P.Y.A, Chaum, D e Rivest, R.J. foram citados mais de 800 vezes.

WoS		***Scopus***	
Autor	**Qtde. citações**	**Autor**	**Qtde. citações**
Hao, F.	232	Ryan, P.Y.A.	999
Shahandashti, S. F.	212	Chaum, D.	840
Wei, V. K.	194	Rivest, R.J.	818
Mccorry, P.	192	Jakobsson, M.	640
Arnott, R. D.	174	Juels, A.	637
Hsu, J.	174	Kremer, S.	596
Moore, P.	174	Wallach, D.S.	570

Tabela 2.2: Autores mais citados (Fonte própria)

Em relação aos artigos, os 5 mais citados na *WoS* estão listados na Tabela 2.3 abaixo.

Título	**Autores**	**Ano**	**Total de citações**	**Citações por ano (média)**
A Smart Contract for Boardroom Voting with Maximum Voter Privacy [41]	McCorry, Patrick; Shahandashti, Siamak F.; Hao, Feng.	2017	192	27,43
Fundamental indexation [42]	Arnott, R.D.; Hsu, J.; Moore, P.	2005	174	9,16
Deep Learning-Based Image Segmentation on Multimodal Medical Imaging [43]	Guo, Zhe; Li, Xiang; Huang, Heng; Guo, Ning; Li, Quanzheng.	2019	140	28
Blockchain-Enabled E-Voting [44]	Kshetri, Nir; Voas, Jeffrey.	2018	133	22,17

Continua na próxima página

Tabela 2.3 – continuação da página anterior				
Título	**Autores**	**Ano**	**Total de citações**	**Citações por ano (média)**
Examining health literacy disparities in the United States: a third look at the National Assessment of Adult Literacy (NAAL) [45]	Hjalmarsson, Fridrik Th.; Hreidarsson, Gunnlaugur K.; Hamdaqa, Mohammad; Hjalmtysson, Gisli.	2016	116	14,50

Tabela 2.3: 5 artigos mais citados - *WoS* (Fonte Própria)

Em [41], os autores propuseram uma solução para o problema da votação segura e privada pela internet usando a tecnologia *blockchain*. Eles apresentam a *Open Vote Network*, um protocolo de votação pela internet descentralizado e com contagem automática que garante a máxima privacidade do eleitor. O protocolo é implementado como um *smart contract* para o *Ethereum* e não depende de nenhuma autoridade confiável para computar a contagem dos votos ou proteger a privacidade do eleitor. O mecanismo de consenso aplicado é o mesmo do *Ethereum*. Os autores testaram a implementação na rede oficial de testes da *Ethereum* para demonstrar sua viabilidade e forneceram uma análise financeira e computacional de seu custo de execução. Em trabalhos futuros, os autores propuseram investigar a viabilidade de realizar uma eleição em escala nacional utilizando *blockchain*.

Os autores do artigo [42] identificaram que os portfólios de mercado tradicionais construídos usando o limite de peso podem não ser a maneira mais eficiente de investir no mercado de ações. Eles propuseram um novo método de construção de portfólios com base nas medidas da *Main Street* sobre o tamanho da empresa, como valor contábil, receitas e dividendos. Os portfólios resultantes superaram o S&P 500 em uma média de 1,97 pontos por ano durante o período de 43 anos testado. Os autores concluíram que os índices construídos usando medidas da *Main Street* sobre o tamanho da empresa são significativamente melhores do que os índices de *Wall Street* ponderados pelo limite máximo. O artigo menciona uma citação de Benjamin Graham que descreve o mercado de ações como uma urna de votação no curto prazo e uma máquina de pesagem no longo prazo. Essa citação sugere que, no curto prazo, o mercado de ações é influenciado pela opinião e pelo sentimento populares, mas no longo prazo, o verdadeiro valor de uma empresa se

reflete no preço de suas ações. No entanto, essa citação não está diretamente relacionada ao tópico principal do artigo.

Em [43], os autores propunham um sistema de segmentação de imagens baseado em *deep learning* que congrega informações de ressonância magnética, tomografia computadorizada e tomografia por emissão de pósitrons. O estudo demonstrou que a rede treinada com imagens multimodais apresenta desempenho superior em comparação com redes treinadas com imagens monomodais. Os autores descobriram que realizar a fusão de imagens na rede geralmente é melhor do que fundir imagens na saída da rede (ou seja, votação). Portanto, o artigo sugere que a fusão de imagens dentro da rede é uma abordagem melhor do que votar nessa tarefa específica. Como se observa, o trabalho não guarda relação direta com processos ou sistemas de votação.

O trabalho [44] propunha o uso da tecnologia *blockchain* como solução para reduzir a fraude eleitoral e aumentar o acesso dos eleitores em processos eletrônicos de votação. Os autores sugerem que um *blockchain* poderia transferir o poder das autoridades eleitorais para o eleitor. No entanto, eles registram a tecnologia ainda estava em um estado incipiente e não havia aplicativos baseados em *blockchain* suficientes para avaliar se essa tecnologia era superior aos sistemas de votação em uso.

O estudo [45] examinou a relação entre desigualdades sociais e alfabetização em saúde nos Estados Unidos. O estudo usou dados da Avaliação Nacional de Alfabetização de Adultos (NAAL) de 2003 para analisar o impacto de vários indicadores de desigualdades sociais na alfabetização em saúde. Os resultados do estudo sugeriam que as desigualdades sociais estão intimamente ligadas às disparidades na alfabetização em saúde. Indicadores objetivos de status social, como renda e educação, são fortes preditores de alfabetização em saúde. No entanto, o estudo também destacava a importância do status social relacional, como o engajamento cívico, na compreensão das disparidades de alfabetização em saúde. O estudo sugeria que intervenções destinadas a melhorar a alfabetização cívica, como promover o voto e o voluntariado, poderiam ajudar a melhorar os níveis de alfabetização em saúde.

A Tabela 2.4 apresenta os 5 artigos mais referenciados na Scopus.

Título	**Autores**	**Ano**	**Total de citações**	**Citações por ano (média)**
Examining the benefits and challenges of using audience response systems: A review of the literature [46]	Kay, R.H.; LeSage, A.	2009	444	31,71
BPMN: An introduction to the standard [47]	Chinosi, M.; Trombetta, A.	2012	420	38,18
Characterizing e-participation in policy-making [48]	Macintosh, A.	2004	387	20,36
A verifiable secret shuffle and its application to E-voting [49]	Andrew, Neff C.	2001	367	16,68
Real-time line detection through an improved Hough transform voting scheme [50]	Fernandes, Leandro A.F.; Oliveira, Manuel M.	2008	354	23,60

Tabela 2.4: 5 artigos mais citados - *Scopus* (Fonte Própria)

Na publicação [46], foram estudados 67 artigos revisados por pares, de 2000 a 2007, para identificar os benefícios e desafios associados ao uso de sistemas de resposta do público na sala de aula. Eles descobriram que tais sistemas podem melhorar o ambiente da sala de aula, o aprendizado e a avaliação, mas os professores enfrentam desafios para aprender e configurar a tecnologia, criar perguntas eficazes e responder ao feedback dos alunos. O uso desses sistemas na sala de aula, permite que os alunos respondam a perguntas de múltipla escolha usando um dispositivo de controle remoto. As respostas são apresentadas instantaneamente em forma de gráfico e revisadas pelo instrutor e pela turma. Embora o artigo não mencione especificamente a votação, o uso desse tipo de sistema pode ser visto como uma forma de votação, pois os alunos têm a oportunidade de expressar suas opiniões e preferências sobre vários tópicos. No entanto, o foco do artigo está nos benefícios

e desafios do uso de sistemas de resposta do público na sala de aula e não em votação em si.

Já em [47], os autores fornecem uma visão geral do padrão *Business Process Model and Notation (BPMN)*, utilizado para representar processos de negócios de maneira gráfica. Eles discutem a evolução do BPMN, sua adoção como padrão em 2006, bem como as diferenças em relação a outros padrões. Ainda, o estudo menciona brevemente que o BPMN pode ser usado para modelar vários tipos de processos, incluindo sistemas de votação por e-mail. No entanto, não fornece detalhes de eventual uso do BPMN no contexto dos processos de votação.

Em [48], a autora argumentava que é necessário consolidar os resultados das primeiras iniciativas, experimentais ou não, bem como as pesquisas existentes sobre democracia eletrônica para entender melhor seus benefícios. Ela propunha uma estrutura analítica que poderia ajudar a identificar a tecnologia apropriada para apoiar diferentes tipos de exercícios de participação cidadã. A estrutura considerava o nível de participação, a tecnologia usada, o estágio do processo de formulação de políticas, entre outras questões e restrições. A autora sugeria ainda que essa estrutura poderia demonstrar como as tecnologias contribuíram para processos democráticos específicos, assim como descrever as condições sob as quais as melhores práticas podem emergir.

No trabalho [49], foi proposto um protocolo criptográfico para embaralhar uma sequência de números inteiros modulares de maneira que a ordem dos elementos na saída seja mantida em segredo. Esse protocolo poderia ser usado em esquemas eleitorais para garantir uma votação segura e universalmente verificável. O protocolo proposto fornecia uma prova de tamanho linear de exatidão para a sequência de saída que poderia ser verificada por qualquer verificador. A proposta seria menos complexa que os protocolos existentes à época. Os autores forneciam uma aplicação do protocolo proposto à votação eletrônica que combinava com as características dos melhores protocolos da época, mas mais eficiente.

Voltado para a análise de imagens, [50] propunha um esquema de votação aprimorado que poderia alcançar desempenho em tempo real mesmo em imagens relativamente grandes. Utilizando a *Hough transform (HT)* como ferramenta para detecção de linha, o custo computacional era muito alto, o que impediu que as implementações de software atingissem desempenho em tempo real. A abordagem proposta operava em agrupamentos de *pixels* e aplicava técnicas quem modelam a incerteza associada à linha de melhor ajuste. Essa abordagem melhorava significativamente o desempenho e produzia um resultado muito mais limpo e tornava a transformação mais robusta para a detecção de linhas espúrias. No contexto deste trabalho, a relação com a votação está no esquema utilizado na HT para detecção de linhas.

2.2.4 Países

Os 15 países nos quais houve o maior número de publicações sobre o tema pesquisado estão representados nas Figuras 2.3 e 2.4, WoS e *Scopus*, respectivamente.

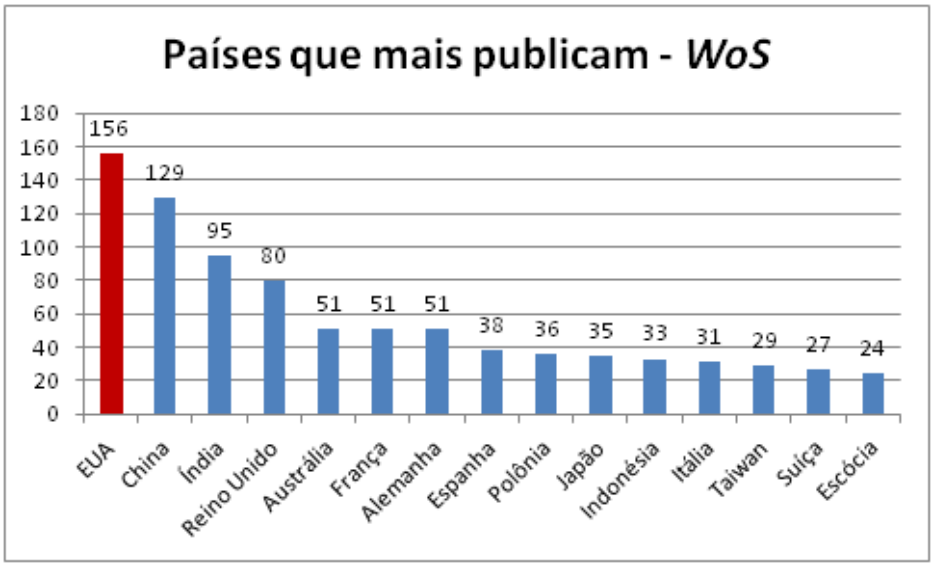

Figura 2.3: Publicações por países - *WoS* (Fonte própria)

Em ambas plataformas, os Estados Unidos figuram em primeiro lugar, tendo China e Índia em segundo e terceiro, mas essas duas com posições invertidas em cada base de dados. O Reino Unido tem a quarta posição nas duas bases e também ocorre mudança de posição entre o quinto, sexto, sétimo e oitavo lugares. A depender da plataforma, Austrália, França, Alemanha e Espanha alternam posições.

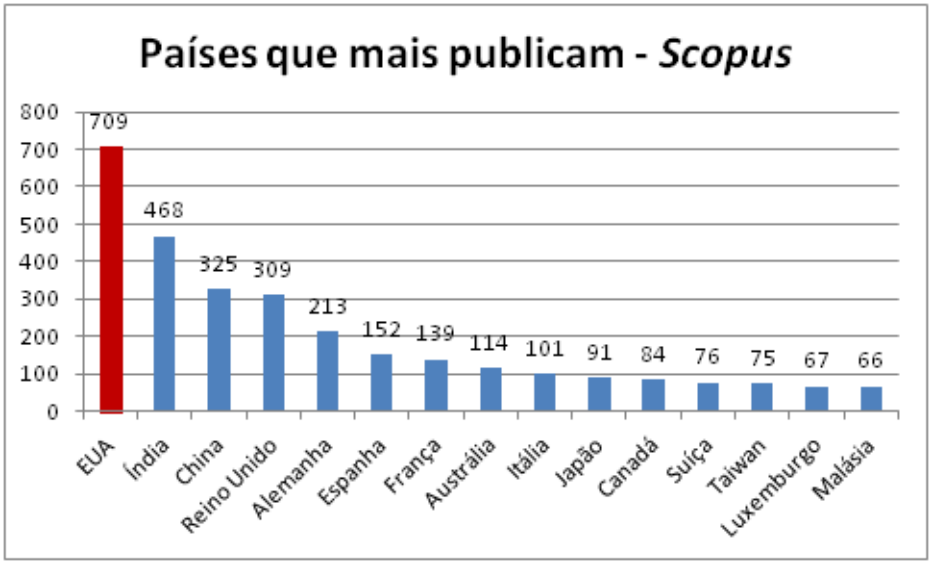

Figura 2.4: Publicações por países - *Scopus* (Fonte própria)

O Brasil possui 11 publicações na *WoS*, ocupando a 32ª posição entre os 84 países com publicações sobre o tema. Na *Scopus*, o país registra 46 publicações, o que resulta na 23ª posição entre 101 países identificados. Cabe salientar que 58 documentos na base da *WoS* e 259 na *Scopus* não possuem a informação do país de origem da publicação.

2.2.5 Universidades

Outra forma de se analisar os resultados da pesquisa é por meio da avaliação das universidades que mais publicaram sobre o tema. As Figuras 2.5 e 2.6 detalham as com maior quantidade de documentos publicados na *WoS* e *Scopus*, respectivamente.

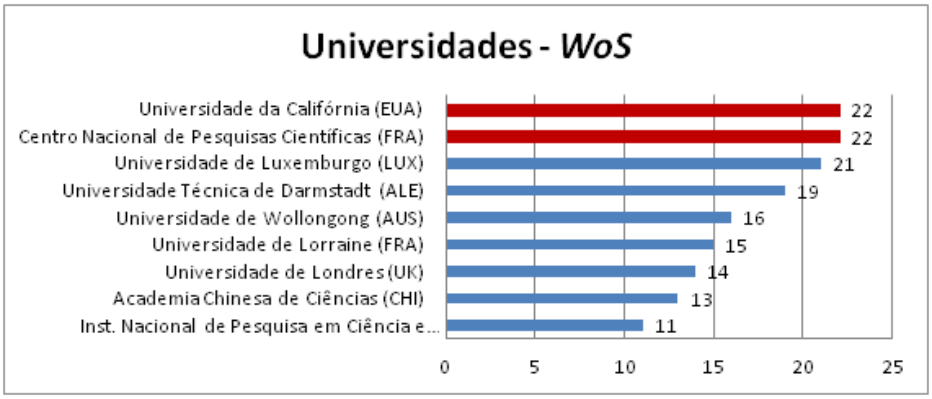

Figura 2.5: Universidades que mais publicaram - *WoS* (Fonte própria)

Na plataforma *WoS*, a norte americana Universidade da Califórnia foi a que mais publicou sobre o tema, seguida pelo Centro Nacional de Pesquisas Científicas da França e da Universidade de Luxemburgo.

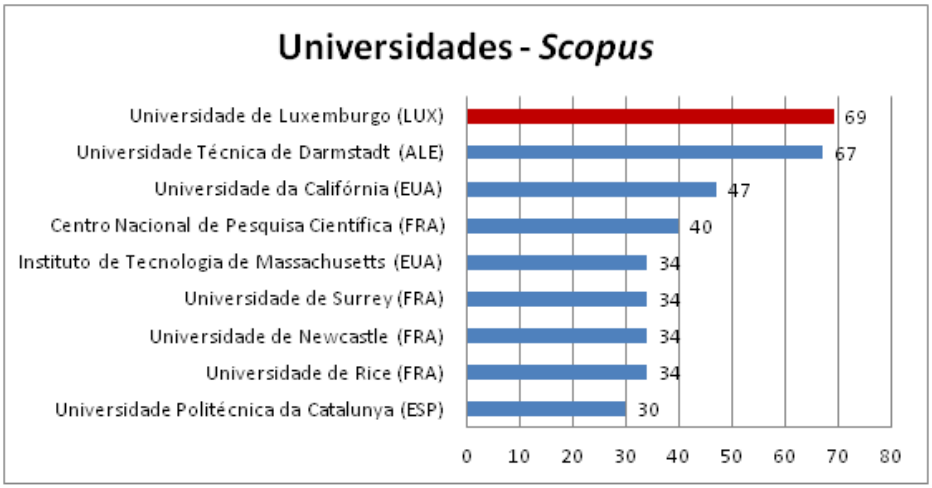

Figura 2.6: Universidades que mais publicaram - *Scopus* (Fonte própria)

Na *Scopus*, a Universidade de Luxemburgo foi a de maior produção científica, seguida pela Universidade Técnica de Darmstadt, da Alemanha, e pela Universidade da Califórnia do EUA.

2.2.6 Áreas de conhecimento

Com base nos termos da pesquisa, a principal área de conhecimento relacionada ao tema foi a Ciência da Computação com 869 ocorrências na plataforma *WoS* e 3080 na *Scopus*, conforme Figuras 2.7 e 2.8 a seguir.

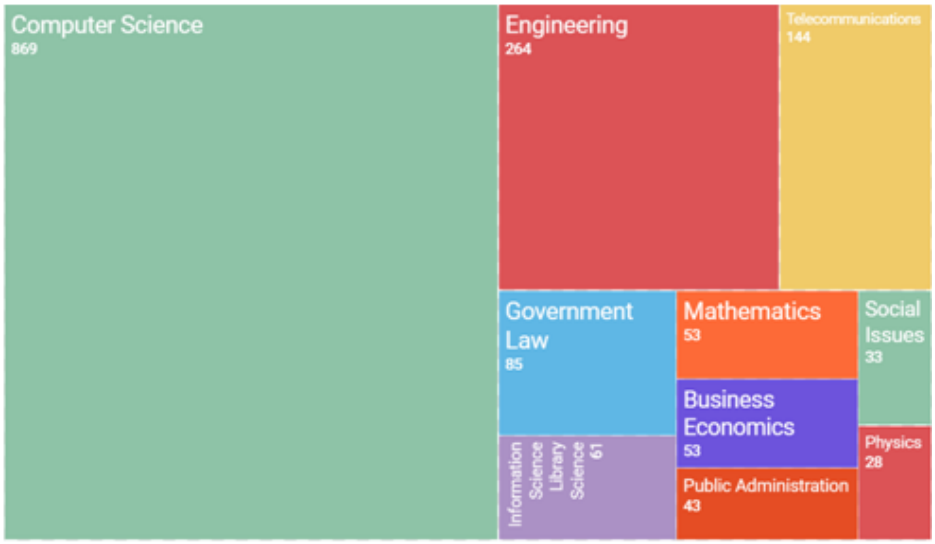

Figura 2.7: Áreas de conhecimento - *WoS* (Fonte própria)

A Figura 2.7 apresenta o detalhamento das demais áreas de conhecimento mais relevantes na *WoS*. Nessa plataforma, além da Ciência da Computação, destacaram-se a área de Engenharia com 264 registros, de Telecomunicações com 144 e de Leis governamentais, 85.

Em se tratando da *Scopus*, as demais áreas que se sobressaíram foram a Engenharia com 1253 ocorrências, a Matemática e as Ciências sociais com 996 e 728, respectivamente, conforme Figura 2.8.

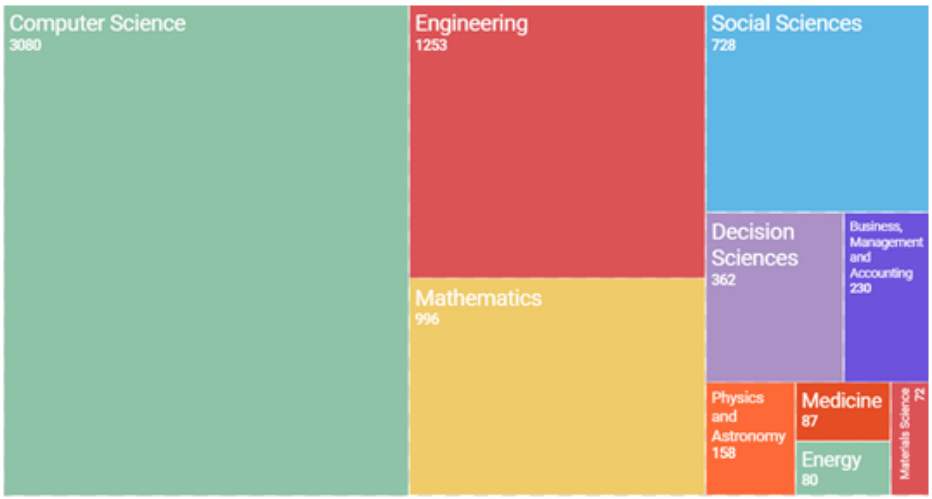

Figura 2.8: Áreas de conhecimento - *Scopus* (Fonte própria)

Vale salientar que um mesmo documento pode se referenciar a mais de uma área de conhecimento em ambas as plataformas.

2.2.7 Palavras-chave

A análise da frequência das palavras-chave permite avaliar a evolução da pesquisa sobre tema ao longo do tempo. Dessa forma, é possível observar como as diferentes abordagens progrediram e identificar por quais alterações as linhas de pesquisa passaram.

As palavras-chave mais significativas na *WoS* foram: *blockchain*, privacidade (*privacy*) e segurança (*security*). A aplicação destes termos será detalhada na sequencia. Salienta-se que foram desconsideradas nessa análise de frequencia as palavras-chave semelhantes aos termos da pesquisa original, tais como "*e-voting*", "*eletronic voting*" e "*e-voting system*".

Em função das suas características de transparência, imutabilidade, alta disponibilidade, confiabilidade e auditabilidade [51][52], o *blockchain*, Figura 2.9, é referenciado na plataforma da *WoS*, pela primeira vez, em 2008, como uma ferramenta capaz de aumentar a confiança na eleição [53]. Entretanto, é a partir de 2016 que aumenta a produção científica ao registrar propostas de desenvolvimento de protocolos de votação seguros, transparentes, verificáveis e eficientes [54][55][56], inclusive com suporte a criptografia pós-quântica [57][58].

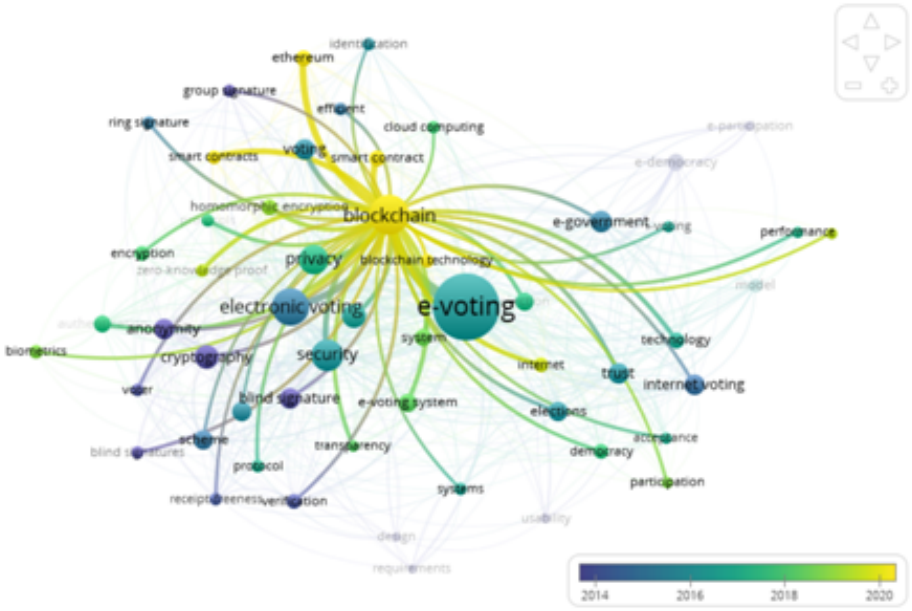

Figura 2.9: Palavra chave - *WoS* - *Blockchain* (Fonte própria)

A depender da gestão da estrutura, [59] defende que a tecnologia do *blockchain* pode reforçar o papel da autoridade eleitoral, ou empoderar os eleitores a ponto de suprimir a necessidade do órgão gestor da eleição [60][61]. Em relação a arquitetura, há registros de aplicações desenvolvidas utilizando a estrutura privada, como o *Hyperledger* [62][63], ou pública, como o *Etherium* [41][64][65], sendo esta última a mais referenciada.

Ainda, a maior parte das publicações propõem soluções testadas em laboratórios, mas há registro da aplicação do *blockchain* em eleições na Coreia do Sul [44], Turquia [66], Africa do Sul [67], Iraque [68] e Estônia [69], ainda que de maneira restrita.

No entanto, autores como [6][70], destacam problemas que ainda precisam ser resolvidos no uso da tecnologia como autenticação remota, anonimato e verificabilidade de ponta a ponta, entre outros. Também há de se atentar para a eficiência da operação do *blockchain* como alertam [71] e [72].

Mais recentemente, existem publicações referenciando a utilização da tecnologia *blockchain* em conjunto com biometria [73], equipamentos de votação adequados à *Internet of Things (IoT)* [74] e Inteligência artificial [75], para aprimorar ainda mais os aspectos de segurança das soluções de votação eletrônica.

Por fim, salienta-se as revisões de literatura realizadas em 2018 [76], 2020 [77] e 2022 [78]. Também merece destaque o impulsionamento à utilização de soluções remotas para votação, em função da pandemia de Covid19 [79].

A segunda palavra-chave mais significativa na *WoS*, privacidade (*privacy*), Figura 2.10, é abordada como uma característica essencial de um sistema de votação [7][80]. Sua primeira referência é datada de 1998 [36], quando os autores a conceituam como um

requisito de segurança dos mais importantes, ao representar a garantia de que o voto do eleitor tem de ser privado e anônimo.

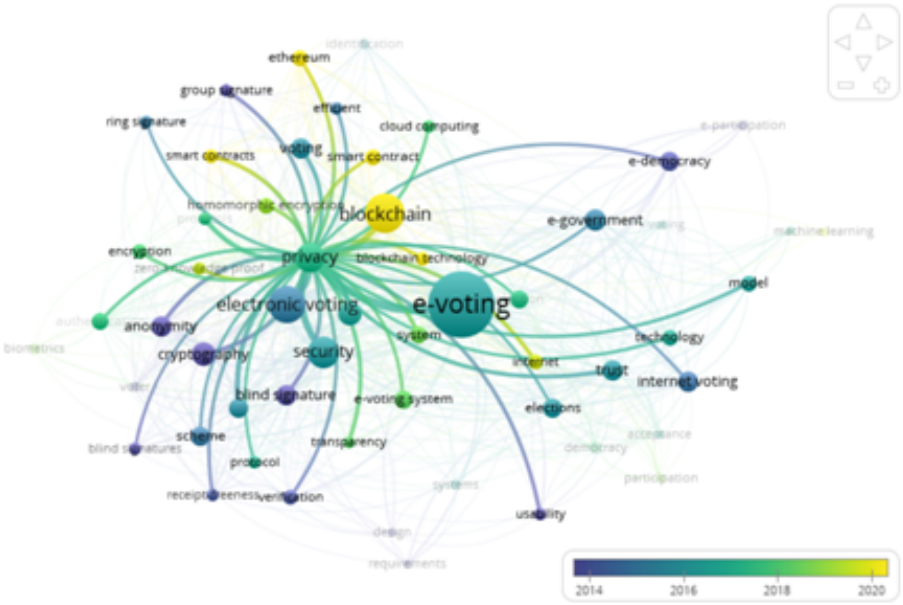

Figura 2.10: Palavra chave - *WoS* - *Privacy* (Fonte própria)

Em relação a sua vigência, [81] define a privacidade eterna (*everlasting*) como aquela resistente mesmo a um adversário computacionalmente ilimitado. Por outro lado, a capaz de resistir a ataques conhecidos atualmente é conhecida como privacidade imediata [82].

Os autores de [83] e [84] apresentam a verificabilidade como a característica dos protocolos/sistemas de votação que demonstram a privacidade. Nesse sentido, [85] conceitua dois tipos de verificabilidade: a individual e a universal. A individual significa que cada voto seja contado corretamente e que qualquer tentativa de manipular a contagem seja detectada. A universal significa que qualquer pessoa, incluindo terceiros que não participam da eleição, pode verificar a exatidão da contagem dos votos.

Quanto às técnicas utilizadas para se construir a verificabilidade da votação eletrônica, destaca-se a criptografia. A ferramenta é aplicada nas mais variadas formas, seja a assinatura cega (*blind signature*) [86][87], a homomórfica [88][89], no fornecimento de provas de conhecimento zero (*Zero Knowledge Proof (ZKP)*) [90][91] ou no embaralhamento das *mix nets* [92][93]. Todavia, há publicações que também citam a impressão do voto [94], a identificação biométrica do eleitor [95][96], o *blockchain* [41][59][64] e a abertura do código-fonte [97] como técnicas capazes aumentar o poder de verificação da corretude da eleição, e assim garantir a privacidade.

Os autores de [98] destacam ainda o *trade-off* entre a verificabilidade e a anonimicidade. Enquanto o anonimato exige a desvinculação do eleitor com o voto, a verificabilidade

demanda a vinculação dos eleitores e o resultado da eleição. Na busca por melhor equalizar essa relação, desenvolveu-se o método de votação fim a fim ou *End-to-End (E2E)* [99][100][101]. Nesse protocolo, o eleitor é capaz de verificar que seu voto foi registrado corretamente pelo equipamento de votação, na mesma medida em que consegue ter a certeza de que seu voto consta íntegro na totalização.

Por fim, [31][102] apresentam a privacidade como uma característica determinante na formação da percepção de confiança na tecnologia, uma das variáveis que influenciam a inteção de uso da votação eletrônica pelos eleitores.

A segurança (*security*), terceira palavra-chave mais relevante na *WoS*, Figura 2.11, tem seu primeiro registro para o período pesquisado em 2002, quando o autor discute o uso da votação eletrônica como meio de aprimorar os processos democráticos nas sociedades da informação modernas e identifica os requisitos de um sistema adequadamente seguro [103].

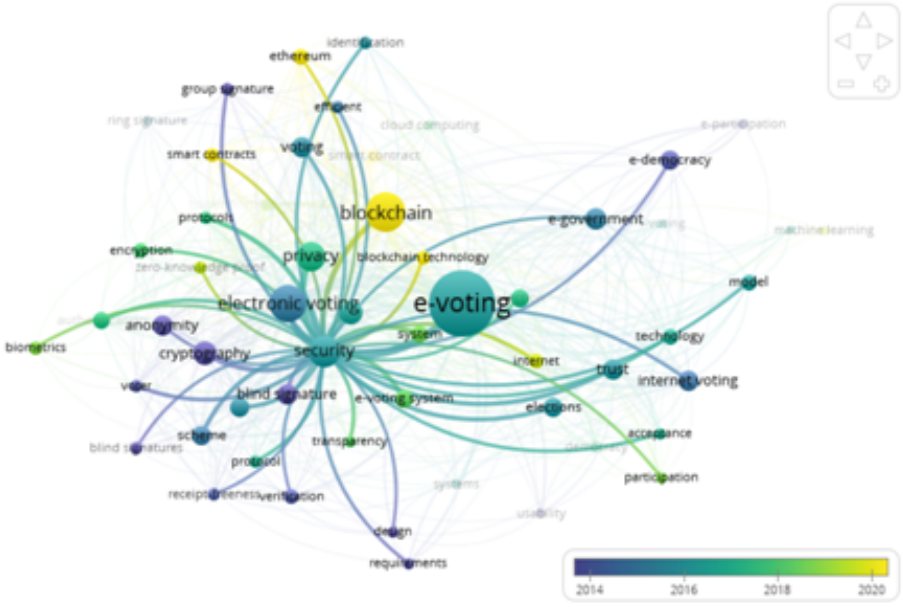

Figura 2.11: Palavra chave - *WoS* - *Security* (Fonte própria)

Assim como a privacidade, a segurança é apresentada como uma característica essencial de um sistema de votação eletrônica [104]. Em função dessa similaridade, aplicam-se à segurança as mesmas técnicas registradas anteriormente. Entretanto, há um destaque maior ainda à criptografia [105][106], em especial as resistentes aos computadores quânticos [107][108][109]. Interessante também são as referências ao uso do reconhecimento facial [110][111], como um dos métodos de verificação biométrica [112][113] para aumentar a segurança.

Outra similiaridade às características da privacidade é a importancia da verificabilidade, neste caso para demonstrar a segurança do sistema/protocolo de votação. Contudo, [114] divide a verificabilidade em validação e verificação. A validação busca resposta para o seguinte questionamento: "Aplicamos o protocolo correto e criamos o sistema certo?". Por outro lado, a verificação tenta responder se foi aplicado o protocolo e contruído o sistema de maneira correta. Ademais, [115] reforça o *trade-off* entre a anonimicidade e a verificabilidade.

Mais um ponto explorado quando se aborda a segurança em sistemas de votação é o desafio da coerção do eleitor [116]. Em [117], os autores analisam vários métodos de proteção, com diferentes níveis de resistência e custos de implementação. Já [118] combina a resistência à coerção com a integridade dos votos e a detecção de votos múltiplos.

Todavia, a palavra-chave segurança é utilizada em um número mais amplo de temas relacionados à eleição. Há artigos que especificam os requisitos de segurança aplicáveis a sistemas de votação eletrônica [7][119][120]. Também há autores que se detém nos aspectos de segurança dos procedimentos operacionais de uma eleição [121][122], assim como em definir uma metodologia para testar os critérios de segurança especificados [123].

Ainda, a segurança dos equipamentos de votação é objeto de avaliação em [124][125][126], inclusive com referência em especificar o hardware com foco na auditoria [127]. E novamente, há autores que apresentam a impressão do voto [128], bem como a abertura dos códigos-fontes dos sistemas [129] como ferramentas de aumento da segurança.

Em virtude do aumento da importância e das formas de utilização da internet, aumentaram as produções científicas sobre segurança na nuvem (*cloud computing*) [2][130] e aplicações de votação por celular (*mobile*) [131][132][133].

Porém, o assunto mais abordado do ponto de vista da segurança é a avaliação de iniciativas práticas de votação eletrônica ou propostas para utilizá-la em determinados países. A Tabela 2.5 abaixo relaciona os artigos e os países nos quais foram estudadas as experiências e/ou propostas de uso do voto eletrônico.

País	**Análise**
Alemanha	[134]
Austrália	[135][136]
Brasil	[17] [18] [19]
Canadá	[137]
Cazaquistão	[138]
Estados Unidos da América	[139] [140]
Estônia	[141] [142] [143] [144] [145]

Continua na próxima página

Tabela 2.5 – continuação da página anterior	
País	**Análise**
Holanda	[145]
Índia	[146]
Indonésia	[147] [148]
Iraque	[68]
Japão	[149]
Namíbia	[142]
Noruega	[150][151][152]
Omã	[153]
Palestina	[154]
Reino Unido	[155]
Suíça	[145]

Tabela 2.5: Artigos sobre segurança da votação eletrônica por país - *WoS* (Fonte Própria)

Por último, salienta-se a elaboração de uma revisão da literatura específica sobre o tema [156] e o registro da segurança como outro fator relevante na formação da percepção de confiança na tecnologia, uma das variáveis que influenciam a inteção de uso da votação eletrônica pelos eleitores [157][158][159][160][161].

Em contrapartida, na *Scopus*, criptografia (*cryptography*), *blockchain* e autenticação (*authentication*) foram as palavras-chave mais significativas.

Na base da *Scopus*, a palavra-chave criptografia (*cryptography*), Figura 2.12, é conceitualizada como uma ferramenta utilizada na busca da garantia da acurácia, transparência, auditabilidade e segurança dos sistemas de votação eletrônica [162][163].

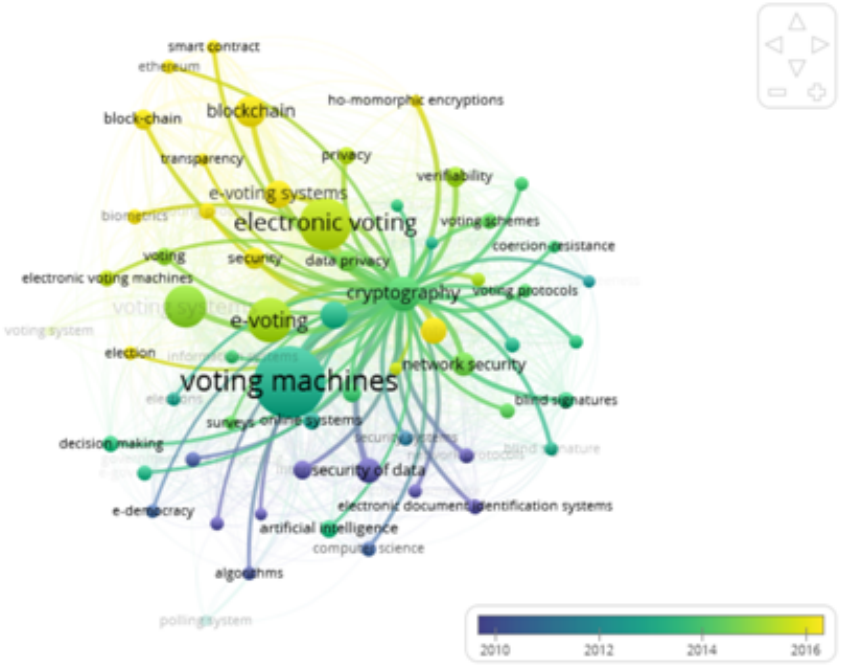

Figura 2.12: Palavra chave - *Scopus* - *Cryptography* (Fonte própria)

Para o período de tempo definido para esta pesquisa, o primeiro registro do termo data de 1998 [36], quando os autores registram o uso da criptografia para garantir a segurança, privacidade e anonimato do voto, bem como para evitar a possibilidade de voto duplo do eleitor.

Ainda no contexto das propriedades de sistemas de votação, publicações da Scopus registram a criptografia como um mecanismo que auxilia a verificabilidade [164][165][166] dos sistemas de votação, ao mesmo tempo que aumenta a resistência à coerção dos eleitores [167][168][169][170]. Nesse sentido, é um fator que impacta nos requisitos que infuenciam a aceitação dos sistemas de votação eletrônica [171][172].

Assim como identificado na *WoS*, na base de publicações da *Scopus* as publicações apresentam a aplicação das mais variadas técnicas de criptografia nos protocolos de votação eletrônica como as provas de conhecimento zero (*ZKP*) [173], *blind signature* [174], homomórfica [175][176], *mix net* [177], *blockchain* [178] e resistentes a computação quântica [179][180]. Contudo, na *Scopus*, ganham mais referências e relevância técnicas como *secret sharing* [181] e *ring signature* [182], além de *visual cryptography* [183][184], para auxílio da autenticação dos eleitores, inclusive com o uso de esteganografia [185][186].

Contudo, os autores de [187] avaliam que a criptografia não resolve todos os problemas dos sistemas de votação eletrônica. Em [188], os autores se debruçam sobre a dificuldade para o eleitor leigo entender a criptografia. Nesse sentido, [189] apresenta metáforas para auxiliar nessa explicação da tecnologia. Aliado a esse contexto e na busca por simplificar a

complexidade que são propostos protocolos de votação eletrônica sem o uso de criptografia [190][191][192][193].

Por fim, destacam-se também as avaliações do uso da criptografia em sistemas de votação eletrônica [194][195][196], bem como a revisão de literatura sobre o tema que também consta da base da *WoS*[106].

O termo *blockchain*, Figura 2.13, assim como na base *WoS*, é referenciado na *Scopus* como uma poderosa ferramenta de modernização [197][198] dos sistemas de votação eletrônica, que auxilia aprimorar os mecanismos de segurança e transparência [51][199][200], na mesma medida que colabora no combate a fraudes [201], bem como em aprimorar a auditabilidade [24][202] dos sistemas.

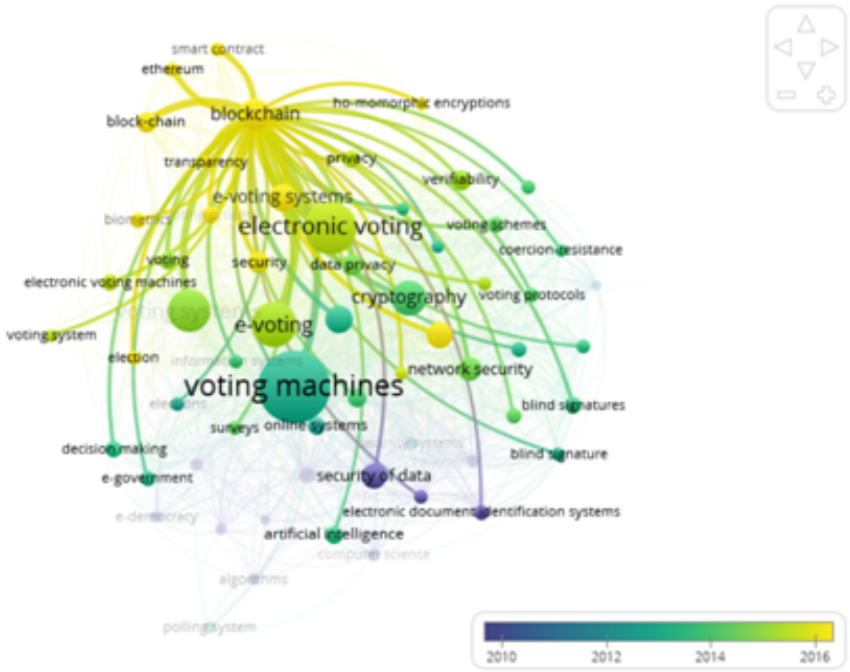

Figura 2.13: Palavra chave - *Scopus* - *Blockchain* (Fonte própria)

A primeira publicação na *Scopus* contendo o termo é de 2016 [203] e apresenta a aplicação da tecnologia na construção de *logs* imutáveis. Em função do maior número de publicações, há uma maior proposição de protocolos de votação utilizando a tecnologia que reforçam a capacidade de aumentar a confiança ao passo que sua arquitetura descentralizada [204][205] diminui a dependência do ente organizador da eleição [206].

Complementar às publicações sobre o tema na *WoS*, na *Scopus*, são registradas análises de *frameworks* de votação com *blockchain* [207][208][209][210], comparação entre plataformas [211][212][213][214], incluindo um comparativo entre aplicações utilizando a plataforma *Etherium* [215].

Adicionalmente, os autores de [216][217] apresentam riscos e vulnerabilidades do *blockchain*, ao passo que os desafios referentes ao desempenho são destacados por [218] e à escalabilidade por [219]. Ademais, em [220], os autores destacam a importância de se considerar as diretrizes para sistemas de votação eletrônica do Conselho Europeu, ao se avaliar a aplicação da tecnologia.

Ainda, simulações de ataques a sistemas de votação com *blockchain* são registradas em [221][222] e os autores de [223][224] apresentam o uso de *Machine learning* como ferramenta auxiliar na identificação e prevenção de intrusões. Há também o reforço da necessidade de resistência ao poder computacional da computação quântica [225], associação à biometria [226] e a utilização de dispositivos *IoT* [227][228][229] para substituir os equipamentos de votação, inclusive com o uso da tecnologia *Near Field Communication* (NFC) [230].

Por último, [231] repisa que a pandemia de Covid19 impulsionou a adoção de soluções remotas incluindo para votação e [232][233][234][235][236] apresentam revisões da literatura sobre a aplicação do *blockchain* nos sistemas de votação. Ao final, os autores de [237] analisam a aplicação da tecnologia, experimentalmente ou não, em alguns países ao passo que apresentam perspectivas para o uso futuro.

A terceira palavra mais citada na base *Scopus*, autenticação (*authentication*), Figura 2.14, é tratada como uma das etapas fundamentais de qualquer sistema de votação, eletrônico ou não [238]. Seu principal objetivo é identificar o eleitor para garantir que apenas os aptos participem da votação, ao passo que também evita o voto duplo de um mesmo eleitor [174]. Entretanto, ao mesmo tempo que é necessário identificar o eleitor, não se pode vincular essa identificação ao voto, para se garantir o sigilo. É nesse ponto que a autenticação se apresenta como um dos requisitos da privacidade [239] e anonimato [240] do eleitor.

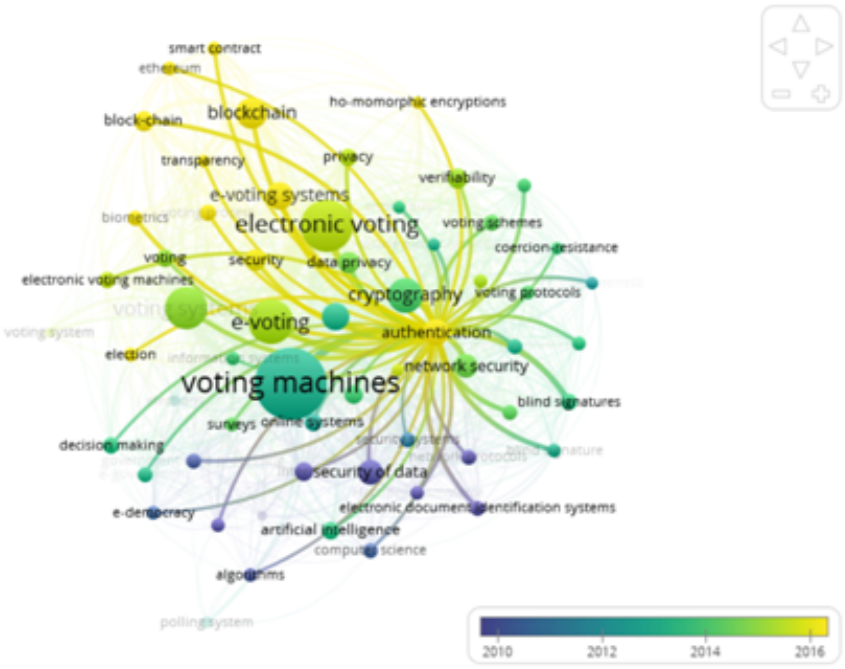

Figura 2.14: Palavra chave - *Scopus* - *Autentication* (Fonte própria)

Para o intervalo de tempo desta pesquisa, a primeira ocorrência do termo é de 2001, quando os autores de [241] abordam a implementação do protocolo de criptografia *deniable authentication*, o qual garante apenas ao destinatário pretendido identificar a origem da mensagem recebida, impedindo que esse destinatário prove a origem de uma mensagem para terceiros, mesmo que tenha cooperação [131]. Assim, o emissor e o destinatário podem confiar na legitimidade e na integridade da mensagem [242].

As publicações indicam a proeminência de protocolos criptográficos e de técnicas de reconhecimento biométrico como as principais ferramentas utilizadas para autenticar eleitores nos sistemas eletrônicos de votação.

Há registro de vários protocolos criptográficos utilizados na autenticação de eleitores. Os autores de [243] listam como principal a assinatura cega (*blind signature*), inlcuindo algumas variações. Além deste, há referências relevantes sobre a utilização da técnica *k-Times Anonymous Authentication (k-TAA)* [244][245], a qual permite a autenticação anônima de membros de um grupo por um número limitado de tentativas, a *Identity-Based Encryption (IBE)* [246], na qual se utiliza a identidade pessoal como chave pública, bem como *secret sharing* [247] e *visual cryptography* [174][175] explicadas anteriormente.

O reconhecimento biométrico é utilizado na autenticação dos sistemas de votação na busca da identificação, quando se individualiza o eleitor entre todo o eleitorado, e da verificação, quando se verifica se a pessoa que se apresenta para votar é o eleitor cadastrado na base de dados [248]. Dentre as várias características biometricas que podem

ser verificadas [249], destacam-se as propostas de utilização da impressão digital [250][251], do reconhecimento facial [252], da íris dos olhos [253] e das veias dos dedos [254].

Vale ressaltar ainda a utilização de dispositivos físicos como *smartcards* [255][256] ou móveis *IoT* [257], além de *QRCodes* [258] na busca por aumentar a eficácia da autenticação de eleitores em sistemas de votação eletrônica.

Adicionalmente, com auxílio do *software VOSViewer*, foi realizada análise da frequencia e dos agrupamentos das palavras-chaves contidas nos títulos ou resumos das publicações objetos dessa pesquisa.

A Figura 2.15 apresenta o resultado da frequencia identificada para os termos na base da *WoS*. Observa-se uma distribuição de termos, com um destaque mais significativo para "*blockchain*", "*security*", "*privacy*" e "*cryptography*".

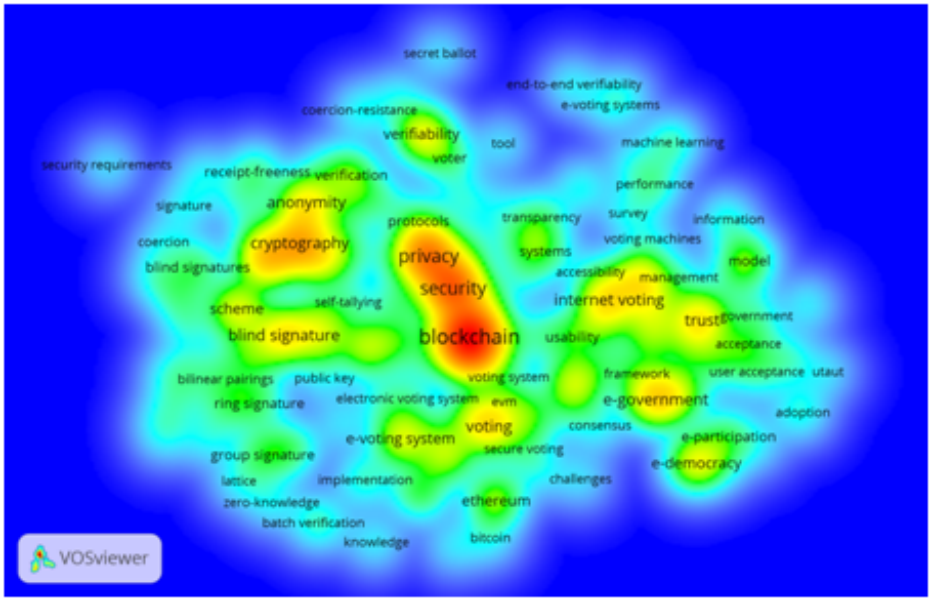

Figura 2.15: Frequencia palavras-chave (títulos e resumo) - *WoS* (Fonte própria)

Analisando-se os agrupamentos (*clusters*), Figura 2.16, os resultados evidenciam a formação de 8 grandes grupos de palavras-chave na base *WoS*.

Figura 2.16: Agrupamento palavras-chave (títulos e resumo) - *WoS* (Fonte própria)

A Figura 2.17 apresenta o mapa de calor de frequencia das palavras-chave na base *Scopus*. Também se observa uma maior concentração dos termos, dessa vez tendo destaque "*cryptography*", "*blockchain*", "*security*", "*security of data*"e "*artificial intelligence*".

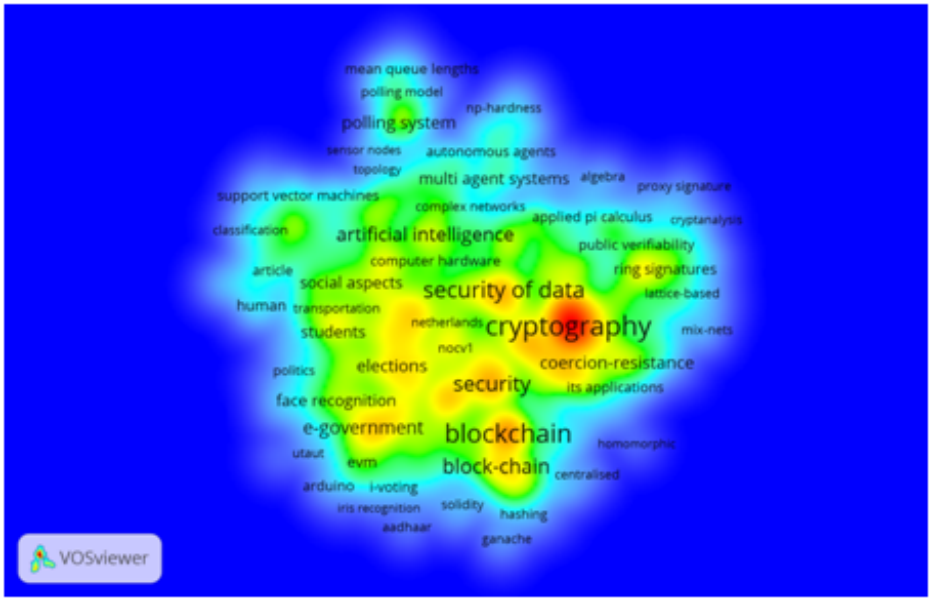

Figura 2.17: Frequencia palavras-chave (títulos e resumo) - *Scopus* (Fonte própria)

Do ponto de vista dos agrupamentos, observa-se a formação de 9 grandes grupos na base da *Scopus*, porém com uma maior sobreposição entre eles, conforme Figura 2.18.

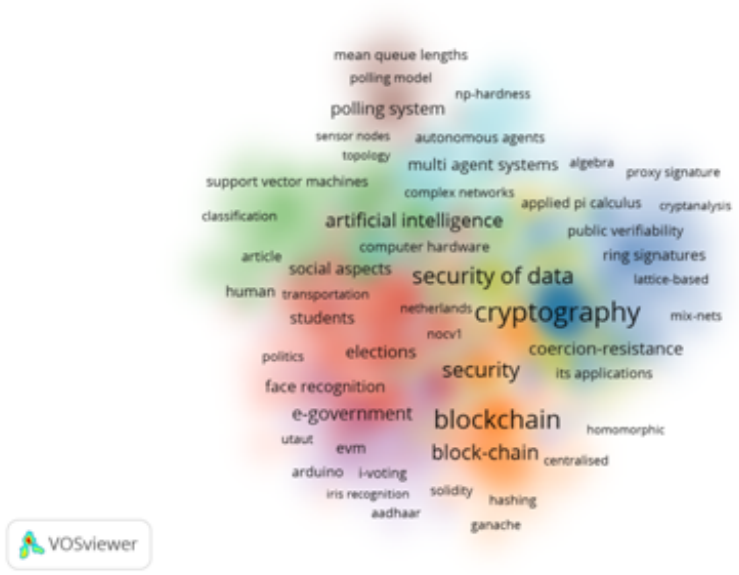

Figura 2.18: Agrupamento palavras-chave (títulos e resumo) - *Scopus* (Fonte própria)

Considerando os resultados obtidos, fica evidenciado relevante grau de similaridade no uso das palavras-chaves nas duas bases de publicações, seja pelo número de agrupamentos encontrados ou pela proximidade dos termos contidos em cada um deles. Vale destacar a maior concentração e gama de termos na base *Scopus*, consequencia da maior quantidade de artigos.

2.3 Detalhamento, Modelo Integrador e Validação por evidências

2.3.1 Cocitação

A cocitação é um índice bibliométrico que identifica relação entre autores e referências. Sua análise permite verificar aqueles artigos que são regularmente citados juntos, podendo sugerir uma semelhança entre esses estudos. Ou seja, é uma medida de similaridade entre as publicações. Possui carater dinâmico, podendo aumentar ao longo do tempo, e extrínseco, vez que a relação é estabelecida por autores de artigos diferentes que se ligam ao artigo citado. Por isso, tem o potencial de exibir a perspectiva das abordagens de pesquisa mais utilizadas [35].

A Figura 2.19 apresenta o mapa de calor de cocitação na base de periódicos *Web of Science (WoS)*. Observa-se uma dispersão entre os autores, mas uma concentração maior na área centro-esquerda e superior do mapa.

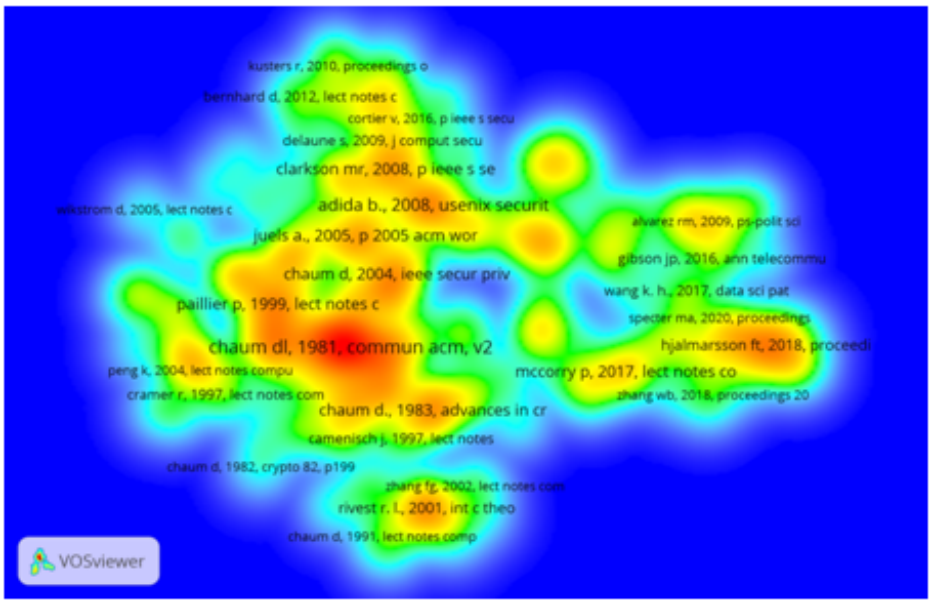

Figura 2.19: Mapa de calor de cocitação - *WoS* (Fonte própria)

Nessa região encontra-se o estudo de maior destaque, Chaum [259] de 1981. Nele, o autor apresenta uma técnica criptográfica que permite ocultar tanto o conteúdo quanto os participantes de uma comunicação eletrônica, mesmo que em um canal não seguro e sem demandar a existência de uma autoridade confiável. Segundo o autor, a técnica poderia ser aplicada ao contexto eleitoral para garantir a qualquer parte interessada verificar se os votos foram contados corretamente. Isso seria possível se os votos fossem enviados de maneira anônima e tivessem sido assinados por pseudônimos de uma lista de eleitores registrados. O mesmo autor possui mais duas publicações de destaque.

A primeira, na região centro-inferior do mapa, de 1983 [260], na qual ele apresenta a técnica de criptografia conhecida por assinatura cega (*blind signature*) e exemplificava sua aplicação em um processo de votação. Nesse processo, o eleitor teria garantido o sigilo e a integridade do seu voto, além de poder verificar se sua contagem foi realizada de maneira correta. Ainda nessa região inferior do mapa, também merece destaque a publicação de Fujioka, Okamoto e Ohta [261], que apresenta um esquema de votação secreta seguro e prático para eleições em grande escala. A proposta visava garantir a privacidade do eleitor, a justiça para os candidatos e o combate a fraudes. Ademais, também destaca-se o artigo de 2001 de Rivest, Shamir e Tauman [262], no qual os autores formalizavam a técnica criptográfica de assinatura em anel (*ring signature*), a qual permite especificar um conjunto de possíveis signatários, sem revelar o signatário real de uma mensagem. Em resumo, esses autores focam em métodos criptográficos que servem de base para utilização em sistemas de votação eletrônicas.

Retornando à área central superior do mapa, o segundo artigo de destaque de Chaum

é de 2004 [263] e aborda os desafios das urnas eletrônicas e a necessidade da garantia tanto da privacidade quanto da integridade incondicional de um sistema de votação. O estudo propõe um sistema de votação com a emissão de recibo impresso que propicia ao eleitor verificar que seu voto está íntegro e consta da totalização, resguardando seu sigilo. Próximo à esquerda, encontra-se a publicação, de 1999, de Paillier [264], na qual o autor propõe um novo mecanismo criptográfico de chave pública que foi derivado em três esquemas, um de permutação e dois homomórficos. Novamente, o foco em algoritmos criptográficos é destaque, mas adiciona-se a tentativa de simplificar um protocolo de votação para facilitar o entendimento de pessoas sem conhecimento técnico.

Logo acima, três concentrações de maior relevância. Primeiro, a publicação de Juels, Catalano e Jakobsson [265], de 2005, na qual os autores apresentam um protocolo de votação eletrônica resistente à coerção do eleitor e formalizam a definição de um sistema de votação livre de coerção. A segunda, o artigo de 2008 de Adida [266], que apresenta o primeiro sistema de votação web aberto, conhecido por Helios. O sistema foi projetado para garantir integridade incondicional, de modo que eventuais tentativas de fraudes de um administrador eleitoral corrompido seriam identificadas. Por fim, também em 2008, Clarkson, Chong e Myers [267] apresentam o Civitas, primeiro sistema de votação eletrônica remoto, resistente à coerção, com garantia de verificação do eleitor e universal. Esse conjunto de artigos priorizam apresentar implementaçõpes de protocolos de votação eletrônica, considerando o atendimento a requisitos que aumentam a capacidade de segurança e de auditoria dos sistemas e, por consequencia, a confiança nas soluções.

À esquerda do mapa de calor, ganha destaque a publicação de Peng et al. [268], de 2004, na qual os autores propõem um protocolo de votação baseado em criptografia homomórfica, mas utilizando a operação matemática de multiplicação e não a adição, mais comum até então. Esse protocolo forneceria forte privacidade dos dados, além da verificabilidade pública. Também tem relevância o estudo de Cramer, Damgård e Schoenmakers [269], que apresenta um método para transformar uma prova de conhecimento (*proof of knowledge*) em um protocolo indistinguível de testemunhas (*witness indistinguishable protocol*), usando um esquema de compartilhamento secreto (*secret sharing*). Mais uma vez, protocolos de criptografia são o foco desse conjunto de estudos.

No extremo à direita, três publicações apresentam maior relevência nas cocitações, são elas: Mccorry, Shahandashti, Siamak e Hao [41] de 2017; Hjálmarsson e Hreiðarsson [54] de 2018; e Alvarez [270] de 2009. As duas primeiras publicações, [41] e [54], propõem solução para o problema da votação segura e privada pela internet usando a tecnologia *Blockchain*. A terceira, [270], discute o uso da internet em eleições, com foco na experiência da Estônia. Nesse conjunto de publicações, observa-se o foco na temática da votação pela internet, em especial com uso do *blockchain*.

A Figura 2.20, exibe o mapa de calor de cocitação dos autores na base *Scopus*. Diferente da *WoS*, observa-se mais grandes pontos de concentração.

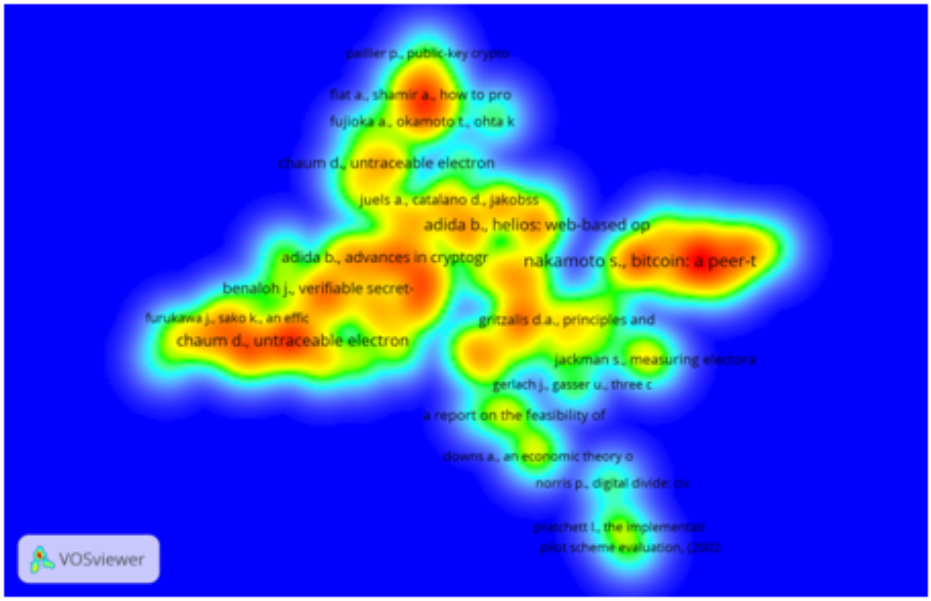

Figura 2.20: Mapa de calor de cocitação - *Scopus* (Fonte própria)

À esquerda, com grande destaque, assim como na WoS, a publicação de Chaum [259], na qual o autor, em 1981, apresenta uma técnica criptográfica que permite ocultar tanto o conteúdo quanto os participantes de uma comunicação eletrônica. Logo acima, o estudo de Furukawa e Sako [271], no qual os autores propõem um protocolo de votação baseado em canais anônimos mistos embaralhados, sem recibo do voto, onde o eleitor pode esconder como votou até mesmo de uma possível tentativa de coação. Na sequência acima, a publicação de 1987 de Benaloh [272] descreve um protocolo para a realização de eleições secretas, com uso de criptografia homomórfica, que garante a privacidade dos votos e, ao mesmo tempo, permite a verificação do resultado por todos os participantes, inclusive por observadores não participantes do pleito. Ainda nesse agrupamento, a tese de doutorado de Adida [11], de 2006, ganha destaque por explorar técnicas criptográficas para implementar eleições secretas e verificáveis, além de apresentar uma revisão da literatura sobre o uso de criptografia em eleições. Esse conjunto de publicações se relacionam por apresentarem e avaliarem técnicas criptográficas aplicadas a sistemas eleitorais.

Na parte centro-superior do mapa, destacam-se duas publicações abordadas anteriormente na análise da base *WoS*, são elas: Adida [266], que em 2008 apresenta o sistema de votação Helios; e Juels, Catalano e Jakobsson [265], que em 2005 apresentam um protocolo de votação eletrônica resistente à coerção do eleitor. Por prováveis diferenças no texto das referências, surge novamente a publicação de Chaum [259], citada no início desta seção.

No extremo superior do mapa de calor, os estudos de Fiat e Shamir [273]; Fujioka, Okamoto e Ohta [261]; e de Paillier [264] são os mais destacados. O primeiro descreve esquemas simples de identificação e assinatura que permitem a qualquer usuário provar sua identidade e a autenticidade de suas mensagens para qualquer outro usuário sem chaves públicas ou compartilhadas. Os dois últimos foram abordados na análise da base *WoS* anteriormente. Esse agrupamento tem como ligação o uso de algortimos de criptografia nos sistemas de votação.

À direita do mapa, se destaca o estudo de Nakamoto [274] que propôs a criação de uma versão puramente *peer-to-peer* do dinheiro eletrônico que permitiria que pagamentos *on-line* fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira, o Bitcoin. Essa publicação é a que apresenta o *blockchain*, recentemente muito referenciado para uso em sistemas de votação para não se depender da confiança na autoridade eleitoral.

Na parte centro-inferior do mapa, com maior destaque a publicação de Gritzalis [103], na qual o autor discute o uso da votação eletrônica como meio de aprimorar os processos democráticos nas sociedades da informação modernas e identifica os requisitos de um sistema adequadamente seguro. Há ainda concentração em torno da publicação de Jackman [275], de 1994, que discute métodos sobre como medir o viés e a responsividade nos sistemas eleitorais, utilizando como referência eleições estaduais e federais na Austrália desde 1949. Ao final, o artigo de Gerlach e Gasser [276], de 2009, discute a implementação do voto eletrônico na Suíça desde 1998, examinando os testes realizados em Genebra e Zurique.

Na sequencia, o relatório de Mote [277], de 2002, apresenta os benefícios potenciais da votação pela Internet e como ela pode reverter a tendência histórica de queda da participação eleitoral nos Estados Unidos. Ainda, a publicação de Downs [278] discute uma teoria geral de equilíbrio entre a tomada de decisão governamental e o mercado privado, além de abordar a motivação de atores econômicos e políticos.

Por fim, destacam-se os estudos de Norris [279]; Pratchett [280]; e Xenakis e Macintosh [281]. O primeiro, de 2001, examina o acesso e o uso da Internet em algumas nações e encontra evidências de uma divisão democrática entre aqueles que usam ou não recursos da Internet para se engajar e participar da vida pública. Em [280], o autor discute os esforços do Reino Unido para desenvolver a votação eletrônica como parte da revolução do governo eletrônico. Por último, em [281], de 2004, os autores discutem os principais problemas que surgiram dos pilotos de votação eletrônica realizados em várias cidades do Reino Unido em 2002.

Observa-se nesse conjunto de artigos a análise de quais requisitos sistemas eletrônicos de votação devem atender, a relevância e o contexto político das decisões governamentais,

bem como a avaliação de casos práticos de eleições em alguns países.

2.3.2 Acoplamento (*Coupling*)

O acomplamento, *coupling*, é mais um índice bibliométrico para identificar a relação entre autores e referências. Porém, é uma medida de associação entre duas publicações citadas. Tem como base a premissa de que artigos que citam trabalhos iguais, possuem similaridade. Diferente da cocitação, o *coupling* tem carater intrísico, vez que é estabelecido por meio das referências feitas pelos próprios autores dos documentos envolvidos. Assim, é uma abordagem estática, cujo os resultados são independentes do tempo em que a análise é realizada. A força do acoplamento é determinada pela quantidade de sobreposições entre suas bibliografias. Por isso, traz a perspectiva de frentes de pesquisa [35]. Para a análise de *coupling* neste estudo, foi utilizado o espaço de tempo do ano de 2020 a 2023.

A Figura 2.21 exibe o mapa de calor de acoplamento na base de publicações *WoS*. A maior concentração encontra-se nos trabalhos de Khan K.M, Arshad e Khan M.M [71] e Caldarelli e Ellul [282]. Ambos abordam o *blockchain*, sendo que no primeiro se observa a eficiência da sua utilização em sistemas de votação e, no segundo, uma revisão da literatura focada em encontrar aspectos convergentes entre os modelos propostos que possam levar a um padrão de fato, universalmente aceito.

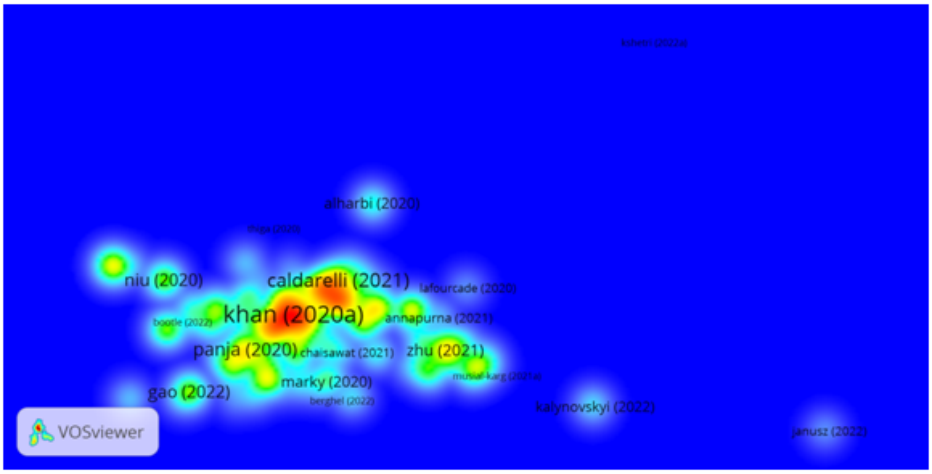

Figura 2.21: Mapa de calor de acoplamento - *WoS* (Fonte própria)

Na parte superior do mapa, destaque para a publicação de Alharbi, Zamzami e Samkri [283] que discute a importância da criptografia homomórfica e suas várias aplicações na proteção da privacidade, além de fornecer uma pesquisa bibliográfica para preencher a lacuna nos sistemas atuais. No extremo acima, o *blockchain* ressurge no trabalho de Kshetri et al [284], no qual os autores apresentam uma pesquisa sobre como a tecnologia

é aplicada para fornecer segurança em aplicações *web*, assim como no combate a ameaças e ataques cibernéticos.

À esquerda, destacam-se os trabalhos de Niu et al. [285] e Feng et al. [286] que analisam a aplicação de algortimos de criptografia quânticos em cenários como a votação eletrônica. Ainda nessa região do mapa, mais dois trabalhos ganham evidência ao abordar aplicação de algoritmos criptográficos. Em [287], Haines et al. analisam que o uso de implementações defeituosas de componentes criptográficos pode levar a fraudes indetectáveis, a partir da avaliação da solução de votação eletrônica privada contratada pela Suíça, em 2019. Já em [88], Gao et al. mencionam que protocolos de criptografia homomórfica podem ser usados em sistemas de votação eletrônica para proteger a privacidade dos eleitores.

Na parte inferior do mapa, destaque para as obras de Challa [288], Hao et al. [155] e Kulyk et al. [289]. O primeiro é mais um trabalho a abordar a criptografia homomórfica ao fornecer uma visão geral dos diferentes tipos de implementações e discutir suas possíveis aplicações em várias áreas. O segundo e terceiro artigos abordam a avaliação de sistemas de votação com verificação fim a fim na Suiça e em um piloto no Reino Unido, respectivamente. Mais a direita, os trabalhos de Zhu, Azizah e Hsiao [102], Annapurna et al. [290] e Musial-karg e Kapsa [291]. O primeiro e o terceiro estudam a confiança na utilização da votação eletrônica na Indonésia e Polônia, respectivamente. Por outro lado, o segundo artigo foca na redução do número de pessoas necessárias para operar a votação ao propor um modelo de urna eletrônica com *Radio Frequency Identification (RFID)* e verificação biométrica facial.

Para terminar, no extremo à direita, salienta-se a publicação de Kalynovskyl et al. [292], que avalia iniciativas de adoção de governo eletrônico, incluindo a votação, e correlaciona com oportunidades de aplicação na Ucrânia, e a de Janusz e Sells [293], na qual os autores avaliam se a distribuição, pelos partidos políticos, dos números de identificação dos candidatos influenciam as chances de eleição e na promoção da desigualdade entre raças ou gênero de candidatos eleitos no Brasil.

A Figura 2.22 apresenta o mapa de calor de acoplamento gerado a partir das publicações da base *Scopus*. Diferentemente da *WoS*, há menos dispersão, porém a maior concentração também encontra-se no trabalho de Khan K.M, Arshad e Khan M.M [71] sobre a eficiência do *blockchain* em sistemas de votação.

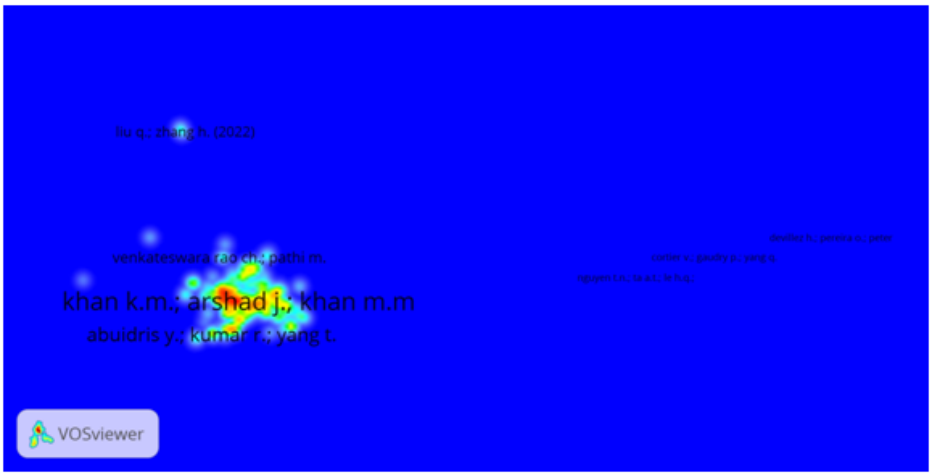

Figura 2.22: Mapa de calor de acoplamento - *Scopus* (Fonte própria)

Logo abaixo, a publicação de Risnanto et al. [8], cujo o objetivo foi de mapear os requisitos para implementar um sistema de votação eletrônica, considerando experiências de países bem e mal sucedidos nessa iniciativa.

Logo acima, Venkateswara [294] propõe um sistema de votação eletrônica para aumentar a confiabilidade das eleições na Índia. A proposta conta com a verificação da impressão digital para identificar o eleitor, bem como o envio de mensagem sms para o celular do eleitor, ao confirmar o voto, no intuito de mitigar a possiblidade de voto duplo e/ou falso.

No extremo superior, Liu e Zhang [295] propõem um método para avaliar a confiabilidade de sistemas de votação com base na teoria da evidência de *Dempster–Shafer (D-S)* e utilização da simulação de Monte Carlo.

Por fim, no extremo à direita, os trabalhos de Nguyen et al. [296]; Cortier, Gaudry e Yang [297]; e Devillez, Pereira e Peters [298] abordam o uso de criptografia nos sistemas de votação eletrônica. O primeiro propõe a utilização de um esquema de votação baseado em rede *unique ring signatures*. No segundo artigo, os autores propõem um método privado e verificável para totalização oculta dos votos, visando evitar a coerção dos eleitores. Por último, os autores do terceiro artigo estudam a criptografia verificável bit a bit e propõem um protocolo homomórfico eficiente e portátil, baseado em bibliotecas do *ElectionGuard*, solução *open source* utilizada em eleições governamentais com verificação fim a fim.

2.3.3 Modelo integrador

A Figura 2.23 congrega em um modelo integrador as principais descobertas nas fontes pesquisa utilizadas. De modo geral, as publicações retratam caracterísitcas, técnicas e avaliações práticas da aplicação de sistemas eletrônicos de votação.

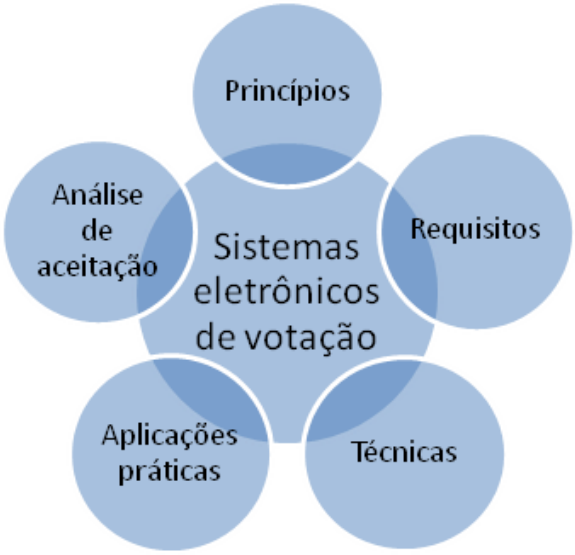

Figura 2.23: Modelo integrador (Fonte própria)

Adicionalmente, a Tabela 2.6 apresenta o detalhamento das informações das publicações agrupadas por semelhança dos temas mais relevantes para a pesquisa.

Autor/Ano	**Título**	**Tema**	**Resultado**	**Semelhanças**
GRITZALIS, D. A. 2002 [103]	*Principles and requirements for a secure e-voting system*	Princípios e requisitos de sistemas eletrônicos de votação	Identifica um conjunto de princípios e requisitos gerais que devem ser atendidos ao projetar um sistema de votação eletrônica	Elenca princípios e requisitos de segurança, privacidade e responsabilidade [7]. Combate a coerção [117]. Verificabilidade, confiabilidade e anonimato [156]

Continua na próxima página

Tabela 2.6 – continuação da página anterior

Autor/Ano	Título	Tema	Resultado	Semelhanças
KHO, Yun-Xing et al. 2022. [106]	*A Review of Cryptographic Electronic Voting*	Criptografia em sistemas de votação eletrônica	Compara estruturas, vantagens e desvantagens de várias abordagens de uso da criptografia na votação eletrônica	Explora técnicas criptográficas para implementar eleições verificáveis por votação secreta [11] Apresenta um conjunto de métricas para comparação das propriedades dos esquemas criptográficos de votação eletrônica [162]
VILLAFIORITA, Adolfo et al. 2009. [128]	*Development, formal verification, and evaluation of an e-voting system with Voter Verifiable Paper Audit Trail (VVPAT)*	Impressão do voto	Apresenta as principais atividades para o desenvolvimento de uma urna eletrônica com teste de auditoria em papel	Propõe um sistema de votação eletrônica com emissão de recibo em papel, baseado em tecnologias criptográficas [94]

Continua na próxima página

Tabela 2.6 – continuação da página anterior

Autor/Ano	Título	Tema	Resultado	Semelhanças
KHASAWNEH, Mohammed et al. 2008. [248]	*A biometric-secure e-voting system for election processes*	Identificação biométrica do eleitor	Propõe um sistema de votação eletrônica on-line que incorpora processos de identificação e autenticação utilizando biometria	Propõe sistema de votação utilizando biometria multimodal, reconhecimento facial e impressão digital, para autenticar o eleitor [113]. Avalia as capacidades da utilização da identificação biométrica em sistemas de votação eletrônica [249]

Continua na próxima página

Tabela 2.6 – continuação da página anterior				
Autor/Ano	**Título**	**Tema**	**Resultado**	**Semelhanças**
JAFAR, Uzma et al. 2021. [208]	*Blockchain for electronic voting system - review and open research challenges*	Utilização de *blockchain* nos sistemas eletrônicos de votação	Identifica problemas que afetam os sistemas de votação eletrônica e como o *blockchain* pode auxiliar a resolvê-los	Fornece uma revisão sistemática dos sistemas de votação eletrônica baseados em *blockchain*, discutindo desafios e oportunidades para sua implementação [77]. Sugere que o *blockchain* pode ser utilizado para resolver desafios de sistemas de votação eletrônica como autenticação, privacidade, integridade de dados, transparência e verificabilidade [6]

Continua na próxima página

Tabela 2.6 – continuação da página anterior				
Autor/Ano	**Título**	**Tema**	**Resultado**	**Semelhanças**
DARMAWAN, Ikhsan. 2021. [299]	*E-voting adoption in many countries: A literature review*	Confiança e adoção de sistemas eletrônicos de votação	Discute a adoção do voto eletrônico em vários países e observa que a falta de confiança e as preocupações de segurança contribuíram para o declínio de sua adoção recentemente	Examina a confiança multidimensional da tecnologia na adoção do voto eletrônico pelos cidadãos de países em desenvolvimento [102]. Argumenta sobre a a distinção entre segurança real e percebida pelos eleitores na votação eletrônica e investiga diferentes significados de confiança [157]

Tabela 2.6: Inventário das pesquisas categorizado por semelhanças (Fonte Própria)

Considerados os principais achados na pesquisa realizada, passa-se a destacar as evidências da importância do tema para a comunidade de pesquisa acadêmica.

2.3.4 Validação por evidências

A utilização da tecnologia de sistemas para informatizar o processo de votação é tema de interesse da meio acadêmico desde quando iniciada a prática.

Inicialmente focada na contextualização, riscos e definição dos requisitos necessários para a construção dos sistemas de votação, como demonstrado na revisão de [119], também há registro da formalização de recomendações como a realizada pela *Association for Computing Machinery (ACM)* [300], que pregava especial atenção à integridade, à se-

gurança e à usabilidade na construção de sistemas de votação eletrônica, bem como da análise dos resultados de normativos legais como a lei americana conhecida como *Help America Vote Act (HAVA)*, que em 2002 previa recursos para melhoria de equipamentos eleitorais, cujos os desafios e controversias foram analisados uma década depois em [301].

Considerando sua relevância para a sociedade, na medida que eleições limpas é um dos pilares da democracia, os estudos sobre votação eletrônica se debruçaram também em avaliar os métodos aplicados para garantir os requisitos necessários. Em geral, esses métodos são baseados em criptografia, como apresentado nas revisões [302] e [106]. Na primeira, os autores exploram várias primitivas criptográficas que visam garantir a privacidade ao passo que oferecem verificabilidade. Na segunda revisão, os autores comparam as estruturas, vantagens e desvantagens de diferentes abordagens criptográficas em sistemas de votação eletrônica.

Porém, a complexidade técnica inerente aos métodos criptográficos aplicados na busca por sistemas de votação honestos e transparentes resulta na incompreensão do funcionamento das soluções por parcela significativa da sociedade que não possui conhecimento técnico [303]. Assim, as publicações acadêmicas começaram também a refletir sobre a confiabilidade dos sistemas de votação eletrônica, como em [304] onde os autores discutem os riscos associados à votação eletrônica e como a confiança do eleitorado é baseada na capacidade de as soluções refletirem com precisão a intenção do eleitor.

Dessa forma, a análise da confiança dos sistemas de votação eletrônica em casos concretos tornou-se objeto dos pesquisadores como pode se verificar nos estudos de caso dos pilotos de votação eletrônica no Reino Unido [305], das eleições na Noruega [151], Estônia [306], Brasil [307], India [8] e Argentina [308], para exemplificar alguns.

Mais recentemente, a criação do Bitcoin [274] despertou nos pesquisadores o interesse em avaliar a possibilidade de a sociedade reduzir a necessidade de depender de uma autoridade organizadora da eleição. Nesse sentido que surgem as publicações aplicando o *blockchain* no contexto da votação eletrônica das quais salienta-se as revisões de literatura sobre o tema [77] e [208].

É neste cenário desafiador que os estudos procuram entender as variáveis e motivações que influenciam a aceitação e adoção da votação eletrônica como se verifica em [102], [309], [157], e [310].

Capítulo 3

Referencial Teórico

A democracia trata da escolha do governo que decidirá as ações a serem tomadas visando o bem estar e a prosperidade dos cidadãos. O voto é a expressão formal dessa escolha [311].

Em se tratando do uso de sistemas de informação no processo eleitoral, a confiança dos eleitores no sistema de votação é essencial para o correto funcionamento da democracia. Contudo, um mero boato é capaz de minar essa confiança [6].

Nesse sentido, a aceitação do uso de tecnologia nos mais variados contextos é influenciada por vários fatores. No cenário eleitoral, há vários registros de estudos focados na análise da aceitação da tecnologia, incluindo a avaliação do uso de urnas eletrônicas similares à brasileira nas eleições indianas [33].

Nesta seção, além de abordar a produção acadêmica sobre modelos de aceitação de tecnologia, também reuni-se material sobre histórico e requisitos de sistemas de votação eletrônica, bem como sobre a confiança em processos eleitorais que fazem uso de tecnologia.

3.1 Modelos de aceitação de tecnologia

Com o crescimento da aplicação dos sistemas de informação nas organizações na busca pelo aumento da produtividade, entender a aceitação de novas tecnologias pelos usuários é uma das áreas de pesquisa mais maduras na literatura contemporânea de sistemas de informação [27].

Para se explicar e mesmo incrementar a aceitação das tecnologias pelos usuários é necessário desvendar o porquê de as pessoas aceitarem ou rejeitarem os computadores. Pode-se destacar alguns motivos da importância dessa avaliação por parte dos usuários: (i) auxílio ao desenvolvimento do sistema de informação; (ii) compreensão do comportamento do usuário; e (iii) mensuração do sucesso do sistema [4].

Nesse sentido, a busca da aceitação da tecnologia pelos usuários é um desafio contínuo de gestão [331]. A pesquisa nesta área resultou em vários modelos teóricos, com raízes em sistemas de informação, psicologia e sociologia, cuja a multiplicidade impõe aos pesquisadores a escolha de um "modelo preferido", desprezando, em grande parte, as contribuições dos demais modelos [27].

Assim, a atividade acadêmica sobre o tema revela uma variedade de perspectivas das partes interessadas, tecnologias e contextos, unidades de análise, teorias e métodos de pesquisa [331].

Em resposta a este contexto e a fim de harmonizar a literatura associada à aceitação de novas tecnologias, nem todas ligadas apenas à tecnologia da informação, os autores de [27] desenvolveram um modelo unificado que reúne visões alternativas sobre a aceitação do usuário e da inovação – A teoria unificada de aceitação e uso da tecnologia (*Unified Theory of Acceptance and Use of Technology* (UTAUT)).

O modelo UTAUT é resultado da avaliação e integração dos elementos de oito modelos de aceitação da Tecnologia [4], são eles: Teoria da Ação Racional (*Theory of Reasoned Action* (TRA)) [312], de 1977; Modelo de Aceitação da Tecnologia (*Technology Acceptance Model* (TAM)) [313], 1989; Modelo Motivacional (*Motivational Model* (MM)) [314], 1997; Teoria do Comportamento Planejado (*Theory of Planned Behavior* (TPB)) [315], 1991; Modelo Combinado (*Combined TAM and TPB* (TAM/TPB)) [316], 1995; Modelo de Utilização do PC (*Model of Personal Computer Utilization* (MPCU)) [317], 1991; Teoria da Difusão da Inovação aplicada em sistemas de informação (*innovation Difusion Theory* (IDT)) [318], 1996; Teoria Social Cognitiva ampliada para o uso de computadores (*Social Cognitive Theory* (SCT))[319], 1995.

Em síntese, [4] descreve assim cada um dos oito modelos avaliados:

1. **Teoria da Ação Racional (TRA)**: defende que o comportamento individual é determinado pelas intenções de comportamento, as quais ocorrem em função da atitude do indivíduo, definida como sentimentos positivos e negativos dele próprio. Para este modelo existe uma norma subjetiva, que envolve a percepção do indivíduo quanto ao que a maioria das pessoas, importantes para ele, pensam que ele deveria ou não desempenhar com relação ao comportamento em questão. Os construtos base do modelo são as normas subjetivas e a atitude para o comportamento.

2. **Modelo de Aceitação da Tecnologia (TAM)**: objetiva avaliar o comportamento de utilização da tecnologia, analisando as atitudes para usar os sistemas de informação, a partir da utilidade percebida e da facilidade de utilização. O modelo discute como construtos principais: normas subjetivas, facilidade de uso percebida e utilidade percebida.

3. **Modelo Motivacional (MM)**: busca entender a adoção e uso de novas tecnologias, a partir da aplicação de teorias motivacionais para explicar o comportamento dos indivíduos. Os construtos deste modelo são a motivação intrísica e extrínsica.

4. **Teoria do Comportamento Planejado (TPB)**: amplia a TRA com a inclusão do construto controle do comportamento percebido como um determinante da intenção e de comportamento do uso da tecnologia. Esse modelo tem como construtos fundamentais: atitude para o comportamento, normas subjetivas e controle comportamental percebido.

5. **Modelo Combinado (TAM/TPB)**: na busca por entender o uso da tecnologia da informação, combina os preditores do TPB com a utilidade percebida do modelo TAM, tem como principais construtos: atitude para o comportamento, normas subjetivas, controle comportamental percebido e utilidade percebida.

6. **Modelo de Utilização do PC (MPCU)**: analisa a aceitação e o uso da tecnologia com base nos construtos ajuste ao trabalho, complexidade, consequências de longo prazo, efeitos em razão do uso, fatores sociais e condições facilitadoras aplicadas à intenção de uso de computadores pessoais.

7. **Teoria da Difução da Inovação (IDT)**: voltado para identificar a aceitação individual da tecnologia, o modelo é resultado da adaptação e refinamento das características de inovação apresentadas por [320]. Os principais construtos dessa teoria são: vantagem relativa, facilidade de uso, imagem, visibilidade, compatibilidade, demonstração de resultados e uso voluntário.

8. **Teoria Social Cognitiva (SCT)**: adaptação e ampliação da teoria originalmente utilizada para estudar o uso de computadores, o modelo utiliza os construtos expectativas de resultados de performance e pessoais, autoeficácia, afeto e ansiedade para avaliar aceitação e o uso de tecnologias da informação em geral.

Com o intuito de unificar esses modelos e gerar um ainda mais completo, que abrangesse os principais construtos relacionados à aceitação da TI, o UTAUT sugere que o Comportamento do Usuário (*Use Behavior*) frente a tecnologia é determinado por quatro constructos: Expectativa de Performance (*Performance Expectancy*), Expectativa de Esforço (*Effort Expectancy*), Influência Social (*Social Influence*) e Condições Facilitadoras (*Facilitating Conditions*); e que as variáveis Gênero (*Gender*), Idade (*Age*), Experiência (*Experience*) e Voluntariedade de Uso (*Voluntariness of Use*) atuam como moderadores desses constructos [321]. A Figura 3.1 ilustra as variáveis do modelo

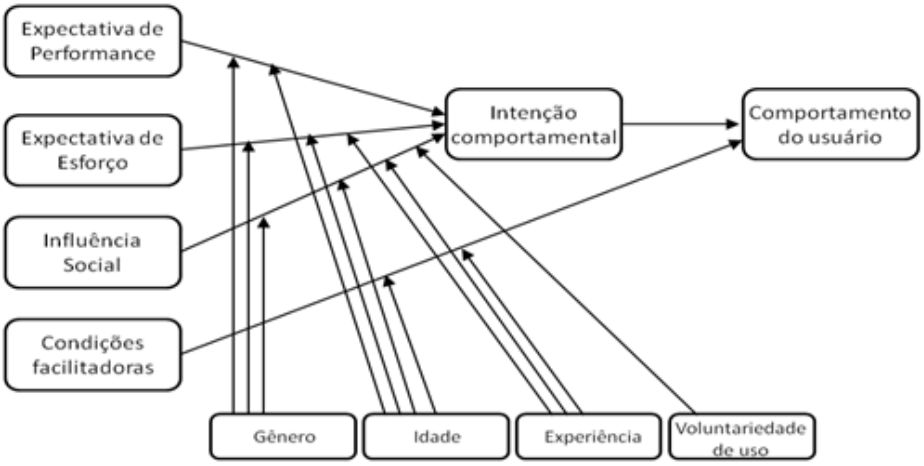

Figura 3.1: Modelo UTAUT (Fonte: Adaptado de [27])

Segundo [4], os construtos são definidos assim:

1. **Expectativa de Performance**: grau em que o indivíduo acredita que usando a tecnologia ele terá ganhos de performance no trabalho . É decorrente da compilação dos modelos TAM, combinado TAM/TPB, MM, MPCU, IDT e SCT.

2. **Expectativa de Esforço**: grau de facilidade associado ao uso da tecnologia. É derivado dos modelos TAM, MPCU e IDT.

3. **Influência Social**: grau de percepção do indivíduo em relação aos demais quanto à crença destes para com a necessidade de uma nova tecnologia ser usada ou não. Pode ser compreendido como o quanto um indivíduo percebe que outras pessoas influentes acreditam que ele ou ela deveria utilizar a nova tecnologia. É importante quando o uso da tecnologia é voluntário, deixando de ser significativo quando o uso é mandatório. Baseia-se nos modelos de norma subjetiva (TRA, TAM, TPB e a combinação TAM/TPB), no de fatores sociais (MPCU) e no de imagem (IDT).

4. **Condições Facilitadoras**: grau pelo qual o indivíduo acredita que existe uma infraestrutura organizacional e técnica para suportar o uso da tecnologia. Concentra conceitos personificados por três diferentes construtos: controle percebido do comportamento, (TPB e combinação TAM/TPB), condições facilitadoras (MPCU) e compatibilidade (IDT).

Ademais, [4] destaca a existência de quatro construtos moderadores: o gênero, a idade, a experiência do indivíduo e a voluntariedade do uso (o grau pelo qual o uso da tecnologia é voluntário ou livre, ou seja, não obrigatório).

Segundo seus autores do UTAUT [27], os estudos empíricos realizados para validar o modelo foram realizados em duas organizações e os resultados confirmaram a existência

de três determinantes diretos da intenção comportamental e dois determinantes diretos do comportamento do usuário, além da influência das quatro variáveis moderadoras. O modelo explicou até 70% da variação da intenção comportamental e 50% do comportamento real do usuário. Em função desses expressivos resultados, os autores acreditavam que o modelo estaria próximo do limite prático para explicar a aceitação individual e as decisões de uso de novas tecnologias. Dessa forma, os autores acreditam que o modelo seja uma ferramenta útil para os gestores que necessitam avaliar a probabilidade de sucesso de uma nova tecnologia e auxilia na compreensão dos fatores determinantes da aceitação do uso, bem como no desenho de intervenções nas tecnologias [4].

Desde a sua criação, o UTAUT tem sido amplamente utilizado na pesquisa de adoção e difusão de tecnologia por pesquisadores que realizam estudos sobre a intenção e o comportamento do usuário, em uma gama de cenários como Internet, websites, tecnologia móvel e sistemas *Enterprise Resource Planning* (ERP), hospitalares, de pagamento, de votação eletrônica, entre outros [321].

Posteriormente, os autores de [322] propuseram o UTAUT2 que explica a aceitação da tecnologia, principalmente no contexto do consumidor. O UTAUT2 incorpora motivação hedônica, hábito e valor de preço como determinantes adicionais da aceitação da tecnologia [33].

3.2 Breve histórico das eleições

De acordo com [11], os primeiros registros sobre votação remontam à Grécia Antiga, onde os homens proprietários de terras votavam em "eleições negativas", nas quais um político que recebesse mais de 6.000 votos era condenado ao exílio por dez anos. Os votos eram registrados em pedaços de porcelana/cerâmica chamados ostraca, daí a origem do termo ostracismo. Outro meio de votação comum à época era o "voto cantado" quando os eleitores se manifestavam oralmente para declarar seu voto [323].

A introdução do papel para o registro do voto ocorreu na República Romana, em 139 antes de Cristo. Entretanto, o voto realizado em locais que garantam a privacidade do eleitor, utilizando cédulas de papel padronizadas visando garantir o sigilo, surgiu na Austrália, apenas em 1836, e se espalhou pela Europa e Estados Unidos [311].

No Brasil, a primeira eleição que se tem registro foi realizada em 1532 e definiu os membros do Conselho Municipal da Vila de São Vicente, atual cidade de São Paulo. Posteriormente, em 1821, com o país integrante do Reino de Portugal e não mais colônia, D. João VI decretou a convocação de brasileiros para escolha de deputados às cortes de Lisboa. Após a declaração da independência, em 1822, D. Pedro I convocou eleições para a Assembléia Geral Constituinte e Legislativa. No período do Império, o voto era

indireto, com restrições de renda e gênero para seu exercício, mas com pequenos períodos de restrição a analfabetos [13].

Após a proclamação da República, em 1889, a tradição de fraudes eleitorais demandava uma modernização na busca por eleições limpas e confiáveis. Nessa esteira, em 1932, foi publicado o primeiro Código Eleitoral do Brasil, que entre outras inovações previu o voto facultativo às mulheres, fixou o voto como secreto e centralizou a organização das Eleições no Poder Judiciário, vez que tanto Executivo quanto Legislativo possuem interesses diretos nas eleições. Esse modelo era adotado em outros países e assim surgiu a Justiça Eleitoral no Brasil. Salienta-se que a obrigatoriedade do voto dos cidadão maiores que 18 anos foi estabelecida em 1935 [13].

Desde então, o país experimenta a experiência de eleger seus representantes de maneira livre e regular, à exceção dos períodos de 1937 a 1945, regime totalitário do Estado Novo no qual as eleições foram suspensas, e de 1964 a 1985, regime militar no qual os direitos políticos foram limitados e as eleições realizadas de maneira indireta [13].

3.3 Evolução dos sistemas de votação e o uso da tecnologia

O processo de votação tradicional evoluiu da contagem de mãos levantadas, de cedulas de papel, passando pela introdução de equipamentos mecânicos e posteriormente eletrônicos [162].

O Conselho Europeu definiu o voto eletrônico (*e-voting*) como uma eleição ou referendo em que meios eletrônicos são utilizados, pelo menos na emissão do voto [324]. O voto eletrônico visa melhorar o processo de votação ao reduzir ou prevenir fraudes pela diminuição da intervença humana, agilizar o processamento do resultado, minimizar os custos de tarefas repetitíveis, e aumentar a participação dos eleitores. Porém, também enfrenta problemas como a dificuldade de compreensão por pessoas sem conhecimentos técnicos, falta de padrões e normas, vulnerabilidades e ataques exploráveis por atacantes com acessos privilegiados, e aumento de custos com a infraestrutura de tecnologia da informação [6].

Segundo [323], os sistemas de votação podem ser divididos em quatro tipos:

1. **Voto cantado**: Antes da introdução das cédulas, o voto era expressado por voz, quando o eleitor anunciava sua escolha que era registrada nos livros de votação. Esse tipo de votação possui algum nível de controle contra a contagem fraudulenta, uma vez que é possível de ser observada. Porém, por não ter privacidade e sigilo, os

eleitores ficam expostos a coerção e tentativas de suborno. Ainda hoje esse modo de votação é utilizado em assembleias deliberativas.

2. **Voto por cédula**: Considerado um dos modos de votação mais antigos, é quando um eleitor recebe uma cédula, de papel ou não, para depositar em uma urna seu voto apenas uma vez. Tem como benefícios ser de fácil entendimento e organização, custo relativamente baixo, permite a votação de analfabetos e pode ser organizado em curto espaço de tempo. Por outro lado, é um processo lento, que exige muitas atividades manuais para sua execução e suas brechas permitem a exploração por agentes mal intencionados.

3. **Voto mecânico ou eletrônico**: Populares a partir da primeira metade do século XX, as máquinas foram introduzidas no intuito de suprir deficiências dos modelos anteriores e garantir a segurança e privacidade dos eleitores. São exemplos de equipamentos de votação mecânicos as máquinas a alavancas e de cartão perfurado, assim como os *scanners* óticos e as urnas eletrônicas do tipo *Direct Recording Eletronic (DRE)* são exemplos de equipamentos eletrônicos. Maiores detalhes desses equipamentos podem ser vistos em [325]. De positivo, os equipamentos eletrônicos de votação permitem a votação em áreas remotas, reduzem o tempo de contagem dos votos, são eficientes em votações com grande número de eleitores e podem propiciar a privacidade e anonimato do eleitor. Do ponto de vista de deficiências, a confiança nos equipamentos é afetada pela abertura dos códigos-fonte dos softwares utilizados e eles são suscetíveis a adulterações antes e depois do processo eleitoral.

4. **Voto online**: Nesse modo, a votação é realizada pela internet. Em função de o procedimento ser todo digital, é mais dinâmico que as máquinas de votação [326]. Em geral, torna o processo de votação mais rápido e com menor custo, a segurança pode ser garantida pelo uso da criptografia, além de propiciar mais comodidade ao eleitor, ao viabilizar o voto de qualquer lugar, e por isso pode aumentar a participação do eleitorado. De outra forma, não é imune a tentativas de fraudes, é mais suscetível à coerção, torna o entendimento do sistema mais complexo, o custo da infraestrutura de funcionamento pode ser alto e pode trazer dificuldade de operação para pessoas sem familiaridade com a tecnologia.

Além dessa classificação, os autores de [6] apresentam que os sistemas de votação podem ser divididos quanto à transmissão e a supervisão do voto. Em relação à primeira característica, os sistemas podem ser remotos, quando os votos são transmitidos automaticamente para um centro de totalização, por exemplo pela internet, ou não remotos, quando os votos são coletados após as eleições e transportados aos centros de contagem/totalização. A supervisão do voto refere-se ao local de votação. Em um sistema

supervisionado, os eleitores votam em centros de votação específicos sob a observação de agentes eleitorais. Em contrapartida, em um sistema não supervisionado, os eleitores podem votar de qualquer lugar.

Não se tratando de classificações, mas de tecnologias que podem ser utilizadas em mais de um dos tipos de sistemas de votação, merecem destaque as seguintes ferramentas:

1. **Criptografia**: Técnica utilização para proteção de dados é a base para garantia dos requisitos de segurança de qualquer sistema eletrônico de votação. Em [106] os autores apresentam uma revisão, na mesma medida que avaliam os respectivos pontos fortes e fracos dos principais métodos criptográficos aplicados em sistemas de votação.

2. **Impressão de votos**: Proposto para propiciar ao eleitor verificar fisicamente se suas escolhas foram gravadas corretamente pelo equipamento de votação, trata-se da impressão das escolhas do eleitor em papel pela máquina de votação, para eventual contagem posterior [94]. Porém, a impressão do voto retoma práticas da votação em papel tradicional e depende da intervenção humana. Suas premissas de segurança são em grande parte socias tais como: os votos impressos serão custodiados de maneira segura, a contagem das cédulas será realizada corretamente, um auditor verificará a contagem de forma justa, entre outras [327].

3. **Biometria**: Utilizada para garantir que apenas eleitores autorizados votem e que esse voto seja dado apenas uma única vez, a identificação biométrica do eleitor em sistemas de votação pode ser realizada por meio da impressão digital, iris dos olhos, face, entre outras características pessoais [249].

4. ***Blockchain***: É uma tecnologia de rede *peer-to-peer* que organiza os dados em uma cadeia de blocos conectados cronologicamente e usa criptografia para garantir que o dado gravado não pode ser alterado, sem que isso não seja evidenciado. Aplicado aos sistemas eletrônicos de votação, suas principais vantagens são a imutabilidade dos dados e sua natureza distribuída. A primeira garante que os votos gravados não serão adulterados e a segunda, que nenhuma entidade tenha controle total do sistema. Entretanto, a tecnologia tem problemas com a privacidade e o anonimato do eleitor [6].

5. **Computação em nuvem (*Cloud computing*)**: É um modelo no qual um provedor de serviço fornece acesso a um conjunto de recursos de computação (redes, servidores, armazenamento, entre outros) sob demanda, que podem ser rapidamente provisionados e liberados com mínimo esforço de gerenciamento. É uma virtualização da infraestrutura de rede que provê elasticidade e indepedência da localização

física. Aplicada ao processo eletrônico de votação, essa tecnologia pode aumentar sua eficiência e eficácia, ao gerar economia na infraestrutura e permitir aplicar as melhores técnicas de segurança online, ao mesmo tempo que permite aprimorar as caracaterísticas de usabilidade, acessibilidade e transparência dos sistemas eletrônicos [2].

6. **Aplicativos móveis (*mobile*)**: Com a ampliação do uso de *smartphones*, os telefones celulares deixaram de ser apenas uma ferramenta de troca de mensagem de voz. Sua flexibilidade e portabilidade permitiram o uso em outras funções, como uma máquina de votar, por exemplo. Porém, em função das limitações e recursos dos equipamentos, esse meio de votação possui desafios maiores em termos de performance e segurança que os sistemas eletrônicos tradicionais [132]. Conhecido como *m-voting*, a autenticação e privacidade dos eleitores, além da integração entre plataformas também são obstáculos a serem enfrentados [133].

No Brasil, a informatização foi uma ferramenta para combater as fraudes que eram frequentes em várias etapas do processo de votação manual. A autorização para o uso de máquinas de votar consta no Código Eleitoral de 1932. Entre os anos 1930 e 1960, alguns protótipos de equipamentos foram apresentados, mas não chegaram a ser utilizados. Em paralelo, com a introdução dos computadores no país, nos anos 1970 se iniciou a informatização da totalização dos resultados das eleições nos estados No início dos anos 1980, houve a criação da rede informatizada de dados que interligou toda a Justiça Eleitoral [328].

Em 1986, houve o recadastramento geral do eleitorado em meio eletrônico e, no final da década e início dos anos 1990, começaram as primeiras experiências com o voto eletrônico em Santa Catarina. No ano de 1993, o resultado do plebiscito para escolha da forma de governo foi totalizado de maneira eletrônica em todos os muniípios do país e, em 1994, foi realizado o processamento eletrônico do resultado das eleições daquele ano [328]. Mas o voto ainda era em papel.

O meio de registro do voto começou a mudar em 1995, quando o Tribunal Superior Eleitoral (TSE) instituiu uma Comissão para informatização do voto. Durante a definição dos requisitos, foram desenvolvidos e avaliados alguns protótipos que resultou na elaboração de um edital de licitação internacional para desenvolvimento, fabricação e distribuição do primeiro modelo de urna eletrônica do Brasil [328].

Assim, em 1996, nas eleições municipais daquele ano, as urnas eletrônicas foram utilizadas nos municípios com mais de 200 mil eleitores, aproximadamente 30% do eleitorado nacional. Nas eleições gerais de 1998, ampliou-se o uso dos equipamentos para os municípios com mais de 40 mil eleitores e a totalidade do eleitorado nacional votou com urnas

eletrônicas nas eleições municipais do ano 2000 [328]. Desde então, a urna eletrônica é o meio de votação utilizado no Brasil.

3.4 Requisitos de sistemas eletrônicos de votação

Um desafio da democracia eletrônica é aprimorar a representatividade e fortalecer os processos que visam o empoderamento dos cidadãos [103]. Assim como outros tipos de sistemas de informação, o voto eletrônico demanda um conjunto de requisitos e propriedades específicos, os quais nem sempre são completamente atendidos [6]. Nenhum protocolo de votação eletrônico satisfaz completamente todas as propriedades ao mesmo tempo, visto que algumas delas são conflitantes entre si [106][329]. Para aumentar uma, a outra será reduzida. Deve se buscar o equilíbrio que atenda a demanda de cada solução [106].

Sendo objeto de pesquisa desde os anos 1980, vários protocolos de votação eletrônica foram desenvolvidos e o conjunto de propriedades e requisitos de segurança necessários foram evoluindo [329]. Por isso, não é surpreendente que os autores proponham diferentes definições para as mesmas propriedades [106]. Não há uma definição reconhecida e padronizada dos requisitos que um sistema eletrônico de votação deve satisfazer.

Nesse sentido, este estudo se socorrerá a alguns autores para melhor contextualizar os requisitos dos sistemas eletrônicos de votação, sem a pretenção de definir uma lista exaustiva. Além dos requisitos, é importante discorrer também sobre as fases dos protocolos de votação, bem como os atores envolvidos e as diretrizes gerais.

Do ponto de vista da votação manual com cédulas de papel, a eleição pode ser divida em quatro grandes etapas: (i) o registro dos eleitores; (ii) a validação da elegibilidade dos eleitores, de modo a garantir a participação apenas dos legalmente aptos; (iii) a votação; e (iv) a contagem dos votos [7].

Já voltado para a votação eletrônica, [106] divide a eleição em três etapas: (i) pré-votação; (ii) votação; e (iii) pós-votação. A definição da lista de candidatos e de eleitores aptos ocorre na fase de pré-votação. Durante a fase de votação, os eleitores aptos depositam seus votos. Por fim, a contagem dos votos e a divulgação dos resultados são realizadas na pós-votação. De maneira semelhante, [162] propõe cinco estágios com atividades muito parecidas. Contudo, os autores acrescentam a verificação como uma atividade a ser realizada durante todo o processo eleitoral.

Quanto aos atores participantes do processo eleitoral, [162] define quatro entidades: (i) Eleitor; (ii) Autoridade Eleitoral; (iii) Candidato; e (iv) Adversário. Os Eleitores aptos escolherão os Candidatos. A Autoridade Eleitoral é a responsável pela condução da eleição e o Adversário é um atacante malicioso que tenta manipular os votos e/ou o resultado, podendo esse ser interno à Autoridade Eleitoral ou externo. De maneira complementar, os

autores de [106] acrescentam às entidades participantes: (i) o Registrador, responsável por autenticar os eleitores; e (ii) o Auditor, que são pessoas autorizadas a verificar e revisar os resultados.

Nesse estudo os requisitos serão divididos em princípios, diretrizes e propriedades que os sistemas eletrônicos devem satisfazer para aumentar a confiança geral.

Como já destacado, [7] define seis princípios a serem adotados pelos sistemas de votação, são eles: (i) Apenas eleitores aptos devem votar; (ii) Cada eleitor vota apenas uma vez; (iii) Ninguém deve ser capaz de conhecer o conteúdo do voto; (iv) Não deve ser possível duplicar votos; (v) Qualquer tentativa de alteração de voto deve ser detectada; (vi) Eleitores devem poder verificar que seu voto foi contado.

Por outro lado, em [103], voltado para sistemas de votação conectados a redes, o autor também apresenta seis princípios a serem satisfeitos, mas de maneira mais completa e maior amplitude que o estudo anterior. A Tabela 3.1 apresenta detalhadamente os princípios e diretrizes propostos. Em que pese o autor considerar sistemas conectados a rede, entende-se que as informações, em geral, são aplicáveis também a sistemas desconectados.

Princípio	**Descrição**	**Diretriz**
Generalidade (*Generality*)	Todo eleitor apto pode participar do processo eleitoral, sem exclusão ou discriminação	A elegibilidade do eleitor deve ser fundamentada e regida por lei
		O processo de votação deve ser acessível a todos os eleitores
		O voto eletrônico deve ser considerado uma forma alternativa de exercício do voto
		A infraestrutura adequada para a eleição deve ser disponibilizada, de modo a permitir que os cidadãos exerçam seu direito de votar
Liberdade (*Freedom*)	O processo eleitoral deve ocorrer sem violência, coerção, pressão, manipulação ou qualquer outra influência, exercida por um ou mais indivíduos ou pelo Estado	Nenhum eleitor pode provar em quem ou como votou
		Não deve ser permitda a divulgação de material de entidades políticas nas cercanias dos locais de votação, bem como no sistema de votação
		Deve ser assegurado o direito ao voto nulo ou em branco

Continua na próxima página

Tabela 3.1 – continuação da página anterior

Princípio	**Descrição**	**Diretriz**
Igualdade (*Equality*)	As cédulas de votação eletrônicas devem ser exibidas de maneira análoga às de papel. Ou seja, garantindo a igualdade entre os partidos políticos, candidatos e eleitores	A "aparência" do sistema de votação não deve favorecer ou discriminar nenhum dos participantes
		Um voto válido não deve ser alterado ou removido durante o processo de votação
		Todo voto tem o mesmo valor para o resultado final
		O sistema deve ser acessível independente do nível educacional, idade ou condição física do eleitor
		Cada eleitor apto pode votar apenas uma vez
Sigilo (*Secrecy*)	A relação entre o voto e o eleitor deve ser irreversível para garantir que os votos sejam realizados livremente	O sigilo do voto deve ser garantido durante todo o processo eleitoral
		Ninguém deve ser capaz de vincular o voto ao eleitor
		Deve haver uma separação clara entre os procedimentos de registro e autenticação do eleitor, bem como da votação e transmissão do voto
		O sistema de votação deve viabilizar tecnicamente o controle e a recontagem dos votos, garantindo o anonimato dos eleitores
Objetividade (*Directness*)	O processo de decisão do eleitor tem de ser direto, sem intermediários. Cada voto tem de ser registrado e contado diretamente	A divulgação de resultados deve ser realizada apenas após o encerramento da votação

Continua na próxima página

Tabela 3.1 – continuação da página anterior		
Princípio	**Descrição**	**Diretriz**
Democracia (*Democracy*)	Os eleitores devem ser capazes de entender o funcionamento da eleição	O sistema de votação deve permitir sua verificação pelos eleitores ou por qualquer interessado na eleição
		As operações eletrônicas devem ser monitoradas e registradas
		O resultado da eleição deve garantir a vontade do eleitor

Tabela 3.1: Princípios e diretrizes (Fonte [103])

Tendo entre suas referências esses princípios e diretrizes, [106] define propriedades ou requisitos que os sistemas de votação devem atender. Os autores os dividem em requistos funcionais e de segurança. Os requisitos funcionais definem as funções que o sistema deve realizar, podendo ser testados diretamente, são eles:

1. **Robustez (*Robustness*)**: Nenhuma parte desonesta pode atrapalhar as eleições.
2. **Justiça (*Fairness*)**: Nenhum resultado parcial pode ser divulgado.
3. **Verificabilidade (*Verifiability*)**: O resultado não pode ser falsificado. Pode ocorrer de maneira individual, quando o eleitor pode verificar que seu voto consta do resultado final, ou universal, quando qualquer um pode verificar que todos os votos constam do resultado final.
4. **Solidez, integridade e correção (*Soundness, completeness and correctness*)**: O resultado final deve conter todos os votos válidos.
5. **Elegibilidade (*Eligibility*)**: Apenas eleitores aptos podem votar.
6. **Liberdade de disputa (*Dispute-freeness*)**: Qualquer partido político pode verificar publicamente se um participante segue o protocolo definido, em qualquer fase da eleição.
7. **Transparência (*Transparency*)**: O voto deve possuir máxima transparência durante a coleta, armazenamento e contagem, preservando-se seu sigilo.
8. **Precisão (*Accuracy*)**: O sistema deve ser isento de erros e os votos válidos registrados e contados corretamente. Este item tem estreita relação com a verificabilidade universal.

9. **Responsabilidade (*Accountability*)**: Se a verificação do voto falhar, o eleitor deve poder provar que votou, tendo seu sigilo preservado.
10. **Praticidade (*Practicality*)**: As funcionalidades e premissas do sistema tem de ser aplicáveis a eleições em grande escala.
11. **Escalabilidade (*Scalability*)**: O sistema deve ser versátil em termos de capacidade computacional, comunicação e armazenamento.

Os requisitos de segurança são funcionalidades as quais visam garantir que o sistema de votação satisfaça propriedades para eliminar possíveis vulnerabilidades. Os autores de [106] definem os listados a seguir:

1. **Privacidade e sigilo do voto (*Privacy and vote secrecy*)**: Os votos tem de ser anônimos.
2. **Prevenção de votação dupla, unicidade e não reutilização (*Double-voting prevention, unicity and unreusability*)**: Eleitores aptos só podem votar uma vez.
3. **Sem comprovação (*Receipt-freeness*)**: O eleitor não pode obter nenhuma informação capaz de provar como ele votou ou identificar seu voto.
4. **Resistente à coerção (*Coercion-resistance*)**: O sistema tem de inviabilizar a tentativa de coerção ao eleitor.
5. **Anonimato (*Anonymity*)**: Não se pode identificar o voto do eleitor.
6. **Autenticação (*Authentication*)**: Apenas eleitores aptos são autorizados a votar.

Como destacado anteriormente, algumas das propriedades exigidas nos sistemas de votação eletrônica são conflitantes entre si. Não à toa, a compatibilização da privacidade e a verificabilidade do voto pode ser considerada um dos maiores desafios computacionais nos sistemas de votação [302].

Inicialmente, os sistemas de votação foram orientados a garantir a privacidade do voto, na mesma medida que buscavam garantir a verificabilidade individual do eleitor. Posteriormente, na busca por aumentar a confiança dos eleitores, os sistemas evoluíram as propriedades de garantia da privacidade e adotaram a rastreabilidade do voto sem a emissão de comprovantes (*receipt-freeness*) e, mais a frente, a proteção à coerção (*coercion-resistance*) [302].

Por outro lado, a verificabilidade individual evoluiu para a universal e, posteriormente, o conceito foi refinado em três outras propriedades para os sistemas de votação: (i) *cast-as-intended*, quando o eleitor é capaz de verificar que o sistema registra o voto de acordo

com sua inteção; (ii) *recorded-as-cast*, quando o eleitor é capaz de verificar que o voto foi gravado corretamente; e (iii) *tallied-as-recorded*, quando qualquer um pode verificar que o resultado está correto a partir dos votos recebidos [302].

O tempo demonstrou que os sistemas de votação evoluíram seu foco de garantir a privacidade, enquanto permitia a verificabilidade, para sistemas com verificabilidade prática, não apenas teórica, enquanto satisfazem robustos requisitos de privacidade. Esses sistemas são conhecidos por terem verificabilidade *End-to-End* (E2E) [302].

Apesar de não haver consenso e uniformidade entre os autores sobre princípios e propriedades que os sistemas de votação eletrônica devem atender, há iniciativas que buscam essa padronização, conforme apresentam os autores do estudo [137]. Essa publicação propõe um modelo de regulação do voto eletrônico, especificamente o *online*, para o Canadá. Em sua avaliação, os autores apresentam como referência o *Voluntary Voting System Guidelines* (VVSG) [330], modelo adotado nos Estados Unidos, assim como as diretrizes do Conselho Europeu [324] para a comunidade européia.

De caráter voluntário para os estados americanos, o VVSG é um conjunto de especificações e requisitos utilizados como referência para avaliação de sistemas de votação nos EUA. Criado pela Comissão de Assistência Eleitoral (*Election Assistance Comission*), lista 15 princípios e 54 diretrizes de avaliação entre funcionalidades básicas, requisitos de acessibilidade e recursos de segurança. A Tabela 3.2 apresenta uma visão consolidada dos itens verificados no VVSG.

Princípio	**Descrição**	**Diretriz**
1. Design de alta qualidade (*High Quality Design*)	O sistema de votação tem de ser projetado para realizar eleições de forma precisa, completa e robusta.	1.1 O sistema de votação deve ser projetado considerando as especificações comunmente aceitas do processo eleitoral.
		1.2 O sistema de votação deve ser projetado para funcionar corretamente em condições operacionais reais.
		1.3 O sistema de votação deve permitir aos avaliadores identificar corretamente as propriedades especificadas.

Continua na próxima página

Tabela 3.2 – continuação da página anterior		
Princípio	**Descrição**	**Diretriz**
2. Implementação de alta qualidade (*High Quality Implementation*)	O sistema de votação tem de ser implementado com alta qualidade, utilizando as melhores práticas.	2.1 O software do sistema de votação é desenvolvido utilizando as melhores e mais confiáveis práticas.
		2.2 O sistema de votação deve ser implementado centrado no usuário, considerando aqueles com deficiências e os trabalhadores eleitorais.
		2.3 A lógica do sistema de votação deve ser clara e bem estruturada.
		2.4 A estrutura do sistema de votação deve ser modular, escalável e robusta.
		2.5 Os processos e dados do sistema de votação devem ser suportados com integridade.
		2.6 O sistema de votação deve suportar erros de maneira robusta e se recuperar de falhas.
		2.7 O sistema de votação deve funcionar de maneira confiável.
3. Transparente (*Transparent*)	O sistema e os processo de votação devem ser projetados para fornecer transparência.	3.1 A documentação do sistema de votação, sua operação, bem como os requisitos de acessibilidade e segurança devem ser descritos de maneira compreensível.
		3.2 Os processos e transações, físicas e digitais, devem estar disponíveis para inspeção.
		3.3 O público deve poder entender e verificar as operações do sistema de votação durante toda a eleição.

Continua na próxima página

Tabela 3.2 – continuação da página anterior

Princípio	**Descrição**	**Diretriz**
4. Interoperável (*Interoperable*)	O sistema de votação deve ser iteroperável com sistemas externos.	4.1 Os dados do sistema de votação que são importados ou exportados devem estar em um formato interoperável.
		4.2 Devem ser utilizados formatos e padrões públicos.
		4.3 Devem ser utilizadas Interfaces de hardware e protocolos de comunicação de mercado.
		4.4 Dispositivos de prateleira podem ser utilizados, se atenderem aos requisitos aplicáveis.
5. Equivalente e Consistente	Todos os eleitores podem acessar e utilizar o sistema de votação, independentemente de suas habilidades.	5.1 Os eleitores devem ter uma experiência consistente durante todo o processo de votação.
		5.2 Os eleitores devem receber informações e opções equivalentes em todos os modos de votação.
6. Privacidade do eleitor (*Voter Privacy*)	Os eleitores podem votar de forma privada e independente.	6.1 O processo de votação deve preservar a privacidade do eleitor durante a votação.
		6.2 Os eleitores podem votar sem ajuda de outras pessoas.
7. Registrado conforme pretendido (*Marked, Verified, and Cast as Intended*)	Os votos devem ser apresentados de maneira compreensível e podem ser registrados e verificados por todos os eleitores.	7.1 O sistema de votação deve apresentar o voto de maneira compreensível para a a maioria dos eleitores, os quais podem ajustar as configurações e preferências para atender as suas necessidades.

Continua na próxima página

Tabela 3.2 – continuação da página anterior

Princípio	Descrição	Diretriz
		7.2 Eleitores e trabalhadores eleitorais podem usar todos os controles com precisão, e os eleitores devem ter controle de todas as mudanças nas cédulas de votação eletrônica.
		7.3 Os eleitores devem entender todas as informações à medida que são apresentadas, incluindo instruções, mensagens do sistema e de erro.
8. Robusto, seguro, utilizável e acessível (*Robust, Safe, Usable, and Accessible*)	O sistema e os processos de votação devem ser robustos, seguros, utilizáveis e acessíveis.	8.1 O hardware, software e acessórios do sistema de votação devem ser robustos e não expor os usuários a condições prejudiciais.
		8.2 O sistema de votação deve atender aos padrões federais de acessibilidade.
		8.3 O sistema de votação deve ser avaliado quanto à usabilidade para os eleitores, incluindo aqueles com deficiência.
		8.4 O sistema de votação deve ser avaliado quanto à usabilidade para os trabalhadores eleitorais.
9. Auditável (*Auditable*)	O sistema de votação deve ser auditável e baseado em evidências.	9.1 Um erro ou falha no software ou hardware do sistema de votação não pode causar um mudança indetectável nos resultados.

Continua na próxima página

Tabela 3.2 – continuação da página anterior

Princípio	**Descrição**	**Diretriz**
		9.2 O sistema de votação deve produzir e disponibilizar registros que propiciam verificar se o resultado da eleição está correto e, na medida do possível, identificar a causa raiz de qualquer irregularidade.
		9.3 Os registros do sistema de votação devem ser resistentes a tentativas intencionais de adulteração e erros acidentais.
		9.4 O sistema de votação deve suportar auditorias eficientes.
10. Sigilo do voto (*Ballot Secrecy*)	O sistema de votação deve proteger o sigilo do voto dos eleitores	10.1 O sigilo do voto deve ser mantido durante todo o processo de votação.
		10.2 O sistema de votação não deve registrar informações sobre o eleitor que possam ser usadas para associar sua identidade as suas escolhas.
11. Controle de acesso (*Access Control*)	O sistema de votação deve autenticar administradores, usuários, dispositivos e serviços antes de conceder acesso a funções sensíveis.	11.1 O sistema de votação deve permitir registrar, monitorar, revisar e modificar o acesso, privilégios, contas, atividades e autorizações.
		11.2 O sistema de votação deve limitar o acesso a funções e dados de acordo com a autorização concedida.

Continua na próxima página

Tabela 3.2 – continuação da página anterior		
Princípio	**Descrição**	**Diretriz**
		11.3 O sistema de votação deve oferecer suporte a mecanismos de autenticação fortes e configuráveis para verificar as identidades de usuários autorizados e incluir mecanismos de autenticação multifator para operações críticas
		11.4 As políticas de controle de acesso sistema de votação devem reforçar os princípios de menos privilégio e separação de responsabilidades
		11.5 O acesso lógico aos ativos do sistema de votação deve ser revogado quando não é mais necessário.
12. Segurança física (*Physical Security*)	O sistema de votação deve impedir ou detectar tentativas de adulteração do hardware.	12.1 O sistema de votação deve suportar mecanismos para detectar acesso físico não autorizado.
		12.2 O sistema de votação deve disponibilizar apenas portas físicas e pontos de acesso essenciais para operações de votação.
13. Proteção de dados (*Data Protection*)	O sistema de votação deve proteger os dados contra acesso, modificação ou exclusão não autorizados.	13.1 O sistema de votação deve impedir o acesso não autorizado ou a manipulação da configuração do registros de votos, de auditoria ou dos dados transmitidos.
		13.2 A fonte e a integridade dos relatórios de totalização devem ser verificáveis.
		13.3 Todos os algoritmos criptográficos devem ser públicos, bem avaliados e padronizados.

Continua na próxima página

Tabela 3.2 – continuação da página anterior		
Princípio	**Descrição**	**Diretriz**
		13.4 O sistema de votação deve proteger a integridade, autenticidade e confidencialidade dos dados transmitidos por todas as redes.
14. Integridade do sistema (*System Integrity*)	O sistema de votação deve desempenhar sua função livre de manipulação intencional ou acidental.	14.1 O sistema de votação deve usar várias camadas de controles para fornecer resiliência contra falhas de segurança ou vulnerabilidades.
		14.2 O sistema de votação deve ser projetado para limitar sua superfície de ataque.
		14.3 O sistema de votação deve manter e verificar a integridade do software, firmware e outros componentes críticos.
		14.4 As atualizações do software do sistema de votação devem ser autorizadas por um administrador antes da instalação.
15. Detecção e monitoramento (*Detection and Monitoring*)	O sistema de votação deve fornecer mecanismos para detectar comportamento anômalo ou malicioso.	15.1 O equipamento do sistema de votação deve registrar atividades e eventos importantes.
		15.2 O sistema de votação deve gerar e armazenar todas as mensagens de erro conforme elas ocorrem.
		15.3 O sistema de votação deve ser protegido contra *malware*.
		15.4 Um sistema de votação com recursos de rede deve empregar defesas modernas contra ciberataques.

Continua na próxima página

Tabela 3.2 – continuação da página anterior		
Princípio	**Descrição**	**Diretriz**

Tabela 3.2: Princípios e diretrizes VVSG (Fonte [330])

A iniciativa européia referência para padronização de requisitos que os sistemas de votação devem atender também possui caráter voluntário para os países membros. O Conselho da Europa define 8 diretrizes e estabelece que apenas os sistemas de votação eletrônica que são seguros, confiáveis, eficientes, tecnicamente robustos, abertos à verificação independente e facilmente acessíveis aos eleitores irão construir a confiança do público, um requisito para a realização de eleições eletrônicas [324]. A Tabela 3.3 elenca as diretrizes do Conselho Europeu para o voto eletrônico.

Princípio	**Diretriz**
1. Sufrágio universal (*Universal suffrage*)	1. A interface do eleitor de um sistema de votação eletrônica deve ser fácil para todos os eleitores entenderem e utilizarem.
	2. O sistema de votação eletrônica deve ser projetado, na medida do possível, para permitir que pessoas com deficiência e necessidades especiais votem independentemente.
	3. A menos que os canais de votação eletrônica remota sejam universalmente acessíveis, eles devem ser apenas um meio adicional e opcional de votação.
	4. Antes de votar por meio eletrônico à distância, o eleitor deve ser informado que a eleição é real ou referendo.
2. Sufrágio igual (*Equal suffrage*)	5. Todas as informações oficiais devem ser apresentadas de maneira igual em todos canais de votação.
	6. Quando canais de votação eletrônicos e não eletrônicos forem usados na mesma eleição ou referendo, deve haver um método seguro e confiável para agregar todos os votos e calcular o resultado.
	7. Deve ser assegurada a identificação única e inequívoca dos eleitores.

Continua na próxima página

Tabela 3.3 – continuação da página anterior

Princípio	**Diretriz**
	8. O sistema de votação eletrônica somente concederá acesso ao usuário após sua a autenticação como eleitor apto.
	9. O sistema de votação eletrônica deve garantir que apenas o número apropriado de votos por eleitor seja armazenado na urna eletrônica e incluído no resultado da eleição.
3. Sufrágio livre (*Free suffrage*)	10. A intenção do eleitor não pode ser afetada pelo sistema de votação, nem por qualquer influência indevida.
	11. Deve ser assegurado que o sistema de votação eletrônica apresente cédulas e informações autênticas ao eleitor.
	12. A forma como os eleitores são orientados no processo de votação eletrônica não deve levá-los a votar precipitadamente ou sem confirmação.
	13. O sistema de votação eletrônica não deve influenciar a preferência do eleitor por qualquer uma das opções de votação.
	14. O sistema de votação eletrônica deve avisar ao eleitor o lançamento de voto inválido.
	15. O eleitor poderá verificar o registro correto do seu voto. Eventual tentativa de modificação do voto deve ser detectada.
	16. O eleitor receberá a confirmação do sistema de que o voto foi registrado com sucesso e que o processo de votação foi concluído.
	17. O sistema de votação eletrônica deve fornecer evidências sólidas de que cada voto é autêntico e consta do resultado final. A verificação das evidências deve ser realizada por meios independentes do sistema de votação eletrônica.

Continua na próxima página

Tabela 3.3 – continuação da página anterior

Princípio	**Diretriz**
	18. O sistema deve fornecer evidências sólidas de que apenas os votos dos eleitores aptos constam do resultado final. A verificação das evidências deve ser realizada por meios independentes do sistema de votação eletrônica.
4. Sufrágio secreto (*Secret suffrage*)	19. A votação eletrônica deve ser organizada de maneira a garantir o sigilo do voto em todas as etapas do processo de votação.
	20. O sistema de votação eletrônica processará e armazenará, pelo tempo que for necessário, apenas os dados pessoais necessários para a realização da eleição.
	21. O sistema de votação eletrônica e qualquer parte autorizada devem proteger os dados de autenticação para que partes não autorizadas não possam fazer uso indevido, interceptar, modificar ou obter conhecimento desses dados.
	22. Os registros de eleitores armazenados ou comunicados pelo sistema de votação eletrônica devem ser acessíveis apenas a pessoas autorizadas.
	23. O sistema de votação eletrônica não deve fornecer ao eleitor prova do teor do voto emitido para utilização por terceiros.
	24. O sistema de votação eletrônica não permitirá a divulgação do resultado até o fechamento da urna eletrônica e o fim da votação.
	25. A votação eletrônica deve garantir o sigilo das escolhas registradas ou apagadas pelo eleitor.
	26. A etapa de apuração deve garantir a anonimicidade do voto, de maneira que não seja possível relacioná-lo com o eleitor.
5. Requisitos regulamentares e organizacionais (*Regulatory and organisational requirement*)	27. Os Estados-Membros que introduzirem o voto eletrônico devem fazê-lo de maneira gradual e progressiva.

Continua na próxima página

Tabela 3.3 – continuação da página anterior

Princípio	**Diretriz**
	28. Antes de introduzir o voto eletrônico, os Estados membros devem realizar as mudanças necessárias na legislação.
	29. A legislação deve regular as responsabilidades pelo funcionamento dos sistemas de votação eletrônica e assegurar o seu controle pelo órgão de gestão eleitoral.
	30. O órgão de gestão eleitoral deve ser responsável pelo processo de contagem dos votos, o qual pode ser acompanhada por qualquer observador.
6. Transparência e observação (*Transparency and observation*)	31. Os Estados-Membros devem ser transparentes em todos os aspetos da votação eletrônica.
	32. O público em geral deverá ser informado, com antecedência e em linguagem clara e simples, sobre: (i) o início da votação; (ii) os requisitos para participação dos eleitores; (iii) o uso correto e o funcionamento do sistema de votação eletrônica; e (iv) o calendário da votação eletrônica, contendo todas as fases.
	33. Os componentes do sistema de votação eletrônica devem ser divulgados para fins de verificação e certificação.
	34. Qualquer observador, na medida permitida por lei, poderá acompanhar as eleições eletrônicas, incluindo a compilação dos resultados.
	35. Devem ser utilizados padrões abertos (*open sources*) para permitir a interoperabilidade entre componentes ou serviços técnicos.
7. Responsabilidade (*Accountability*)	36. Os Estados-Membros devem desenvolver e manter atualizados requisitos técnicos, de avaliação e de certificação, além de assegurar que eles refletem os princípios jurídicos e democráticos pertinentes.

Continua na próxima página

Tabela 3.3 – continuação da página anterior

Princípio	**Diretriz**
	37. Antes da introdução de um sistema de votação eletrônica e de maneira regular, especialmente após a introdução de alterações significativas, a conformidade do sistema com os requisitos técnicos deve ser verificada por organismo independente, em certificação formal ou outro controle apropriado.
	38. O certificado, ou qualquer outro documento emitido, deve identificar claramente o objeto da avaliação e possuir salvaguardas para evitar que seja modificado inadvertidamente.
	39. O sistema de votação eletrônica deve ser auditável. O processo de auditoria deve ser aberto, abrangente e relatar possíveis problemas e ameaças.
8. Confiabilidade e segurança (*Reliability and security*)	40. O órgão de gestão eleitoral deve ser responsável pelo cumprimento de todas as exigências, mesmo em caso de falhas e ataques, bem como pela disponibilidade, confiabilidade, usabilidade e segurança do sistema de votação eletrônica.
	41. Só devem ter acesso à infraestrutura central, aos servidores e aos dados eleitorais as pessoas autorizadas pela entidade gestora eleitoral. As nomeações dessas pessoas devem ser claramente regulamentadas.
	42. Antes da realização de qualquer eleição, o órgão de gestão eleitoral deve assegurar-se de que o sistema é genuíno e funciona corretamente.
	43. Um procedimento deve ser estabelecido para instalação de atualizações e correções dos softwares relevantes.
	44. Se armazenados ou comunicados fora de ambientes controlados, os votos deverão ser criptografados.

Continua na próxima página

Tabela 3.3 – continuação da página anterior	
Princípio	**Diretriz**
	45. Os votos e as informações do eleitor devem ser mantidos lacrados até o início do processo de contagem.
	46. O órgão de gestão eleitoral deve tratar todo o material criptográfico de maneira segura.
	47. Na ocorrência de incidentes que possam ameaçar a integridade do sistema, os responsáveis pela operação devem informar imediatamente o órgão de gestão eleitoral.
	48. A autenticidade, disponibilidade e integridade dos cadernos de votação e da lista de candidatos devem ser mantidas.
	49. O sistema de votação electrônica deve identificar eventuais votos irregulares.

Tabela 3.3: Princípios e diretrizes do Conselho Europeu (Fonte [324])

Diante das informações apresentadas, apesar de não se encontrar uma referência reconhecida como única e uma padronização, observa-se que as várias iniciativas de definição de princípios, diretrizes e propriedades para os sistemas eletrônicos de votação são convergentes e possuem similaridades.

3.5 Confiança em sistemas eletrônicos de votação

A informatização do processo de votação pode ser motivada por objetivos diversos, a depender do país. Se por um lado os países europeus tendem a utilizar o voto eletrônico como medida para aumentar a participação de eleitores [331], a América Latina busca explorar o potencial de aumento de confiança [332]. A confiança é fator crítico para implantar o voto eletrônico. Países que falharam na sua implementação sentiram a importância da falta dela [8].

É difícil definir um conceito único para a confiança, considerando os vários campos do conhecimento que o empregam e o exploram, tais como: administração, filosofia, sociologia, psicologia, marketing, computação (interação homem-máquina), psicologia, governo eletrônico, comércio eletrônico, entre outros [333]. Em [334], o autor registra que alguns acadêmicos definem a confiança como a expectativa de que outras pessoas, instituições ou grupos com os quais interagimos realizarão ações alinhadas ao nosso interesse. Por outro

lado, [335] considera a confiança como a crença de alguém de que a outra parte não a prejudicará e se comportará de maneira benéfica, razoável, previsível e adequada. Após uma revisão da literatura sobre o tema, a mesma autora anotou em [336] que a confiança tem relação com compromisso e consciência, sendo: interpessoal; dinâmica ou temporal, variando a cada situação; e voluntária.

Quando se fala em eleição, a confiança pode ser representada pela aceitação do resultado, especialmente por parte dos perdedores [304]. Ainda, pode ser conceituada pela convicção dos eleitores na contagem correta dos seus votos [332]. Ampliando o conceito, a confiança pode ser entendida como um estado cognitivo dos eleitores, associado as suas experiências de vida com os múltiplos atores envolvidos no contexto político e socioeconômico de um país [8]. Para confiar em um sistema de votação, há que se confiar no governo, na tecnologia, e na entidade organizadora da eleição [8].

Eleição eletrônica é um dos crescentes serviços disponibilizados por governos, com auxílio ou não de empresas, conceituados como *e-governament*. Para exemplificar, pode-se citar os serviços eletrônicos educacionais (*e-learning*), bancários (*e-banking*), comerciais (*e-commerce*) e de saúde (*e-health*), entre outros. Os serviços eletrônicos governamentais envolvem três principais atores quando se aborda a questão da confiança: a tecnologia, os cidadãos e as organizações [20]. De acordo com esses autores, a confiança é um componente fundamental e que, essencialmente, depende da convicção da garantia da privacidade e da segurança dos dados. Complementam ainda que, naturalmente, os cidadãos tendem a suspeitar do poder dos governos e, geralmente, desconhecem como seus dados serão utilizados. Não a toa, estudos demonstraram a confiança como fator mais relevante para adoção do *e-governament* [102].

Por outro lado, a tecnologia aplicada à votação tem impacto substancial na segurança real e percebida das eleições [304]. A tecnologia aborda uma série de considerações relevantes relacionadas à confiança do eleitor na votação eletrônica, como a autenticação dos votantes, além da integridade e a confidencialidade dos dados [102]. Nesse contexto, em um estudo para avaliar as variáveis que influenciam a adoção do voto eletrônico, estes autores propuseram um modelo de confiança na tecnologia, além de defenderem que a confiança tem de estar presente nas três grandes fases do processo eletrônico de votação: o registro dos eleitores, a votação e a totalização dos votos.

Esse modelo de confiança na tecnologia [102] é composto por quatro elementos ou dimensões: segurança, privacidade, usabilidade e validade.

1. **Segurança (*Security*)**: considerada uma das maiores preocupações relacionadas ao voto eletrônico, os autores a definem como a proteção contra ameaças que possam destruir, divulgar indevidamente ou modificar dados, tornar o serviço indisponível, ou mesmo concretizar uma fraude. Inclui, mas não está limitada ao controle de

acesso e à integridade de dados, bem como o controle de alteração de software e a segurança física dos locais e equipamentos. É capaz de influenciar decisivamente a crença dos eleitores de que a tecnologia em uso consegue garantir informações precisas e transações seguras.

2. **Privacidade (*Privacy*)**: está relacionada ao anonimato do eleitor e à confidencialidade dos dados durante a votação. O sistema de votação deve garantir o sigilo do voto e impedir o eleitor de provar em quem votou. Sem isso, tanto a coação quanto a venda de votos podem ser estimuladas. Se a privacidade não for protegida, os eleitores podem não confiar no sistema.

3. **Usabilidade (*Usability*)**: guarda relação com a facilidade ou o grau de esforço para se utilizar a solução. Na votação eletrônica, contempla a estrutura da cédula de votação e quão fácil ou intuitivo é a utilização do sistema de votação. É um indicador para se verificar a qualidade e a capacidade de o sistema atingir sua missão com sucesso.

4. **Validade (*Validity*)**: no contexto eleitoral, as fraudes eletrônicas se tornaram uma grande preocupação, em função das notícias constamente veiculadas. A votação eletrônica tem o potencial de ampliar o potencial e a abrangência de uma fraude, quando comparada ao voto manual. Nesse contexto, a validade se aplica aos eleitores e aos resultados. A não verificação da elegibilidade do eleitor, bem como a produção de resultados imprecisos, impactam na confiança os eleitores.

Assim, a confiança na tecnologia de votação eletrônica pode ser definida como a disposição de os cidadãos estarem suscetíveis à tecnologia, com base em suas expectativas de segurança, privacidade, usabilidade e validade do sistema de votação [102].

Quando se refere à autoridade organizadora da eleição, [10] defende que a independência é importante para garantir que os vencedores e os vencidos reconheçam a eleição como justa e legítima, aumentando assim a confiança nos eleitos. Por esse motivo, o autor entende não haver função pública mais importante para proteção da democracia que a realização de eleições que reflitam a intenção dos eleitores e garantam a confiança do eleitorado.

O autor apresenta ainda uma tipologia para classificar as entidades gestoras da eleição em três categorias: (i) as independentes; (ii) as governamentais; e (iii) as mistas. As independentes são institucionalmente independentes e autônomas do Poder Executivo. As governamentais pertecem ao Poder Executivo e as mistas, pertencem ao Poder Executivo, mas com grau de supervisão externa.

Nesse contexto de avaliar a indenpedência das entidades gestoras da eleição para identificar seu grau de confiança no uso da tecnologia, [10] apresenta quatro questionamentos:

1. **Qual o papel da entidade no processo de tomada de decisão sobre o uso de tecnologia no processo eleitoral?** O uso da tecnologia impacta o processo eleitoral. Portanto, a forma como a entidade gestora se envolve na decisão de uso ou não de tecnologias reflete seu grau de independência para condução das eleições.
2. **Quem é o dono da tecnologia utilizada?** Quanto mais propriedade e controle a entidade gestora da eleição possuir sobre as tecnologias utilizadas, maior será a sua independência.
3. **Quem fornece o suporte tecnológico no dia da eleição?** Caso a entidade gestora da eleição não seja capaz de prestar esse apoio, será dependente de algum terceiro.
4. **Como o desenho institucional afeta o uso e a propriedade da tecnologia?** Verifica se a situação formal da entidade gestora da eleição se reflete na prática. Por exemplo, se a entidade é formalmente independente, mas não possui autonomia sobre o uso de tecnologia no processo eleitoral, na prática, ela é menos independente do que se espera em virtude da sua situação legal/formal.

Além dessa visão sobre a confiança aplicada às entidades gestoras da eleição, [331] acrescenta, utilizando a teoria de identidade social, que a confiança depende também das pessoas por trás da tecnologia. Segundo estes autores, a percepção de os cidadãos identificarem pessoas "iguais a eles" na entidade eleitoral pode influenciar suas avaliações e comportamento em relação à tecnologia.

Em uma visão mais ampla do conceito da confiança, ela pode ser compreendida como um elemento tecno-social do processo eleitoral eletrônico, considerando as intituições políticas e as condições sócio-econômicas de um país [8]. Nessa abordagem, o foco da confiança não se restringe apenas ao equipamento de votação e inclui outros atores envolvidos no processo eleitoral como provedores de serviço, partidos políticos, observadores externos e a mídia em geral.

Nessa visão ampliada, a confiabilidade do voto eletrônico é vista como um aspecto da integridade da eleição, considerando a confiança pública no processo e a aceitação dos resultados. As más práticas eleitorais criam percepções de que as eleições são fraudulentas e prejudicam a confiança dos cidadãos nas instituições ou no processo eleitoral, levando a protestos que desafiam a legitimidade dos resultados [8]. Os autores apresentam ainda um modelo de integridade eleitoral, detalhado na Figura 3.2.

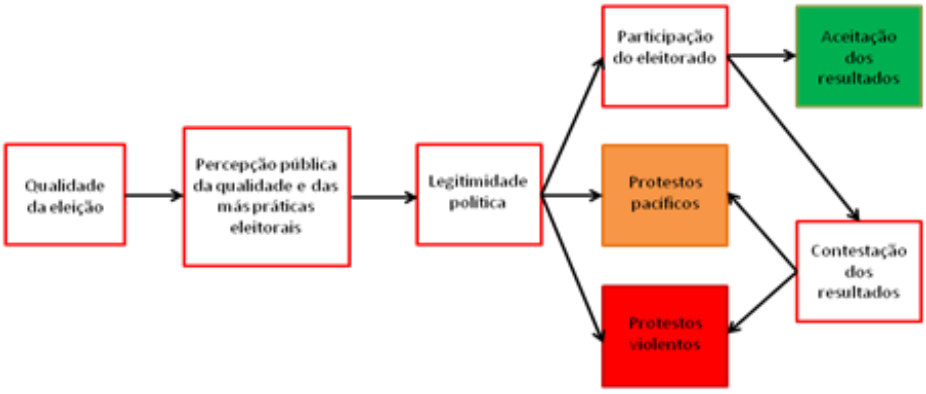

Figura 3.2: Modelo de integridade eleitoral (Fonte: Adaptado de [8])

Depreende-se desse modelo de integridade eleitoral que a participação do eleitorado na eleição é condicionada pela sua percepção na legitimidade política do processo e na confiança no voto eletrônico. Consequentemente, o resultado será aceito ou haverá protestos, pacíficos ou violentos. Assim, eventuais dúvidas de legitimidade política e descontentamento com outros aspectos do ciclo eleitoral, anteriores ou posteriores ao dia da eleição, podem levar a eventuais protestos. Um desafio para o estudo da confiança no voto eletrônico é identificar as várias preocupações públicas expressas nas ações observadas pós-eleitorais [8].

Ainda de acordo com essa publicação [8], na qual os autores visam identificar e explicar a confiança dos cidadãos na votação eletrônica na Índia utilizando como referência as iniciativas de Brasil e Holanda, são apresentados quatro mecanismos na tentativa de explicar como é produzida a confiança no voto eletrônico, são eles:

1. **Associação do voto eletrônico com o fortalecimento da democracia**. A confiança no voto eletrônico tende a aumentar quando os eleitores percebem sua contribuição para a realização de eleições democráticas e justas. Do contrário, a mera utilização da tecnologia por conveniência da entidade organizadora das eleições não desperta nos cidadãos a convicção dos possíveis benefícios.

2. **O relacionamento do voto eletrônico com a reputação da entidade gestora da eleição**. Além da necessidade de reconhecer a competência da entidade gestora da eleição para aplicar a tecnologia, a confiança do eleitor no voto eletrônico também é influenciada pela credibilidade política da entidade na condução do processo eleitoral.

3. **A promoção de uma atitude pública positiva em relação ao uso da tecnologia da informação**. Cada país tem entendimentos diferentes sobre os possíveis benefícios e riscos do uso da tecnologia. É a chamada "cultura digital". Em alguns

países, a atitude predominante é acolher o uso da tecnologia como ferramenta de melhoria da vida da população. Entretanto, em outras nações destaca-se a preocupação com os riscos e aspectos negativos do uso da tecnologia.

4. **A disposição de confiança em meio às más práticas eleitorais**. A atitude dos eleitores em relação ao voto eletrônico também é afetada pela sua experiência com o processo eleitoral como um todo, incluindo suas relações com as casas legislativas. A confiança é formada pelas vivências dos eleitoreis durante todo o ciclo eleitoral, não apenas no momento da votação.

Os autores destacam ainda que confiança não é um resultado binário absoluto de que ela existe ou não. A combinação dos quatro mecanismos indica uma posição entre a confiança absoluta e a suspeita profunda, refletindo em uma maior disposição para confiar ou suspeitar das soluções de votação eletrônica [8].

De maneira semelhante, a partir de uma visão ampliada da formação da confiança em sistemas eletrônicos de votação, o IDEA elaborou a Pirâmide de Confiança do Voto Eletrônico [337], conforme Figura 3.3.

Figura 3.3: Pirâmide de confiança do voto eletrônico (Fonte: Adaptado de [337])

Segundo os autores, a Pirâmide é formada por 3 níveis. No topo, encontra-se o processo eleitoral confiável, que deve ser o objetivo principal de qualquer iniciativa, além de contar com alto nível de participação e confiança pública. Essa confiança pública é formada, inicialmente, no contexto político-social em que o voto eletrônico é introduzido. Quanto mais confiáveis forem a autoridade eleitoral e o ambiente político, bem como maior a participação da sociedade no processo, mais confiança pública.

Por outro lado, o contexto político-social é incluenciado pelo ambiente técnico-operacional. Eventuais deficiências nas bases operacionais, técnicas ou jurídicas poderão até resistir caso o ambiente sócio-político seja favorável. Porém, acabarão por vir à tona e poderão desacreditar não apenas o voto eletrônico, mas o processo eleitoral como um todo.

De outra maneira, mesmo que os aspectos técnicos e os fundamentos operacionais da solução de votação eletrônica sejam sólidos, podem não resistir a um contexto sócio-político negativo. O fraco apoio social e político dificulta a implementação de uma solução confiável, pois é mais fácil para os opositores da iniciativa minar a confiança na tecnologia de votação.

Ainda, seja no ambiente político-social ou no técnico-operacional, é difícil demonstrar a confiabilidade da solução de votação eletrônica no curto ou médio prazo. Por isso, o tempo de implantação da solução é fundamental para superar o desafio de fazer com que o público não especializado compreenda a confie no voto eletrônico.

Detalhando o nível intermediário da pirâmide, o contexto político-social é composto pela Autoridade Eleitoral, a Política, a Sociedade e o Prazo. Os autores defendem que, ao se adotar um processo de votação eletrônico, transfere-se a responsabilidade que se encontra nos milhares locais de votação para a autoridade eleitoral. Dessa forma, a integridade da autoridade gestora da eleição é fundamental na formação da confiança na solução. Esse conceito de integridade é amplo e envolve o acesso de outras partes interessadas como partidos e candidatos, além de precisar considerar como são dirimidos os conflitos, assim como se a população reconhece procedentes os alegados benefícios com a informatização do voto.

Quanto à Política, sistemas de votação eletrônica podem ser mais facilmente aceitos quando existe consenso político sobre seus benefícios. A oposição dos atores políticos pode ser técnica, quando possuem preocupações legítimas, ou apenas política, caso entendam que podem perder vantagens ou não confiam na autoridade eleitoral. Portanto, alinhar apoio multipartidário para aprovação de alterações legislativas necessárias à introdução de sistemas de votação eletrônica é de suma importância.

Em relação à Sociedade, quanto maior o envolvimento de organizações sociais e especialistas, desde a concepção da solução, maior a chance de aumentar a confiança no voto eletrônico. Deve-se ampliar ao máximo a transparência fornecendo informações sobre a solução, bem como ouvir as dúvidas e críticas da sociedade para esclarecê-las e corrigir eventuais inconsistências. Nem sempre as críticas serão apenas de cunho técnico, pode-se questionar se o voto eletrônico reforça a exclusão digital, assim como os custos envolvidos. Por isso as decisões devem sempre ser embasadas em uma análise de benefícios e desvantagens da adoção do voto eletrônico.

No contexto político-social, o prazo para aceitação da solução de voto eletrônico demora mais que sua implementação técnica. No geral, serão necessários vários ciclos eleitorais sem falhas técnicas ou controvérsias políticas e acreditação nos resultados, antes que os cidadãos e as partes interessadas sejam confiantes na solução. Esse contexto reforça a importância de campanhas de informação e sensibilização da população em geral.

O terceiro e último nível da Pirâmide, o contexto técnico-operacional, compreende capacidade técnica da autoridade eleitoral, fornecedores, tecnologia, normas e leis e, novamente, prazo.

A capacidade técnica da autoridade eleitoral é essencial para conseguir supervisionar, controlar e manter a propriedade da solução de votação eletrônica. Sem isso, aumenta-se a indesejada dependência de fornecedores, que é tolerável para algumas tarefas como transporte e logística, mas não recomendada para tarefas críticas como registrar e contar os votos. Espera-se que a autoridade eleitoral tenha pleno conhecimento das tarefas críticas para poder intervir, com o máximo de transparência, caso seja necessário. Essa capacidade contempla também a habilidade de explicar à sociedade os detalhes do processo de votação eletrônica, disseminando esclarecimentos sobre etapas e técnicas utilizadas. A confiança no voto eletrônico dependerá do grau de familiaridade da sociedade com a solução no dia da eleição.

Por mais que possa realizar internamente, a autoridade eleitoral ainda assim necessitará recorrer ao mercado de tecnologia. Assim, o desenvolvimento de soluções de votação eletrônica deve considerar os custos envolvidos, não apenas para implantação, mas durante todo seu ciclo de vida incluindo armazenamento, manutenção e atualizações. Os procedimentos de aquisição devem ser abertos e ampliar ao máximo a concorrência, com a autoridade disponibilizando o máximo de detalhes das especificações técnicas. Com isso, além de aumentar a chance de o mercado atender as especificações corretamente, evita-se a dependência de fornecedores, assim como eventuais tentativas de corrupção. Não menos importante é controlar os prazos das aquisições, pois os marcos do processo eleitoral são fixos e podem ensejar a redução do período de testes das soluções. A falta de cuidado em relação aos fornecedores pode ter grande influência na confiança sobre a solução.

Em relação à tecnologia a ser utilizada, sua escolha deve considerar a realidade local e contar com a maior transparência possível, incluindo a participação da sociedade. Isso inclui divulgar informações suficientes que expliquem não apenas o funcionamento do processo, mas também os mecanismos de prevenção a fraudes e/ou erros, incluindo as equipes internas da autoridade eleitoral. Adicionalmente, deve se prever, divulgar e explicar os mecanismos existentes de auditoria para se demonstrar a veracidade dos resultados. Quanto mais abertas, públicas, transparentes e independentes, mais confiança as auditorias trarão à solução.

A implantação da tecnologia no processo de votação tem reflexo no arcabouço jurídico que suporta as Eleições. Os normativos têm de ser revistos para garantir que a solução seja compatível com os princípios democráticos vigentes, bem como criar as regulamentações necessárias para as novas questões e relações que serão criadas tais como identidade digital, sigilo do voto, proteção de dados, certificações e auditorias, entre outras. A tecnologia e normativos devem evoluir e amadurecer em conjunto durante alguns ciclos eleitorais. Para tanto, é necessário estabelecer um consenso político forte e multipardiário.

Em comum em todas as atividades técnico-operacionais, está o prazo para execução. Seja para definir requisitos, implementar e testar as tecnologias, criar a capacidade técnica na autoridade eleitoral, atualizar os normativos e educar a população, nada acontece em curto prazo. Por isso, é necessário se estabelecer planos de desenvolvimento, testes, avaliação e implatação graduais. A cada ciclo se aprende com o anterior e melhora-se para o próximo. Esse tipo de abordagem gradual proporcionará tempo para amadurecer tecnicamente a solução, na mesma medida que permite aos cidadãos e às partes interessadas se familiarizarem com as novidades.

Em uma última visão sobre a confiança em soluções de votação eletrônica, os autores de [332] apresentam que esta pode ser impactada por características do eleitorado. Este estudo aponta a diminuição da confiança, à medida que aumenta o nível educacional dos eleitores. Esse comportamento inversamente proporcional se reflete também em relação à idade e ao conhecimento técnico do eleitor. Quanto maiores estes, menor a confiança nas soluções eletrônicas de votação. Segundo os autores, uma possível explicação para esse fato é que pessoas mais novas e com mais conhecimentos técnicos podem ter mais consciências das vulnerabilidades de soluções de tecnologia da informação. Entretanto, os autores destacam que os resultados encontrados em análises na America Latina, apesar de semelhantes aos encontrados na Bélgica, foram opostos aos encontrados em estudos semelhantes realizados nos Estados Unidos da América. Dessa forma, ressaltam que a análise do impacto de características do eleitorado na confiança em soluções de votação eletrônica não é conclusiva e precisava de aprofundamento.

3.5.1 Índice de Percepção de Integridade Eleitoral (PEI)

Apesar de o processo eleitoral ser reflexo do histórico, costumes e regras de cada país, há iniciativas que mapeiam aspectos comuns, de modo a viabilizar uma análise comparativa entre nações. Essa avaliação visa identificar boas práticas e pontos fortes e fracos, de maneira que os países possam utilizar como referência para aprimorar seus respectivos processos, aumentando sua confiança. Não se trata de rotular um processo eleitoral de bom ou ruim. Essa simplificação seria injusta, uma vez que as necessidades e a realidade de cada país são diferentes.

Dentre algumas iniciativas existentes de análise e comparação de processos eleitorais, destaca-se o *The Electoral Integrity Project* [338]. Originalmente criada por pesquisadores das Universidades de Harvard (EUA) e Sidney (Austrália), em 2012, atualmente a pesquisa é conduzida pela *Royal Military College of Canada*, na Universidade da Rainha (Canadá), e pela Universidade de *East Anglia* (Reino Unido). O estudo tem como base responder a três questões:

1. **Como e quando as eleições falham, ao longo do ciclo eleitoral?**.
2. **Quais são as consequências do fracasso de uma eleição, tais como segurança, acessibilidade e confiança?**.
3. **O que pode ser feito para mitigar esses problemas, baseando-se em evidências acadêmicas?**.

Considerando a diversidade dos países e na busca por resposta às questões relacionadas acima, o projeto definiu um índice que classifica as eleições de cada país: o Índice de Percepção da Integridade Ileitoral (*Perceptions of Electoral Integrity* (PEI)). Em sua 9ª edição, reflete a avaliação de observadores eleitorais sobre 11 características dos sistemas eleitorais de 169 países, em 497 eleições no período de julho de 2012 a dezembro de 2022. Os itens avaliados são: (1) Leis eleitorais (*Electoral laws*); (2) Procedimentos eleitorais (*Electoral procedures*); (3) Distritos (*Boundaries*); (4) Registro de eleitores (*Voter registration*); (5) Registro de partidos políticos (*Party registration*); (6) Campanha eleitoral (*Campaign media*); (7) Financiamento de campanha (*Campaign finance*); (8) Processo de votação (*Voting process*); (9) Contagem de voto (*Vote count*); (10) Resultados (*Results*); e (11) Autoridade eleitoral (*Electoral authorities*).

Em relação ao desempenho dos países no índice PEI, a Tabela 3.4 apresenta a classificação dos 3 países melhores colocados em cada edição, além da posição do Brasil em relação ao mundo e aos países americanos, bem como índice de maturidade do processo eleitoral brasileiro. Esse índice de maturidade varia entre: Muito alta, Alta, Média, Baixa e Muito baixa. Salienta-se a predominância dos países nórdicos entre os melhores colocados, com a aparição da Estônia, na edição mais recente.

Edição PEI (ano)	**1º lugar**	**2º lugar**	**3º lugar**	Posição do Brasil		
				No mundo	**Na América**	**Maturidade**
2.0 (2014)	Noruega	Alemanha	Holanda	-	-	-
3.0 (2015)	Finlândia	Dinamarca	Noruega	28	3	Alta

Continua na próxima página

Tabela 3.4 – continuação da página anterior						
Edição PEI (ano)	**1º lugar**	**2º lugar**	**3º lugar**	Posição do Brasil		
				No mundo	**Na América**	**Maturidade**
4.0 (2016)	Dinamarca	Finlândia	Noruega	34	4	Alta
5.0 (2017)	Dinamarca	Finlândia	Noruega	34	4	Alta
6.0 (2018)	Dinamarca	Finlândia	Noruega	34	5	Alta
7.0 (2019)	Dinamarca	Finlândia	Noruega	49	8	Alta
8.0 (2022)	Finlândia	Dinamarca	Suécia	48	10	Alta
9.0 (2023)	Finlândia	Dinamarca	Estônia	41	6	Alta

Tabela 3.4: Classificação índice PEI (Fonte: Adaptado de [338])

Ao analisar os resultados específicos do Brasil, observa-se que, apesar do período avaliado ser de 2012 a 2022, apenas as eleições de 2014, 2018 e 2022 formam a avaliação do país. Com a edição mais recente, a maior parte dos indicadores melhorou em relação aos anos anteriores, como se observa na Tabela 3.5. A partir dessa melhora, o país subiu de posição tanto em relação ao mundo quanto aos países americanos. Cabe ressaltar a manutenção da maturidade "Alta" em todas as avaliações.

Pleito	**Índice PEI**	**Leis eleitorais**	**Procedimentos eleitorais**	**Distritos**	**Registro de eleitores**	**Registro de partidos políticos**	**Campanha eleitoral**	**Financiamento de campanha**	**Processo de votação**	**Contagem de voto**	**Resultados**	**Autoridade eleitoral**
Eleições 2014	68	74	87	73	75	63	48	38	65	92	64	82
Eleições 2018	60	66	69	67	72	47	44	36	59	85	68	57
Eleições 2022 (legislativa)	73	90	94	70	89	74	49	49	67	92	47	99
Eleições 2022 (presidencial)	69	83	94	76	80	50	68	43	66	93	35	90

Tabela 3.5: Pontuação do Brasil no índice PEI (Fonte: Adaptado de [338])

Apesar da invasão às sedes dos poderes posterior à divulgação dos resultados, o índice de integridade do Brasil se manteve estável após as Eleições 2022. A iniciativa de con-

frontar os resultados da eleição fora dos limites do sistema jurídico impactou severamente na seção "Resultados" (*Results*) [338]. Vale destacar que, no caso brasileiro, os piores indicadores estão relacionados ao financiamento de campanha e registro partidário, os quais guardam pouca relação com o uso de tecnologia ou não no processo eleitoral.

3.5.2 Modelo de confiança no voto eletrônico do Brasil

Publicado em 2013, após acompanhamento en loco nas Eleições de 2004 e 2006, o estudo [307] analisou o processo de desenvolvimento inicial da confiança no voto eletrônico no Brasil na década de 1990, bem como a manutenção dessa confiança na condução das eleições brasileiras até aquele momento.

A autora argumenta ainda que a confiança no voto eletrônico é algo mais restrito que a confiança na eleição, em função de a votação ser apenas uma das atividades do processo eleitoral. Nesse sentido, o trabalho baseia sua avaliação na percepção dos cidadãos a partir de mecanismos que geram confiança em sistemas da informação, nas organizações públicas e no processo político, além de diferenciar a confiança na solução técnica e na instituição organizadora das eleições.

O estudo aponta que a confiança inicial para adoção do voto eletrônico no Brasil, em meados dos anos 1990, foi formada especialmente:

1. **por suas raízes históricas**, que contemplam a restauração da democracia no país bem como uma política governamental positiva em relação à adoção de soluções de tecnologia da informação.
2. **pelo desenvolvimento de uma solução técnica segura e robusta**, que fortaleceu a reputação das autoridades eleitorais como guardiãs competentes das eleições.
3. **pelo reconhecimento da sociedade da legitimidade da motivação de utilizar a tecnologia**, para tornar as eleições mais justas e limpas.

Por outro lado, o trabalho apresenta que influenciam na manutenção da confiança no sistema eletrônico de votação:

1. a integração do voto eletrônico a processos democráticos que permitem a participação de múltiplos atores sociais nas várias etapas do processo de preparação das eleições.
2. a adoção de ações de inclusão digital para cultivar a percepção da sociedade de que a tecnologia da informação é uma ferramenta de modernização e prosperidade.
3. a continuidade do reforço mútuo de confiança entre o sistema de votação e a autoridade eleitoral.

Consolidando essas informações, a autora propos o processo de formação da confiança no voto eletrônico brasileiro ilustrado na Figura 3.4.

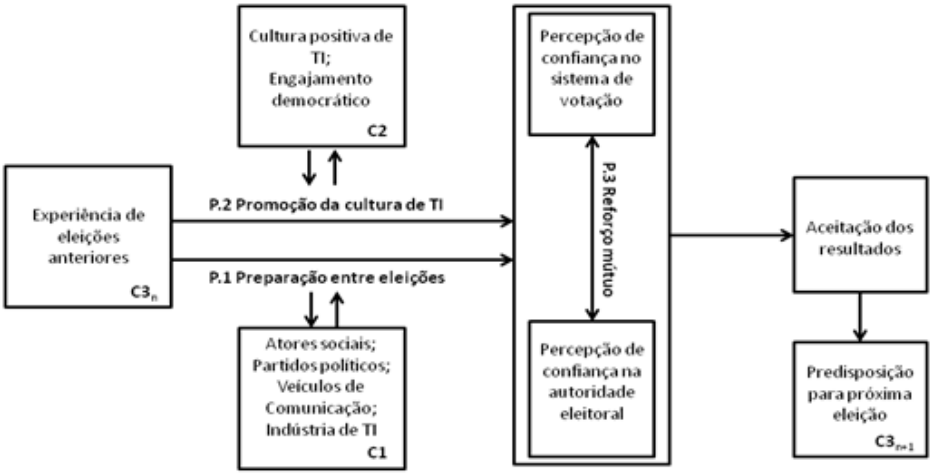

Figura 3.4: Formação de confiança no voto eletrônico brasileiro (Fonte: Adaptado de [307])

O retângulo C1 contempla os principais atores da sociedade que influenciam as percepções de confiança no voto eletrônico. Já C2 registra os elementos que influenciam a disposição para gerar a confiança. Por outro lado, os retângulos C3 retratam a disposição dos cidadãos em perceber o voto eletrônico como confiável, a partir de eleições anteriores ($C3_n$) ou contribuindo para futuras eleições ($C3_{n+1}$).

A seta P1 refere-se às atividades de atualização tecnológica e preparação dos sistemas e procedimentos de votação em entre as eleições. Sobre este ponto, a autora destaca a ampla publicidade adotada para tais atividades no Brasil.

Ainda, a seta P2 refere-se às ações dos variados atores, governamentais ou não, na promoção do uso da tecnologia da informação como força de desenvolvimento do país. Nessa questão destacam-se as políticas de combate a exclusão digital e ampliação de acesso à internet, em especial para comunidades pobres em áreas rurais e urbanas.

Por fim, a seta P3 refere-se à intrísica relação entre a autoridade eleitoral e o sistema de voto eletrônico. À medida que aumentam os mecanismos de auditoria e fiscalização disponibilizados à sociedade, assim como a realização de eleições livres de fraudes, menor o impacto das críticas de eventuais vulnerabilidades da tecnologia. Consequentemente, aumenta-se a percepção da lisura e confiança tanto no sistema quanto na autoridade eleitoral.

Ao final, salienta-se ainda análise da autora em relação aos diferentes cenários de cada país, sobretudo a respeito da maturidade do processo democrático. Em países com regimes democráticos recentes ou frágeis, como o Brasil, o voto eletrônico tende a ser implantado

para substituir processos de votação historicamente fraudulentos e pouco confiáveis. Nesses cenários, a medida tende a ser vista pela população como positiva e benéfica.

Diferente é a situação de países cuja a democracia está madura e bem estabelecida. Nesses casos, espera-se que os processos de votação tenham a confiança da sociedade e, por isso, não se aplica a motivação de buscar superar a desconfiança no meio de votação vigente como justificativa para adoção do voto eletrônico. Este cenário impõe outros desafios à formação da confiança na votação eletrônica que podem inclusive inviabilizar a iniciativa.

Capítulo 4

Processo Eletrônico de Votação do Brasil

O processo eleitoral molda-se às necessidades da sociedade de cada país. São fatores importantes que impactam nessas necessidades: o histórico, a maturidade democrática, a disponibilidade de recursos, os costumes e cultura, o grau de confiança da população nas instituições, entre outros.

Nesse contexto, é necessário reconhecer que não há processo de votação perfeito, que resolve todos os problemas. Todos eles deixam um custo que pode ser aceito ou não por aquela sociedade. Assim, não existe um sistema melhor que outro, o que existe é um que mais se adeque às necessidades do país para que exista confiança nos resultados e que, por isso, possam ser considerados legítimos [339].

Nesse sentido, existem variadas soluções de processo eleitoral adotadas pelos países, cada um voltado às suas necessidades e realidade. No caso brasileiro, o processo eleitoral evoluiu para a informatização no intuito de reduzir a intervenção humana e, por consequencia, as oportunidades para ocorrência de erros não intencionais e fraudes [12][13].

Porém, a informatização tornou a compreensão do processo de votação mais complexa [340]. O processo possui várias etapas, atores e ferramentas, além da relação entre esses entes e também os objetivos a serem alcançados ao longo de cada fase. Essa complexidade pode influenciar o entendimento e gerar variadas representações e interpretações sobre o processo de votação.

Nesse cenário, torna-se relevante estabelecer um meio de descrever o processo de votação brasileiro amparado em parâmetros científicos, visando sua melhor compreensão. Para tanto, este estudo buscou referências na filosofia. A inspiração para esse referencial vem da disciplina de Modelagem e Simulação de sistemas. Autores desse ramo de conhecimento entendem que dois cientistas podem descrever o mesmo sistema utilizando diferentes ca-

tegorizações e que, por isso, é necessário primeiro se construir uma conceituação prévia [341].

No intuito de construir essa conceituação, [342] utiliza os conceitos da Ontologia, Epistemologia e Semiótica. Os autores definem a Ontologia como o estudo do que existe, o que são objetos, suas relações e propriedades. Por outro lado, conceituam a Epistemologia como o estudo do conhecimento, com foco em identificar as condições necessárias e suficientes para sua construção, além de descobrir como as verdades são justificadas. Por fim, declaram que a Semiótica aborda a relação de simbolos, o significado de cada um e qual o uso pretendido. Adicionalmente, em [341], o autor destaca também a importância da Teleologia como o estudo da ação e do propósito, que resulta em métodos.

Ainda, na busca por entender as divergências de significados e falhas de comunicação, os autores de [343] destacam que as pessoas utilizam conceitos e interpretações internas para descrever e compreeender o mesmo referente do mundo real. Ademais, enfatizam a complexidade da comunicação eficaz e o desafio de se alcançar uma referência precisa entre indivíduos diferentes.

Com o intuito de estabelecer mecanismos para a comunicação eficaz, os autores introduzem o conceito da função simbólica no uso da linguagem, em sua teoria semiótica. Nessa visão, essa função facilita a transmissão de pensamentos e idéias por meio de símbolos, como palavras ou sinais, que evocam referências ou conceitos específicos na mente dos destinatários.

Porém, eles destacam a existência de um fenômeno no qual as pessoas acreditam que as palavras possuem uma capacidade intrínseca de influenciar a realidade ou evocar resultados específicos, a chamada "magia da palavra". Salientam ainda que os indivíduos podem ignorar os verdadeiros mecanismos de comunicação e falhar em transmitir os significados pretendidos com precisão, quando ficam excessivamente fixados nas supostas propriedades mágicas da linguagem.

No intuito de contrapor a chamada magia da palavra, os autores introduzem a "ciência do simbolismo". Esse aspecto de sua teoria visa iluminar a verdadeira natureza da linguagem como um sistema de símbolos e signos, e não como entidades místicas com poderes inerentes. Ao enfatizar a natureza simbólica da linguagem, eles buscam dissipar conceitos errôneos e oferecer diretrizes para usá-la de maneira eficaz. Para tanto, propõem tornar os significados explícitos, definindo e delineando claramente as relações entre as palavras e seus referentes.

É nesse contexto que os autores apresentam o Triângulo Semiótico, Figura 4.1. Segundo essa teoria, a relação entre um Símbolo (palavra) e seu Referente (o objeto real ou conceito que ele representa) não é direta. Ao contrário, ocorre por meio de um Conceito/-Pensamento ou Referência. A base do triângulo representa essa relação, destacando que

a conexão entre um Símbolo e seu Referente não é imediata, mas envolve um processo cognitivo de interpretação e compreensão. Por isso a importância de expandir o Símbolo de tal modo que reflita o Conceito/Pensamento do seu Referente com precisão.

Dessa forma, tanto o falante quanto o ouvinte podem compartilhar a compreensão do Referente. Os autores enfatizam a importância da claridade/objetividade nessa definição de símbolos, afirmando que é essencial conhecer os pontos de partida (entendimento compartilhado) e as rotas de definição (o processo de alcançar o referente) para estabelecer uma correspondência clara de referência. Destacam ainda que uma definição bem-sucedida do Símbolo é aquela que parte de um ponto de referência comum e familiar para ambas as partes envolvidas na comunicação. Em seguida, segue um caminho de explicação bem definido para levar ao Referente pretendido.

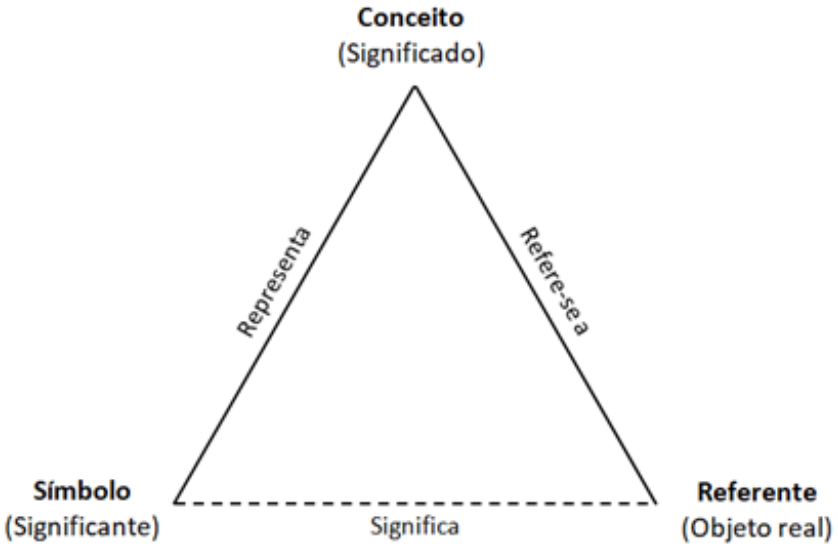

Figura 4.1: Triangulo Semiótico (Fonte [343])

Essa variação de possíveis entendimentos sobre o mesmo significado alinha-se ao conceito filosófico do interpretativismo, no qual sustenta-se que a realidade é relativa e não pode ser separada do indivíduo que a observa. Dessa forma, a verdade não é absoluta, mas sim uma construção do observador. Por isso, ela pode conflitar com outras visões, mas tem de ser consistente [341].

No sentido de integrar esses conceitos filosóficos à descrição do Processo Eletrônico de Votação do Brasil, propõem-se uma visão adaptada do Triângulo Semiótico, conforme a Figura 4.2.

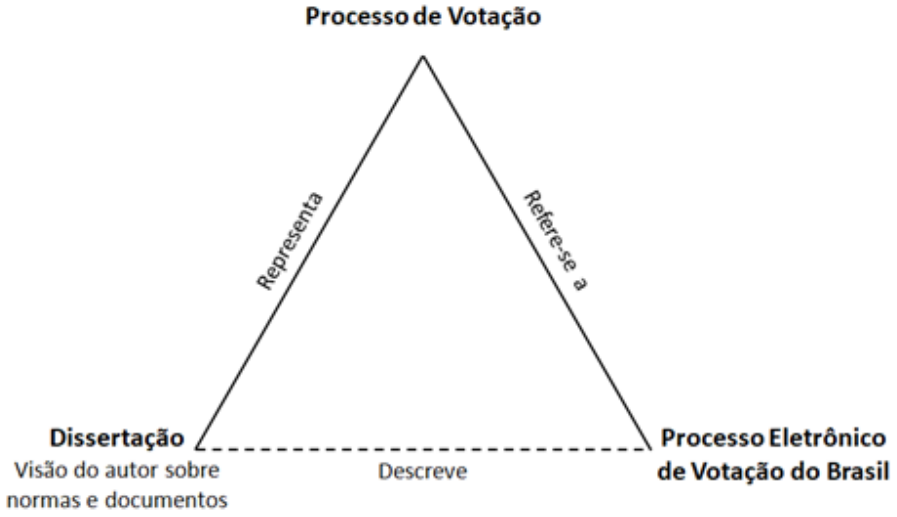

Figura 4.2: Triangulo Semiótico Adaptado (Fonte própria)

Essa visão adaptada baseia-se na Semiótica para localizar a relação conceito/símbolo/referente deste trabalho. Nesse caso, o Processo Eletrônico de Votação do Brasil, o Referente, é uma implementação real do conceito de Processo de Votação, cuja a descrição, o Símbolo, são as normas e documentos que o regulamentam e estão representados nesta dissertação, seguindo a visão deste autor.

4.1 Visão geral

Considerando que o Processo Eletrônico de Votação do Brasil é teolológico, uma vez que possui próposito, propõem-se sua descrição em uma abordagem onto-epistemo-teleológica, amparada no pensamento holístico preconizado por [344], no qual a descrição da função (*function*), da estrutura (*structure*), do processo (*process*) e do contexto (*context*) tornam possível a compreensão de um sistema/processo como um todo, não apenas em partes.

Segundo este autor, a função define os resultados esperados; a estrutura, os componentes e seus relacionamentos; o processo explicita a sequência de atividades e o conhecimento necessário para produzir o resultado; e o contexto descreve o ambiente único no qual o sistema está situado. A Figura 4.3 ilustra esse o processo de investigação iterativa para entendimento da complexidade proposto.

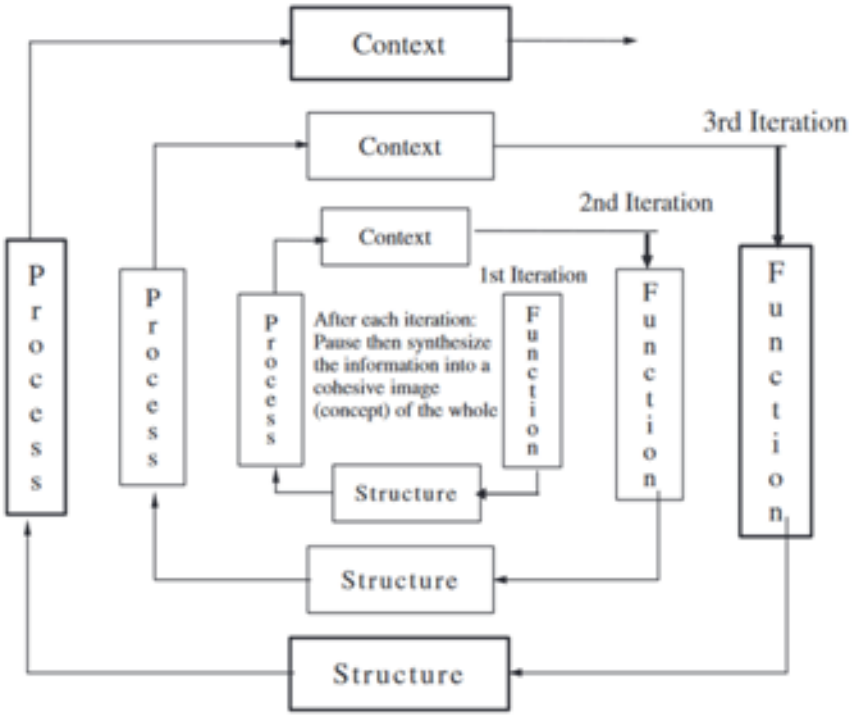

Figura 4.3: Processo Iterativo de Investigação (Fonte [344])

Ainda segundo [344], a iteração entre a visão das funções, estruturas, processos e contexto é a chave para entender a complexidade de um sistema/processo. A cada iteração é possível examinar suposições e propriedades do elementos em conjunto, validá-las ou não, identificar compatibilidades, e resolver conflitos. As sucessivas iterações estabelecerão um entendimento integrado.

Nesta abordagem, para definição das funções de um sistema de votação eletrônica, utilizou-se como referência o *Voluntary Voting System Guidelines* (VVSG) [330], que elenca 12 funções principais de um processo de votação:

1. Definir as características da eleição e da cédula de votação (*Define elections and ballot styles*).
2. Configurar equipamentos de votação (*Configure voting equipment*).
3. Identificar e validar as configurações dos equipamentos de votação (*Identify and validate voting equipment configurations*).
4. Realizar testes lógicos e de acurácia (*Perform logic and accuracy tests*).
5. Disponibilizar votação para os eleitores (*Activate ballots for voters*).
6. Registrar voto do eleitor (*Record votes cast by voters*).

7. Contar votos (*Count votes*).
8. Rotular cédulas que necessitam de tratamento especial (*Label ballots needing special treatment*).
9. Gerar relatórios (*Generate reports*).
10. Exportar dados eleitorais, incluindo resultados (*Export election data including election results*).
11. Arquivar dados eleitorais (*Archive election data*).
12. Disponibilizar dados para auditoria (*Produce records in support of audits*).

Quanto a estrutura, socorreu-se à organização proposta pela Agência de Cibersegurança e Infraestrutura (*Cybersecurity and Infrastructure Security Agency* (CISA)), em sua publicação sobre avaliação de risco para a infraestrutura eleitoral [345]. Neste trabalho, a infraestrutura eleitoral é definida como um conjunto diversificado de sistemas, redes e processos, alguns interligados eletronicamente, que devem funcionar de maneira integrada para realização de eleições. A publicação destaca os seguintes componentes críticos da infraestrutura eleitoral:

1. **Base de dados de eleitores** (*Voter registration databases*): contém o registro dos dados dos eleitores. Compreende também os equipamentos que hospedam as bases de dados, bem como as aplicações que fornecem o acesso aos dados.
2. **Cadernos de votação** (*Electronic and paper pollbooks*): contém a lista de eleitores por local de votação, baseado nas informações da base de dados de eleitores. Podem ser *online*, desconectados (*stand alone*) e impressos.
3. **Preparação do voto** (*Ballot preparation*): é o processo que inclui a definição dos distritos de votação, a distribuição dos candidatos por distrito e o leiaute das cédulas de votação. Compreende ainda as imagens dos candidatos, os aúdios para locais de votação especiais, bem como os insumos para a totalização dos dados por local de votação.
4. **Sistemas do equipamento de votação** (*Voting machine systems*): compreende os processos e equipamentos utilizados para registro do voto dos eleitores. Inclui também a carga dos sistemas e dados nos equipamentos de votação.
5. **Sistemas de apuração e totalização** (*Vote tabulation and aggregation systems*): contempla os processos e equipamentos para contagem e totalização dos votos, de maneira centralizada ou não.

6. **Sites oficiais** (*Official websites*): são os canais utilizados pela autoridade eleitoral para se comunicar com o público, fornecendo orientações, esclarecendo dúvidas e divulgando o resultado do pleito.

7. **Instalações de armazenamento** (*Storage facilities*): compreende os locais (físicos e lógicos) utilizados para armazenar os sistemas e equipamentos antes do dia da eleição.

8. **Locais de votação** (*Polling places*): são os locais nos quais os eleitores votam.

9. **Instalações eleitorais** (*Election offices*): locais que a autoridade eleitoral realiza atividades oficiais.

Em relação ao processo, buscou-se uma organização que fosse genérica e suficientemente completa, de modo a não ser restrita a uma visão específica de processo de votação, Nessa linha, utilizou-se como referência a proposta utilizada no *Electoral Maturity Model* [346], conforme Figura 4.4. Segundo essa publicação, as atividades e a sequência de execução propostas se enquadram em grande parte das eleições da atualidade, sejam elas realizadas de forma totalmente manual ou com algum tipo de auxílio tecnológico.

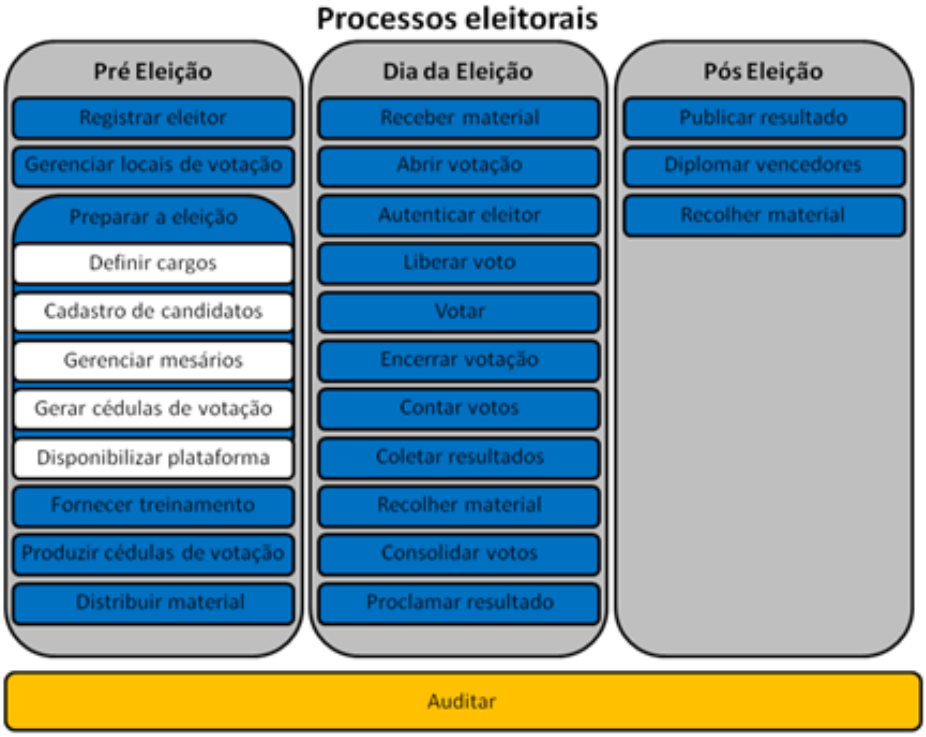

Figura 4.4: Processos de votação (Fonte: Adaptado de [346])

A seguir, a descrição dos processos apresentados no *Electoral Maturity Model*:

1. **Registrar eleitor** (*Voter registration*): É o processo onde os cidadãos se registram para votar. Pode ocorrer continuamente ou se encerrar alguns meses antes da eleição.
2. **Gerenciar locais de votação** (*Polling location management*): compreende as atividades para identificar, avaliar e preparar os locais de votação para a eleição.
3. **Preparar a eleição** (*Election preparation*): envolve todas as atividades necessárias à preparação dos instrumentos de voto utilizados durante a eleição. Suas principais atividades internas incluem:

    - **Definir cargos** (*Contest*): Reunir as informações de todos os cargos em disputa e as respectivas localidades.
    - **Cadastro de Candidatos** (*Candidate registration*): processo pelo qual os candidatos podem se inscrever para concorrer a um cargo específico.
    - **Gerenciar Mesários** (*Poll worker management*): selecionar e gerenciar os mesários da eleição.
    - **Gerar cédulas de votação** (*Ballot generation*): implica na geração de todos os instrumentos necessários para a eleição. Isto inclui não apenas as cédulas onde o eleitor seleciona suas opções, mas também todos os materiais necessários para a realização da eleição, tais como: listas de eleitores, formulários de contagem, tinta indelével, entre outros.
    - **Disponibilizar plataforma** (*Platform readiness*): refere-se ao processo de certificar que toda a infraestrutura eleitoral está pronta para eleição, podendo incluir a realização de testes de campo e até mesmo eleições simuladas.

4. **Fornecer treinamento** (*Training*): refere-se à preparação e formação de todos os atores da infra-estrutura eleitoral, tais como: eleitores, mesários, operadores de suporte, armazenamento e totalização.
5. **Produzir cédulas de votação** (*Ballot production*): abrange a produção propriamente dita de todos os instrumentos de votação, bem como a sua preparação e embalagem em kits eleitorais. Algumas das atividades realizadas são: impressão de cédulas, de formulários de totalização, produção de urnas e preparação dos kits dos locais de votação.
6. **Distribuir material** (*Logistics & distribution*): entregar os kits eleitorais a cada local de votação.
7. **Receber material** (*Kit setup*): receber, verificar e organizar o Kit na seção eleitoral.

8. **Abrir votação** (*Open Voting*): permitir a entrada dos eleitores nos locais de votação.
9. **Autenticar eleitor** (*Voter authentication*): verificar a identidade de cada eleitor, bem como validar se está apto a votar.
10. **Liberar voto** (*Voting session activation*): refere-se à ação em que o mesário possibilita ao eleitor votar, disponibilizando-lhe o instrumento de voto.
11. **Votar** (*Voting*): Principal processo, refere-se à atividade em que o eleitor seleciona suas opções preferidas no instrumento de votação.
12. **Encerrar votação** (*Close voting*): ato de encerrar o período de votação. Após esta etapa, os eleitores não estão mais autorizados a votar.
13. **Contar votos** (*Counting*): encerrada a votação, os mesários abrem a urna e iniciam a validação e contagem de cada voto emitido. Este processo geralmente termina com a preparação e preenchimento de um formulário de contagem (por seção eleitoral) que é entregue para um centro de consolidação.
14. **Coletar resultados** (*Results collection*): recolhimento das contagens de cada seção eleitoral para um centro de consolidação que pode ser centralizado ou distribuído por todo o país.
15. **Recolher material** (*Kit wrap-up*): Coleta do kit eleitoral, relatório de resultados e qualquer outro material nas seções eleitorais.
16. **Consolidar votos** (*Consolidation*): trata-se da agregação das contagens das seções eleitorais em um repositório no qual os resultados finais serão calculados.
17. **Proclamar resultado** (*Proclamation*): Uma vez consolidados todos os resultados, aplica-se as regras necessárias para determinar os vencedores a partir dos votos.
18. **Publicar resultado** (*Result Publication*): disponibilizar ao público o resultado da eleição.
19. **Diplomar vencedores** (*Official credential issuance*): refere-se à produção e entrega do documento formal de proclamação a cada vencedor.
20. **Recolher material** (*Wrap-up*): Recolhimento e consolidação de kits eleitorais dos locais de votação para um armazém centralizado.
21. **Auditar** (*Audits*): Auditar as atividades.

4.2 Visão aplicada

Nesta seção serão aplicadas, ao processo eletrônico de votação do Brasil, as referências de funções, estrutura e processo apresentadas anteriormente. Salienta-se que será apresentada uma visão ampla, sem o intuito de detalhar em profundidade toda a complexidade do processo e esgotar questão. De maneira complementar, em cada função serão exibidos os mecanismos de segurança e auditoria divulgados pelo TSE.

Para uma melhor compreensão da organização do Processo Eletrônico de Votação do Brasil, cabe esclarecer a relação dos órgãos da Justiça Eleitoral Brasileira. O Tribunal Superior Eleitoral atua como órgão central e cada Unidade da Federação possui um Tribunal Regional Eleitoral (TRE), conforme Seção IV da Constituição Federal do Brasil [347]. Essa organização se reflete no papel desses entes durante a execução do processo eleitoral.

Os autores de [18], apresentam uma visão geral do processo eleitoral e os papéis do TSE e TREs, do ponto de vista da garantia da segurança e auditoria, conforme a Figura 4.5.

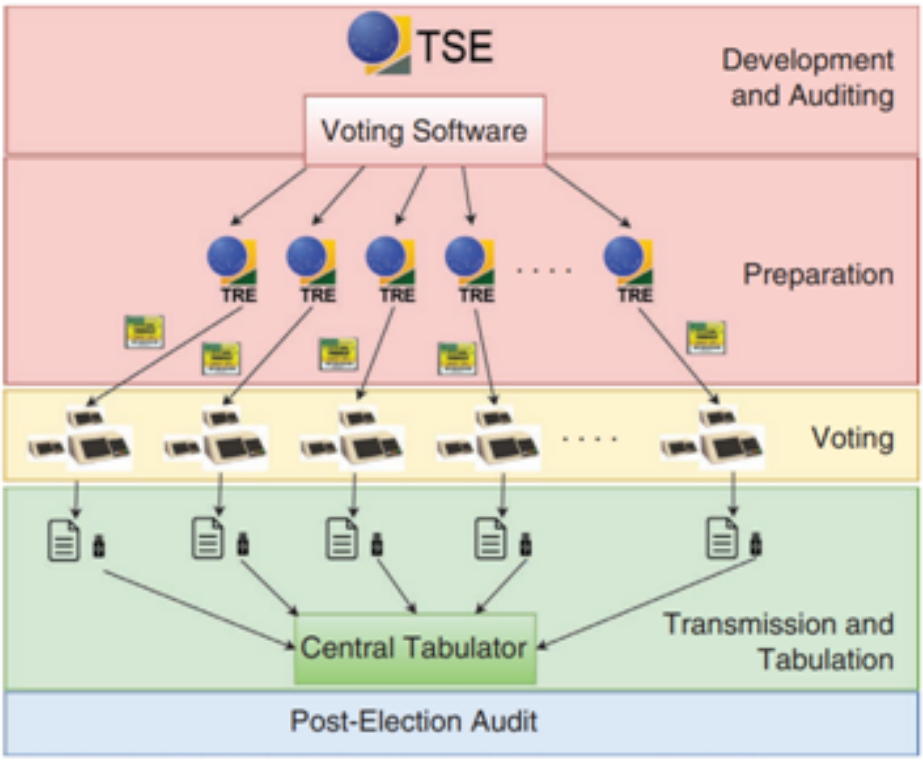

Figura 4.5: Papéis do TSE e TRE no processo eleitoral (Fonte [18])

Apesar da visão voltada para a garantia da segurança exibida na Figura 4.5, a ilustração apresenta o papel de orgão central do TSE no desenvolvimento e promoção da auditoria dos sistemas de votação, que são distribuídos para os TREs realizarem a carga

e preparação das urnas eletrônicas, as quais serão utilizadas para coleta dos votos dos eleitores nos locais de votação e que terão seus resultados coletados e transmitidos ao TSE para a totalização e divulgação dos resultados.

Ademais, as atividades para realização do processo eleitoral são formalmente estabelecidas pelo TSE em normativos específicos para cada pleito. Neste estudo foram utilizadas as Resoluções publicadas para as Eleições 2022 [348].

Apresentadas essas informações gerais, segue abaixo a aplicação ao processo eletrônico de votação do Brasil das referências de funções, estrutura e processo declarados no item 4.1 acima.

1. **Função 1**: Definir as características da eleição e da cédula de votação.

    - **Contexto**: A Constituição Federal do Brasil [347], em seus artigos 27, 28, 29, 32, 45, 46 e 77, define que serão eleitos, respectivamente, Deputados Estaduais, Governadores, Prefeitos e Vereadores, Deputados Distritais, Deputados Federais, Senadores e Presidente da República. A Lei 9.504/1995 [349] regulamenta em seu artigo primeiro, que são realizadas duas eleições: uma para os cargos de Presidente da República, Senadores, Governadores e Deputados Federais, Estaduais e Distritais; e outra para Prefeitos e Vereadores. Ademais, a mesma Lei 9.504 define, em seu artigo 59, os dados dos candidatos a serem exibidos na urna eletrônica, bem como a ordem de votação dos cargos eletivos. Por fim, o art. 119 da Resolução TSE 23.669/2021 [350] estabelece a exibição dos dados na urna eletrônica.
    - **Estrutura**: Congresso Nacional, composto pela Câmara dos Deputados e Senado Federal.
    - **Processo**: Os parlamentares discutem, votam e publicam os normativos aplicáveis à definição das características das eleições e identificação dos candidatos para votação.
    - **Mecanismos de segurança e auditoria**: Não se aplica.

2. **Função 2**: Configurar equipamentos de votação.

    - **Contexto**: A preparação dos equipamentos de votação compreende ações referentes aos software e hardware do dispositivo. Os softwares utilizados para identificação e votação do eleitor são desenvolvidos pela Justiça Eleitoral e ficam disponível para auditoria da sociedade. Ao final do período de desenvolvimento, são assinados digitalmente, inclusive por outras entidades que não a Justiça Eleitoral, e carregados nos equipamentos de votação em cerimônias públicas, abertas à sociedade [351]. Os hardwares, as urnas eletrônicas, tem seus

requisitos definidos pela Justiça Eleitoral e a produção e contratada por meio de licitação pública. A empresa vencedora do procedimento licitatório fabrica os equipamentos e os entrega nos tribunais regionais eleitorais. Ao receberem, os tribunais regionais são responsáveis por certificar digitalmente cada urna eletrônica, de modo a torná-las aptas para uso em eleições oficiais. Após disponibilizados aos TREs, os sistemas são carregados nas urnas eletrônicas nas cerimônias públicas de carga e preparação [15].

- **Estrutura**: Além das urnas eletrônicas, compreende a Autoridade Certificadora das Urnas Eletrônicas, insfraestrutura de chaves públicas de gestão dos certificados digitais dos equipamentos de votação [15]. Quanto aos sistemas, envolve os de verificação da biometria do eleitor, registro e apuração do voto. Em relação aos dados, engloba as seções eleitorais e seus respectivos eleitores aptos e candidatos registrados. Por fim, compreende os locais físicos de preparação e carga das urnas eletrônicas, que são divulgados previamente por edital público [15].
- **Processo**: Envolve a produção, distribuição e certificação digital dos equipamentos de votação, bem como o desenvolvimento dos sistemas de verificação da biometria do eleitor, registro e apuração dos votos. Ao final, contempla as cerimônias públicas de carga e preparação das urnas eletrônicas [351][15].
- **Mecanismos de segurança e auditoria**: os principais relacionados às urnas eletrônicas e aos seus sistesmas são a assinatura digital e a cadeia de segurança [352]. A assinatura digital visa garantir que os sistemas desenvolvidos e carregados nas urnas eletrônicas possam ser verificados a qualquer tempo para garantir que são os mesmos abertos e submetidos à auditoria pública. A cadeia de segurança visa garantir que as urnas eletrônicas executem apenas softwares assinados digitalmente pela Justiça Eleitoral, assim como que os sistemas de votação serão executados apenas em urnas eletrônicas certificadas pela Justiça Eleitoral [352]. A assinatura dos sistemas a serem carregados nas urnas eletrônicas é verificada nas cerimônias públicas de carga e preparação [15].

3. **Função 3**: Identificar e validar as configurações dos equipamentos de votação.

    - **Contexto**: A garantia da autenticidade das urnas eletrônicas preparadas para a eleição começa pela assinatura dos sistemas de votação. Isso ocorre em cerimônia pública ao final do período de desenvolvimento dos sistemas, chamada de Cerimônia de Assinatura Digital e Lacração dos Sistemas [351]. Os softwares a serem utilizados nas urnas eletrônicas são assinados pela Justiça Eleitoral e pelas instuições auditoras interessadas. Posteriormente, os resumos cripto-

gráficos (*hash*) dessas assinaturas são publicados no site do TSE [351]. Na sequencia, a carga desses sistemas assinados digitalmente nas urnas eletrônicas é realizada, em todo o país, em cerimônia pública, com ampla divulgação e convocada por edital. Nessas cerimônias, além de obrigatoriamente se verificar a assinatura digital da Justiça Eleitoral, faculta-se a verificação também às instituições auditoras que tenham assinado os sistemas na Cerimônia de Lacração [351]. Por fim, no dia da eleição, de ofício, a Justiça Eleitoral verifica novamente a assinatura digital de algumas urnas eletrônicas prontas para votação nos locais de votação aleatoriamente selecionados, o Teste de Autenticidade dos Sistemas Eleitorais [351].

- **Estrutura**: Urnas eletrônicas, além dos sistemas de verificação da biometria do eleitor, registro e apuração do voto.
- **Processo**: : Envolve o desenvolvimento, assinatura digital e carga nas urnas eletrônicas dos sistemas de verificação da biometria do eleitor, registro e apuração dos votos.
- **Mecanismos de segurança e auditoria**: Cerimônia de Lacração dos Sistemas de Votação, na qual os sistemas são assinados digitalmente, as Cerimônias de Carga e Preparação das Urnas eletrônicas, quando os sistemas são inseridos em todos os equipamentos de votação, e o Teste de Autenticidade dos Sistemas Eleitorais, quando no dia da eleição, dentro da seção eleitoral, urnas aleatoriamente selecionadas tem a assinatura digital dos sistemas verificadas [15].

4. **Função 4**: Realizar testes lógicos e de acurácia.

    - **Contexto**: Além de ficarem abertos para auditoria desde outubro do ano não eleitoral até a Cerimônia de Lacração, os sistemas de votação utilizados nas urnas eletrônicas também são submetidos aos Testes Públicos de Segurança dos Sistemas Eleitorais (TPS), que faculta a qualquer cidadão brasileiro maior de 18 anos montar planos de ataques ao sistema e executá-los nas urnas eletrônicas, na sede do TSE em Brasília [15]. Ademais, em uma iniciativa piloto, em 2022, o TSE disponibilizou o código-fonte dos sistemas para universidades públicas brasileiras poderem auditá-los em seus ambientes próprios, sem necessidade de se deslocar à sede do TSE [353]. Ainda, no dia da eleição, a Justiça Eleitoral realiza o Teste de Integridade, que corresponde a retirar a urna eletrônica pronta para uso em uma seção eleitoral aleatoriamente sorteada e realizar uma votação em claro, com os mesmos votos registrados na urna eletrônica e também manualmente, em um ambiente aberto, filmado e auditado

por empresa independente [15]. Ao final do dia, o resultado da votação aberta na urna eletrônica e da votação manual são comparados e verificados se foram iguais.

- **Estrutura**: Urnas eletrônicas, além dos sistemas de verificação da biometria do eleitor, registro e apuração do voto, bem como de transmissão e recebimento de resultados.
- **Processo**: Envolve o desenvolvimento dos sistemas de verificação da biometria do eleitor, registro e apuração dos votos, bem como de transmissão e recebimento de resultados. Ainda, os procedimentos para realização dos TPS, bem como dos Testes de Integridade no dia da eleição[351][354].
- **Mecanismos de segurança e auditoria**: Testes Públicos de Segurança dos Sistemas Eleitorais [354], quando qualquer cidadão pode tentar quebrar as barreiras de segurança dos sistemas e das urnas eletrônicas, a disponibilização do código-fonte dos sistemas eleitorais para auditoria de universidades públicas brasileiras e o Teste de Integridade no dia da Eleição [15].

5. **Função 5**: Disponibilizar votação para os eleitores.

    - **Contexto**: O primeiro turno de eleição inicia às 8h, artigo 109 da Resolução TSE 23.669/2021 [350], do primeiro domingo de outubro, artigos 27, 28 e 77 da Constituição Federal [347]. Para chegar até esse momento, os eleitores aptos foram definidos após o fechamento do Cadastro Eleitoral, os candidatos foram registrados, os mesários convocados (conforme artigos 91, 8 e 120 da Lei 9.504/1997 [349], respectivamente); os sistemas eleitorais foram desenvolvidos, testados, auditados e carregados nas urnas eletrônicas; os equipamentos e material de votação distribuídos para todos os locais de votação do país (art. 133 da Lei 9.504/1997 [349]).
    - **Estrutura**: Sistemas de registro de eleitores; de candidaturas; de verificação da biometria do eleitor, registro e apuração dos votos; de transmissão e recebimento de resultados; de totalização; e de divulgação de resultados. Além das urnas eletrônicas e material de votação da seção eleitoral.
    - **Processo**: Depois de definidos os eleitores aptos, os candidatos registrados, os mesários convocados, os sistemas desenvolvidos e carregados nas urnas eletrônicas e os equipamentos e materiais de votação distribuídos, o dia de eleição inicia com a emissão da Zerésima em cada seção eleitoral. O Artigo 142, Capítulo III, do Título IV, da Lei 9.504/1997 [349] e o art. 109 da Resolução TSE 23.669/2021 [350] trazem mais detalhes dos procedimentos operacionais do ínicio da votação.

- **Mecanismos de segurança e auditoria**: Zerésima, relatório impresso pela urna eletrônica para demonstrar que a eleição inicia sem votos registrados no equipamento [15].

6. **Função 6**: Registrar voto do eleitor.

   - **Contexto**: O eleitor deve exercer seu direito de votar das 8h às 17h horas do dia da eleição. Para tanto, precisa estar em situação regular e identificar-se perante o mesário de sua seção eleitoral.
   - **Estrutura**: Urna eletrônica, sistemas de sistemas de verificação da biometria do eleitor, registro e apuração dos votos.
   - **Processo**: Para exercer seu direito ao voto, o eleitor deve se deslocar a sua seção eleitoral específica, identificar-se ao mesário portando documento com foto, verificar sua impressão biométrica no terminal do mesário e dirigir-se à cabina de votação para, na urna eletrônica, digitar os números dos candidatos de cada cargo e confirmar seu voto. O art. 146 da Lei 9.504/1997 [349] e o art. 113 da Resolução TSE 23.669/2021 [350] trazem mais detalhes dos procedimentos operacionais do ato de votar.
   - **Mecanismos de segurança e auditoria**: Identificação biométrica do eleitor, para evitar que um eleitor se passe por outro na votação; Cabina de votação, para resguardar o sigilo do voto do eleitor; Registro Digital do Voto (RDV), arquivo que contém todos os votos, exatamente como registrado pelo eleitor, gravados de maneira embaralhada, para não se ferir o sigilo do voto; e *Logs* de Segurança das urnas urnas eletrônicas, com o registro das operações realizadas no equipamento de votação [15].

7. **Função 7**: Contar votos.

   - **Contexto**: A contagem dos votos, apuração, é realizada pela automaticamente urna eletrônica, após acionamento dos mesários, ao fim da votação (arts. 136 e 137 da Resolução TSE 23.669/2021 [350]). O resultado é impresso no Boletim de Urna (art. 138 da Resolução TSE 23.669/2021 [350]) e também fica disponível para coleta por celular utilizando *QRCode* [15].
   - **Estrutura**: Urna eletrônica, sistema de apuração de votos, aplicativo de apuração de votos (BU na mão), site do TSE.
   - **Processo**: Após encerramento da votação, em função de encerrado o horário de votação e não haver mais eleitores na fila, o mesário digita o código de encerramento da urna, que inicia automaticamente a contagem dos votos,

apuração. Ao final, o resultado é gravado no equipamento, impresso em várias vias de papel e também apresentado em QRCode na tela da urna (Seção VI, do Capitulo I, Do Titulo II, da Resolução TSE 23.669/2021 [350]).

- **Mecanismos de segurança e auditoria**: Boletim de urna (BU), relatório com o resultado da seção eleitoral que além de impresso dentro da seção eleitoral, também é publicado na internet assim que recebido para totalização; e aplicativo BU na mão, para ler os QRCodes com os resultados de cada seção eleitoral. Destaca-se que a Justiça Eleitoral publica as regras de criação do *QRCode*, de modo que qualquer interessado pode desenvolver seu próprio aplicativo, sem precisar utilizar o da Justiça Eleitoral [15].

8. **Função 8**: Rotular cédulas que necessitam de tratamento especial.

    - **Contexto**: Não se aplica ao cenário brasileiro. Para se resguardar o sigilo do voto, não há qualquer diferenciação entre os votos dos eleitores.
    - **Estrutura**: Não se aplica.
    - **Processo**: Não se aplica.
    - **Mecanismos de segurança e auditoria**: Não se aplica.

9. **Função 9**: Gerar relatórios.

    - **Contexto**: Durante as várias etapas do processo eletrônico de votação, um conjunto de informações são produzidas e divulgadas. Após a assinatura digital dos sistemas eleitorais na Cerimônia de Lacração, os resumos criptográficos de cada sistema são publicados no site do TSE [355]. Nas cerimônias de carga e preparação das urnas eletrônicas, são impressos os extratos de carga que vinculam a urna eletrônica preparada e o conjunto de lacres de segurança afixados após a carga dos sistemas. Também nessas Cerimônias, é gerada a Tabela de Correspondência, que relacionada o número único de identificação das urnas eletrônicas preparadas por seção eleitoral. Há ainda os relatórios com os resultados dos TPS e dos Testes de Integridade, bem como, no dia de votação, a impressão na urna eletrônica da Zerésima, BU, *Logs* de segurança das urnas eletrônicas, entre outros. Por fim, após a realização do pleito, a Justiça Eleitoral ainda publica os *Log* de Segurança de cada urna eletrônica, bem como os RDV de cada seção eleitoral [15].
    - **Estrutura**: Urnas eletrônicas. Sistema de geração dos dados para preparação das urnas eletrônicas. Site do TSE.

- **Processo**: A geração e publicação de informações ocorre desde a assinatura digital dos sistemas e permeia as cerimônias de carga e preparação das urnas eletrônicas, os TPS e de integridade, além das impressões geradas pelas urnas eletrônicas no dia da votação [351].
- **Mecanismos de segurança e auditoria**: Além da publicação do dos resumos criptográficos (*hash*) dos sistemas lacrados, a publicação da Tabela de Correspondência, cuja relação de urnas preparadas para eleição serve de insumo para verificação no momento da Totalização. Ao receber um BU, é verificado se ele é proveniente da urna preparada para aquela seção eleitoral. Além destes, destacam-se a Zerésima e também o BU, que contém o resultado da seção eleitoral, bem como o RDV e os *Logs* de Segurança de cada urnas eletrônicas [15].

10. **Função 10**: Exportar dados eleitorais, incluindo resultados.

    - **Contexto**: Considerando a regra geral da divulgação das informações, além da divulgação dos resultados no dia da eleição, a Justiça Eleitoral divulga os dados estatísticos sobre eleitorado, candidatos e resultados. Esses dados disponibilizados em seu formato original, dados brutos, assim como em formato estatístico.
    - **Estrutura**: Sistemas de registro de eleitores; de candidaturas; de verificação da biometria do eleitor, registro e apuração dos votos; de totalização; e de divulgação de resultados. Além do aplicativo de resultados e site do TSE [350].
    - **Processo**: Ao final de cada pleito, os dados são disponibilizados em formato original (bruto) e estatístico no site do TSE. Ainda, há a emissão do Relatório de Resultado da Totalização para avaliação dos partidos políticos [350].
    - **Mecanismos de segurança e auditoria**: Salienta-se a divulgação dos Boletim de urna, tanto dentro das seções eleitorais de maneira impressa ou digital (*QRCodes*), quanto no site do TSE, assim que recebidos para Totalização [15]. Outros itens de destaque são as páginas de Dados Abertos [356] e de Estatísticas Eleitorais [357] no site do TSE.

11. **Função 11**: Arquivar dados eleitorais.

    - **Contexto**: Ao final de cada pleito, os dados referentes aos eleitores, candidatos e resultados são atualizados nas respectivas bases de dados dos sistemas eletrônicos correspondentes.

- **Estrutura**: Sistemas de registro de eleitores; de candidaturas; de apuração dos votos; de totalização; e de divulgação de resultados.
- **Processo**: A cada etapa finalizada do processo eleitoral, as informações são registradas nos sistemas eletrônicos correspondentes. Os dados de eleitores são registrados e atualizados ao fim do fechamento do Cadastro Eleitoral e do período de candidaturas (conforme artigos 91 e 8 da Lei 9.504/1997 [349], respectivamente) e os de resultado, ao fim do pleito [350].
- **Mecanismos de segurança e auditoria**: Divulgação dos dados armazenados nas páginas de Dados Abertos [356] e Estatísticas Eleitorais [357].

12. **Função 12**: Disponibilizar dados para auditoria.

    - **Contexto**: Os dados de auditoria vão sendo disponibilizados à medida que avançam as etapas do Processo Eletrônico de Votação Brasileiro. Além de disponibilizados no site do TSE, tambem ficam à disposição da sociedade no momento em que os eventos ocorrem, como quando impressos pela urna eletrônica na seção eleitoral ou trasnmitidos pela internet como nos Testes de Integridade [350][351].
    - **Estrutura**: Os registros de auditoria são disponibilizados à sociedade no site do TSE ou disponibilizados aos entes fiscalizadores[350][351].
    - **Processo**: Assim como no arquivamento dos dados, os registros de auditoria vão sendo atualizados e disponibilizados a cada etapa finalizada do processo eleitoral. É um procedimento que permeia todos os estágios[350][351].
    - **Mecanismos de segurança e auditoria**: Os Resumos Criptográficos (*Hash*) dos sistemas assinados eletronicamente, que servem de base para verificar a autenticidade dos sistemas carregados nas urnas eletrônicas [355]; as Tabelas de Correspondências, com a relação das urnas eletrônicas preparadas para cada seção eleitoral; os Boletim de urna, Registro Digital do Voto e *Log* de Segurança de cada urna eletrônica utilizada na eleição [15]; e a dilvugação dos dados de eleitores, candidatos e resultados em formato original, na página de Dados Abertos [356] e de estatística eleitorais [357].

Por fim, importante destacar que todos os procedimentos e etapas podem ser acompanhados e auditados pela sociedade por meio de entidades formalmente estabelecidas por normativo público do TSE. Para o ano de 2022, conforme art. 6 da Resolução TSE 23.673/2021 [351], havia a previsão da participação, entre outros, do Ministério Público Federal, do Congresso Nacional, dos Partidos políticos, do Tribunal de Contas da União,

da Polícia Federal e dos Departamentos de Tecnologia de universidades que se credenciassem no TSE. Salienta-se ainda a possibilidade de os eleitores auditarem os sistemas de votação, por meio da participação dos Testes Públicos de Segurança dos Sistemas Eleitorais, assim como os resultados, utilizando os Boletim de urna.

4.3 Principais críticas

De acordo com os autores de [9], a adoção do voto eletrônico propicia uma melhor gestão logística das eleições e a divulgação mais rápida dos resultados. Essa rapidez é importante para reduzir suspeitas e, por consequência casos de violência. Ainda, a votação eletrônica pode reduzir os votos nulos e ampliar a participação de analfabetos e de eleitores com deficiência, além de auxiliar a extinguir fraudes eleitorais históricas.

Entretanto, ainda segundo estes autores, a utilização de tecnologias na votação gera riscos de má gestão, falta de confiabilidade na correta gravação dos votos, na garantia do sigilo do voto e na transparência, na medida em que limita as possibilidades de recontagem dos votos e permite a introdução de novas possibilidades de fraude eleitoral por meio da manipulação da tecnologia. Salienta-se ainda que a tecnologia torna a compreensão do processo e seus mecanismos de segurança mais complexa para o público sem conhecimento técnico, além de representar elevados custos para sua implantação e manutenção ao longo do tempo [24].

No caso brasileiro, a motivação para adotar a votação eletrônica foi reduzir a intervenção humana em etapas críticas do processo, de modo a evitar erros intencionais ou não. Desde a informatização, o TSE alega não ter havido nenhum registro comprovado de fraudes, assim como terem sido eliminados procedimentos excusos históricos [12].

Porém, apesar de reconhecidos avanços em sua implantação, existem críticas ao processo eletrônico de votação brasileiro. As principais concentram-se em questões sociais/organizacionais, além de técnicas, que contemplam a segurança, transparência e auditabilidade do processo [307].

As críticas voltadas para os aspectos sociais referem-se ao impacto das desigualdes sociais do país, que podem reforçam o caráter da exclusão digital de parcela da população que enfrentam barreiras para o uso da tecnologia [358]. Outro posicionamento recorrente é de que a tecnologia torna mais complexo o entendimento do processo para quem não possui conhecimento técnico [340]. Ainda, questiona-se o alto custo investido para manutenção e contínua evolução da solução de votação eletrônica [358]. Por fim, também é motivo de dúvida a centralização de poderes do TSE para organizar, executar e julgar as ações referentes às eleições [19].

Em relação às críticas técnicas, a arquitetura da urna eletrônica é questionada por propiciar a vulnerabilização do sigilo do voto, em função de os terminais de identificação do eleitor e de votação estarem interligados por um cabo físico [19]. Adicionalmente, levantam-se dúvidas sobre as garantias de que o software disponibilizado para auditoria antes das eleições é o mesmo que está sendo utilizado nas urnas eletrônicas no dia da votação, assim como as vulnerabilidades identificadas durante a realização dos Testes Públicos de Segurança dos Sistemas Eleitorais [19].

Sobre o TPS, seguramente a ferramenta mais significativa de transparência para a sociedade em geral e a comunidade técnica, em que pese o reconhecimento da importância do evento para aprimoramento do sistema eletrônico de votação [17], os técnicos reclamam das limitações e regras para execução operacional dos testes, tais como: prazo exíguo para realização das análises e ataques, escopo limitado dos sistemas disponibilizados para avaliação, e lentidão nos procedimentos operacionais de realização dos testes, entre outros [16][17][19].

Entretanto, a principal crítica ao processo eletrônico de votação refere-se à alegação de que a confiança na urna eletrônica depende da análise de seu software e hardware. Essa característica afrontaria o princípio da independência do software, o qual prevê que um erro, intencional ou não, no sistema eletrônico de votação não deve ser capaz de gerar impactos indetectáveis no resultado da eleição [359].

Esse questionamento deve-se ao tipo de equipamento de votação utilizado no Brasil, conhecido como DRE. Nessa arquitetura, em regra, todos os registros são gravados apenas digitalmente [359]. De modo a viabilizar um método de auditoria independente do equipamento, a Academia sugere a adoção do método de votação fim a fim e/ou a impressão do voto.

A verificabilidade fim a fim permite que o eleitor possa conferir, por meio de algoritmos criptográficos que garantem a corretude, se o seu voto foi registrado como pretendido (*cast as intended*), gravado como registrado (*recorded as cast*) e contado como gravado (*tallied as recorded*) [100]. Em 2022, o TSE divulgou estar realizando estudos para a implementação de solução de votação fim a fim em conjunto com a Universidade de São Paulo [360], mas sem ter publicado maiores detalhamentos.

A impressão do voto é motivo de intensos debates na sociedade brasileira, tendo sido testado nas eleições de 2002, além de ter sido proposto pelo Congresso Nacional e considerado inconstitucional pelo Supremo Tribunal Federal em outras duas oportunidades, em 2015 e 2018, com a alegação de potencial quebra do sigilo do voto [16].

Em 2021, novamente o Congresso Nacional analisou, rejeitou e arquivou uma nova proposta legislativa sobre o tema, mas dessa vez com proposições que previam, além da impressão do voto pela urna eletrônica [361]:

1. a obrigatoriedade da publicação na internet de todos os programas utilizados no processo de votação;
2. a apuração manual pelos mesários ao final da votação;
3. a guarda e transporte dos recipientes com os votos impressos pelas Forças Armadas ou de segurança pública;
4. a Justiça Federal como foro para resolver denúncias eleitorais e não mais a Justiça Eleitoral;
5. a possibilidade de pedido de recontagens de votos em até 15 dias após o pleito, entre outros

Em síntese, a proposta definia a prevalência do voto impresso sobre o eletrônico, com a retomada de procedimentos manuais de contagem, mas agora sendo realizada nas mais de 400.000 seções eleitorais do país.

Sobre a confiança na impressão do voto, interessante destacar o trabalho [327], no qual o autor destaca que a "sensação de segurança" em relação à votação manual reside em aspectos sociais quando se assume que o eleitor é capaz de marcar a cédula sem erros, que as cédulas serão guardadas, transportadas e contadas corretamente e que a contagem será verificada acertadamente, entre outros procedimentos.

Apesar de o trabalho abordar a votação manual, as questões levantadas são relevantes para a impressão do voto uma vez que, à exceção da maneira de marcar a cédula de votação pela a urna eletrônica, todos os demais procedimentos são semelhantes para se garantir e preservar a urna com os votos impressos, sua guarda, seu transporte e a contagem das cédulas. Em [12], é possível relembrar fraudes que permearam o histórico da votação manual no Brasil e podem retornar com a impressão do voto.

Nesse sentido, o autor de [327] defende que, apesar das fragilidades conhecidas, as vulnerabilidades da votação manual são consideradas aceitáveis em função do seu tempo de amadurecimento, mas que não se aceita aprimorar os sistemas de votação com o tempo de utilização. Para seus críticos, eles deveriam ser perfeitos desde sua criação. Ou seja, há uma tolerância às fraudes da votação manual por uma suposta sensação de maior controle gerada pelo tempo de uso desse meio de votar.

Sobre essa questão, o TSE posiciona-se no sentido de que a impressão do voto retoma práticas antigas que justificaram a implementação do voto eletrônico no país, bem como de que o eleitor não tem a garantia de que o voto que ele vê impresso pela urna eletrônica na seção eleitoral será efetivamente contado na totalização, considerando o histórico brasileiro de fraudes no processo de votação manual [362].

Ainda sobre a impressão do voto, essa foi a maior demanda da parcela contrária ao voto eletrônico no conturbardo cenário das Eleições 2022, mesmo com a rejeição da proposta no Congresso Nacional no ano anterior.

Em um contexto de intenso questionamento à lisura do processo, essa parcela da sociedade e os candidatos que a representava, apresentaram várias alegações de fraudes, tendo como ápice um relatório de auditoria das Forças Armadas [363], um relatório elaborado por um suposto especialista argentino [364] e uma denúncia formal do Partido Liberal do candidato derrotado na corrida à Presidência [365]. Vale destacar que os registros de auditoria disponibilizados pela Justiça Eleitoral permitiram à sociedade brasileira concluir não ter havido nenhuma fraude nas Eleições 2022, como análise realizada pela Universidade de São Paulo [366].

Nesse complexo contexto das Eleições 2022, os institutos de pesquisa acompanharam a sensação de confiança da população brasileira nas urnas eletrônicas. A Tabela 4.1 apresenta o percentual dos cidadãos que confiam (muito ou em alguma medida) nas urnas eletrônicas, segundo os pesquisadores da Atlas/Intel [367][368], Confederação Nacional dos Transportes (CNT) (Rodadas 149, 152 e 153) [369], Data Folha [370] e Genial/Quaest [371][372].

Período	**Atlas/Intel**	**CNT**	**Data Folha**	**Genial/Quaest**
Dez/2020	-	-	69%	-
Mar/2021	-	-	82%	-
Jul/2021	-	79,5%	-	-
Set/2021	-	-	-	70%
Mai/2022	-	68%	73%	75%
Jul/2022	-	-	79%	-
Ago/2022	-	69,4%	-	76%
Set/2022	54,1%	-	-	-
Out/2022	52,5%	-	-	-

Tabela 4.1: População que confia na urna eletrônica (Fonte própria)

A Figura 4.6 ilusta as mesmas informações de percentual da população que confia nas urnas eletrônicas, mas de maneira gráfica.

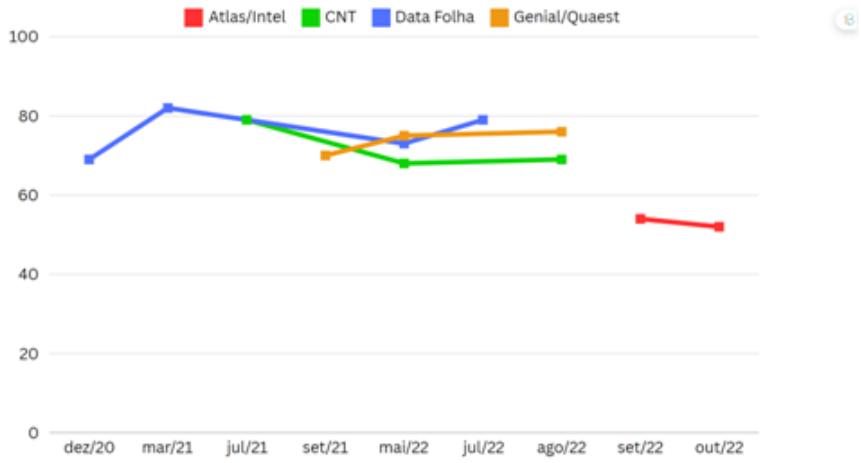

Figura 4.6: População que confia na urna eletrônica (Fonte própria)

Apesar de tratar-se de institutos de pesquisa diversos e metodologias diferentes, é possível observar uma similaridade nos números, exceto na medição realizada pelo instituto Atlas/Intel em setembro e outubro de 2022, véspera e mês das Eleições daquele ano. Nesse período, percebe-se uma sensível redução do nível da confiança nas urnas eletrônicas, muito possivelmente refletindo o alge do acirrado e complexo contexto eleitoral daquela Eleição.

Capítulo 5

Modelo e Hipóteses

Como apontado anteriormente, a avaliação da aceitação do uso de tecnologias é motivo de estudo na Academia há vários anos. Dentre os vários modelos existentes, o modelo o *Unified Theory of Acceptance and Use of Technology* (UTAUT), proposto por [27], tem várias aplicações nos mais variados contextos, inclusive o eleitoral. Em função dos expressivos resultados na explicação da intenção comportamental e do comportamento real do usuário, o modelo foi definido como referência para este trabalho.

O estudo de revisão de literatura [321] identificou que grande parte das publicações sobre UTAUT são relacionadas às áreas de negócios, de gestão, de sistemas de informação e de tecnologia. Mas também há registros limitados de aplicação no jornalismo, na psicologia, na educação e na medicina. É considerado um dos modelos teóricos mais estabelecidos de pesquisa em sistemas de informação e sua aplicação em diferentes campos e estudos validaram extensivamente sua robustez na busca pelo entendimento do uso de novas tecnologias [373].

Aprofundando-se nos sistemas avaliados quando aplicado o UTAUT, o estudo [321] aponta proeminência de sistemas de uso geral como Windows, internet e computadores pessoais; seguido de sistemas de comunicação, como de tecnologia móvel e mensagens instantâneas; sistemas de escritório, que incluem aplicativos de desktop e bancos de dados; e por último, sistemas especializados tais como de gestão integrada (ERP) e de votação eletrônica. Quanto a este último, a votação eletrônica, o modelo usualmente sofre adaptações a depender do contexto de cada país.

Em [28], estudo realizado na Coréia do Sul preliminar a uma primeira experiência de votação eletrônica, os autores adaptaram o modelo UTAUT ajustando o conceito das variáveis originais, bem como adicionando as variáveis: Expectativa de custo (*Cost Expectancy*), Segurança (*Safety*) e Ubiquidade (*Ubiquity*). A primeira avalia a crença de que o voto eletrônico tem utilidade econômica. A segunda, o grau de segurança dos provedores de votação eletrônica. E a terceira, o reconhecimento dos usuários de que é possível

utilizar o voto eletrônico quando e onde ele quiser.

Quando utilizado no Vietnã [29], no contexto de avaliação de uma votação remota, o modelo UTAUT foi adaptado para incluir as variáveis: Satisfação (*Satisfaction*), Autoeficácia (*Self-efficacy*), Confiança (*Trust*) e Compatibilidade (*Compatibility*). A Satisfação explica como a votação móvel pode satisfazer os usuários. A Autoeficácia refere-se à avaliação do indivíduo sobre sua capacidade de realizar a ação de votar de maneira eletrônica. A Confiança é considerada um fator importante em muitos aspectos sociais que envolvem incerteza e dependência, especialmente no que diz respeito a decisões e novas tecnologias. Por fim, a Compatibilidade é entendida como a percepção de quanto uma inovação é percebida como adequada, consistente com os valores existentes, experiências passadas e as necessidades de potenciais adotantes.

Em Gana [30], uma versão simplificada do modelo UTAUT foi utilizada para avaliar a adoção de um sistema de votação eletrônica. Nesse estudo, os autores selecionaram do modelo original as variáveis Expectativa de Performance (*Performance Expectancy*) e Expectativa de Esforço (*Effort Expectancy*), e adicionaram a Confiança do Cidadão nas Instituições (*Citizen Trust in Institutions*). Essa nova variável avalia até que ponto os cidadãos acreditam e têm confiança na capacidade do órgão gestor da eleição para gerir e conduzir eleições, dentro dos limites legais e éticos que regem a administração eleitoral.

No Chile [31], os autores alteraram o modelo UTAUT original para avaliar a aceitação de um sistema de votação eletrônica por estudantes de uma universidade do país. Dentre as mudanças propostas, os autores suprimiram a variável Condições Facilitadoras e adicionaram a Confiança na Tecnologia (*Confianza em la Tecnologia*), que por sua vez é composta pela Segurança Percebida (*Seguridad Percibida*) e Privacidade Percebida (*Privacidad Percibida*).

Em [32], os autores avaliaram a aceitação do uso de um sistema de votação *online*, separando a população em estudades universitários, entre 18 e 25 anos, e cidadãos em geral, acima de 60 anos de cidades americanas. No estudo, os autores adaptaram o modelo UTAUT original suprimindo a variável Condições Facilitadoras (*Facilitating Conditions*) e adicionando as variáveis: Confiança na internet (*Trust in the internet*), Confiança no Governo (*Trust in the Government*) e Ansiedade do Computador (*Computer Anxiety*). As duas primeiras variáveis avaliam a confiança no meio de votação, a internet, e na entidade gestora da eleição. Por outro lado, a terceira examina se o medo do uso incorreto do sistema de votação online pode estar correlacionado com a intenção de uso da tecnologia.

Por fim, em [33] é apresentada uma adaptação do modelo UTAUT para avaliar a aceitação de urnas eletrônicas na Índia. Em função da similaridade dos contextos indianos e brasileiros, este estudo foi utilizado como referência e, por isso, será analisado em maior nível de detalhes a seguir.

Os autores propõem que a intenção de uso das urnas eletrônicas na Índia pode ser influenciada pelas variáveis: Percepção de Segurança (*Perceived Security*), Confiança na Tecnologia (*Trust in Technology*), Expectativa de Performance (*Performance Expectancy*), Expectativa de Esforço (*Effort Expectancy*) e Influência Social (*Social Influence*). Além de conter a Idade (*Age*) e o Gênero (*Gender*) como variáveis moderadoras. A Figura 5.1 apresenta o modelo proposto pelos autores.

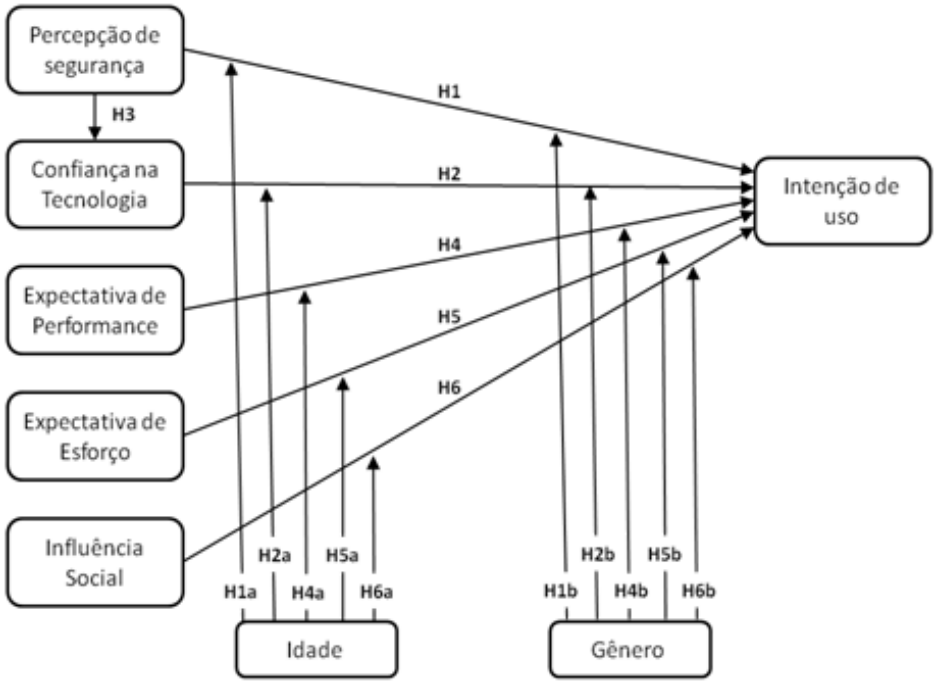

Figura 5.1: Modelo UTAUT adaptado para Índia (Fonte: Adaptado de [33])

Como se observa, os autores adaptaram o modelo UTAUT original para acrescentar os construtos de Percepção de Segurança (*Perceived Security*) e Confiança na Tecnologia (*Trust in Technology*), além de desconsiderar a variável Condições Facilitadoras (*Facilitating Conditions*).

Segundo os pesquisadores, a primeira variável acrescida corresponde a percepção dos cidadãos de que a tecnologia funciona de maneira correta e confiável e pode influenciar a confiança dos eleitores na tecnologia. Por outro lado, a Confiança na Tecnologia reflete a crença sobre a capacidade da tecnologia em si, ao invés das vontades ou motivações para sua utilização.

Na visão dos autores, essas novas variáveis são capazes de afetar a intenção de uso das urnas eletrônicas para coleta dos votos, uma vez que os cidadãos tem consciência da possibilidade de manipulação do conteúdo e quebra da privacidade do voto, ou da existência de vulnerabilidades e falhas de segurança, além de um possível mal funcionamento nas tecnologias de votação eletrônica.

Considerando as semelhanças entre os dois países, tais como: nível de desenvolvimento econômico, tamanho das populações e territórios, desigualdade social e educacional, entre outras, e por ser um estudo focado no equipamento de votação nos moldes utilizado no Brasil, sem conexão à internet e exigindo a presença do eleitor em um local de votação, este trabalho indiano foi escolhido como referência, porém realizando algumas adaptações para o cenário brasileiro. A Figura 5.2 ilustra o modelo proposto originalmente para este estudo aplicado ao Brasil.

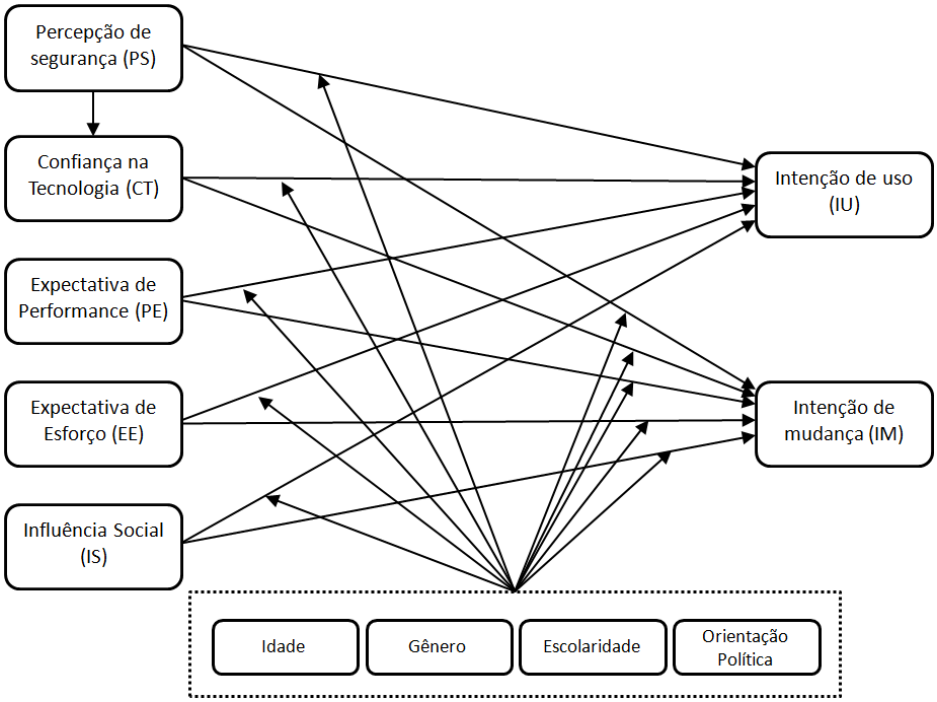

Figura 5.2: Modelo originalmente proposto (Fonte própria)

Contudo, os resultados demonstraram que este modelo originalmente proposto (Figura 5.2) possuía inconsistências estruturais que foram sanadas com adaptação para um modelo de segunda ordem, no qual a variável Confiança Global uniu as variáveis Percepção de Segurança (PS) e Confiança na Tecnologia (CT). Maiores detalhes sobre essa questão constam do Capítulo 7. A figura (5.3) ilustra o modelo proposto ao final.

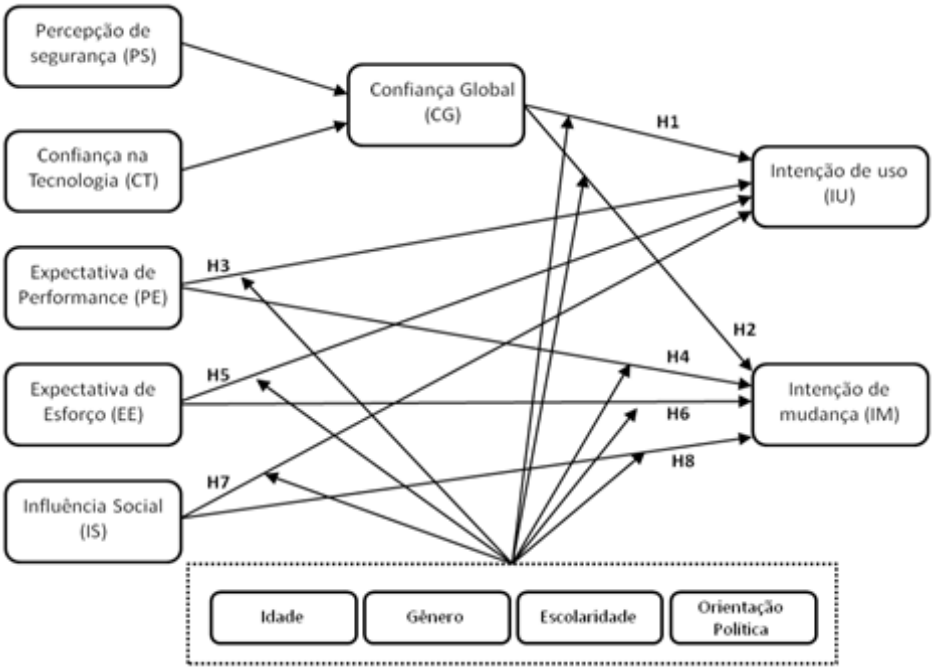

Figura 5.3: Modelo proposto (Fonte própria)

A Tabela 5.1 apresenta o detalhamento das variáveis que compõem o modelo proposto em questão.

Variável	**Descrição**
Percepção de Segurança (PS)	Percepção do eleitor sobre a acurácia e confidencialidade voto com o uso das urnas eletrônicas.
Confiança na Tecnologia (CT)	Crença do eleitor na capacidade da tecnologia da urna eletrônica.
Confiança Global (CG)	De segunda ordem, representa a união da percepção de segurança (PS) e confiança na tecnologia (CT).
Expectativa de Performance (PE)	Percepção do eleitor de quanto a urna eletrônica o ajudará a ter ganhos para votação.
Expectativa de Esforço (EE)	Percepção do eleitor da facilidade de uso da urna eletrônica.
Influencia Social (IS)	Percepção do eleitor de quanto sua avaliação do uso da urna eletrônica é influenciada pela opinião de outras pessoas.
Intenção de uso (IU)	Percepção da intenção do eleitor de continuar utilizando a urna eletrônica.

Continua na próxima página

Tabela 5.1 – continuação da página anterior	
Variável	**Descrição**
Intenção de Mudança (IM)	Percepção da intenção do eleitor de mudar a urna eletrônica para incluir a impressão do voto em papel
Variáveis moderadoras	
Idade	Tempo de vida do eleitor desde o seu nascimento
Gênero	Experiência individual relacionada ao gênero com o qual o eleitor se identifica.
Escolaridade	Nível de instrução ou formação educacional formal alcançado pelo eleitor.
Orientação política	Ideologia e preferências políticas do eleitor.

Tabela 5.1: Variáveis do modelo proposto (Fonte própria)

Em relação ao modelo de referência indiano [33], foram incluídas as variáveis Confiança Global (CG) e a Intenção de Mudança (IM), além das variáveis moderadoras Escolaridade e Orientação Política. A Confiança Global (CG) representa a fusão das variáveis Percepção de Segurança (PS) e Confiança da Tecnologia (CT), conforme explicado anteriormente.

Por outro lado, o ciclo eleitoral desde 2018 e o resultado das Eleições 2022 explicitaram uma forte divisão política na sociedade brasileira [373], no qual posicionamentos a favor e contra o processo eleitoral ficaram bastante evidenciados. Dentre esses posicionamentos contrários, a impressão do voto pelas urnas eletrônicas [16] é um dos que tem maior destaque. Nesse sentido, na tentativa de identificar eventuais influências desse cenário de polarização, foi adicionado ao modelo de referência indiano [33] a Intenção de Mudança (IM) para um equipamento de votação que imprima o voto.

Em relação às variáveis moderadoras, é de conhecimento público a desigualdade de instrução da população brasileira. Ainda, a formação educacional afeta a relação dos indivíduos com a tecnologia. Confome apontado em [332], a confiança no voto eletrônico diminui à medida que aumenta o nível educacional e o conhecimento técnico do eleitor. Nesse sentido, vê-se valor em avaliar o impacto da escolaridade na intenção de uso das urnas eletrônicas no Brasil. Adicionalmente, também alinhado à tentativa de capturar eventuais influências do momento de polarização política, se propõe a adição da variável orientação política do eleitor. O ideário de fraude nas urnas eletrônicas está no topo dos assuntos que mobilizam as redes com perfil à direita do espectro político e entraram mais verticalmente na arena de discussão pública desde 2018 [374]. Assim, é razoável acreditar que a escolaridade e a orientação política do eleitor possam ter influência na aceitação das urnas eletrônicas.

Dessa forma, tomando por referência o modelo indiano [33] e as adaptações para o Brasil, foram definidas as hipóteses que constam da Tabela 5.2.

Id	**Hipótese**
H1	Confiança Global (CG) influencia a Intenção de uso (IU).
H2	Confiança Global (CG) influencia a Intenção de mudança (IM).
H3	Expectativa de performance (PE) influencia a Intenção de uso (IU).
H4	Expectativa de performance (PE) influencia a Intenção de mudança (IM).
H5	Expectativa de esforço (EE) influencia a Intenção de uso (IU).
H6	Expectativa de esforço (EE) influencia a Intenção de mudança (IM).
H7	Influência social (IS) influencia a Intenção de uso (IU).
H8	Influência social (IS) influencia a Intenção de mudança (IM).

Tabela 5.2: Hipóteses do modelo proposto (Fonte própria)

As hipóteses 1 e 2 refletem a visão unificada da Percepção de Segurança (PS) e Confiança na Tecnologia (CT) para a formação da Confiança Global (CG). As hipóteses de 3, 5 e 7 foram baseadas no estudo indiano [33], assim como a influência das variáveis moderadoradas Idade e Gênero. Em sentido complementar, as hipóteses 4, 6 e 8 são inovações ao modelo da Índia para avaliar a Intenção de Mudança (IM) que possui comportamento oposto à Intenção de Uso (IU), assim como o acréscimo das variáveis Escolaridade e Orientação Política.

Esse modelo será calculado e apresentado na seção dedicada aos resultados.

Capítulo 6

Método de pesquisa

Este capítulo detalha as etapas para atingir os objetivos da pesquisa. Nele estão contidos e descritos os procedimentos adotados, as informações coletadas, assim como os métodos utilizados.

6.1 Tipo de pesquisa

Considerando as definições de [375] e [376], conforme ilustrado na Figura 6.1, essa pesquisa é classificada da seguinte maneira:

1. **Quanto à natureza**: Pesquisa aplicada, cujo objetivo é gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos [376].
2. **Quanto aos objetivos**: Explicativa, pois visa a identificação dos fatores que determinam ou que contribuem para a ocorrência dos fenômenos [375], e descritiva, uma vez que descreve as características de determinada população ou fenômeno, estabelece relações entre variáveis, além de incluir o uso de técnicas padronizadas de coleta de dados [375].
3. **Quanto às formas de abordagem**: Quantitativa, por traduzir em números opiniões e informações para classificar e analisar os resultados da pesquisa [376] e qualitativa, pois há uma relação dinâmica entre o mundo real e o sujeito, que não pode ser traduzido em números [376].
4. **Quanto à estratégia**: Estudo de caso piloto, caracterizado pelo estudo profundo e exaustivo de um ou de poucos objetos, de maneira que permita o seu amplo e detalhado conhecimento [375].

5. **Quanto às técnicas de coleta de dados**: Questionário, técnica relacionada com o problema, a hipótese ou os pressupostos da pesquisa, cuja função é obter elementos para que os objetivos propostos possam ser alcançados [376].

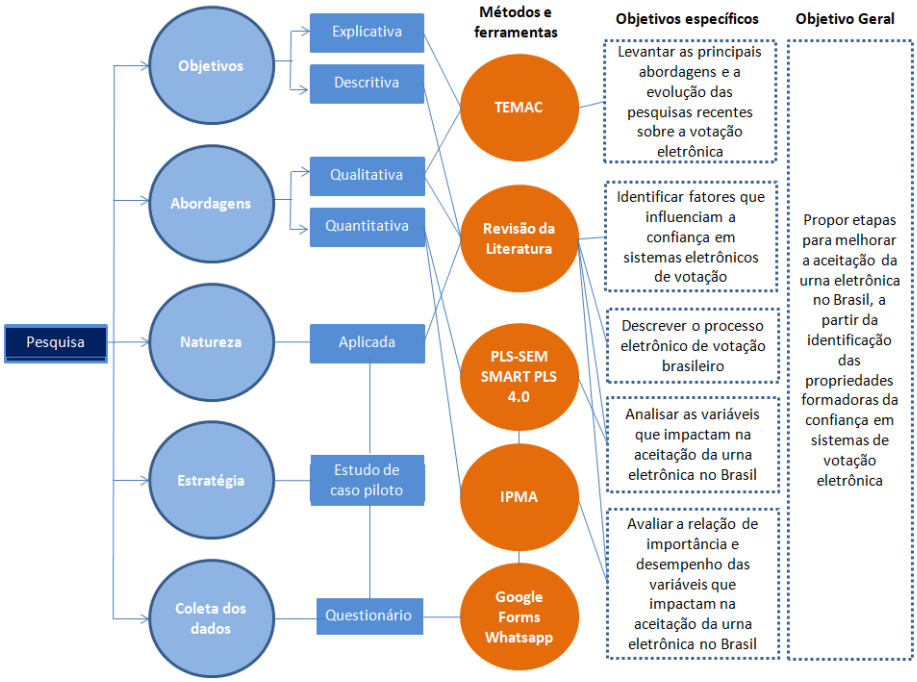

Figura 6.1: Tipo de pesquisa (Fonte própria)

A aplicação dos métodos ocorreu em duas etapas: a primeira foi a aplicação adaptada da Teoria do Enfoque Meta Analítico (Temac) [35] e a segunda, a aplicação de questionário adaptado do estudo [33] e análise dos dados por meio da modelagem de equações estruturais de mínimos quadrados parciais (*Partial Least Squares - Structural Equation Modeling* (PLS-SEM)).

A primeira etapa da pesquisa foi realizada com a utilização de maneira adaptada do Temac para levantar as principais abordagens e a evolução das pesquisas recentes sobre a votação eletrônica. A busca foi realizada utilizando-se pelos termos "*e-voting*" or "*voting machine*" nas bases de dados WoS e *Scopus*, desde 1996 (1996-2023). Como resultado, foram obtidos 1.033 registros na primeira base e 3.806 na segunda.

O Temac é dividido em três etapas: 1. Preparação da pesquisa; 2. Apresentação e interrelação dos dados e; 3. Detalhamento, modelo integrador e validação por evidências [35].

A primeira etapa tem por objetivo responder a quatro perguntas:

1. Qual o descritor ou palavra-chave de pesquisa?
2. Qual o campo espaço-tempo da pesquisa?

3. Quais as bases de dados serão utilizadas?

4. Quais áreas de conhecimento serão utilizadas?

Na segunda etapa, é documentada a interrelação dos dados e a terceira etapa consiste em analisar de forma mais aprofundada os principais resultados e abordagens por meio do estudo com índices bibliométricos *Co-citation* e *Coupling*. Dessa forma, é possível compreender e convergir os resultados encontrados na literatura e identificar as informações mais relevantes e que agregam o maior valor para o tema de pesquisa.

A segunda parte da pesquisa se fundamenta nas informações oriundas do referencial teórico, as quais permitiram identificar fatores que influenciam a confiança em sistemas eletrônicos de votação, bem como demonstrar os mecanismos que formam a confiança no sistema eletrônico de votação do Brasil.

Por fim, a confiança nas urnas eletrônicas foi avaliada quantitativa e qualitativamente, por meio da aplicação de questionário a eleitores brasileiros e da análise dos resultados utilizando-se a modelagem de equações estruturais de mínimos quadrados parciais (PLS-SEM) para mensurar os fatores que mais influenciam a aceitação das urnas eletrônicas, servindo de base para a criação de um modelo de priorização de ações.

6.2 Local da pesquisa

O estudo foi aplicado no Brasil, com a participação voluntária de variados tipos de eleitores. O Brasil é o maior país da América do Sul e da região da América Latina, sendo o quinto maior do mundo em área territorial (equivalente a 47,3% do território sulamericano) e o sexto em população (com mais de 207,8 milhões de habitantes). Com pouco mais de 150 milhões de eleitores, é considerada a 4ª maior democracia do mundo, atrás de Índia, Estados Unidos e Indonésia.

6.3 Objeto da pesquisa

O objeto de estudo é a percepção dos eleitores sobre fatores que influenciam a aceitação das urnas eletrônicas no Brasil. Adicionalmente, também foi objeto de estudo a influência de características como idade, gênero, escolaridade e orientação política na moderação dos resultados encontrados.

6.4 Instrumento da coleta de dados

A pesquisa bibliográfica permitiu levantar e entender as informações mais relevantes sobre sistemas eletrônicos de votação e, no referencial teórico, constam as principais abordagens sobre a confiança e aceitação de tecnologia na votação eletrônica, bem como a descrição do processo eletrônico de votação brasileiro.

Na seção Modelo e Hipóteses são apresentadas variáveis, e seus relacionamentos, que influenciam a aceitação das urnas eletrônicas no Brasil, bem como adaptações propostas para adequação à reallidade brasileira.

A partir dessas referências, adaptou-se o modelo conceitual de [33] para consolidar os principais fatores para avaliar a aceitação das urnas eletrônicas no Brasil, cabendo alguns ajustes para adequação ao contexto de recente polarização política do país, conforme Figura 5.3.

Dessa forma, como instrumento de coleta de dados, foi elaborado questionário estruturado *online* derivado de [33], composto de 18 perguntas as quais foram adaptadas ao contexto brasileiro, conforme Tabela 6.1.

Construto	**Pergunta**
1.Percepção de Segurança (PS)	PS1. Eu acredito que as urnas eletrônicas mantém meu voto seguro.
	PS2. A urna eletrônica gera resultados corretos.
	PS3. A urna eletrônica é relativamente livre de falhas/erros.
2.Confiança na Tecnologia (CT)	CT1. Eu acredito que a urna eletrônica é confiável.
	CT2. A urna eletrônica mantém meu voto secreto.
	CT3. Eu acredito que a urna eletrônica tem boa reputação.
3.Expectativa de Performance (PE)	PE1. A urna eletrônica é útil.
	PE2. Utilizar a urna eletrônica torna mais rápida minha votação.
	PE3. Utilizar a urna eletrônica torna mais fácil minha votação.
4.Expectativa de Esforço (EE)	EE1. Eu compreendo o processo de votação com a urna eletrônica.
	EE2. É fácil votar na urna eletrônica.
	EE3. Eu acredito que é fácil aprender a votar na urna eletrônica.
5.Influência Social (IS)	IS1. Pessoas que influenciam meu comportamento recomendam o uso da urna eletrônica.

Continua na próxima página

Tabela 6.1 – continuação da página anterior	
Construto	**Pergunta**
	IS2. Pessoas que são importantes para mim recomendam o uso da urna eletrônica.
6.Intenção de uso (IU)	IU1. Eu pretendo continuar utilizando a urna eletrônica no futuro.
	IU2. No meu entendimento, a urna eletrônica tem de ser utilizada em todas as eleições.
7.Intenção de Mudança (IM)	IM1. Eu gosto de utilizar a urna eletrônica, mas prefiro que ela imprima o voto.
	IM2. Se a urna imprimir o voto, eu terei mais vontade de utilizá-la.

Tabela 6.1: Indicadores do modelo proposto (Adaptado de [33])

O instrumento descrito para coleta de dados subisidiou a elaboração de um formulário eletrônico, composto por blocos de questões separados por construto, com perguntas fechadas, cujo detalhamento está discriminado na próxima seção.

6.5 Aplicação da metodologia

O formulário para operacionalizar a coleta de dados deste estudo foi composto por blocos de questões com perguntas fechadas, as quais foram medidas utilizando-se a escala Likert de 7 pontos, onde 1 significava discordo totalmente e 7, concordo totalmente.

A disponibilização ocorreu por aplicativos de troca de mensagens online entre os dias 13 e 17 de fevereiro de 2023. Ao final do período de levantamento de dados, foram recebidas 1.851 respostas. Mais detalhes sobre os dados recebidos nas respostas podem ser verificados no endereço eletrônico do Datalab (link) da Universidade de brasília.

Os resultados foram mensurados utilizando-se a modelagem de equações estruturais de mínimos quadrados parciais (PLS-SEM).

Em relação ao tamanho mínimo da amostra, o método PLS-SEM considera o poder estatístico das estimativas [377]. Nesse sentido, utilizando-se o software Gpower, foi calculada a amostra necessária para o modelo proposto, Figura 7.6, que possui em sua análise mais complexa quatro relações.

Considerando um tamanho do efeito médio (0.15), uma potência estatística de 95% e margem de erro de 5%, a amostra para cálculo do modelo foi de 129 respondentes, conforme Figura 6.2. Ou seja, a amostra utilizada é mais que 10 vezes maior que a mínima necessária.

[1] -- *Monday, July 29, 2024 -- 12:56:25*
F tests – Linear multiple regression: Fixed model, R^2 deviation from zero

Analysis:	A priori: Compute required sample size		
Input:	Effect size f^2	=	0.15
	α err prob	=	0.05
	Power (1–β err prob)	=	0.95
	Number of predictors	=	4
Output:	Noncentrality parameter λ	=	19.3500000
	Critical F	=	2.4447662
	Numerator df	=	4
	Denominator df	=	124
	Total sample size	=	129
	Actual power	=	0.9505747

Figura 6.2: Tamanho mínimo da amostra (Fonte própria)

A modelagem de equações estruturais (*Structural Equation Modeling* (SEM)) é uma ferramenta analítica para testar as relações de causa/efeito de variáveis que são medidas indiretamente, conhecidas como latentes. A popularidade do método deriva do fato de a análise ser possível a partir de um modelo, sem a necessidade de testar uma teoria ou conceitos completos [378].

Quando se trabalha com modelos teóricos complexos, isto é, composto por vários construtos, a modelagem pode ser definida a partir da covariância, o método *Covariance Based* (CB-SEM), ou da variância, com o *Partial Least Squares - Structural Equation Modeling* (PLS-SEM). Enquanto o CB-SEM tem um caráter confirmatório e envolve fatores, o PLS-SEM é mais valoroso para pesquisas exploratórias e contempla compostos [378].

O PLS-SEM é considerada uma abordagem flexível para a construção de modelos a partir de suposições, bem como a adaptação de outros modelos. Adicionalmente, é útil quando o objetivo é explicar e prever construtos. Outra razão para escolher o PLS-SEM é a possibilidade de analisar o efeito das variáveis moderadoras [379][378][380].

Dessa forma, o uso do PLS-SEM neste estudo apresentou-se mais adequado em função da complexidade do modelo sugerido, uma adaptação do UTAUT para o contexto das urnas eletrônicas que contém inclusive variável de segunda ordem, bem como a existência de relações de moderação como será demonstrado no capítulo a seguir.

Capítulo 7

Resultados e análises

Neste capítulo serão apresentados os resultados encontrados com a aplicação da modelagem de equações estruturais (SEM) nos dados levantados por meio do formulário eletrônico da pesquisa.

A análise foi realizada com auxilio da ferramenta SmartPLS 4.1.0.1 [381], que permite avaliar se os dados levantados na pesquisa condizem com a teoria estudada, a partir da verificação do grau de correlação e regressão entre as múltiplas variáveis e seus indicadores. Ainda, o programa também indica as relações de alinhamento e influência entre as variáveis.

Além da descrição da amostra, apresenta-se o modelo conforme metodologia definida por [382], a qual prevê a descrição, validação e valoração do modelo por meio de testes estatísticos.

De maneira complementar, ainda serão avaliados também os efeitos das variáveis moderadoras, bem como a relação importância/desempenho, *Importance-Performance Map Analysis* (IPMA), [383] das variáveis do modelo proposto.

7.1 Descrição da amostra

A amostra deste estudo é composta de brasileiros usuários de aplicativos troca de mensagens online, familiarizados com o ato de votar nas eleições. Do ponto de vista demográfico, a amostra de 1.851 respostas ao formulário eletrônico foram estratificadas nos seguintes perfis:

1. **Quanto ao gênero**: 59,5% Masculino; 39,7% Feminino; 0,6% Prefiro não informar; e 0,2% Outros. De acordo com o Censo Demográfico de 2022 [384], a distribuição da população brasileira é de 51,5% de mulheres e 48,5% de homens. Ou seja, a estratificação por gênero da pesquisa possui diferenças significativas em relação ao Censo 2022, conforme ilustra a Figura 7.1.

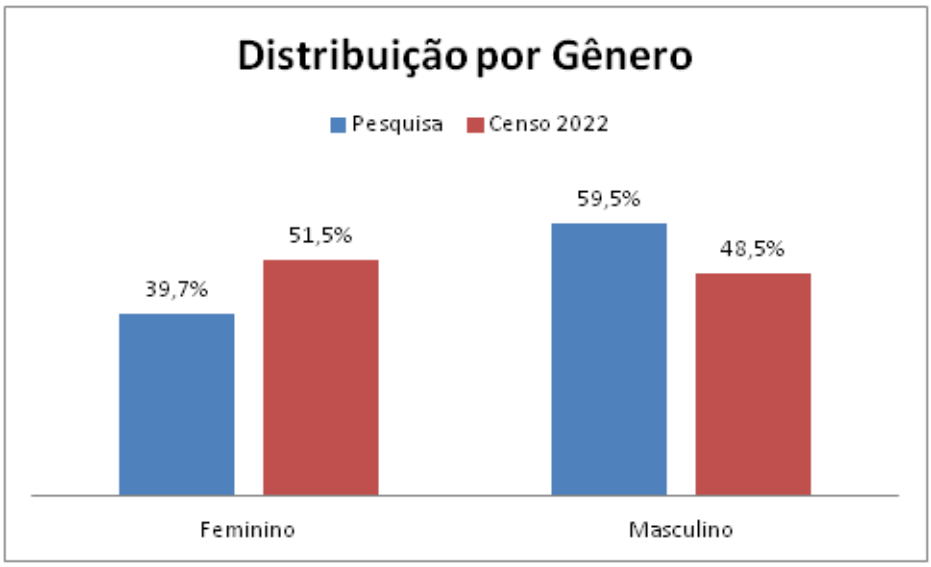

Figura 7.1: Distribuição da amostra por gênero (Fonte própria)

2. **Quanto a idade**: 30,1% entre 40 e 49 anos; 28,5% entre 50 e 59 anos; 15,8% entre 60 e 70 anos; 14,5% entre 30 e 39 anos; 5,8% entre 18 e 29 anos; 5,1% acima de 70 anos; e 0,2% entre 16 e 18 anos. Essas faixas etárias foram inspiradas na definição adotada pela Justiça Eleitoral. Entretanto, ela possui diferenças em relação à utilizada no Censo 2022 [384], em especial entre as idades de 16 a 29 anos, que o Censo subdivide em duas: entre 15 e 19; e entre 20 e 29 anos. Nesse sentido, foi necessário adaptar a comparação a essas faixas iniciais. Também na estratificação por idade, identifica-se diferença de distribuição entre a amostra da pesquisa e o Censo 2022, conforme apresentado na Figura 7.2.

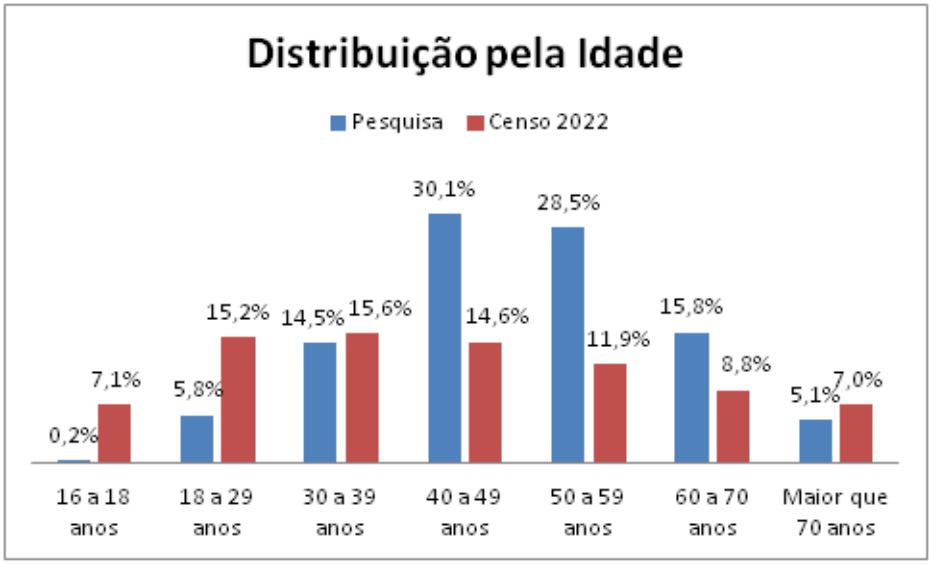

Figura 7.2: Distribuição da amostra por idade (Fonte própria)

3. **Quanto à escolaridade**: 93,4% Ensino Superior, subdividido em: 50,5% Pós-graduação, 24,2% Ensino superior, 11,9% Mestrado e 6,8% Doutorado; 5,8% Ensino médio; 0,4% Ensino fundamental; e 0,4% Prefiro não informar. Comparado aos números do IBGE em 2022 [385], conforme Figura 7.3, observa-se uma maior concentração de respondentes da pesquisa em pessoas com nível superior, quando este é o nível de instrução menos representativo da população brasileira.

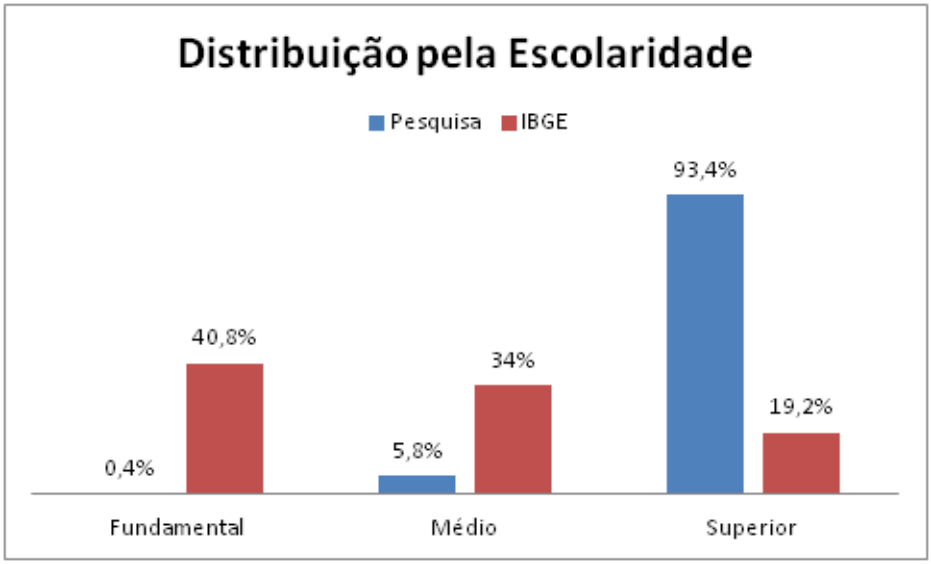

Figura 7.3: Distribuição da amostra pela escolaridade (Fonte própria)

4. **Quanto à orientação política**: 36,8% Prefiro não informar; 24,1% Esquerda; 22,8% Centro; e 16,3% Direita. Para este tema, utilizou-se como referência de comparação a pesquisa Panorama Político do DataSenado, cuja a 20ª edição foi publicada no ano de 2023 [386]. Interessante destacar que ambas pesquisas foram realizadas após às Eleições 2022, pleito realizado sob forte polarização política. Ao confrontar os dados entre as duas fontes, também observa-se diferenças significativas da distribuição, com destaque para os respondentes que preferiram não informar sua orientação política, conforme Figura 7.4.

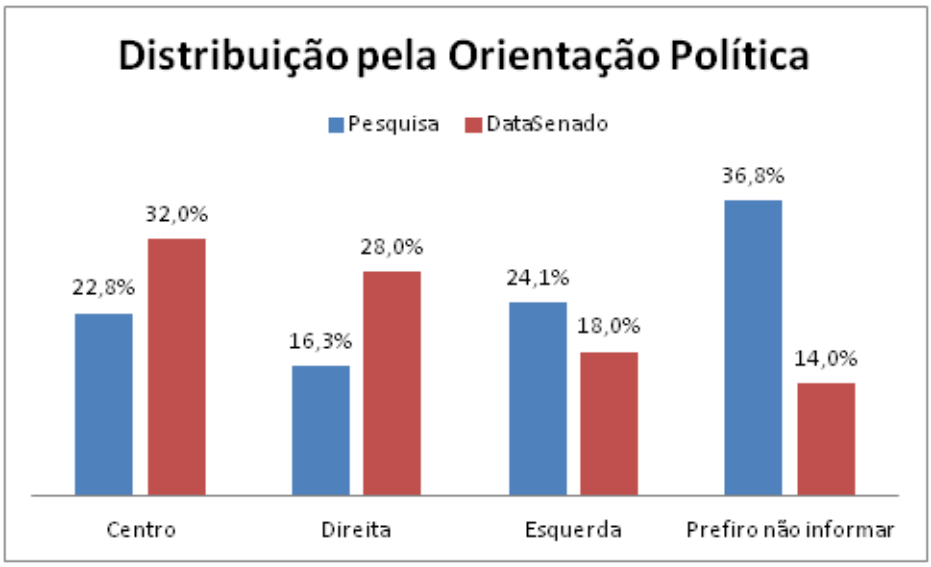

Figura 7.4: Distribuição da amostra pela orientação política (Fonte própria)

Realizada a descrição da amostra, observa-se que a característica mais discrepante comparada à população brasileira é a Escolaridade dos respondentes da pesquisa. Essencialmente, o público da pesquisa é formado por pessoas com Ensino Superior. Segue-se agora para as análises PLS-SEM do modelo proposto.

7.2 Modelo de Segunda Ordem

Como apresentado no Capítulo 5, o modelo originalmente proposto para esta pesquisa fora inspirado no estudo indiano [33] e havia sido definido como a Figura 5.2. Esse modelo é considerado de primeira ordem por refletir os conceitos e variáveis em um único grau de abstração [380].

Contudo, esse modelo de primeira ordem apresentou problemas de colinearidade nas variáveis Intenção de Uso (IU), Percepção de Segurança (PS) e a Confiança na Tecnologia (CT). Ou seja, pelos resultados obtidos, os indicadores dessas variáveis estavam se sobrepondo, comprometendo a integridade do modelo. A figura 7.5 apresenta o modelo de primeira ordem na ferramenta SmartPLS.

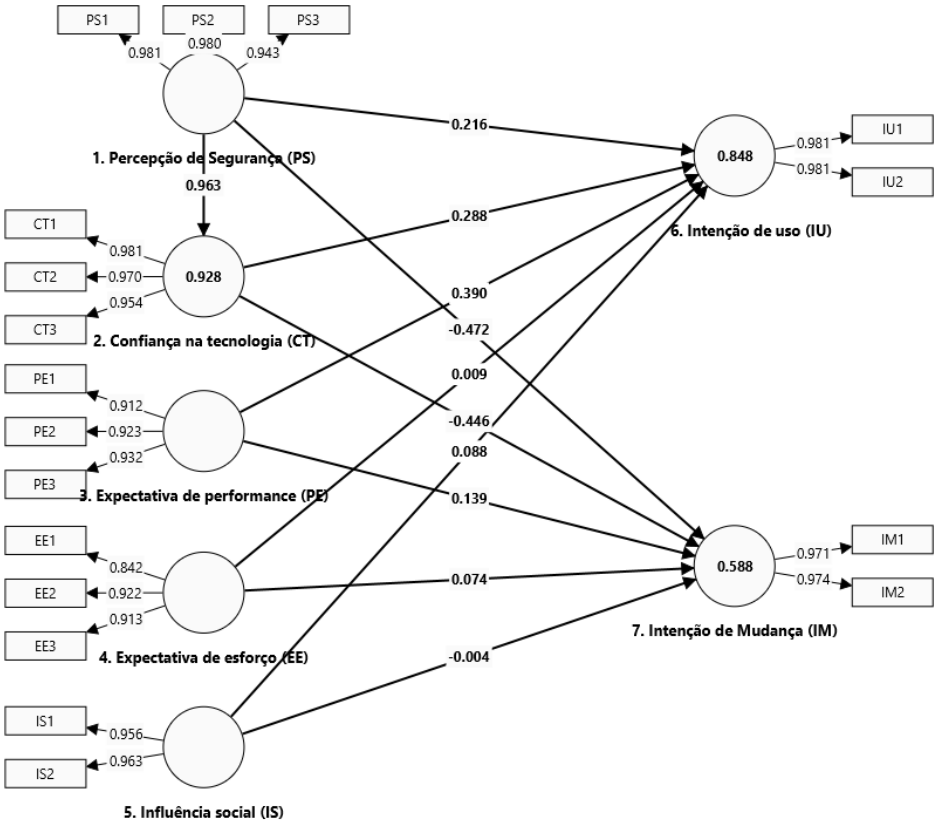

Figura 7.5: Modelo de primeira ordem (Fonte própria)

Este problema de colinearidade foi idenficado a partir da realização de um teste chamado de fator de inflação da variância, *Variance Inflation Factor* (VIF) [387]. Valores de VIF acima de 5 são considerados inadequados. A tabela 7.1 apresenta os valores de VIF encontrados para o modelo de primeira ordem.

Indicador	**VIF**
EE1	1.659
EE2	4.470
EE3	4.250
IM1	4.858
IM2	4.858
IS1	3.425
IS2	3.425
IU1	6.948
IU2	6.948
PE1	2.397
PE2	4.205

Continua na próxima página

Tabela 7.1 – continuação da página anterior	
Variável	**VIF**
PE3	4.458
PS1	17.947
PS2	17.891
PS3	4.425
CT1	11.889
CT2	9.316
CT3	5.545

Tabela 7.1: Fator de Inflação de Variância (VIF) do modelo original (Fonte própria)

Em casos assim, a literatura sugere avaliar a criação de variáveis de segunda ordem de modo a mitigar os problemas de colinearidade, em função da reorganização dos indicadores e/ou contrutos[380]. Modelos de segunda ordem nada mais são que a representação de modelos complexos em mais de um nível de abstração [380], neste caso dois níveis.

Para tanto, criou-se a variável Confiança Global (CG) para unificar os conceitos dos construtos Percepção de Segurança (PS) e Confiança na Tecnologia (CT). Ao se fazer essa ação, ambos construtos foram convertidos em indicadores da variável de segunda ordem, a Confiança Global (CG).

Em função de o método trabalhar de maneira depurativa, da mais significativa para as menores discrepâncias, a criação da variável de segunda ordem impactou também a colinearidade da variável Intenção de Uso (IU). Ao final, os valores se todas as variáveis se comportaram dentro dos limites esperados, como será detalhado na seção 7.3.4.

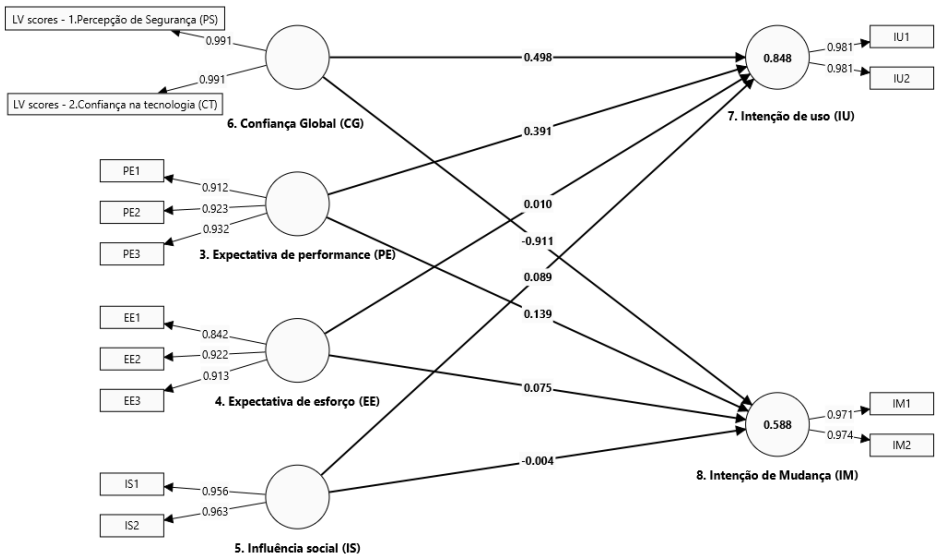

Figura 7.6: Modelo proposto de segunda ordem (Fonte própria)

Diante deste contexto, foi proposto o modelo de segunda ordem conforme ilustrado na Figura 7.6 e cuja análise será detalhada nos tópicos a seguir.

7.3 Valoração do modelo de medida

A valoração do modelo de medida refere-se à avaliação da confiabilidade e da validade das relações entre os indicadores e as variáveis (construtos) para garantir que se reflita com precisão os construtos pretendidos, bem como que o modelo se ajusta bem aos dados coletados [378].

A confiabilidade é avaliada por item (indicador) e também por construto (interna) [378]. Quanto à validade, são duas avaliações: a convergente e a discriminante [379].

7.3.1 Confiabilidade de item

A confiabilidade de item, também conhecida como carga (*loading*), busca identificar a força da correlação entre as variáveis e seus indicadores, indicando se estes estão atrelados às variáveis corretas dentro do modelo. É medida pela variância entre o indicador e seu construto [378]. Os valores podem variar entre -1 e 1, sendo considerado satisfatório quando superiores a 0,707 [379]. Correlações acima de 0,707 elevadas ao quadrado geram o valor da comunalidade, que explica o nível de variância que o indicador tem na variável latente [388]. Como resultado, espera-se que o indicador possua, ao menos, 50% de influência [388]. Neste estudo, é possível afirmar que o modelo possui confiabilidade de item, uma vez que o menor valor encontrado foi 0,842, no indicador EE1, conforme Figura 7.6.

7.3.2 Confiabilidade interna

A confiabilidade interna busca comprovar a consistência do conjunto de indicadores, ao avaliar se os indicadores são suficientes para explicar suas respectivas variáveis [378]. Em outras palavras, se o número de questões consegue explicar aquela variável.

Pode ser medida pelo Alfa de Cronbach (α) e a confiabilidade composta (rho_c). A diferença entre os métodos reside na maior precisão da confiabilidade composta, uma vez que ela não assume que todos os indicadores são igualmente confiáveis. Em que pese a maior confiabilidade para as equações estruturais [378], apresentam-se ambas informações neste estudo. Em relação aos valores, quanto mais próximo de 1 maior a confiabilidade interna, sendo considerado aceitável valores acima de 0,7 [379]. Conforme Tabela 7.2, os resultados obtidos nesta pesquisa foram satisfatórios.

Desse modo, considerando a aprovação nos testes de confiabilidade de item e interna, pode-se compreender que o modelo é confiável, passando-se para a avaliação de validade.

7.3.3 Validade convergente

A validade convergente busca compreender se todos se os indicadores estão associados ao construto correto [378]. A Validade convergente espera que os indicadores possuam uma variância média de ao menos 50% com sua respectiva variável latente [379][378]. Para tanto, utiliza o teste da variância média extraída, *Average Variance Extracted* (AVE). Essa medida de convergência afere a variância média do construto e seus indicadores. Podendo variar entre 0 e 1, valores iguais ou superiores a 0,5 são considerados aceitáveis [379], como é o caso do estudo atual. Conforme Tabela 7.2, o menor valor encontrado foi 0,798 para o construto Expectativa de Esforço (EE).

Variável	α	**rho_c**	**AVE**
3.Expectativa de performance (PE)	0,914	0,945	0,851
4.Expectativa de esforço (EE)	0,873	0,922	0,798
5.Influência social (IS)	0,914	0,959	0,921
6.Confiança Global (CG)	0,981	0,991	0,981
7.Intenção de uso (IU)	0,961	0,981	0,963
8.Intenção de mudança (IM)	0,942	0,972	0,946

Tabela 7.2: Confiabilidade interna e validade convergente (Fonte própria)

Verificada a validade convergente do modelo, passa-se agora a verificação da validade discriminante.

7.3.4 Validade discriminante

A validade discriminante indica quanto um construto é diferente dos demais. Ou seja, se ele mede o que se deseja medir [378]. Segundo critério de Fornell e Larcker [389], a quantidade de variação que um construto captura de seus indicadores (AVE) deve ser maior que a variância que o mesmo construto compartilha com outras variáveis (isto é, a correlação quadrática entre os dois construtos). Para facilitar esta avaliação, a raiz quadrada do AVE de cada construto deve ser maior que correlações que esta tem com o resto das variáveis do modelo. A Tabela 7.3 apresenta os resultados encontrados que confirmam a validade discriminante das variáveis deste trabalho.

Variável	PE	EE	IS	CG	IU	IM
3.Expectativa de performance (PE)	**0,922**					
4.Expectativa de esforço (EE)	0,782	**0,893**				
5.Influência social (IS)	0,690	0,579	**0,959**			
6.Confiança Global (CG)	0,791	0,639	0,787	**0,991**		
7.Intenção de uso (IU)	0,854	0,685	0,756	0,883	**0,981**	
8.Intenção de mudança (IM)	-0,526	-0,401	-0,581	-0,756	0,636	**0,972**

Tabela 7.3: AVE utilizando Fornell e Larcker (Fonte própria)

De acordo com os resultados apresentados, fica demonstrado que o modelo proposto atende aos critérios de confiabilidade e validade da valoração do modelo de medida.

7.4 Valoração do modelo estrutural

Uma vez que a confiabilidade e a validade do modelo estejam estabelecidas, trata-se de avaliar as relações hipotéticas entre os construtos e a capacidade de explicação do modelo. Essa é a avaliação do modelo estrutural que analisa o coeficiente de determinação (R^2), o coeficiente de caminho (β) e a significância a partir da técnica de *Bootstrapping* [378].

Porém, antes de avançar nessa análise, importante realizar um novo teste de colinearidade, o *Variance Inflation Factor* (VIF). Se anteriormente no modelo de medida foi avaliada a relação entre os indicadores e as variáveis, agora avalia-se das variáveis para as variáveis. Dessa forma, o VIF visa garantir que o cálculo duplo do modelo (modelos de medida e estrutural) não comprometa os valores encontrados. A Tabela 7.4 demonstra que os valores de VIF das variáveis também ficaram abaixo do valor de referência adequado, qual seja 5 [379].

Variável	VIF
3.Expectativa de performance (PE) → 7.Intenção de uso (IU)	4,124
3.Expectativa de performance (PE) → 8.Intenção de mudança (IM)	4,124
4.Expectativa de esforço (EE) → 7.Intenção de uso (IU)	2,590
4.Expectativa de esforço (EE) → 8.Intenção de mudança (IM)	2,590
5.Influência social (IS) → 7.Intenção de uso (IU)	2,723
5.Influência social (IS) → 8.Intenção de mudança (IM)	2,723
6.Confiança Global (CG) → 7.Intenção de uso (IU)	3,795
6.Confiança Global (CG) → 8.Intenção de mudança (IM)	3,795

Continua na próxima página

Tabela 7.4 – continuação da página anterior	
Variável	**VIF**

Tabela 7.4: Fator de Inflação de Variância - VIF (Fonte própria)

Superada a avaliação do VIF das variáveis, segue-se para avaliar a capacidade de explicação do modelo.

7.4.1 Coeficiente de Determinação (R^2)

O coeficiente de determinação (R^2) em equações estruturais é uma medida que indica o quão bem os indicadores latentes explicam a variância de uma variável endógena no modelo [379].

Variando entre 0 e 1, quanto mais próximo de 1 mais elevado o potencial explicativo das relações. Segundo a escala de Hair [378], valores acima de 0,50 denotam potencial explicativo moderado na relação e, acima de 0,75, substancial.

Neste estudo, foram obtidos os valores de 0,848 para Intenção de Uso (IU) e 0,588 para Intenção de Mudança (IM), conforme Figura 7.6. Isso representa dizer que a Intenção de Uso (IU) foi explicada em 84% pelas variáveis Confiança Global (CG), Expectativa de Performance (PE), Expectativa de Esforço (EE) e Influência Social (IS). Por outro lado, a Intenção de Mudança (IM), em 58%. Segundo [387], percentuais acima de 13% podem ser considerados satisfatórios. Ou seja, o potencial explicativo do modelo é satisfatório, sendo a variável Intenção de Uso a mais bem explicada. Para compreender quais variáveis mais implicam nas explicações é necessário estudar o Beta.

7.4.2 Coeficiente de Caminho (β)

O coeficiente de caminho (*path coefficient*) ou Beta (β) busca verificar o grau de influência de cada relação e a validade das hipóteses propostas [381]. Na prática, o β visa calcular os valores das setas que ligam os construtos, que são chamados de caminhos (*paths*).

Variando entre -1 e 1, quanto mais perto de 1 mais um construto explica outro. Por outro lado, valores próximos a 0 indicam baixa capacidade de explicação e valores negativos indicam comportamentos inversos entre os construtos [378]. Os valores de Beta que são considerados ideais são: $\beta \geq 0{,}3$ ou $\beta <$ -0,3, entretanto os valores $\beta \geq 0{,}2$ ou $\beta <$ -0,2 também são significativos em relação à análise [390].

Ainda, a significância ou a precisão das estimativas dos Betas pode ser avaliada por meio de um procedimento de *bootstrapping*. Essa é uma técnica de reamostragem não paramétrica, utilizada para mitigar possíveis erros causados pela distribuição da amostra [379]. O procedimento compreende substituir a amostra original para criar ao menos 5.000

amostras bootstrap, de modo que se determine a confiança estatística dos parâmetros utilizados [379]. A técnica visa garantir a estabilidade das estimativas das amostras, para isto, é necessário conseguir avaliar os valores: T-valor (*t-student*) e P-valor (*p-value*). Os valores que são utilizados como base a fim de garantir a confiança no modelo são: T-valor $\geq$ 1,64 e P-valor (p) $<$ 0,05 [379]. A Tabela 7.5 apresenta os valores encontrados neste estudo.

Hipóteses	β	%	**T-valor**	Intervalo de confiança		
				5%	**95%**	**Suportada**
H1. CG → IU	0,498	43,973%	15,879***	0,446	0,548	Sim
H2. CG → IM	-0,911	68,872%	34,807***	-0,953	-0,867	Sim
H3. PE → IU	0,391	33,391%	12,255***	0,339	0,444	Sim
H4. PE → IM	0,139	-7,311%	5,338***	0,096	0,181	Sim
H5. EE → IU	0,010	0,685%	0,468*	-0,024	0,044	Não
H6. EE → IM	0,075	-3,008%	3,05**	0,034	0,115	Sim
H7. IS → IU	0,089	6,728%	4,493***	0,057	0,123	Sim
H8. IS → IM	-0,004	0,232%	0,156*	-0,044	0,035	Não

* p<0,05; ** p<0,01; *** p<0,001

CG: Confiança Global; IU: Intenção de Uso; IM: Intenção de Mudança

PE: Expectativa de Performance; EE: Expectativa de Esforço; IS: Influência Social

Tabela 7.5: Valoração do modelo estrutural (Fonte própria)

Considerando as referências dos testes T-valor e P-valor, conforme Tabela 7.5, foram suportadas as hipóteses H1, H2, H3, H4, H6 e H7, assim como rejeitadas as hipóteses H5 e H8.

Dessa forma, é possível afirmar que Intenção de Uso (IU) foi influenciada em 43,973% pela Confiança Global (CG), H1, em 33,391% pela Expectativa de Performance (PE), H2, em 6,728% pela Influência Social (IS), H7, e não sofreu impacto da Expectativa de Esforço (EE), H5.

Por outro lado, os resultados demonstraram que a Intenção de Mudança (IM) foi influenciada em 68,872% pela Confiança Global (CG), H2, em 7,311% pela Expectativa de Performance (PE), H4, em 3,008% pela Expectativa de Esforço (EE), H6, e não sofreu impacto da Influência Social (IS), H8.

A análise detalhada dos resultados será realizada no tópico a seguir.

7.5 Análise e discussão das hipóteses

Nesta seção, cada hipótese será analisada seguindo a sequência numérica, mas separando-se pelas variáveis Intenção de Uso (IU) e Intenção de Mudança (IM) para um melhor entendimento.

7.5.1 Intenção de Uso (IU)

Depreende-se dos cálculos do modelo, conforme dados da Figura 7.6 e da Tabela 7.5, que a Intenção de Uso (IU) da urna eletrônica no Brasil foi explicada em 84%, sendo a Confiança Global (CG) a variável mais relevante, 44%, seguida pela Expectativa de Performance (PE), 33%, e da Influência Social (IS), 7%. Neste estudo, a Expectativa de Esforço (EE) não se mostrou significativa.

Os 84% de poder explicativo da intenção de uso da urna eletrônica no Brasil significam que as variáveis, ver Tabela 5.1, e os indicadores, ver Tabela 6.1, definidos no modelo são bastante assertivos, cobrindo expressiva parcela dos fatores que influênciam o comportamento dos cidadãos quando manifestam a intenção de utilizar o equipamento de votação brasileiro. A seguir, a análise de cada uma das hipóteses do modelo.

H1 - Confiança Global (CG) influencia a Intenção de uso (IU)

Relação mais relevante na intenção de uso das urnas eletrônicas, o suporte a essa hipótese indica que os indicadores relacionados à segurança e sigilo do voto, à corretude e acurácia de resultados, além da ausência de falhas/erros são os mais significativos. Isso porque a variável Confiança Global (CG) representa a fusão das variáveis Percepção de Segurança (PS) e Confiança na Tecnologia (CT).

Esse resultado é consistente com os encontrados no estudo Indiano [33] no qual as variáveis, Percepção de Segurança (PS) e Confiança na Tecnologia (CT), também foram as mais significativas. Além da pesquisa da Índia, também possuem resultados semelhantes as pesquisas realizadas no Chile [31], Vietnã [29], Gana [30] e EUA [32], ressaltando haver diferenças nas visões sobre as variáveis de confiança e segurança nestes estudos.

O achado também guarda relação com as palavras-chave mais representativas sobre o voto eletrônico encontradas nas bases de conhecimento *Web of Science* (WoS) e *Scopus*, como demonstrado na Revisão do Estado da Arte, Capítulo 2 acima. De maneira direta, o termo "*Security*" é o terceiro mais citado nas publicações da WoS. Quanto aos demais, os outros dois mais relevantes da WoS ("*blockchain*" e "*privacy*") e os três mais citados da *Scopus* ("*cryptography*", "*blockchain*" e "*authentication*"), todos estão intimamente relacionados à temática da percepção da segurança e confiança na tecnologia.

Ademais, as questões relacionadas à segurança, ao sigilo e à acuracidade do voto são centrais nos requisitos e princípios aplicáveis aos sistemas de votação, conforme apresentado no Referencial Teórico acima, Capítulo 3. Assim, o resultado encontrado nesta pesquisa está alinhado aos objetos de estudo das produções acadêmicas sobre a votação eletrônica.

Interessante salientar ainda a visão da autora [307] que, em seu estudo sobre confiança no sistema de votação eletrônica do Brasil, subdividiu a confiança na confiabilidade do sistema de votação eletrônico em si e no TSE, como entidade organizadora das eleições. Acerca do termo confiabilidade, seu conceito está relacionado à ausência de erros e ao correto funcionamento, enquanto a segurança, a ataques e tentativas de invasão [102]. Ou seja, a união dos aspectos de percepção da segurança e da confiança na tecnologia para formação da confiança no sistema eletrônico de votação já se fazia presente no modelo proposto pela autora em 2013.

H3 - Expectativa de Performance (PE) influencia a Intenção de uso (IU)

Também é significativa, porém em menor grau de importância, a percepção do eleitor de quanto a urna eletrônica traz ganhos para a votação, no sentido de ser útil para tornar mais rápido e facil o ato de votar. Essa é a compreensão decorrente do suporte à hipótese H3.

Esse resultado seria esperado em função de a busca por tornar mais ágil o processo de votar estar entre as principais motivações da implantação da votação eletrônica [8][9]. No caso brasileiro, apesar de o combate à fraude ter sido a motivação principal para adoção do voto eletrônico [12][13], a rapidez para divulgação dos resultados no mesmo dia, em um país com dimensões continentais, a padronização dos procedimentos de votação e a facilidade para votar são valores percebidos inclusive pelos críticos do sistema de votação eletrônica [16][17][18].

Ainda neste contexto de facilitar o ato de votar, importante destacar os impactos de inclusão para pessoas analfabetas e/ou com algum tipo de deficiência física propiciados pela adoção da urna eletrônica [9]. A exibição da foto dos candidatos, o uso de áudio para descrever cargos, nomes dos candidatos e números digitados, o uso da linguagem de sinais na tela do equipamento, bem como a presença do braile nas teclas da urna, ampliaram as possibilidades de participação de cidadãos brasileiros antes excluídos do processo democrático [352].

Interessante destacar também que o valor dos benefícios de agilizar e facilitar o ato de votar tem de ser percebidos pelos eleitores. Caso contrário, quando percebido que eles se aplicam apenas aos entes organizadores da eleição, tende-se a rejeitar a votação eletrônica,

em função de os riscos de segurança e privacidade superarem os alegados benefícios ao processo democráticos [8].

Vale salientar ainda que a relevância da Expectativa de Performance também foi encontrada no estudo indiano [33], assim como no coreano [28], vietnamita [29], ganês [30], chileno [31] e americano [32].

H5 - Expectativa de Esforço (EE) influencia a Intenção de uso (IU)

Única hipótese não suportada em relação à Intenção de Uso (IU), esse achado indica que questões relacionadas à usabilidade da urna eletrônica, incluindo compreensão e aprendizado do processo de votação com o equipamento, não foram significativos neste estudo.

Em uma primeira vista, pode-se receber com surpresa esse resultado, considerando o posicionamento de alguns autores em relação ao aumento da complexidade para compreensão do processo de votação a partir da introdução da tecnologia [340]. Dessa forma, seria esperado que o estudo demonstrasse algum grau de representatividade da Expectativa de Esforço na intenção de uso da urna eletrônica.

Uma possível explicação para esta descoberta pode ser o tempo de utilização das urnas eletrônicas nas eleições brasileiras e as ações educativas realizadas no período. São mais de 25 anos de utilização do equipamento, com variadas campanhas educativas e de esclarecimento à população.

Vale destacar que esse mesmo resultado foi encontrato nos estudos coreano [28], ganês [30] e indiano [33]. Ou seja, para as amostras desses estudos, aprimorar soluções para aumentar a usabilidade, compreensão de funcionamento e aprendizado sobre o processo de votação pode ter pouco resultado, caso feitas de maneira isolada das outras variáveis que demonstraram relevância.

H7 - Influência Social (IS) influencia a Intenção de uso (IU)

Com menor significância mas ainda relevante, estão as questões relacionadas a quanto os eleitores são suscetíveis à influência de outras pessoas em sua intenção de utilizar a urna eletrônica. Esse é o contexto do suporte à hipótese H7.

Como apresentado por [4], a influência social perde importância quando o uso da tecnologia analisada é mandatório. Nesse sentido, a baixa significância desta variável encontrada neste estudo está condizente com a obrigatoriedade do voto no Brasil. Contudo, vale destacar que, à exceção do estudo ganês [30], esse resultado está alinhado aos também encontrados nos trabalhos coreano [28], vietnamita [29], chileno [31], americano [32] e indiano [33]. Neste último, os autores destacam que a relevância da opinião de pessoas do círculo social, de formadores de opinião e do boca a boca sugere às autoridades gover-

namentais a possibilidade de elaborar estratégias de comunicação para ampliar o uso dos equipamentos de votação.

Alinhada à sugestão do estudo indiano, as Eleições 2022 foram palco de intensas campanhas de comunicação e debates tanto institucionais da Justiça Eleitoral em defesa do uso das urnas eletrônicas, quanto de parcela da população para criticá-la, inclusive com o uso de desinformação [339]. Observa-se então que, apesar da menor relevância identificada no estudo, a influência social é uma variável largamente trabalhada nas eleições brasileiras, especialmente no ambiente da internet.

Resumo da análise

Em síntese, interpretando-se os resultados relacionados à variavel Intenção de Uso (IU), percebe-se que a sensação de segurança que a urna eletrônica agregou ao processo eleitoral é decisiva para aqueles que tem a intenção de utilizá-la, mesmo que não se tenha total compreensão do seu funcionamento. Ainda, em que pese a significância percebida do valor e dos benefícios decorrentes da utilização das urnas eletrônicas, a compreensão sobre seu funcionamento não é fundamental na decisão de utilizar os equipamentos de votação. Por fim, constata-se também a influência de formadores de opinião ou pessoas próximas na intenção de uso das urnas eletrônicas.

Interessante registrar a semelhança dos resultados encontrados com os obtidos no estudo indiano [33] utilizado como referência para este trabalho. Assim como neste estudo, a pesquisa realizada na Índia identificou a Percepção de Segurança (PS) e a Confiança na Tecnologia (CT) como as variáveis mais significativas na inteção de uso das urnas eletrônicas naquele país. Ainda, também como os achados deste estudo, o trabalho indiano identificou que a Expectativa de Performance (PE) e a Influência Social (IS) também influênciam na intenção de uso dos equipamentos de votação, assim como a falta de impacto da Expectativa de Esforço (EE).

Em relação ao modelo original UTAUT [27], os resultados encontrados são consistente em relação à significância da Expectativa de Performance (PE) e da Influência Social (IS) na intenção de uso (IU). Entretanto, seria esperado que também fosse suportada a hipótese de influência da Expectativa de Esforço (EE), o que não se comprovou, assim como também ocorreu no estudo indiano.

7.5.2 Intenção de Mudança (IM)

Quanto aos resultados encontrados para a variável Intenção de Mudança (IM), que considera a necessidade de a urna eletrônica imprimir o voto, uma inovação deste estudo em relação ao trabalho de referência indiano [33], o modelo proposto foi capaz de explicá-la

em 58%, conforme Tabela 7.5. Ou seja, diferentemente da Intenção de Uso (IU), o poder explicativo do modelo é menor para essa variável, indicando a existência de mais fatores a serem observados quando se trata de entender a intenção de mudar para permitir a impressão do voto pela urna eletrônica no Brasil.

Assim como na análise da Intenção de Uso, a Confiança Global (CG) também foi a variável mais significativa, porém com influência ainda maior para a mudança. Os resultados demonstraram que 68,8% da Intenção de Mudança (IM) é explicada pela Confiança Global (CG), seguida pela Expectativa de Performance (PE), -7%, Expectativa de Esforço (EE), -3%, e, ao contrário da Intenção de Uso (IU), a Influência Social (IS) não foi significativa. A existência de valores percentuais negativos indica apenas a influência da variável no coeficiente de determinação (R^2), nesses casos retirando valor. Ou seja, essas variáveis, PE e EE, influenciam na Intenção de Mudança (IM), mas possuem impacto negativo, subtraindo valor da relação (R^2).

H2 - Confiança Global (CG) influencia a Intenção de mudança (IM)

O valor de β negativo e o suporte para a hipótese H2 indicam que a Confiança Global (CG) influencia a Intenção de Mudança (IM), porém de maneira contrária. Assim, a Intenção de Mudança (IM) aumenta quando há redução da Confiança Global (CG) e diminui à medida que a Confiança Global (CG) aumenta.

Esse achado está condizente com as críticas ao Processo Eletrônico de Votação brasileiro apresentadas na Seção 4.3 acima, cuja a mais destacada é a necessidade de utilizar a impressão do voto como meio independente de auditoria do sistema de votação. Como apresentado pelos autores de [9], a utilização de tecnologias na votação gera, entre outras questões, falta de confiabilidade na correta gravação dos votos, na garantia do sigilo do voto e na transparência, na medida em que limita as possibilidades de recontagem dos votos e permite a introdução de novas possibilidades de fraude eleitoral.

Sobre essa possibilidade de aumento da confiança na eleição com a introdução do voto impresso, vale destacar resultado 149º rodada de pesquisas da Confederação Nacional dos Transportes [369], de Julho de 2021, na qual 58% dos entrevistados informaram ser a favor da impressão do voto para aumentar a confiança nos resultados. Porém, há que se destacar também o potencial de retomada de fragilidades no processo de votação, como apresentado na Seção 4.3.

H4 - Expectativa de Performance (PE) influencia a Intenção de mudança (IM)

Apesar de menos significativo, o suporte à H4 indica a disposição de abrir mão da agilidade e da facilidade proporcionadas pelo uso da urna eletrônica, em nome de um alegado aumento da transparência e da auditabilidade propiciado pela impressão do voto.

Esse ponto de vista defende que a votação e a divulgação de resultados, além de rapidez, tem de proporcionar confiança para a população o que não seria possível com as urnas eletrônicas sem a impressão do voto [339].

H6 - Expectativa de Esforço (EE) influencia a Intenção de mudança (IM)

Na mesma direção, o suporte à hipótese H6, em que pese a baixa representatividade no modelo, indica que a não compreensão do processo de votação com uso da urna eletrônica é motivo para sugerir a introdução da impressão do voto.

Esse achado corrobora os estudos que consideram o uso da tecnologia como um dificultador para a população sem conhecimento técnico entender o processo de votação [6][340]. Nesse caso, a introdução da impressão do voto seria capaz de permitir ao cidadão comum entender e acreditar no processo de votação, sem ter de recorrer à opinião de especialistas técnicos [339].

Interessante fazer um destaque deste item nas visões da intenção de uso e de mudança. Enquanto a compreensão do funcionamento da urna eletrônica não foi significativa para quem declara intenção de utilizar o equipamento, hipótese H5, para quem deseja a mudança, é uma questão relevante, conforme suporte à H6.

H8 - Influência Social (IS) influencia a Intenção de mudança (IM)

Com alguma surpresa, a hipótese H8 não foi suportada pelo modelo, ou seja, a Influência Social (IS) não é capaz de impactar na intenção de mudança (IM). O inesperado deste resultado encontra-se na expressiva divulgação da importância da impressão do voto para os críticos da votação eletrônica, seja no meio acadêmico ou mesmo entre a população que defende a mudança da urna eletrônica. Em função da mobilização que temas relacionados à possibilidade de fraude eleitoral geram nas redes sociais [374], era de se esperar alguma influência dessa variável.

Resumo da análise

Ao final, os resultados relacionados à variavel Intenção de Mudança (IM) demonstram que a mesma sensação de segurança percebida para definir a intenção de uso da urna eletrônica é ainda mais relevante quando se deseja a mudança para incluir a impressão do voto. Ou seja, quem defende a necessidade de a urna eletrônica imprimir o voto o faz essencialmente por não confiar na tecnologia para resguardar a segurança da votação.

Ademais, a agilidade e a facilidade proporcionadas pela votação eletrônica, que são percebidos como benefício para intenção de uso do equipamento de votação, também são significativos para a intenção de mudança, porém no sentido de poder se abrir mão

dessas benesses em nome de um suposto aumento da transparência e auditabiidade com a impressão do voto. Ainda, também significativo é o impacto da impressão do voto para tornar mais compreensível o processo de votação para o público sem conhecimento técnico.

7.6 Efeitos moderadores

As informações sociodemográficas dos respondentes da pesquisa, além de caracterizar a amostra, foram utilizadas em testes para revelar se impactam ou não o resultado final do modelo, ou seja, se o modelo é único para toda amostra ou existem diferentes modelos contidos nos dados originais.

Neste contexto, foram avaliadas as variáveis moderadoras: Gênero, Idade, Escolaridade e Orientação Política. Destas, Gênero e Orientação Política são de ordem categórica, assim como Idade e Escolaridade são do tipo contínua. A seguir a análise dos resultados das variáveis moderadoras do modelo, conforme Figura 5.3.

7.6.1 Gênero

De acordo com a Tabela 7.6, foi encontrada diferença entre os gêneros para as hipóteses H1, H2, H3 e H7.

Hipóteses	β **Geral**	β **Feminino**	β **Masculino**	**P-valor**	**Diferença**
H1. CG → IU	0,498	0,541	0,353	0,000	Sim
H2. CG → IM	-0,911	-0,945	-0,826	0,030	Sim
H3. PE → IU	0,391	0,357	0,540	0,001	Sim
H4. PE → IM	0,139	0,151	0,143	0,873	Não
H5. EE → IU	0,010	0,021	-0,049	0,100	Não
H6. EE → IM	0,075	0,086	0,042	0,392	Não
H7. IS → IU	0,089	0,065	0,146	0,042	Sim
H8. IS → IM	-0,004	-0,007	-0,005	0,966	Não

*CG: Confiança Global; IU: Intenção de Uso; IM: Intenção de Mudança

*PE: Expectativa de Performance; EE: Expectativa de Esforço; IS: Influência Social

Tabela 7.6: Moderação por Gênero (Fonte própria)

Considerando os resultados encontrados, a Confiança Global (CG) é mais significativa para as mulheres tanto para a Intenção de Uso (IU), H1, quanto em relação à Intenção de Mudança (IM), H2. Esse resultado ganha relevância em função de não ter sido encontrado

nem no modelo UTAUT [27], nem no estudo indiano [33]. Em ambos os casos, não houve diferença significativa entre os gêneros.

Por outro lado, os homens são mais impactados pelas questões relacionadas às variáveis Expectativa de Performance (PE), H3, e Influência Social (IS), H7. Em relação à Expectativa de Performance (PE), esse mesmo resultado foi encontrado no estudo indiano [33] e no modelo UTAUT [27]. Porém, sobre a Influência Social (IS), o resultado é o mesmo dos estudos chileno [31] e indiano [33], mas o inverso do UTAUT [27]. Neste último, a Influência Social (IS) foi mais significativa para as mulheres.

Dentre as hipóteses em que não se identificou diferença entre os gêneros, vale destacar a variável Expectativa de Esforço (EE) na relação com a Intenção de Uso (IU). Tanto no modelo UTAUT [27] quanto no estudo indiano [33], as mulheres foram mais impactadas pela Expectativa de Esforço (EE), o que não se confirmou nesta pesquisa.

7.6.2 Idade

Em relação ao impacto da Idade no modelo, os resultados apresentam que houve diferença significante apenas nas relações da Confiança Global (CG) com a Intenção de Uso (IU) e na Expectativa de Esforço (EE) com a Intenção de mudança (IM), conforme Tabela 7.7.

Hipóteses	β	**T-valor**	**P-valor**
Idade x (CG $\rightarrow$ IU)	-0,036	2,468	0,014
Idade x (EE $\rightarrow$ IM)	0,053	2,727	0,006

*CG: Confiança Global; IU: Intenção de Uso;

*EE: Expectativa de Esforço; IM: Intenção de Mudança

Tabela 7.7: Moderação por Idade (Fonte própria)

A Figura 7.7 ilustra graficamente o resultado e auxilia a compreender o impacto da idade na relação da Confiança Global (CG) e a Intenção de Uso (IU).

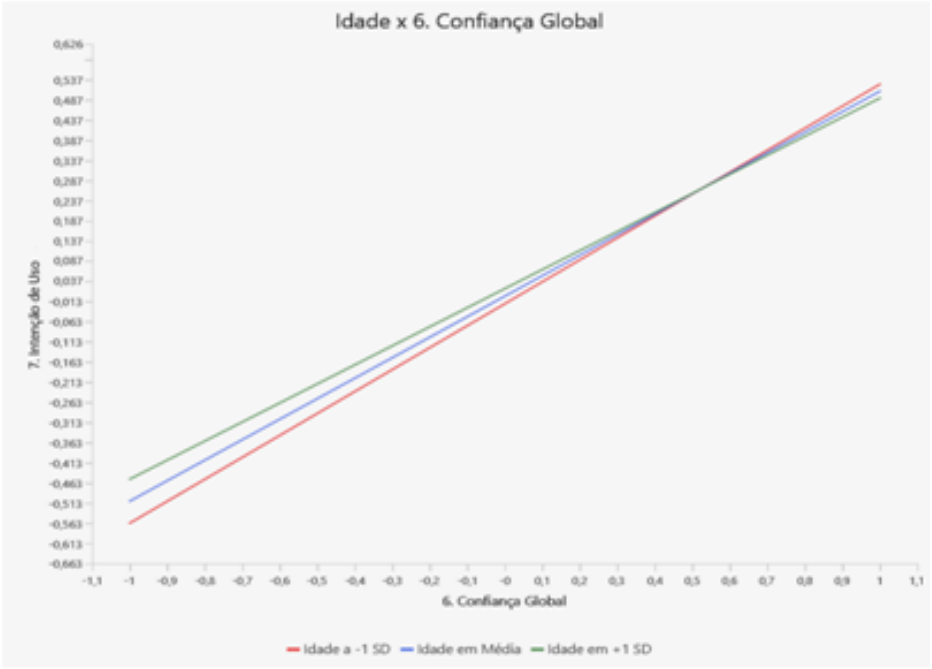

Figura 7.7: Moderação por Idade na relação CG e IU (Fonte própria)

Pode-se observar três linhas na imagem. A azul refere-se ao efeito médio, a partir de uma idade média, que se comporta em um crescimento linear da Intenção de Uso à medida que aumenta a confiança na urna eletrônica.

Porém, quando se compara a linha verde de pessoas com mais idade versus a linha vermelha de pessoas com menos idade, observa-se uma inclinação levemente mais íngrime da reta vermelha. Isso significa que a confiança global é um requisito importante na intenção de uso das urnas eletrônicas para ambos os públicos, com uma sutil maior relevância para os mais jovens. Ou seja, considerando que a Confiança Global (CG) é a união das variáveis Percepção de Segurança (PS) e Confiança na Tecnologia (CT), questões relacionadas à segurança e à integridade do voto são mais relevantes para pessoas mais novas.

Esse resultado pode indicar um maior conhecimento técnico dos riscos associados ao uso da tecnologia por parte de pessoas mais jovens, em que pese ser recorrente no público idoso a desconfiança e aversão ao uso da tecnologia em geral.

Interessante destacar que resultado semelhante foi encontrado no estudo de avaliação para adotar a votação online realizado nos Estados Unidos [32], adaptado para confiança na internet. Entretanto, tanto no modelo UTAUT [27] quanto no estudo indiano [33], a idade não teve impacto significativo na aceitação do uso de tecnologia nos processos de votação daqueles países.

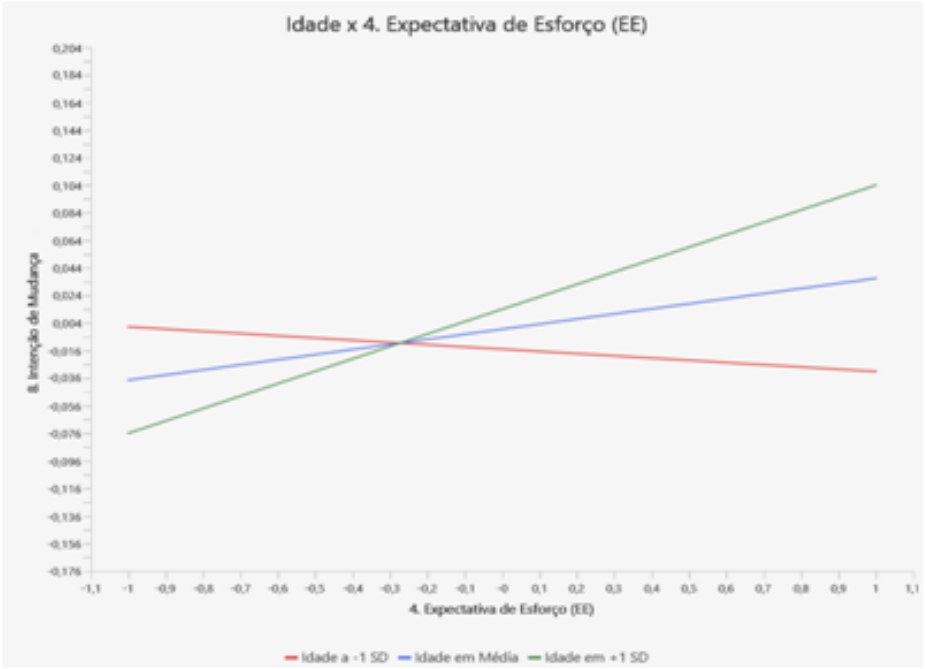

Figura 7.8: Moderação por Idade na relação EE e IM (Fonte própria)

De maneira similar, a Figura 7.8 ilustra graficamente o impacto da idade na relação da Expectativa de Esforço (EE) e a Intenção de Mudança (IM). Novamente, a linha azul refere-se ao modelo sem o efeito da idade e apresenta um leve aumento da Intenção de Mudança (IM) à medida que aumenta a Expectativa de Esforço (EE).

Ao se comparar a linha verde das pessoas mais velhas com a vermelha dos mais jovens, a reta com inclinação ascendente é a linha das pessoas com mais idade. Ou seja, à medida de que aumenta a idade, mais a Expectativa de Esforço (EE) impacta na Intenção de Mudança (IM).

Interpretando-se no contexto de que a mudança avaliada na variável é a impressão do voto pela urna eletrônica, sugere-se que os eleitores mais velhos entendem ser mais fácil e compreensível o processo de votação com a introdução do voto impresso.

Vale destacar que a Expectativa de Esforço (EE) também foi significativa para as pessoas com mais idade nos estudos americano [32], indiano [33] e no modelo UTAUT [27].

Por fim, cabe destacar ainda que brasileiros abaixo de 24 anos conhecem apenas a votação eletrônica, uma vez que a implantação do equipamento de votação em todo o país ocorreu em 2000.

7.6.3 Escolaridade

O estudo de [332] apresentou que a confiança no voto eletrônico diminui à medida que aumenta a escolaridade. Entretanto, nesta pesquisa o resultado encontrado foi em outra direção. Conforme Tabela 7.8, a escolaridade impactou apenas a relação entre a Expectativa de Performance (PE) e a Intenção de Mudança (IM).

Hipóteses	β	**T-valor**	**P-valor**
Escolaridade x (PE → IM)	-0,034	2,638	0,004

*PE: Expectativa de Performance; IM: Intenção de Mudança

Tabela 7.8: Moderação por Escolaridade (Fonte própria)

A Figura 7.9 ilustra o impacto dessa variável na relação PE e IM. A reta azul representa o modelo sem o efeito da escolaridade e apresenta um aumento da Intenção de Mudança (IM) à medida que aumenta a Expectativa de Performance (PE).

Figura 7.9: Moderação por Escolaridade na relação PE e IM (Fonte própria)

Contudo, comparando-se a linha verde das pessoas com maior nível educacional com a vermelha dos menos escolarizados, a reta com maior inclinação ascendente é a das pessoas com menos instrução. Dessa forma, identificou-se que quanto menor a escolaridade, mais a Expectativa de Performance (PE) impacta na Intenção de Mudança (IM).

Ou seja, para o eleitorado menos educacionalmente instruído, o desejo para que a urna eletrônica imprima o voto, a Intenção de Mudança (IM), aumenta à medida que

mais se percebe as facilidades e rapidez trazidas pelo equipamento de votação. Esse resultado pode indicar que essa fração do eleitorado enxerga a impressão do voto como um elemento adicional à urna eletrônica, que não prejudicaria os benefícios de performance do equipamento.

7.6.4 Orientação política

Em função da polarização política vivida nas Eleições 2022 e da intensa mobilização nas redes sobre fraudes na votação eletrônica [374], decidiu-se por avaliar o impacto da orientação política na intenção de uso da urna eletrônica. A seguir, os resultados encontrados sempre comparando-se duas vertentes isoladamente, uma restrição do método de avaliação.

Sem dúvida a comparação mais esperada é do espectro polítco à Direita e à Esquerda. A Tabela 7.9 indica que no confronto entre essas duas ideologias políticas houve diferença significativa na relação da Confiança Global (CG) e da Expectativa de Esforço (EE) na Intenção de Mudança (IM), bem como da Influência Social (IS) na Intenção de Uso (IU).

Hipóteses	β **Geral**	β **Direita**	β **Esquerda**	**P-valor**
H2. CG → IM	-0,911	-0,793	-0,239	0,000
H6. EE → IM	0,075	0,201	-0,146	0,000
H7. IS → IU	0,089	0,212	0,048	0,014

*CG: Confiança Global; IU: Intenção de Uso; IM: Intenção de Mudança

*PE: Espectativa de Performance; IS: Influência Social

Tabela 7.9: Moderação por Orientação Política na relação Direita e Esquerda (Fonte própria)

Em relação à Confiança Global (CG) ela impacta de maneira mais relevante a Intenção de Mudança das pessoas que se declaram de Direita, mantendo a relação inversa encontrada no resultado geral. Ou seja, o público de orientação política à Direita é mais sensível a querer a impressão do voto, à medida que diminui a confiança.

Adicionalmente, o eleitorado à Direita também é mais impactado que os esquerdistas quanto à percepção da Expectativa de Esforço (EE). Ou seja, o público à Direita entende que à medida que a votação torna-se mais complexa, maior é a intenção de impressão do voto. Vale destacar o valor negativo do β dos eleitores à Esquerda. Para os integrantes desse espectro político, as variáveis são inversamente proporcionais. À medida que o processo de votação torna-se mais complexo, menor a intenção de mudança.

Sobre a Intenção de Uso (IU), os resultados demonstram que o público direitista é significativamente mais impactado pela Influência Social (IS) que os esquerdistas.

Quando se compara os eleitores de Direita com os centristas, conforme Tabela 7.10, são mantidas as diferenças significativas do impacto da Expectativa de Esforço na Intenção de Mudança (IM) e da Influência Social na Intenção de Uso (IU), assim como na comparação com a Esquerda. Porém, como novidade, tem-se que a Intenção de Uso (IU) dos centristas é muito mais impactada pela Confiança Global (CG) do que a dos direitistas. Ou seja, os eleitores de Centro tem a confiança como motivador para utilizar os equipamentos de votação.

Hipóteses	β **Geral**	β **Direita**	β **Centro**	**P-valor**
H1. CG → IU	0,498	0,298	0,539	0,005
H6. EE → IM	0,075	0,201	0,054	0,039
H7. IS → IU	0,089	0,212	0,051	0,011

*CG: Confiança Global; IU: Intenção de Uso; IM: Intenção de Mudança

*EE: Expectativa de Esforço; IS: Influência Social

Tabela 7.10: Moderação por Orientação Política na relação Direita e Centro (Fonte própria)

Por fim, a Tabela 7.11 apresenta os resultados da comparação do espectro político declarado à Esquerda e os de Centro. Ambas relações mais significativas referem-se à Intenção de Mudança (IM). De modo ainda mais representativo, a intenção de mudar é mais impactada pela Confiança Global (CG) para o público de Centro que os de Esquerda, mas com valores inversamente proporcionais ainda maiores que os de Direita. Dessa forma, a diferença entre os eleitores de Centro e de Esquerda é ainda mais significativa quando se trata da relação Confiança e Intenção de Mudança.

Hipóteses	β **Geral**	β **Esquerda**	β **Centro**	**P-valor**
H2. CG → IM	-0,911	-0,239	-0,879	0,000
H6. EE → IM	0,075	-0,146	0,054	0,015

*CG: Confiança Global; IM: Intenção de Mudança; EE: Expectativa de Esforço

Tabela 7.11: Moderação por Orientação Política na relação Esquerda e Centro (Fonte própria)

Ainda, também de maneira similar ao encontrado na comparação da Esquerda com a Direita, pessoas que se declaram de Centro também são mais impactadas que os esquerdistas quanto à percepção da Expectativa de Esforço (EE). Ou seja, o público ao Centro também entende que à medida que a votação torna-se mais complexa, maior é a intenção imprimir o voto.

7.6.5 Resumo dos efeitos moderadores

A fim de auxiliar o entendimento dos efeitos moderadores do modelo, a Tabela 7.12 apresenta a consolidação dos resultados encontrados para cada hipótese e os impactos das variáveis moderadoras.

Hipóteses	**Moderadores significantes**	**Efeito**
H1. CG → IU	Gênero e Idade	Significativo para mulheres, mais jovens e centristas
H2. CG → IM	Gênero e Orientação política	Significativo para mulheres, centristas e também de direita
H3. PE → IU	Gênero	Significativo para homens
H4. PE → IM	Escolaridade	Significativo para pessoas com menos instrução
H5. EE → IU	-	-
H6. EE → IM	Idade e Orientação política	Significativo para pessoas mais velhas e de direita
H7. IS → IU	Gênero e Orientação política	Significativo para homens e pessoas de direita
H8. IS → IM	-	-

*CG: Confiança Global; IU: Intenção de Uso; IM: Intenção de Mudança

*PE: Espectativa de Performance; EE: Expectativa de Esforço; IS: Influência Social

Tabela 7.12: Resumo dos efeitos moderadores (Fonte própria)

Diante das informações apresentadas é possível traçar ações para públicos segmentados e com objetivos específicos de potencializar resultados positivos ou minimizar negativos.

7.7 Priorização de ações de melhoria

Para definir ações de melhoria da confiança na urna eletrônica brasileira, foram calculados mapas de Importância vs. Desempenho, *Importance-Performance Map Analysis* (IPMA), que permitem priorizar atividades a serem realizadas. Foram calculados mapas para as variáveis Intenção de Uso (IU) e Intenção de Mudança (IM).

A análise de IPMA amplia os resultados do PLS-SEM ao combinar as dimensões da importância e do desempenho das variáveis e/ou indicadores do modelo. O resultado gerado pelo método propicia priorizar variáveis ou indicadores que possuem mais impacto no conceito em análise no modelo [383].

A partir dos resultados encontrados no IPMA, as variáveis ou indicadores candidatos a serem priorizados são aqueles que possuem importância alta e baixo desempenho. Localizando no mapa, são os itens que estão mais a direita e mais abaixo.

Vale salientar que os resultados da análise PLS-SEM foram realizados no modelo de segunda ordem (Figura 5.3), no qual a variável de segunda ordem Confiança Global (CG) unifica os indicadores das variáveis de primeira ordem Percepção de Segurança (PS) e Confiança na Tecnologia (CT). Contudo, para variáveis de segunda ordem, a análise IPMA possui limitações de priorizar os indicadores individualmente. Por isso, para este caso, o IPMA reflete as variáveis de primeira ordem e não ordena seus indicadores por prioridade.

7.7.1 Intenção de Uso (IU)

A Figura 7.10 apresenta o IPMA da variável Intenção de Uso do modelo proposto neste estudo (Figura 5.3) e suas variáveis/indicadores, Tabela 6.1.

Observa-se no mapa que a variável de primeira ordem Confiança na Tecnologia (CT) é a mais importante por estar mais à direita. Assim, seus indicadores são os mais relevantes, quais sejam: "**CT1** - Eu acredito que a urna eletrônica é confiável"; "**CT2** - A urna eletrônica mantém meu voto secreto"; e "**CT3** - Eu acredito que a urna eletrônica tem boa reputação". Ressalta-se não haver a priorização entre os indicadores, em função das limitações da análise IPMA, considerando-se esta variável fazer parte de uma de segunda ordem no modelo proposto. Em relação ao desempenho, a variável tem o segundo pior resultado do mapa.

Praticamente com a mesma alta importância e baixo desempenho, encontra-se a variável Percepção de Segurança (PS). Nesse caso, por tratar-se de variável de primeira ordem absorvida por outra de segunda ordem no modelo proposto, também há limitações para priorizar seus indicadores, quais sejam: "**PS1** - Eu acredito que as urnas eletrônicas mantém meu voto seguro"; "**PS2** - A urna eletrônica gera resultados corretos"; e "**PS3** - A urna eletrônica é relativamente livre de falhas/erros".

Na sequência da importância aparecem os indicadores da variável Expectativa de Performance (PE), priorizados na seguinte sequência: "**PE1** - A urna eletrônica é útil"; "**PE3** - Utilizar a urna eletrônica torna mais rápida minha votação"; e "**PE2** - utilizar a urna eletrônica torna mais fácil minha votação". Esses indicadores também figuram entre os de pior desempenho no mapa na mesma sequência.

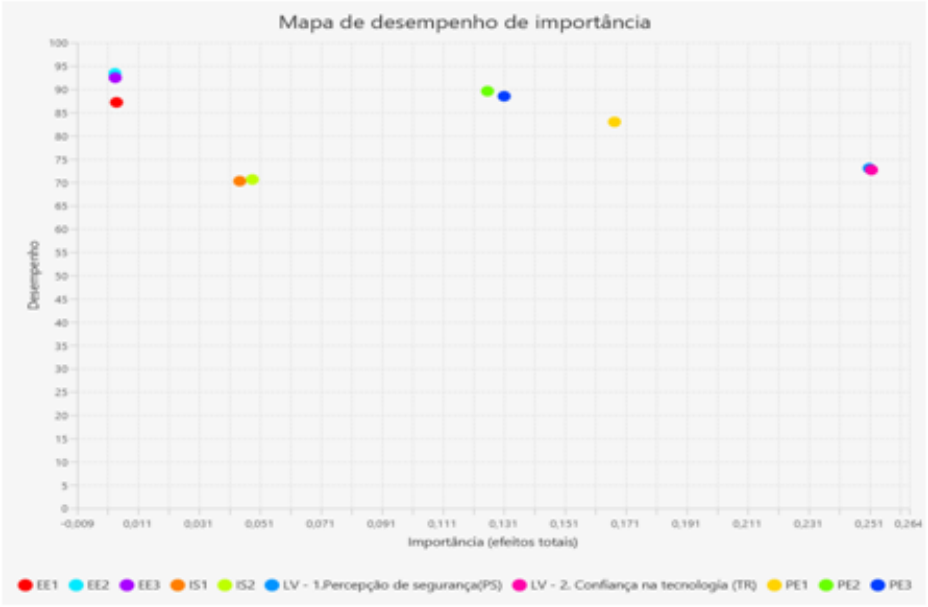

Figura 7.10: IPMA da Intenção de Uso (Fonte própria)

Do ponto de vista do desempenho, vale destacar ainda que os piores resultados são dos indicadores da variável Influência Social (IS). Em último está o indicador "**IS1** - Pessoas que influenciam meu comportamento recomendam o uso da urna eletrônica", seguido de "**IS2** - Pessoas que são importantes para mim recomendam o uso da urna eletrônica". Porém, devido a sua baixa importância, têm menos relevância para priorização.

Dessa forma, diante resultados do mapa de Importância vs. Desempenho da intenção de uso das urnas eletrônicas, verifica-se que os respondentes da pesquisa consideram muito importante as características de segurança do equipamento de votação, assim como a percepção de benefícios que o dispositivo agrega ao ato de votar.

Nesse sentido, para esse nicho da sociedade, é importante a realização de ações que continuamente aprimorem as propriedades de segurança da urna eletrônica, bem como tragam ainda mais benefícios aos cidadãos durante a votação. Para ambos contextos, é necessário trabalhar na melhoria da comunicação das características do processo atual e na proposição de inovações.

Por último, aliando-se a análise IPMA com os efeitos das variáveis moderadoras (Tabela 7.12), no momento de definir os detalhes de implementação e de comunicação com o grande público, deve-se considerar que para quem tem a intenção de utilizar a urna eletrônica, os temas relacionados à Confiança Global (CG) são mais significativos para as pessoas do gênero feminino, os mais jovens e com orientação política ao centro. Adicionalmente, as questões relacionadas aos benefícios gerados pelo equipamento de votação (Expectativa de Performance - PE) são mais relevantes para pessoas do sexo masculino.

7.7.2 Intenção de Mudança (IM)

Por outro lado, o IPMA da Intenção de Mudança (IM), quando se deseja que a urna eletrônica imprima o voto, apresenta uma maior concentração de indicadores com alta importância, conforme a Figura 7.11.

Figura 7.11: IPMA da Intenção de Mudança (Fonte própria)

Ao se observar os resultados do mapa, os indicadores mais importantes são, em ordem decrescente: "**PE1** - A urna eletrônica é útil"; "**PE3** - Utilizar a urna eletrônica torna mais rápida minha votação"; e "**PE2** - Utilizar a urna eletrônica torna mais fácil minha votação". Todos da variável Expectativa de Performance (PE) e também com baixos níveis de desempenho.

Em seguida na ordem de alta importância e baixo desempenho surgem os indicadores da variável Expectativa de Esforço (EE) na seguinte ordenação: "**EE1** - Eu compreendo o processo de votação com a urna eletrônica"; "**EE3** - Eu acredito que é fácil aprender a votar na urna eletrônica"; e "**EE2** - É fácil votar na urna eletrônica".

Em relação ao desempenho, os indicadores com piores resultados são os da variável Influência Social (IS), sendo "**IS1** - Pessoas que influenciam meu comportamento recomendam o uso da urna eletrônica" levemente mais baixo que "**IS2** - Pessoas que são importantes para mim recomendam o uso da urna eletrônica". Novamente, por terem menores valores de importância, são menos priorizáveis que os indicadores de Expectativa de Performance (PE) e Expectativa de Esforço (EE).

Interessante destacar os resultados das variáveis relacionadas à Confiança Global (CG). Tanto a Confiança na Tecnologia (CT) quanto a Percepção de Segurança (PS) figuram

entre os piores desempenhos mas com índices de importância amplamente mais baixos que as demais variáveis.

De acordo com esses resultados, para as pessoas que anseiam pela mudança de a urna eletrônica imprimir o voto, os temas mais importantes estão relacionados aos benefícios trazidos pelo dispositivo de votação, assim como a percepção de facilidade e compreensão do seu uso. Porém, com um viés negativo ou inverso por se tratar de uma variável que representa a mudança.

Dessa forma, o que potencializa a intenção de mudança é a falta da percepção de benefícios, facilidade e compreensão de uso da urna eletrônica, ou mesmo a possibilidade de abrir mão dessas características em troca da impressão do voto.

Ou seja, a busca pela diminuição da intenção de mudança passa por ações que ampliem a percepção dos benefícios na votação com uso da urna eletrônica, em paralelo ao aumento da facilidade de uso e da compreensão do processo de votação eletrônica.

Por fim, novamente aliando a análise IPMA com os efeitos das variáveis moderadoras (Tabela 7.12), deve se considerar que, para aqueles interessados na impressão do voto, os temas relacionados a Expectativa de Performance (PE) afetam as pessoas com menos escolaridade e a Expectativa de Esforço (EE), pessoas mais velhas e com orientação poliítica à direita.

7.7.3 Propostas de melhorias priorizadas

Em virtude do contexto brasileiro, considera-se melhoria as ações que visem promover os aspectos potencializadores da inteção de uso das urnas eletrônicas, bem como reduzir aquelas que motivam a intenção de mudança para a impressão do voto, por retomarem fragilidades na proteção dos votos em papel.

Assim, considerando os resultados encontrados nas análises de Importância vs. Desempenho e que a urna eletrônica é parte de um processo maior, sugere-se a realização das seguintes ações para melhorar a confiança no sistema eletrônico de votação:

1. **Etapa 1**: Aumentar o conhecimento da sociedade sobre as características do processo eletrônico de votação.

    - No site do TSE, aprimorar a página sobre as urnas eletrônicas para explicar o processo eletrônico de votação, descrevendo de maneira simples e de fácil compreensão as etapas do processo eletrônico de votação e os mecanismos de segurança e auditoria aplicáveis em cada momento. Como referência para organizar as informações, sugere-se utiilizar o Ciclo Eleitoral do IDEA [391], ilustrado na Figura 7.12.

Figura 7.12: Ciclo Eleitoral (Adaptado de [391])

- Além de aprimorar as informações das etapas do processo eletrônico de votação, apresentar de maneira comparativa com os procedimentos realizados à época da votação manual. Dessa forma, além de conhecer melhor a solução atual, a sociedade poderá relembrar ou conhecer pela primeira vez as fragilidades que permeiam a proteção dos votos impressos para garantir que sejam contados corretamente e que motivaram a adoção da urna eletrônica.

2. **Etapa 2**: Aprimorar os mecanismos de auditoria do processo eletrônico de votação.

   - Aplicar o conceito dos Casos de Garantia (*Assurance Cases*) [392] para evidenciar que as propriedades sistema eletrônico de votação são efetivamente cumpridas. Com a aplicação dos Casos de Garantia, a sociedade terá acesso, de maneira estruturada, às evidências que a Justiça Eleitoral produz para sustentar as declarações de que o sistema é seguro, livre de fraudes, rápido, inclusivo, entre outras afirmações.

- De modo complementar, sugere-se o registro dessas evidências em uma estrutura de *blockchain* público, de modo que seja possível demonstrar a imutabilidade dos registros gerados a cada etapa do processo eletrônico de votação. Assim, reforça-se que nem mesmo a Justiça Eleitoral seria capaz de modificar as evidências disponibilizadas.
- Continuamente, ampliar o escopo do Testes Públicos de Segurança dos Sistemas Eleitorais (TPS) para refletir, com a maior fidedignidade possível, o universo de sistemas e equipamentos envolvidos no processo de votação eletrônica.
- Promover, com afinco, a participação e acompanhamento das entidades organizadas da sociedade civil nas oportunidades de auditoria.

3. **Etapa 3**: Implementar o estado da arte em auditoria e segurança de sistema eletrônico de votação.

    - Dar continuidade à implementação do método de votação fim a fim, *End-to-End* (E2E) [100], conforme tratativas iniciadas com a Universidade de São Paulo [360], para aumentar a percepção do eleitor de que seu voto é registrado como pretendido (*cast as intended*), gravado como registrado (*recorded as casted*) e contado como gravado (*tallied as recorded*).
    - Implementar a compilação determinística para geração do conjunto de softwares a ser utilizado na urna eletrônica. Esse método reproduz byte por byte os pacotes binários a partir de uma determinada fonte. Com isso, qualquer interessado pode criar cópias idênticas, a partir dos mesmos códigos fonte e ambientes de compilação [393]. A adoção desse método pode aumentar a confiança de que o código disponibilizado para auditoria pública, assinado na Cerimônia de Lacração dos Sistemas de Votação e instalado nas urnas eletrônicas é o mesmo e verificável a qualquer tempo.

4. **Etapa 4**: Aumentar os benefícios da população em utilizar as urnas eletrônicas.

    - Permitir que o voto possa ser realizado não apenas na seção eleitoral de origem do eleitor, mas em qualquer local de votação do país, resguardando-se a sua proteção para garantir o voto livre, sigiloso e sem coerção.
    - Permitir que eleitores com severas restrições de mobilidade, por exemplo tetraplégicos e acamados, possam exercer seu direto sem a necessidade do auxílio de terceiros, ou mesmo nem precise se deslocar aos locais de votação, resguardando as proteções para garantir o sigilo e segurança necessários do voto.

- Viabilizar que eleitores regularmente domiciliados no exterior possam votar nas Eleições Gerais, sem ter de obrigatoriamente se deslocar às representações diplomáticas.

Espera-se que esse conjunto de propostas tenha potencial de aumentar a intenção de uso das urnas eletrônicas brasileiras, bem como diminuir a intenção de mudança por focar nos itens de melhor relação Importância vs. Desempenho identificados neste estudo. Entrentanto, considera-se essas medidas de aprimoramento com caráter adicional ao que é realizado pela Justiça Eleitoral.

Capítulo 8

Considerações Finais

Este estudo teve como problema de pesquisa identificar quais fatores influenciam a aceitação da urna eletrônica e o interesse em imprimir o voto nas eleições brasileiras.

Como resultado, encontrou-se que a percepção de segurança e a confiança na tecnologia são as variáveis mais relevantes a influenciar a intenção de uso das urnas eletrônicas brasileiras. Para aqueles favoráveis ao uso do equipamento de votação, essas variáveis influenciam de maneira positiva, sendo percebidas como qualidades potencializadas pela digitalização do voto. Por outro lado, para os críticos, de modo ainda mais significativo, é a falta de confiança na tecnologia e baixa percepção de segurança que motivam o anseio de mudança para que o equipamento imprima o voto como medida complementar ao sistema eletrônico de votação.

Adicionalmente, o estudo verificou que a expectativa de performance, relacionada à percepção de benefícios trazidos pelo equipamento de votação, também influencia a aceitação da urna eletrônica no Brasil. Neste caso, tanto os defensores do uso da urna quanto os que desejam pela impressão do voto percebem a utilidade do equipamento ao trazer mais rapidez e facilidade ao ato de votar, sendo mais representativo para os favoráveis ao dispositivo de votação.

Ainda, os resultados apontaram que questões relacionadas à compreensão do processo de votação com a urna eletrônica, a expectativa de esforço, não são significativas para os defensores do uso do equipamento de votação. O que não se repete para os que anseiam pela impressão do voto. Para este público, essa variável é significativa e tem poder de influência.

Ademais, o estudo identificou ainda que a opinião de outras pessoas para utilizar a urna eletrônica, a influência social, é significativa para os que tem a intenção de utilizar o equipamento, mas não para aqueles que defendem a impressão do voto.

No tocante a variáveis moderadoras, o estudo revelou que os apoiadores da utilização da urna eletrônica tem a percepção de segurança e a confiança na tecnologia mais signifi-

cativas para mulheres, indivíduos mais jovens e pessoas com orientação política ao centro. Por outro lado, a expectativa de performance é significativa para os homens e a influência social para homens e pessoas à direita do espectro político.

Por sua vez, para os interessados na impressão do voto, a percepção de segurança e a confiança na tecnologia são mais sginificativas para mulheres e pessoas com orientação política ao centro e à direita. No caso da expectativa de performance, ela é mais significativa para pessoas com menor escolaridade e a expectativa de esforço, para pessoas mais velhas e de direita.

Por último, os resultados revelaram ainda que ações para reforçar a percepção de segurança e a confiança na tecnologia, bem como para a ampliar a percepção de benefícios são as mais propícias para aumentar a intenção de uso das urnas eletrônicas no Brasil, considerando terem a melhor relação alta importância e baixo desempenho.

De outro modo, para atuação junto ao público que anseia pela impressão do voto, as ações voltadas à percepção de benefícios com o uso do equipamento de votação e a compreensão do processo de votação são as que tiveram a melhor relação alta importância e baixo desempenho e são candidatas a serem priorizadas.

A partir desses resultados, o estudo apresentou um conjunto de propostas organizadas em etapas para aumentar o conhecimento da sociedade sobre as características do processo eletrônico de votação, aprimorar os mecanismos de segurança, implementar o estado da arte em auditoria de sistema eletrônico de votação e ainda aumentar os benefícios para a população em utilizar as urnas eletrônicas.

Desse modo, foi alcançado o objetivo geral definido para o estudo, que era propor etapas para melhorar a aceitação da urna eletrônica no Brasil, a partir da identificação das propriedades formadoras da confiança em sistemas de votação eletrônica.

Para alcançar o objetivo proposto, foi realizada uma pesquisa do tipo aplicada, explicativa, quantitativa e qualitativa, em um estudo de caso utilizando-se questionário.

Quanto à metodologia, foi utilizado a Teoria do Enfoque Meta Analítico (Temac) para identificar as principais abordagens e a evolução das pesquisas sobre a votação eletrônica desde 1996, ano de criação da urna eletrônica do Brasil. Posteriormente, foram apresentados os fatores que influenciam a confiança em sistemas eletrônicos de votação, bem como descrito o processo eletrônico de votação brasileiro, a partir de conceitos da Ontologia, Epistemologia e Semiótica.

Na sequência, foram avaliadas as variáveis que impactam na aceitação da urna eletrônica e o interesse na impressão do voto no Brasil, a partir de dados levantados em formulário eletrônico, disponibilizado por aplicativo de mensagem em fevereiro de 2023, cujas questões foram alicerçadas em modelo próprio, concebido com base no *Unified Theory of Acceptance and Use of Technology* (UTAUT). Ao final, utilizou-se a análise de

importância/desempenho, *Importance-Performance Map Analysis* (IPMA), para proposição de ações com intuito de aumentar a confiança nas urnas eletrônicas.

Como consequência, do ponto de vista teórico, o estudo contribui para a comunidade científica ao ampliar o campo de aplicação do modelo UTAUT para o contexto eleitoral brasileiro, algo que não se tem conhecimento de ter sido realizado anteriormente. Pelo prisma prático, as propostas apresentadas contribuem com a busca pelo aumento da confiança nas urnas eletrônicas no país. Ademais, em relação à sociedade, a pesquisa é útil e relevante por auxiliar a compreensão sobre como é construída a confiança em processos eletrônicos de votação.

Acerca das limitações do estudo, vale destacar o perfil demográfico da amostra. Quando comparada às características gerais da população brasileira, houve diferenças relevantes na distribuição por gênero e idade, mas especialmente pela escolaridade. A expressiva maioria, mais de 90%, das pessoas que responderam ao questionário possuem nível superior.

Outra limitação que merece atenção é o potencial de explicação do modelo proposto para analisar o anseio de agregar a impressão do voto à urna eletrônica. Comparando-se os 58% encontrados para explicar a variável intenção de mudança contra os 84% referentes à intenção de uso, observa-se que há lacunas no modelo que propiciam novas oportunidades para melhor entender as motivações que levam as pessoas a desejarem a implementação do voto impresso.

Nesse sentido, seja para melhorar o entendimento sobre intenção de mudar para adicionar o voto impresso ou acerca da utilização da urna eletrônica, vislumbra-se que o modelo pode ser aprimorado com a inclusão de mais variáveis relacionadas à percepção dos eleitores sobre a transparência do processo eletrônico de votação, com o uso da urna eletrônica. Acredita-se que essa variável foi considerada de maneira lateral no modelo proposto, mas merece uma atenção maior em função de sua relevância na formação da confiança nos resultados de uma eleição.

Ainda sobre aprimoramentos no modelo, pode-se pensar em avaliar também o efeito moderador das variáveis renda e raça dos eleitores na confiança das urnas eletrônicas. A avaliação dessas características da população pode proporcionar a realização de ações específicas para determinados públicos e aumentar a assertividade de tais iniciativas.

Por fim, compreende-se também a existência de oportunidade de explorar o estudo da maturidade dos processos de trabalho para realização da votação eletrônica, considerando-se os aspectos de transparência e confiança. Quão abertos e conhecidos são esses processos pela sociedade e quais garantias são disponibilizadas pela Justiça Eleitoral para formar a percepção de que eles são realizados como esperado e livre de falhas intencionais ou não? Acredita-se que a criação de um modelo de maturidade capaz de responder a esses

questionamentos seja de grande valia para ampliar a divulgação de detalhes de cada um desses processos de trabalho, bem como dessas evidências de correto funcionamento. Por óbvio, esses resultados seriam capazes de impactar a confiança no processo eletrônico de votação brasileiro.

Referências

[1] Aron, Joel D: *Information systems in perspective.* ACM Computing Surveys (CSUR), 1(4):213–236, 1969. 1

[2] Zissis, Dimitrios e Dimitrios Lekkas: *Securing e-government and e-voting with an open cloud computing architecture.* Government Information Quarterly, 28(2):239–251, 2011. 1, 26, 56

[3] Hevner, Alan R, Salvatore T March, Jinsoo Park e Sudha Ram: *Design science in information systems research.* MIS quarterly, páginas 75–105, 2004. 1

[4] Bobsin, Debora, Monize Sâmara Visentini e Ionara Rech: *Em busca do estado da arte do utaut: ampliando as considerações sobre o uso da tecnologia.* INMR-Innovation & Management Review, 6(2):99–118, 2009. 1, 4, 48, 49, 51, 52, 137

[5] Hossain, Niamat Ullah Ibne, Raed M Jaradat, Michael A Hamilton, Charles B Keating e Simon R Goerger: *A historical perspective on development of systems engineering discipline: a review and analysis.* Journal of Systems Science and Systems Engineering, 29:1–35, 2020. 1

[6] Pawlak, Michał e Aneta Poniszewska-Marańda: *Trends in blockchain-based electronic voting systems.* Information Processing & Management, 58(4):102595, 2021. 1, 23, 45, 48, 53, 54, 55, 57, 140

[7] Anane, Rachid, Richard Freeland e Georgios Theodoropoulos: *E-voting requirements and implementation.* Em *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, páginas 382–392. IEEE, 2007. 1, 23, 26, 42, 57, 58

[8] Risnanto, Slamet, Yahaya Bin Abd Rahim, Nanna Suryana Herman e A Abdurrohman: *E-voting readiness mapping for general election implementation.* Journal of Theoretical and Applied Information Technology, 98(20):3280–3290, 2020. 2, 3, 41, 47, 74, 75, 77, 78, 79, 136, 137

[9] Avgerou, Chrisanthi, Silvia Masiero e Angeliki Poulymenakou: *Trusting e-voting amid experiences of electoral malpractice: The case of indian elections.* Journal of Information Technology, 34(3):263–289, 2019. 2, 106, 136, 139

[10] Loeber, Leontine: *Use of technology in the election process: Who governs?* Election Law Journal: Rules, Politics, and Policy, 19(2):149–161, 2020. 2, 76

[11] Adida, Ben: *Advances in cryptographic voting systems*. 2006. 2, 37, 43, 52

[12] Eleitoral, Tribunal Superior: *Histórico das fraudes nas eleições*. `https://www.justicaeleitoral.jus.br/urna-eletronica/historico-das-fraudes-nas-eleicoes.html`, acesso em 2023-08-28. 2, 5, 88, 106, 108, 136

[13] Cajado, Ane Ferrari Ramos, Thiago Dornelles e Amanda Camylla Pereira: *Eleições no Brasil: uma história de 500 anos*. 2014. 2, 4, 5, 53, 88, 136

[14] Monteiro, José, Saulo Lima, Robson Rodrigues, Paulo Alvarez, Marciano Meneses, Fernando Mendonça e Rodrigo Coimbra: *Protegendo o sistema operacional e chaves criptográficas numa urna eletrônica do tipo t-dre*. Em *Anais do IV Workshop de Tecnologia Eleitoral*, páginas 1–12. SBC, 2019. 2

[15] Eleitoral, Tribunal Superior: *Auditoria e fiscalização*. `https://www.justicaeleitoral.jus.br/urna-eletronica/oportunidades-de-auditoria-e-fiscalizacao.html`, acesso em 2023-08-28. 2, 99, 100, 101, 102, 103, 104, 105

[16] Silva, Rodrigo Cardoso: *The public security test of brazilian e-voting system: the challenges in pre-electoral observation*. Em *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, páginas 349–358, 2020. 2, 107, 116, 136

[17] Pegorini, Jessica Iara, Alinne Crintinne C. Souza, Andre Roberto Ortoncelli, Rodrigo Tomaz Pagno e Newton Carlos Will: *Security and threats in the brazilian e-voting system: a documentary case study based on public security tests*. Em *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance*, páginas 157–164, 2021. 2, 26, 107, 136

[18] Aranha, Diego F e Jeroen van de Graaf: *The good, the bad, and the ugly: Two decades of e-voting in brazil*. IEEE Security & Privacy, 16(6):22–30, 2018. 2, 4, 26, 97, 136

[19] Aranha, Diego F, Pedro YS Barbosa, Thiago NC Cardoso, Caio Lüders Araújo e Paulo Matias: *The return of software vulnerabilities in the brazilian voting machine*. Computers & Security, 86:335–349, 2019. 2, 26, 106, 107

[20] Ejdys, Joanna: *Trust-based determinants of future intention to use technology*. , 14(1 (eng)):60–68, 2020. 3, 75

[21] Bayaga, Anass, Michael Kyobe e Jacques Ophoff: *Criticism of the role of trust in e-government services*. Em *2020 Conference on Information Communications Technology and Society (ICTAS)*, páginas 1–6. IEEE, 2020. 3

[22] McKnight, D Harrison, Vivek Choudhury e Charles Kacmar: *Developing and validating trust measures for e-commerce: An integrative typology*. Information systems research, 13(3):334–359, 2002. 3

[23] Roghanizad, M Mahdi e Derrick J Neufeld: *Intuition, risk, and the formation of online trust*. Computers in Human Behavior, 50:489–498, 2015. 3

[24] Pawlak, Michał, Aneta Poniszewska-Marańda e Natalia Kryvinska: *Towards the intelligent agents for blockchain e-voting system*. Procedia Computer Science, 141:239–246, 2018. 3, 29, 106

[25] AboSamra, Kareem M, Ahmed A AbdelHafez, Ghazy MR Assassa e Mona FM Mursi: *A practical, secure, and auditable e-voting system*. Journal of information security and applications, 36:69–89, 2017. 3

[26] Eleitoral, Tribunal Superior: *Eleições no brasil. a conquista da transparência e da legitimidade*. `https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/institucional/museu-do-voto/exposicoes/arquivos-1/portfolio-eleicoes-no-brasil-a-conquista-da-transparencia-e-da-legitimidade/@@download/file/exposicoes-portfolio-eleicoes-no-brasil.pdf`, acesso em 2023-08-28. 4

[27] Venkatesh, Viswanath, Michael G Morris, Gordon B Davis e Fred D Davis: *User acceptance of information technology: Toward a unified view*. MIS quarterly, páginas 425–478, 2003. 4, 48, 49, 51, 111, 138, 142, 143, 144

[28] Kim, Ki Youn, Dae Jung Kim e Bong Gyou Lee: *Pre-test analysis for first experiences of korean e-voting services*. Em *Future Information Technology: 6th International Conference, FutureTech 2011, Loutraki, Greece, June 28-30, 2011, Proceedings, Part II*, páginas 272–279. Springer, 2011. 4, 111, 137

[29] Van, Hung Trong, Myung Bae Kim, Jae Hun Sa, Jong Bae Kim e G Gim: *The factors affecting user behavior on mobile voting in vietnam*. International Journal of Multimedia and Ubiquitous Engineering, 11(6):311–318, 2016. 5, 112, 135, 137

[30] Mensah, Isaac Kofi: *Impact of performance expectancy, effort expectancy, and citizen trust on the adoption of electronic voting system in ghana*. International Journal of Electronic Government Research (IJEGR), 16(2):19–32, 2020. 5, 112, 135, 137

[31] Fuster, Rudyard e Elizabeth E Grandón: *Determinants of e-voting acceptance in chile: An approach based on the utaut model*. Em *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, páginas 1–6. IEEE, 2021. 5, 25, 112, 135, 137, 142

[32] Powell, Anne, Clay K Williams, Douglas B Bock, Thomas Doellman e Jason Allen: *e-voting intent: A comparison of young and elderly voters*. Government Information Quarterly, 29(3):361–372, 2012. 5, 112, 135, 137, 143, 144

[33] Chauhan, Sumedha, Mahadeo Jaiswal e Arpan Kumar Kar: *The acceptance of electronic voting machines in india: a utaut approach*. Electronic Government, an International Journal, 14(3):255–275, 2018. 5, 48, 52, 112, 113, 116, 117, 119, 121, 122, 127, 135, 137, 138, 142, 143, 144

[34] Eleitoral, Tribunal Superior: *Plano estratégico 2021-2026*. https://www.tse.jus.br/transparencia-e-prestacao-de-contas/governanca-gestao/plano-estrategico-2021-2026, acesso em 2023-08-28. 6

[35] Mariano, Ari Melo e Maíra Santos Rocha: *Revisão da literatura: apresentação de uma abordagem integradora*. Em *AEDEM International Conference*, volume 18, páginas 427–442, 2017. 8, 9, 10, 34, 39, 119

[36] Mu, Yi e Vijay Varadharajan: *Anonymous secure e-voting over a network*. Em *Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217)*, páginas 293–299. IEEE, 1998. 10, 23, 28

[37] Van Oyen, Mark P e Demosthenis Teneketzis: *Optimal batch service of a polling system under partial information*. Mathematical Methods of Operations Research, 44:401–419, 1996. 10

[38] Borrell, Joan e Josep Rifà: *An implementable secure voting scheme*. Computers & Security, 15(4):327–338, 1996. 11

[39] Ephrati, Eithan e Jeffrey S Rosenschein: *Deriving consensus in multiagent systems*. Artificial intelligence, 87(1-2):21–74, 1996. 11

[40] Juang, Wen Shenq e Chin Laung Lei: *A collision-free secret ballot protocol for computerized general elections*. Computers & Security, 15(4):339–348, 1996. 12

[41] McCorry, Patrick, Siamak F Shahandashti e Feng Hao: *A smart contract for boardroom voting with maximum voter privacy*. Em *Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers 21*, páginas 357–375. Springer, 2017. 14, 15, 23, 24, 36

[42] Arnott, Robert D, Jason Hsu e Philip Moore: *Fundamental indexation*. Financial Analysts Journal, 61(2):83–99, 2005. 14, 15

[43] Guo, Zhe, Xiang Li, Heng Huang, Ning Guo e Quanzheng Li: *Deep learning-based image segmentation on multimodal medical imaging*. IEEE Transactions on Radiation and Plasma Medical Sciences, 3(2):162–169, 2019. 14, 16

[44] Kshetri, Nir e Jeffrey Voas: *Blockchain-enabled e-voting*. Ieee Software, 35(4):95–99, 2018. 14, 16, 23

[45] Rikard, RV, Maxine S Thompson, Julie McKinney e Alison Beauchamp: *Examining health literacy disparities in the united states: a third look at the national assessment of adult literacy (naal)*. BMC public health, 16:1–11, 2016. 15, 16

[46] Kay, Robin H e Ann LeSage: *Examining the benefits and challenges of using audience response systems: A review of the literature*. Computers & Education, 53(3):819–827, 2009. 17

[47] Chinosi, Michele e Alberto Trombetta: *Bpmn: An introduction to the standard*. Computer Standards & Interfaces, 34(1):124–134, 2012. 17, 18

[48] Macintosh, Ann: *Characterizing e-participation in policy-making.* Em *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, páginas 10–pp. IEEE, 2004. 17, 18

[49] Neff, C Andrew: *A verifiable secret shuffle and its application to e-voting.* Em *Proceedings of the 8th ACM conference on Computer and Communications Security*, páginas 116–125, 2001. 17, 18

[50] Fernandes, Leandro AF e Manuel M Oliveira: *Real-time line detection through an improved hough transform voting scheme.* Pattern recognition, 41(1):299–314, 2008. 17, 18

[51] Moura, Teogenes e Alexandre Gomes: *Blockchain voting and its effects on election transparency and voter confidence.* Em *Proceedings of the 18th annual international conference on digital government research*, páginas 574–575, 2017. 22, 29

[52] Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram e Konstantinos Markantonakis: *E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy.* Em *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, páginas 1561–1567. IEEE, 2018. 22

[53] Little, Linda, Tim Storer, Pam Briggs e Ishbel Duncan: *E-voting in an ubicomp world: Trust, privacy, and social implications.* Social Science Computer Review, 26(1):44–59, 2008. 22

[54] Hjálmarsson, Friðrik Þ, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa e Gísli Hjálmtỳsson: *Blockchain-based e-voting system.* Em *2018 IEEE 11th international conference on cloud computing (CLOUD)*, páginas 983–986. IEEE, 2018. 22, 36

[55] Khan, Kashif Mehboob, Junaid Arshad e Muhammad Mubashir Khan: *Secure digital voting system based on blockchain technology.* International Journal of Electronic Government Research (IJEGR), 14(1):53–62, 2018. 22

[56] Tso, Raylin, Zi Yuan Liu e Jen Ho Hsiao: *Distributed e-voting and e-bidding systems based on smart contract.* Electronics, 8(4):422, 2019. 22

[57] Esgin, Muhammed F, Raymond K Zhao, Ron Steinfeld, Joseph K Liu e Dongxi Liu: *Matrict: efficient, scalable and post-quantum blockchain confidential transactions protocol.* Em *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, páginas 567–584, 2019. 22

[58] Gao, Shiyao, Dong Zheng, Rui Guo, Chunming Jing e Chencheng Hu: *An anti-quantum e-voting protocol in blockchain with audit function.* IEEE Access, 7:115304–115316, 2019. 22

[59] Shahzad, Basit e Jon Crowcroft: *Trustworthy electronic voting using adjusted blockchain technology.* Ieee Access, 7:24477–24488, 2019. 23, 24

[60] Hsiao, Jen Ho, Raylin Tso, Chien Ming Chen e Mu En Wu: *Decentralized e-voting systems based on the blockchain technology.* Em *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17*, páginas 305–309. Springer, 2018. 23

[61] Li, Jing, Xianmin Wang, Zhengan Huang, Licheng Wang e Yang Xiang: *Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing.* Journal of Parallel and Distributed Computing, 130:91–97, 2019. 23

[62] Poniszewska-Marańda, Aneta, Stanislaw Rojek e Michal Pawlak: *Decentralized electronic voting system using hyperledger fabric.* Em *2022 IEEE International Conference on Services Computing (SCC)*, páginas 339–348. IEEE, 2022. 23

[63] Mukherjee, Prodipta Promit, Arika Afrin Boshra, Mallik Mohammad Ashraf e Milon Biswas: *A hyper-ledger fabric framework as a service for improved quality e-voting system.* Em *2020 IEEE Region 10 Symposium (TENSYMP)*, páginas 394–397. IEEE, 2020. 23

[64] Yavuz, Emre, Ali Kaan Koç, Umut Can Çabuk e Gökhan Dalkılıç: *Towards secure e-voting using ethereum blockchain.* Em *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, páginas 1–7. IEEE, 2018. 23, 24

[65] Lyu, Jiazhuo, Zoe L Jiang, Xuan Wang, Zhenhao Nong, Man Ho Au e Junbin Fang: *A secure decentralized trustless e-voting system based on smart contract.* Em *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, páginas 570–577. IEEE, 2019. 23

[66] Bulut, Rumeysa, Alperen Kantarcı, Safa Keskin e Şerif Bahtiyar: *Blockchain-based electronic voting system for elections in turkey.* Em *2019 4th International Conference on Computer Science and Engineering (UBMK)*, páginas 183–188. IEEE, 2019. 23

[67] Masombuka, Mmalerato, Petrus Duvenage e Bruce Watson: *A cybersecurity imperative on an electronic voting system in south africa-2024 and beyond.* Em *ICCWS 2021 16th International Conference on Cyber Warfare and Security*, página 204. Academic Conferences Limited, 2021. 23

[68] Jumaa, Maral Hassan e Ahmed Chalak Shakir: *Iraqi e-voting system based on smart contract using private blockchain technology.* Informatica, 46(6), 2022. 23, 27

[69] Adiputra, Cosmas Krisna, Rikard Hjort e Hiroyuki Sato: *A proposal of blockchain-based electronic voting system.* Em *2018 second world conference on smart trends in systems, security and sustainability (WorldS4)*, páginas 22–27. IEEE, 2018. 23

[70] Daramola, Olawande e Darren Thebus: *Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections.* Em *Informatics*, volume 7, página 16. MDPI, 2020. 23

[71] Khan, Kashif Mehboob, Junaid Arshad e Muhammad Mubashir Khan: *Investigating performance constraints for blockchain based secure e-voting system.* Future Generation Computer Systems, 105:13–26, 2020. 23, 39, 40

[72] Baudier, Patricia, Galina Kondrateva, Chantal Ammi e Eric Seulliet: *Peace engineering: The contribution of blockchain systems to the e-voting process.* Technological Forecasting and Social Change, 162:120397, 2021. 23

[73] Nimje, Resham e DM Bhalerao: *Blockchain based electronic voting system using biometric.* Em *Sustainable Communication Networks and Application: ICSCN 2019*, páginas 746–754. Springer, 2020. 23

[74] Li, Yannan, Willy Susilo, Guomin Yang, Yong Yu, Dongxi Liu, Xiaojiang Du e Mohsen Guizani: *A blockchain-based self-tallying voting protocol in decentralized iot.* IEEE Transactions on Dependable and Secure Computing, 19(1):119–130, 2020. 23

[75] Li, Huilin, Yannan Li, Yong Yu, Baocang Wang e Kefei Chen: *A blockchain-based traceable self-tallying e-voting protocol in ai era.* IEEE transactions on network science and engineering, 8(2):1019–1032, 2020. 23

[76] Andrian, Henry Rossi, Novianto Budi Kurniawan *et al.*: *Blockchain technology and implementation: A systematic literature review.* Em *2018 international conference on information technology systems and innovation (ICITSI)*, páginas 370–374. IEEE, 2018. 23

[77] Taş, Ruhi e Ömer Özgür Tanrıöver: *A systematic review of challenges and opportunities of blockchain for e-voting.* Symmetry, 12(8):1328, 2020. 23, 45, 47

[78] Benabdallah, Ali, Antoine Audras, Louis Coudert, Nour El Madhoun e Mohamad Badra: *Analysis of blockchain solutions for e-voting: a systematic literature review.* IEEE Access, 10:70746–70759, 2022. 23

[79] Risnanto, Slamet, Yahaya Abd Rahim, Kodrat Mahatma, Asep Effendi, Hendra Garnida *et al.*: *U-vote: Ubiquitous voting model for general election in global pandemic.* Em *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, páginas 1–5. IEEE, 2020. 23

[80] Keller, Arthur M, David Mertz, Joseph Lorenzo Hall e Arnold Urken: *Privacy issues in an electronic voting machine.* Em *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, páginas 33–34, 2004. 23

[81] Moran, Tal e Moni Naor: *Split-ballot voting: everlasting privacy with distributed trust.* ACM Transactions on Information and System Security (TISSEC), 13(2):1–43, 2010. 24

[82] Ge, Huangyi, Sze Yiu Chau, Victor E Gonsalves, Huian Li, Tianhao Wang, Xukai Zou e Ninghui Li: *Koinonia: verifiable e-voting with long-term privacy.* Em *Proceedings of the 35th Annual Computer Security Applications Conference*, páginas 270–285, 2019. 24

[83] Kusters, Ralf, Tomasz Truderung e Andreas Vogt: *Clash attacks on the verifiability of e-voting systems.* Em *2012 IEEE Symposium on Security and Privacy*, páginas 395–409. IEEE, 2012. 24

[84] Cortier, Véronique, David Galindo, Ralf Küsters, Johannes Müller e Tomasz Truderung: *Sok: Verifiability notions for e-voting protocols.* Em *2016 IEEE Symposium on Security and Privacy (SP)*, páginas 779–798. IEEE, 2016. 24

[85] Iovino, Vincenzo, Alfredo Rial, Peter B Rønne e Peter YA Ryan: *Universal unconditional verifiability in e-voting without trusted parties.* Em *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, páginas 33–48. IEEE, 2020. 24

[86] García, DA López: *A flexible e-voting scheme for debate tools.* computers & security, 56:50–62, 2016. 24

[87] Zhu, Hongfei, Yu an Tan, Liehuang Zhu, Quanxin Zhang e Yuanzhang Li: *An efficient identity-based proxy blind signature for semioffline services.* Wireless Communications and Mobile Computing, 2018(1):5401890, 2018. 24

[88] Gao, Chong zhi, Jin Li, Shibing Xia, Kim Kwang Raymond Choo, Wenjing Lou e Changyu Dong: *Mas-encryption and its applications in privacy-preserving classifiers.* IEEE Transactions on Knowledge and Data Engineering, 34(5):2306–2323, 2020. 24, 40

[89] Sun, Yuhong, Shiyu Wang, Fengyin Li e Hua Wang: *A privacy preserving and format-checkable e-voting scheme.* Em *International Conference on Wireless Algorithms, Systems, and Applications*, páginas 475–488. Springer, 2022. 24

[90] Krzywiecki, Łukasz e Mirosław Kutyłowski: *Lagrangian e-voting: Verifiability on demand and strong privacy.* Em *International Conference on Trust and Trustworthy Computing*, páginas 109–123. Springer, 2010. 24

[91] Esgin, Muhammed F, Ron Steinfeld, Joseph K Liu e Dongxi Liu: *Lattice-based zero-knowledge proofs: new techniques for shorter and faster constructions and applications.* Em *Annual International Cryptology Conference*, páginas 115–146. Springer, 2019. 24

[92] Peng, Kun: *A general and efficient countermeasure to relation attacks in mix-based e-voting.* International Journal of Information Security, 10:49–60, 2011. 24

[93] Haines, Thomas e Johannes Müller: *Sok: techniques for verifiable mix nets.* Em *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, páginas 49–64. IEEE, 2020. 24

[94] Lee, Yunho, Seungjoo Kim e Dongho Won: *How to trust dre voting machines preserving voter privacy.* Em *2008 IEEE International Conference on e-Business Engineering*, páginas 302–307. IEEE, 2008. 24, 43, 55

[95] Alrodhan, Waleed A, Ali Alturbaq e Saud Aldahlawi: *A mobile biometric-based e-voting scheme.* Em *2014 World Symposium on Computer Applications & Research (WSCAR)*, páginas 1–6. IEEE, 2014. 24

[96] Petcu, Daniel e Dan Alexandru Stoichescu: *A hybrid mobile biometric-based e-voting system.* Em *2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, páginas 37–42. IEEE, 2015. 24

[97] Kiayias, Aggelos, Michael Korman e David Walluck: *An internet voting system supporting user privacy.* Em *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, páginas 165–174. IEEE, 2006. 24

[98] Zou, Xukai, Huian Li, Yan Sui, Wei Peng e Feng Li: *Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties.* Em *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, páginas 136–144. IEEE, 2014. 24

[99] Joaquim, Rui, Paulo Ferreira e Carlos Ribeiro: *Eviv: An end-to-end verifiable internet voting system.* computers & security, 32:170–191, 2013. 25

[100] Kiayias, Aggelos, Thomas Zacharias e Bingsheng Zhang: *End-to-end verifiable elections in the standard model.* Em *Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II 34*, páginas 468–498. Springer, 2015. 25, 107, 154

[101] Shahandashti, Siamak F e Feng Hao: *Dre-ip: a verifiable e-voting scheme without tallying authorities.* Em *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II 21*, páginas 223–240. Springer, 2016. 25

[102] Zhu, Yu Qian, Anik Hanifatul Azizah e Bo Hsiao: *Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries.* Information Development, 37(2):193–208, 2021. 25, 40, 46, 47, 75, 76, 136

[103] Gritzalis, Dimitris A: *Principles and requirements for a secure e-voting system.* Computers & Security, 21(6):539–556, 2002. 25, 38, 42, 57, 58, 60

[104] Chaeikar, Saman Shojae, Alireza Jolfaei, Nazeeruddin Mohammad e Pouya Ostovari: *Security principles and challenges in electronic voting.* Em *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)*, páginas 38–45. IEEE, 2021. 25

[105] Küsters, Ralf e Johannes Müller: *Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations.* Em *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings 2*, páginas 21–41. Springer, 2017. 25

[106] Kho, Yun Xing, Swee Huay Heng e Ji Jian Chin: *A review of cryptographic electronic voting.* Symmetry, 14(5):858, 2022. 25, 29, 43, 47, 55, 57, 58, 60, 61

[107] Xu, Rui, Liusheng Huang, Wei Yang e Libao He: *Quantum group blind signature scheme without entanglement.* Optics Communications, 284(14):3654–3658, 2011. 25

[108] Yin, Xun Ru, Wen Ping Ma e Wei Yan Liu: *A blind quantum signature scheme with χ-type entangled states.* International Journal of Theoretical Physics, 51:455–461, 2012. 25

[109] Zheng, Mengce, Kaiping Xue, Shangbin Li e Nenghai Yu: *A practical quantum designated verifier signature scheme for e-voting applications.* Quantum Information Processing, 20:1–22, 2021. 25

[110] Ríos-Sánchez, Belén, David Costa-da Silva, Natalia Martín-Yuste e Carmen Sánchez-Ávila: *Deep learning for facial recognition on single sample per person scenarios with varied capturing conditions.* Applied Sciences, 9(24):5474, 2019. 25

[111] Revathy, G, K Bhavana Raj, Anil Kumar, Spurthi Adibatti, Priyanka Dahiya e TM Latha: *Investigation of e-voting system using face recognition using convolutional neural network (cnn).* Theoretical Computer Science, 925:61–67, 2022. 25

[112] Mansingh, PM Benson, T Joby Titus e VS Sanjana Devi: *A secured biometric voting system using rfid linked with the aadhar database.* Em *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, páginas 1116–1119. IEEE, 2020. 25

[113] Anandaraj, S, R Anish e PV Devakumar: *Secured electronic voting machine using biometric.* Em *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, páginas 1–5. IEEE, 2015. 25, 44

[114] Cetinkaya, Orhan e Deniz Cetinkaya: *Validation and verification issues in e-voting.* Em *Proceedings of the European Conference on E-Government, ECEG*, volume 5, páginas 63–70, 2007. 26

[115] Langer, Lucie, Hugo Jonker e Wolter Pieters: *Anonymity and verifiability in voting: understanding (un) linkability.* Em *Information and Communications Security: 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010. Proceedings 12*, páginas 296–310. Springer, 2010. 26

[116] Chung, Yu Fang e Zhen Yu Wu: *Casting ballots over internet connection against bribery and coercion.* The Computer Journal, 55(10):1169–1179, 2012. 26

[117] Jamroga, Wojciech e Masoud Tabatabaei: *Preventing coercion in e-voting: Be open and commit.* Em *Electronic Voting: First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings 1*, páginas 1–17. Springer, 2017. 26, 42

[118] Hao, Yuanjing, Zhixin Zeng e Liang Chang: *An improved coercion-resistant e-voting scheme.* Security and Communication Networks, 2021(1):5448370, 2021. 26

[119] Moynihan, Donald P: *Building secure elections: e-voting, security, and systems theory.* Public administration review, 64(5):515–528, 2004. 26

[120] Kosmopoulos, Athanassios: *Aspects of regulatory and legal implications on e-voting.* Em *International Conference on Conceptual Modeling*, páginas 589–600. Springer, 2004. 26

[121] Kiayias, Aggelos, Thomas Zacharias e Bingsheng Zhang: *Ceremonies for end-to-end verifiable elections*. Em *Public-Key Cryptography–PKC 2017: 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II 20*, páginas 305–334. Springer, 2017. 26

[122] Weldemariam, Komminist, Adolfo Villafiorita e Andrea Mattioli: *Assessing procedural risks and threats in e-voting: Challenges and an approach*. Em *E-Voting and Identity: First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers 1*, páginas 38–49. Springer, 2007. 26

[123] Ramilli, Marco e Marco Prandini: *An integrated application of security testing methodologies to e-voting systems*. Em *Electronic Participation: Second IFIP WG 8.5 International Conference, ePart 2010, Lausanne, Switzerland, August 29–September 2, 2010. Proceedings 2*, páginas 225–236. Springer, 2010. 26

[124] Molnar, David, Tadayoshi Kohno, Naveen Sastry e David Wagner: *Tamper-evident, history-independent, subliminal-free data structures on prom storage-or-how to store ballots on a voting machine*. Em *2006 IEEE Symposium on Security and Privacy (S&P'06)*, páginas 6–pp. IEEE, 2006. 26

[125] Sastry, Naveen, Tadayoshi Kohno e David Wagner: *Designing voting machines for verification*. Em *USENIX Security Symposium*, 2006. 26

[126] Dunn, Michael e Laurence Merkle: *Overview of software security issues in direct-recording electronic voting machines*. Em *Proceedings of the ICCWS 2018 13th International Conference on Cyber Warfare and Security, Washington, DC, USA*, páginas 8–9, 2018. 26

[127] Gardner, Ryan W, Sujata Garera e Aviel D Rubin: *Designing for audit: A voting machine with a tiny tcb: (short paper)*. Em *Financial Cryptography and Data Security: 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers 14*, páginas 312–319. Springer, 2010. 26

[128] Villafiorita, Adolfo, Komminist Weldemariam e Roberto Tiella: *Development, formal verification, and evaluation of an e-voting system with vvpat*. IEEE Transactions on Information Forensics and Security, 4(4):651–661, 2009. 26, 43

[129] Zissis, Dimitrios e Dimitrios Lekkas: *The security paradox, disclosing source code to attain secure electronic elections*. Em *Proceedings of the 9th European Conference on e-Government*, 2009. 26

[130] Will, Mark A, Brandon Nicholson, Marc Tiehuis e Ryan KL Ko: *Secure voting in the cloud using homomorphic encryption and mobile agents*. Em *2015 International Conference on Cloud Computing Research and Innovation (ICCCRI)*, páginas 173–184. IEEE, 2015. 26

[131] Li, Chun Ta, Min Shiang Hwang e Chi Yu Liu: *An electronic voting protocol with deniable authentication for mobile ad hoc networks*. Computer Communications, 31(10):2534–2540, 2008. 26, 31

[132] Ahmad, Tohari, Jiankun Hu e Song Han: *An efficient mobile voting system security scheme based on elliptic curve cryptography.* Em *2009 Third International Conference on Network and System Security*, páginas 474–479. IEEE, 2009. 26, 56

[133] Iyamu, Tiko: *Creating a technical architecture framework for m-voting application.* African Journal of Science, Technology, Innovation and Development, 14(1):86–93, 2022. 26, 56

[134] Langer, Lucie: *Towards legally binding online elections in germany.* Em *Proceedings of the 4th International Conference on E-government: ICEG 2008*, página 247. Citeseer, 2008. 26

[135] Buckland, Richard e Roland Wen: *The future of e-voting in australia.* IEEE Security & Privacy, 10(5):25–32, 2012. 26

[136] Halderman, J Alex e Vanessa Teague: *The new south wales ivote system: Security failures and verification flaws in a live online election.* Em *E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5*, páginas 35–53. Springer, 2015. 26

[137] Essex, Aleksander e Nicole Goodman: *Protecting electoral integrity in the digital age: developing e-voting regulations in canada.* Election Law Journal: Rules, Politics, and Policy, 19(2):162–179, 2020. 26, 62

[138] Kassen, Maxat: *Politicization of e-voting rejection: reflections from kazakhstan.* Transforming Government: People, Process and Policy, 14(2):305–330, 2020. 26

[139] Johnson, Nathan, Brian M Jones e Kyle Clendenon: *E-voting in america: Current realities and future directions.* Em *Social Computing and Social Media. Human Behavior: 9th International Conference, SCSM 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I 9*, páginas 337–349. Springer, 2017. 26

[140] Abba, Abdullahi Lawal, Mohammed Awad, Zakaria Al-Qudah e Abdul Halim Jallad: *Security analysis of current voting systems.* Em *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, páginas 1–6. IEEE, 2017. 26

[141] Heiberg, Sven e Jan Willemson: *Verifiable internet voting in estonia.* Em *2014 6th international conference on electronic voting: Verifying the vote (evote)*, páginas 1–8. IEEE, 2014. 26

[142] Mpekoa, Noluntu e Darelle Van Greunen: *E-voting experiences: A case of namibia and estonia.* Em *2017 IST-Africa Week Conference (IST-Africa)*, páginas 1–8. IEEE, 2017. 26, 27

[143] Yilmaz, Savaş e Isa Sertkaya: *Improving the individual verification of estonian internet voting scheme.* Em *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*, páginas 38–47. IEEE, 2020. 26

[144] Nurse, Jason RC, Ioannis Agrafiotis, Arnau Erola, Maria Bada, Taylor Roberts, Meredydd Williams, Michael Goldsmith e Sadie Creese: *An assessment of the security and transparency procedural components of the estonian internet voting system*. Em *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5*, páginas 366–383. Springer, 2017. 26

[145] Schryen, Guido e Eliot Rich: *Security in large-scale internet elections: a retrospective analysis of elections in estonia, the netherlands, and switzerland*. IEEE Transactions on Information Forensics and Security, 4(4):729–744, 2009. 26, 27

[146] Sivaraman, PR, R Jaiganesh, P Ragupathy e R Ramkumar: *Hi-tech electoral machine for election commission of india*. Biosc. Biotech. Res. Comm. Special Issue, 13(3):13–17, 2020. 27

[147] Sensuse, Dana Indra, Pandu Bintang Pratama *et al.*: *Conceptual model of e-voting in indonesia*. Em *2020 International Conference on Information Management and Technology (ICIMTech)*, páginas 387–392. IEEE, 2020. 27

[148] Saputri, Zuyina Ayuning, Amang Sudarsono e Mike Yuliana: *E-voting security system for the election of eepis bem president*. Em *2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)*, páginas 147–152. IEEE, 2017. 27

[149] Hisamitsu, Hiroki e Keiji Takeda: *The security analysis of e-voting in japan*. Em *E-Voting and Identity: First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers 1*, páginas 99–110. Springer, 2007. 27

[150] Ansper, Arne, Sven Heiberg, Helger Lipmaa, Tom André Øverland e Filip Van Laenen: *Security and trust for the norwegian e-voting pilot project e-valg 2011*. Em *Nordic Conference on Secure IT Systems*, páginas 207–222. Springer, 2009. 27

[151] Cortier, Véronique e Cyrille Wiedling: *A formal analysis of the norwegian e-voting protocol*. Em *Principles of Security and Trust: First International Conference, POST 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24-April 1, 2012, Proceedings 1*, páginas 109–128. Springer, 2012. 27, 47

[152] Heiberg, Sven, Helger Lipmaa e Filip Van Laenen: *On e-vote integrity in the case of malicious voter computers*. Em *Computer Security–ESORICS 2010: 15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22, 2010. Proceedings 15*, páginas 373–388. Springer, 2010. 27

[153] AlAbri, Raya, Abdul Khalique Shaikh, Saqib Ali e Ali Hamad Al-Badi: *Designing an e-voting framework using blockchain technology: A case study of oman*. International Journal of Electronic Government Research (IJEGR), 18(2):1–29, 2022. 27

[154] Shat, Fouad e Elias Pimenidis: *Social media and e-voting–a secure and trusted political forum for palestine*. Em *Global Security, Safety and Sustainability-The Security Challenges of the Connected World: 11th International Conference, ICGS3 2017, London, UK, January 18-20, 2017, Proceedings 11*, páginas 290–302. Springer, 2016. 27

[155] Hao, Feng, Shen Wang, Samiran Bag, Rob Procter, Siamak F Shahandashti, Maryam Mehrnezhad, Ehsan Toreini, Roberto Metere e Lana YJ Liu: *End-to-end verifiable e-voting trial for polling station voting*. IEEE Security & Privacy, 18(6):6–13, 2020. 27, 40

[156] Gibson, J Paul, Robert Krimmer, Vanessa Teague e Julia Pomares: *A review of e-voting: the past, present and future*. Annals of Telecommunications, 71:279–286, 2016. 27, 42

[157] Pieters, Wolter: *Acceptance of voting technology: between confidence and trust*. Em *International Conference on Trust Management*, páginas 283–297. Springer, 2006. 27, 46, 47

[158] Yao, Yurong e Lisa Murphy: *Remote electronic voting systems: an exploration of voters' perceptions and intention to use*. European Journal of Information Systems, 16(2):106–120, 2007. 27

[159] Distler, Verena, Marie Laure Zollinger, Carine Lallemand, Peter B Roenne, Peter YA Ryan e Vincent Koenig: *Security-visible, yet unseen?* Em *Proceedings of the 2019 CHI conference on human factors in computing systems*, páginas 1–13, 2019. 27

[160] Palas Nogueira, João e Filipe de Sá-Soares: *Trust in e-voting systems: a case study*. Em *Knowledge and Technologies in Innovative Information Systems: 7th Mediterranean Conference on Information Systems, MCIS 2012, Guimaraes, Portugal, September 8-10, 2012. Proceedings*, páginas 51–66. Springer, 2012. 27

[161] Rana, Ahmed, Ibrahim Zincir e Samsun Basarici: *The security and the credibility challenges in e-voting systems*. Em *European Conference on Cyber Warfare and Security*, página 229. Academic Conferences International Limited, 2015. 27

[162] Sampigethaya, Krishna e Radha Poovendran: *A framework and taxonomy for comparison of electronic voting schemes*. computers & security, 25(2):137–153, 2006. 27, 43, 53, 57

[163] Bryans, Jeremy W, Bev Littlewood, Peter YA Ryan e Lorenzo Strigini: *E-voting: Dependability requirements and design for dependability*. Em *First International Conference on Availability, Reliability and Security (ARES'06)*, páginas 8–pp. IEEE, 2006. 27

[164] Escala, Alex, Sandra Guasch, Javier Herranz e Paz Morillo: *Universal cast-as-intended verifiability*. Em *International Conference on Financial Cryptography and Data Security*, páginas 233–250. Springer, 2016. 28

[165] Cortier, Véronique e Joseph Lallemand: *Voting: You can't have privacy without individual verifiability.* Em *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, páginas 53–66, 2018. 28

[166] Smyth, Ben e Michael R Clarkson: *Surveying definitions of election verifiability.* Information Processing Letters, 177:106267, 2022. 28

[167] Kiong, NC e A Samsudin: *Incoercible secure electronic voting scheme based on chaffing and winnowing.* Em *9th Asia-Pacific Conference on Communications (IEEE Cat. No. 03EX732)*, volume 2, páginas 838–843. IEEE, 2003. 28

[168] Fan, Chun I e Wei Zhe Sun: *Uncoercible anonymous electronic voting.* Em *9th Joint International Conference on Information Sciences (JCIS-06)*, páginas 373–377. Atlantis Press, 2006. 28

[169] Fan, Chun I e Wei Zhe Sun: *An efficient multi-receipt mechanism for uncoercible anonymous electronic voting.* Mathematical and Computer Modelling, 48(9-10):1611–1627, 2008. 28

[170] Benaloh, Josh, Tal Moran, Lee Naish, Kim Ramchen e Vanessa Teague: *Shufflesum: coercion-resistant verifiable tallying for stv voting.* IEEE Transactions on Information Forensics and Security, 4(4):685–698, 2009. 28

[171] Bruschi, Danilo, Fiorella De Cindio, D Ferrazzi, Giusi Poletti e Emilia Rosti: *Internet voting: Do people accept it? do they trust it?* Em *Proceedings. 13th International Workshop on Database and Expert Systems Applications*, página 437. IEEE, 2002. 28

[172] Riedl, Reinhard: *Rethinking trust and confidence in european e-government: Linking the public sector with post-modern society.* Em *Building the E-Service Society: E-Commerce, E-Business, and E-Government*, páginas 89–108. Springer, 2004. 28

[173] Baudron, Olivier, Pierre Alain Fouque, David Pointcheval, Jacques Stern e Guillaume Poupard: *Practical multi-candidate election system.* Em *Proceedings of the twentieth annual ACM symposium on Principles of distributed computing*, páginas 274–283, 2001. 28

[174] Ibrahim, Subariah, Maznah Kamat, Mazleena Salleh e Shah Rizan Abdul Aziz: *Secure e-voting with blind signature.* Em *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.*, páginas 193–197. IEEE, 2003. 28, 30

[175] Saini, Sanjay e Joydip Dhar: *An eavesdropping proof secure online voting model.* Em *2008 International Conference on Computer Science and Software Engineering*, volume 3, páginas 704–708. IEEE, 2008. 28

[176] Anggriane, Shifa Manaruliesya, Surya Michrandi Nasution e Fairuz Azmi: *Advanced e-voting system using paillier homomorphic encryption algorithm.* Em *2016 International Conference on Informatics and Computing (ICIC)*, páginas 338–342. IEEE, 2016. 28

[177] Gomułkiewicz, Marcin, Marek Klonowski e Mirosław Kutyłowski: *Rapid mixing and security of chaum's visual electronic voting.* Em *European Symposium on Research in Computer Security*, páginas 132–145. Springer, 2003. 28

[178] Yang, Xuechao, Xun Yi, Surya Nepal e Fengling Han: *Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain.* Em *Web Information Systems Engineering–WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part I 19*, páginas 18–35. Springer, 2018. 28

[179] Sundar, D Sam e Nitin Narayan: *A novel voting scheme using quantum cryptography.* Em *2014 IEEE Conference on Open Systems (ICOS)*, páginas 66–71. IEEE, 2014. 28

[180] Shi, Wei Min, Yi Hua Zhou e Yu Guang Yang: *A real quantum designated verifier signature scheme.* International Journal of Theoretical Physics, 54:3115–3123, 2015. 28

[181] Iftene, Sorin: *General secret sharing based on the chinese remainder theorem with applications in e-voting.* Electronic Notes in Theoretical Computer Science, 186:67–84, 2007. 28

[182] Malina, Lukas, Jan Hajny, Petr Dzurenda e Sara Ricci: *Lightweight ring signatures for decentralized privacy-preserving transactions.* Em *ICETE (2)*, páginas 692–697, 2018. 28

[183] Rajendra, AB e HS Sheshadri: *Visual cryptography in internet voting system.* Em *Third International Conference on Innovative Computing Technology (INTECH 2013)*, páginas 60–64. IEEE, 2013. 28

[184] Naidu, P Sanyasi, Reena Kharat, Ruchita Tekade, Pallavi Mendhe e Varsha Magade: *E-voting system using visual cryptography & secure multi-party computation.* Em *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, páginas 1–4. IEEE, 2016. 28

[185] Rura, Lauretha, Biju Issac e Manas Kumar Haldar: *Secure electronic voting system based on image steganography.* Em *2011 IEEE Conference on Open Systems*, páginas 80–85. IEEE, 2011. 28

[186] Rura, Lauretha, Biju Issac e Manas Kumar Haldar: *Implementation and evaluation of steganography based online voting system.* International Journal of Electronic Government Research (IJEGR), 12(3):71–93, 2016. 28

[187] Davtyan, Seda, Aggelos Kiayias, Laurent Michel, Alexander Russell e Alexander A Shvartsman: *Integrity of electronic voting systems: fallacious use of cryptography.* Em *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, páginas 1486–1493, 2012. 28

[188] Han, Wei, Dong Zheng e Ke fei Chen: *Filling the gap between voters and cryptography in e-voting.* Journal of Shanghai Jiaotong University (Science), 14:257–260, 2009. 28

[189] Neumann, Stephan, Oksana Kulyk e Melanie Volkamer: *A usable android application implementing distributed cryptography for election authorities*. Em *2014 Ninth International Conference on Availability, Reliability and Security*, páginas 207–216. IEEE, 2014. 28

[190] Malkhi, Dahlia, Ofer Margo e Elan Pavlov: *E-voting without 'cryptography' extended abstract*. Em *Financial Cryptography: 6th International Conference, FC 2002 Southampton, Bermuda, March 2002 Revised Papers 6*, páginas 1–15. Springer, 2003. 29

[191] Rivest, Ronald L e Warren D Smith: *Three voting protocols: Threeballot, vav, and twin*. USENIX/ACCURATE Electronic Voting Technology (EVT 2007), 2007. 29

[192] Arnaud, Mathilde, Véronique Cortier e Cyrille Wiedling: *Analysis of an electronic boardroom voting system*. Em *E-Voting and Identify: 4th International Conference, Vote-ID 2013, Guildford, UK, July 17-19, 2013. Proceedings 4*, páginas 109–126. Springer, 2013. 29

[193] Uzunay, Yusuf e Kemal Bicakci: *Trusted3ballot: improving security and usability of three ballot voting system using trusted computing*. Em *2014 5th International Conference on Intelligent Systems, Modelling and Simulation*, páginas 534–539. IEEE, 2014. 29

[194] Wagner, David: *Cryptographic protocols for electronic voting*. Em *Advances in Cryptology-CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings 26*, páginas 393–393. Springer, 2006. 29

[195] Cetinkaya, Orhan: *Analysis of security requirements for cryptographic voting protocols*. Em *2008 Third International Conference on Availability, Reliability and Security*, páginas 1451–1456. IEEE, 2008. 29

[196] Moayed, Majid Javid, Abdul Azim Abdul Ghani e Ramlan Mahmod: *A survey on cryptography algorithms in security of voting system approaches*. Em *2008 International Conference on Computational Sciences and its Applications*, páginas 190–200. IEEE, 2008. 29

[197] Carr, LeRoy, Anthony J Newtson e James Joshi: *Towards modernizing the future of american voting*. Em *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, páginas 130–135. IEEE, 2018. 29

[198] Khandelwal, Amish: *Blockchain implimentation on e-voting system*. Em *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, páginas 385–388. IEEE, 2019. 29

[199] Agbesi, Samuel e George Asante: *Electronic voting recording system based on blockchain technology*. Em *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, páginas 1–8. IEEE, 2019. 29

[200] Adeshina, Steve A e Adegboyega Ojo: *Maintaining voting integrity using blockchain.* Em *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, páginas 1–5. IEEE, 2019. 29

[201] Srivastava, Gautam, Ashutosh Dhar Dwivedi e Rajani Singh: *Crypto-democracy: A decentralized voting scheme using blockchain technology.* Em *15th International Joint Conference on e-Business and Telecommunications. ICETE 2018*, páginas 508–513. SCITEPRESS Digital Library, 2018. 29

[202] Pawlak, Michał, Jakub Guziur e Aneta Poniszewska-Marańda: *Voting process with blockchain technology: auditable blockchain voting system.* Em *Advances in Intelligent Networking and Collaborative Systems: The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018)*, páginas 233–244. Springer, 2019. 29

[203] Cucurull, Jordi e Jordi Puiggali: *Distributed immutabilization of secure logs.* Em *Security and Trust Management: 12th International Workshop, STM 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings 12*, páginas 122–137. Springer, 2016. 29

[204] Sudharsan, B, Nidhish Krishna MP, M Alagappan *et al.*: *Secured electronic voting system using the concepts of blockchain.* Em *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, páginas 0675–0681. IEEE, 2019. 29

[205] Alfain, Zidna Wildan, Hermawan Setiawan e I Komang Setia Buana: *Analysis of centralized vs decentralized electronic voting.* Em *2022 IEEE 8th Information Technology International Seminar (ITIS)*, páginas 173–177. IEEE, 2022. 29

[206] Hanifatunnisa, Rifa e Budi Rahardjo: *Blockchain based e-voting recording system design.* Em *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, páginas 1–6. IEEE, 2017. 29

[207] Patidar, Kriti e Swapnil Jain: *Decentralized e-voting portal using blockchain.* Em *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, páginas 1–4. IEEE, 2019. 29

[208] Jafar, Uzma, Mohd Juzaiddin Ab Aziz e Zarina Shukur: *Blockchain for electronic voting system—review and open research challenges.* Sensors, 21(17):5874, 2021. 29, 45, 47

[209] Huang, Jun, Debiao He, Mohammad S Obaidat, Pandi Vijayakumar, Min Luo e Kim Kwang Raymond Choo: *The application of the blockchain technology in voting systems: A review.* ACM Computing Surveys (CSUR), 54(3):1–28, 2021. 29

[210] Sahib, Rihab H e Eman S Al-Shamery: *A review on distributed blockchain technology for e-voting systems.* Em *Journal of Physics: Conference Series*, volume 1804, página 012050. IOP Publishing, 2021. 29

[211] Saraf, Chinmay e Siddharth Sabadra: *Blockchain platforms: A compendium*. Em *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, páginas 1–6. IEEE, 2018. 29

[212] Jafar, Uzma e Mohd Juzaiddin Ab Aziz: *A state of the art survey and research directions on blockchain based electronic voting system*. Em *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, páginas 248–266. Springer, 2021. 29

[213] Donepudi, Swapna e K Thammi Reddy: *Comparing and elucidating blockchain based voting mechanisms*. Em *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, páginas 1181–1185. IEEE, 2022. 29

[214] Varaprasada Rao, K e Sandeep Kumar Panda: *Secure electronic voting (e-voting) system based on blockchain on various platforms*. Em *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2*, páginas 143–151. Springer, 2022. 29

[215] Anilkumar, Vysakh, Joseph Antony Joji, Asif Afzal e Reshma Sheik: *Blockchain simulation and development platforms: survey, issues and challenges*. Em *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, páginas 935–939. IEEE, 2019. 29

[216] Odaudu, Salefu Ngbede, Umoh J Imeh e Umar Abubakar: *Bids: Blockchain based intrusion detection system for electoral process*. Em *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, páginas 1–15. IEEE, 2019. 30

[217] Abuidris, Yousif, Abdelrhman Hassan, Abdalla Hadabi e Issameldeen Elfadul: *Risks and opportunities of blockchain based on e-voting systems*. Em *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*, páginas 365–368. IEEE, 2019. 30

[218] Alvi, Syada Tasmia, Linta Islam, Tamanna Yesmin Rashme e Mohammed Nasir Uddin: *Bsevoting: A conceptual framework to develop electronic voting system using sidechain*. Em *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, páginas 10–15. IEEE, 2021. 30

[219] Kohad, Hemlata Wamanrao, Sunil Kumar e Asha Ambhaikar: *Design of a novel side chaining model for improving the performance of security aware e-voting applications*. Em *Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022*, páginas 13–28. Springer, 2023. 30

[220] Cucurull, Jordi, Adrià Rodríguez-Pérez, Tamara Finogina e Jordi Puiggali: *Blockchain-based internet voting: systems' compliance with international standards*. Em *Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers 21*, páginas 300–312. Springer, 2019. 30

[221] Khan, Kashif Mehboob, Junaid Arshad e Muhammad Mubashir Khan: *Simulation of transaction malleability attack for blockchain-based e-voting*. Computers & Electrical Engineering, 83:106583, 2020. 30

[222] Khan, Kashif Mehboob, Junaid Arshad e Muhammad Mubashir Khan: *Empirical analysis of transaction malleability within blockchain-based e-voting*. Computers & Security, 100:102081, 2021. 30

[223] Cheema, Muhammad Asaad, Nouman Ashraf, Asad Aftab, Hassaan Khaliq Qureshi, Muhammad Kazim e Ahmad Taher Azar: *Machine learning with blockchain for secure e-voting system*. Em *2020 first international conference of smart systems and emerging technologies (SMARTTECH)*, páginas 177–182. IEEE, 2020. 30

[224] Ali, Youssef Abdelrahman Fekry, Omar Tarek Mohamed Ahmed, Mohamad Ahmad Mohamad Diab, Mohamed Abd Elhalim Sayed, Mohamed Khaled Abd Elaziz e Bassam W Aboshosha: *Blockchain-based online e-voting system*. Em *2023 International Conference on Smart Computing and Application (ICSCA)*, páginas 1–8. IEEE, 2023. 30

[225] Gupta, Sweta, Aparna Gupta, Ishan Y Pandya, Abhishek Bhatt e Komal Mehta: *End to end secure e-voting using blockchain & quantum key distribution*. Materials Today: Proceedings, 80:3363–3370, 2023. 30

[226] Alvi, Syada Tasmia, Mohammed Nasir Uddin e Linta Islam: *Digital voting: A blockchain-based e-voting system using biohash and smart contract*. Em *2020 third international conference on smart systems and inventive technology (ICSSIT)*, páginas 228–233. IEEE, 2020. 30

[227] Alam, Asraful, SM Zia Ur Rashid, Md Abdus Salam e Ariful Islam: *Towards blockchain-based e-voting system*. Em *2018 international conference on innovations in science, engineering and technology (ICISET)*, páginas 351–354. IEEE, 2018. 30

[228] Han, Gang, Yannan Li, Yong Yu, Kim Kwang Raymond Choo e Nadra Guizani: *Blockchain-based self-tallying voting system with software updates in decentralized iot*. IEEE Network, 34(4):166–172, 2020. 30

[229] Toma, Cristian, Marius Popa, Catalin Boja, Cristian Ciurea e Mihai Doinea: *Secure and anonymous voting d-app with iot embedded device using blockchain technology*. Electronics, 11(12):1895, 2022. 30

[230] Echchaoui, Hanane, Boudrali Roumaissa e Rachid Boudour: *A proposal of blockchain and nfc-based electronic voting system*. Em *International Conference on Artificial Intelligence in Renewable Energetic Systems*, páginas 66–75. Springer, 2022. 30

[231] Agbehadji, Israel Edem, Abdultaofeek Abayomi, Richard C Millham e Owusu Nyarko-Boateng: *Blockchain technology adoption for general elections during covid-19 pandemic and beyond*. Em *Computational Intelligence and Data Analytics: Proceedings of ICCIDA 2022*, páginas 533–549. Springer, 2022. 30

[232] Vivek, SK, RS Yashank, Yashas Prashanth, N Yashas e M Namratha: *E-voting systems using blockchain: An exploratory literature survey.* Em *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, páginas 890–895. IEEE, 2020. 30

[233] Xiao, Shuai, Xu An Wang, Wei Wang e Han Wang: *Survey on blockchain-based electronic voting.* Em *Advances in Intelligent Networking and Collaborative Systems: The 11th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2019)*, páginas 559–567. Springer, 2020. 30

[234] Salman, Saba Abdul Baqi, Sufyan Al-Janabi e Ali Makki Sagheer: *A review on e-voting based on blockchain models.* Iraqi Journal of Science, páginas 1362–1375, 2022. 30

[235] Weiss, Dylan, Jacob Wolmer e Avimanyou Vatsa: *Blockchain-based electronic voting system for modern democracy: a review.* Em *2022 Ieee Integrated Stem Education Conference (ISEC)*, páginas 162–166. IEEE, 2022. 30

[236] Jafar, Uzma, Mohd Juzaiddin Ab Aziz, Zarina Shukur e Hafiz Adnan Hussain: *A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems.* Sensors, 22(19):7585, 2022. 30

[237] Vladucu, Maria Victoria, Ziqian Dong, Jorge Medina e Roberto Rojas-Cessa: *E-voting meets blockchain: A survey.* IEEE Access, 11:23293–23308, 2023. 30

[238] Al-Ameen, Abdalla e Samani A Talab: *The technical feasibility and security of e-voting.* Int. Arab J. Inf. Technol., 10(4):397–404, 2013. 30

[239] Kavakli, Evangelia, Stefanos Gritzalis e Kalloniatis Christos: *Protecting privacy in system design: the electronic voting case.* Transforming Government: People, Process and Policy, 1(4):307–332, 2007. 30

[240] Li, Peng, Junzuo Lai e Yongdong Wu: *Publicly traceable attribute-based anonymous authentication and its application to voting.* Security and Communication Networks, 2021(1):6611518, 2021. 30

[241] Deng, X, CH Lee e H Zhu: *Deniable authentication protocols.* IEE Proceedings-Computers and Digital Techniques, 148(2):101–104, 2001. 31

[242] Rizal Nurjaman, Asep e Ari Moesriami Barmawi: *Strengthening the security of deniable authentication scheme using zero-knowledge proof.* Em *Proceedings of the 2021 11th International Conference on Communication and Network Security*, páginas 27–34, 2021. 31

[243] Yeow, Kin Woon, Syh Yuan Tan, Swee Huay Heng e Rouzbeh Behnia: *Applications of undeniable signature schemes.* Em *2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, páginas 133–138. IEEE, 2015. 31

[244] Teranishi, Isamu, Jun Furukawa e Kazue Sako: *K-times anonymous authentication.* Em *International Conference on the Theory and Application of Cryptology and Information Security*, páginas 308–322. Springer, 2004. 31

[245] Nguyen, Lan e Rei Safavi-Naini: *Dynamic k-times anonymous authentication.* Em *Applied Cryptography and Network Security: Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005. Proceedings 3*, páginas 318–333. Springer, 2005. 31

[246] Chaieb, Marwa, Souheib Yousfi, Pascal Lafourcade e Riadh Robbana: *Verify-your-vote: A verifiable blockchain-based online voting protocol.* Em *Information Systems: 15th European, Mediterranean, and Middle Eastern Conference, EMCIS 2018, Limassol, Cyprus, October 4-5, 2018, Proceedings 15*, páginas 16–30. Springer, 2019. 31

[247] Gutub, Adnan, Nouf Al-Juaid e Esam Khan: *Counting-based secret sharing technique for multimedia applications.* Multimedia Tools and Applications, 78:5591–5619, 2019. 31

[248] Khasawneh, Mohammed, Mohammad Malkawi, Omar Al-Jarrah, Laith Barakat, Thaier S Hayajneh e Munzer S Ebaid: *A biometric-secure e-voting system for election processes.* Em *2008 5th international symposium on mechatronics and its applications*, páginas 1–8. IEEE, 2008. 31, 44

[249] Hof, Sonja: *E-voting and biometric systems?* 2004. 32, 44, 55

[250] Okokpujie, Kennedy, Noma Osaghae Etinosa, Samuel John e Etta Joy: *Comparative analysis of fingerprint preprocessing algorithms for electronic voting processes.* Em *IT Convergence and Security 2017: Volume 2*, páginas 212–219. Springer, 2018. 32

[251] Ibrahim, Mohamed, Kajan Ravindran, Hyon Lee, Omair Farooqui e Qusay H Mahmoud: *Electionblock: an electronic voting system using blockchain and fingerprint authentication.* Em *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*, páginas 123–129. IEEE, 2021. 32

[252] Komatineni, Sudeepthi e Gowtham Lingala: *Secured e-voting system using two-factor biometric authentication.* Em *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, páginas 245–248. IEEE, 2020. 32

[253] Okokpujie, KO, Samuel Ndueso John, Etinosa Noma-Osaghae, Charles Ndujiuba e IP Okokpujie: *An enhanced voters registration and authentication application using iris recognition technology.* International Journal of Civil Engineering and Technology (IJCIET), 10(2):57–68, 2019. 32

[254] Sharma, Sapna e Shilpy Agrawal: *Personal authentication based on vascular pattern using finger vein biometric.* Journal of Discrete Mathematical Sciences and Cryptography, 24(5):1167–1178, 2021. 32

[255] Watson, Anthony e Vincent Cordonnier: *Voting in the new millennium: evoting holds the promise to expand citizen choice.* Em *Electronic Government: First International Conference, EGOV 2002 Aix-en-Provence, France, September 2–6, 2002 Proceedings 1*, páginas 234–239. Springer, 2002. 32

[256] Kofler, Robert, Robert Krimmer, Alexander Prosser e M K Unger: *The role of digital signature cards in electronic voting.* Em *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, páginas 7–pp. IEEE, 2004. 32

[257] Rathee, Geetanjali, Razi Iqbal, Omer Waqar e Ali Kashif Bashir: *On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities.* IEEE Access, 9:34165–34176, 2021. 32

[258] Falkner, Stefanie, Peter Kieseberg, Dimitris E Simos, Christina Traxler e Edgar Weippl: *E-voting authentication with qr-codes.* Em *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2*, páginas 149–159. Springer, 2014. 32

[259] Chaum, David L: *Untraceable electronic mail, return addresses, and digital pseudonyms.* Communications of the ACM, 24(2):84–90, 1981. 35, 37

[260] Chaum, David: *Blind signatures for untraceable payments.* Em *Advances in Cryptology: Proceedings of Crypto 82*, páginas 199–203. Springer, 1983. 35

[261] Fujioka, Atsushi, Tatsuaki Okamoto e Kazuo Ohta: *A practical secret voting scheme for large scale elections.* Em *Advances in Cryptology—AUSCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques Gold Coast, Queensland, Australia, December 13–16, 1992 Proceedings 3*, páginas 244–251. Springer, 1993. 35, 38

[262] Rivest, Ronald L, Adi Shamir e Yael Tauman: *How to leak a secret.* Em *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, páginas 552–565. Springer, 2001. 35

[263] Chaum, David: *Secret-ballot receipts: True voter-verifiable elections.* IEEE security & privacy, 2(1):38–47, 2004. 36

[264] Paillier, Pascal: *Public-key cryptosystems based on composite degree residuosity classes.* Em *International conference on the theory and applications of cryptographic techniques*, páginas 223–238. Springer, 1999. 36, 38

[265] Juels, Ari, Dario Catalano e Markus Jakobsson: *Coercion-resistant electronic elections.* Em *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, páginas 61–70, 2005. 36, 37

[266] Adida, Ben: *Helios: Web-based open-audit voting.* Em *USENIX security symposium*, volume 17, páginas 335–348, 2008. 36, 37

[267] Clarkson, Michael R, Stephen Chong e Andrew C Myers: *Civitas: Toward a secure voting system.* Em *2008 IEEE Symposium on Security and Privacy (sp 2008)*, páginas 354–368. IEEE, 2008. 36

[268] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson e Byoungcheon Lee: *Multiplicative homomorphic e-voting*. Em *International Conference on Cryptology in India*, páginas 61–72. Springer, 2004. 36

[269] Cramer, Ronald, Ivan Damgård e Berry Schoenmakers: *Proofs of partial knowledge and simplified design of witness hiding protocols*. Em *Annual International Cryptology Conference*, páginas 174–187. Springer, 1994. 36

[270] Alvarez, R Michael, Thad E Hall e Alexander H Trechsel: *Internet voting in comparative perspective: the case of estonia*. PS: Political Science & Politics, 42(3):497–505, 2009. 36

[271] Sako, Kazue e Joe Kilian: *Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth*. Em *Advances in Cryptology—EUROCRYPT'95: International Conference on the Theory and Application of Cryptographic Techniques Saint-Malo, France, May 21–25, 1995 Proceedings 14*, páginas 393–403. Springer, 1995. 37

[272] Benaloh, Josh Daniel Cohen: *Verifiable secret-ballot elections*. Yale University, 1987. 37

[273] Fiat, Amos e Adi Shamir: *How to prove yourself: Practical solutions to identification and signature problems*. Em *Conference on the theory and application of cryptographic techniques*, páginas 186–194. Springer, 1986. 38

[274] Nakamoto, Satoshi e A Bitcoin: *A peer-to-peer electronic cash system*. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2):15, 2008. 38, 47

[275] Jackman, Simon: *Measuring electoral bias: Australia, 1949–93*. British Journal of Political Science, 24(3):319–357, 1994. 38

[276] Gerlach, Jan e Urs Gasser: *Three case studies from switzerland: E-voting*. Berkman Center Research Publication No, 3(2009):2020–2021, 2009. 38

[277] Mote Jr, CD: *Report of the national workshop on internet voting: issues and research agenda*. Em *Proceedings of the 2002 annual national conference on Digital government research*, páginas 1–59, 2002. 38

[278] Downs, Anthony: *An economic theory of political action in a democracy*. Journal of political economy, 65(2):135–150, 1957. 38

[279] Norris, Pippa: *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge university press, 2001. 38

[280] Pratchett, Lawrence: *The Implementation of Electronic Voting in the UK*. Local Government Association, 2002. 38

[281] Xenakis, Alexandros e Ann Macintosh: *Major issues in electronic voting in the context of the uk pilots*. Journal of E-government, 1(1):53–74, 2004. 38

[282] Caldarelli, Giulio e Joshua Ellul: *Trusted academic transcripts on the blockchain: A systematic literature review.* Applied Sciences, 11(4):1842, 2021. 39

[283] Alharbi, Ayman, Haneen Zamzami e Eman Samkri: *Survey on homomorphic encryption and address of new trend.* International Journal of Advanced Computer Science and Applications, 11(7), 2020. 39

[284] Kshetri, Naresh, Chandra Sekhar Bhushal, Purnendu Shekhar Pandey *et al.*: *Bct-cs: Blockchain technology applications for cyber defense and cybersecurity: A survey and solutions.* International Journal of Advanced Computer Science and Applications, 13(11), 2022. 39

[285] Niu, Xu Feng, Wen Ping Ma, Bu Qing Chen, Ge Liu e Qi Zheng Wang: *A quantum proxy blind signature scheme based on superdense coding.* International Journal of Theoretical Physics, 59:1121–1128, 2020. 40

[286] Feng, Hanwen, Jianwei Liu, Dawei Li, Ya Nan Li e Qianhong Wu: *Traceable ring signatures: general framework and post-quantum security.* Designs, Codes and Cryptography, 89:1111–1145, 2021. 40

[287] Haines, Thomas, Sarah Jamie Lewis, Olivier Pereira e Vanessa Teague: *How not to prove your election outcome.* Em *2020 IEEE Symposium on Security and Privacy (SP)*, páginas 644–660. IEEE, 2020. 40

[288] Challa, Ratnakumari: *Homomorphic encryption: Review and applications.* Advances in Data Science and Management: Proceedings of ICDSM 2019, páginas 273–281, 2020. 40

[289] Kulyk, Oksana, Melanie Volkamer, Monika Müller e Karen Renaud: *Towards improving the efficacy of code-based verification in internet voting.* Em *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24*, páginas 291–309. Springer, 2020. 40

[290] Annapurna, K, V Chandrani, P Mounika e P Teja Sree: *Design of authenticated radio frequency identification based electronic voting machine.* Em *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, páginas 658–665. IEEE, 2021. 40

[291] Musiał-Karg, Magdalena e Izabela Kapsa: *Polish mass media coverage and public opinion on e-democracy. the case of electronic voting.* Media Studies, 12(23):3–18, 2021. 40

[292] Kalynovskyi, Bohdan, Andrii Khalota, Pavlo Horodnytskyi e Daryna Radomska: *Use of electronic forms of direct democracy: international experience and perspective ukrainians.* Cuestiones Políticas, 40(72), 2022. 40

[293] Janusz, Andrew e Cameron Sells: *Race and campaign resources: candidate identification numbers in brazil.* Journal of Politics in Latin America, 14(2):211–223, 2022. 40

[294] Ch, Venkateswara Rao *et al.*: *Arduino based electronic voting system with biometric and gsm features*. Em *2022 4th international conference on smart systems and inventive technology (ICSSIT)*, páginas 685–688. IEEE, 2022. 41

[295] Liu, Qiang e Hailin Zhang: *Reliability evaluation of weighted voting system based on d–s evidence theory*. Reliability Engineering & System Safety, 217:108079, 2022. 41

[296] Nguyen, Tuong Ngoc, Anh The Ta, Huy Quoc Le, Dung Hoang Duong, Willy Susilo, Fuchun Guo, Kazuhide Fukushima e Shinsaku Kiyomoto: *Efficient unique ring signatures from lattices*. Em *European Symposium on Research in Computer Security*, páginas 447–466. Springer, 2022. 41

[297] Cortier, Véronique, Pierrick Gaudry e Quentin Yang: *A toolbox for verifiable tally-hiding e-voting systems*. Em *European Symposium on Research in Computer Security*, páginas 631–652. Springer, 2022. 41

[298] Devillez, Henri, Olivier Pereira e Thomas Peters: *How to verifiably encrypt many bits for an election?* Em *European Symposium on Research in Computer Security*, páginas 653–671. Springer, 2022. 41

[299] Darmawan, Ikhsan: *E-voting adoption in many countries: A literature review*. Asian Journal of Comparative Politics, 6(4):482–504, 2021. 46

[300] Grove, Jeff: *Acm statement on voting systems*. Communications of the ACM, 47(10):69–70, 2004. 46

[301] King, Merle S e Brian Hancock: *Electronic voting security 10 years after the help america vote act*. IEEE Security & Privacy, 10(5):50–52, 2012. 47

[302] Jonker, Hugo, Sjouke Mauw e Jun Pang: *Privacy and verifiability in voting systems: Methods, developments and trends*. Computer Science Review, 10:1–30, 2013. 47, 61, 62

[303] Mercuri, Rebecca T: *Trusting in transparency*. Communications of the ACM, 48(5):15–19, 2005. 47

[304] Evans, David e Nathanael Paul: *Election security: Perception and reality*. IEEE Security & Privacy, 2(1):24–31, 2004. 47, 75

[305] Xenakis, Alexandros e Ann Macintosh: *Trust analysis of the uk e-voting pilots*. Social Science Computer Review, 23(3):312–325, 2005. 47

[306] Ehin, Piret e Mihkel Solvak: *Party cues and trust in remote internet voting: data from estonia 2005–2019*. Em *Electronic Voting: 6th International Joint Conference, E-Vote-ID 2021, Virtual Event, October 5–8, 2021, Proceedings 6*, páginas 75–90. Springer, 2021. 47

[307] Avgerou, Chrisanthi: *Explaining trust in it-mediated elections: A case study of e-voting in brazil*. Journal of the Association for Information Systems, 14(8):2, 2013. 47, 85, 86, 106, 136

[308] Pomares, Julia, Ines Levin, R Michael Alvarez, Guillermo Lopez Mirau e Teresa Ovejero: *From piloting to roll-out: voting experience and trust in the first full e-election in argentina*. Em *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, páginas 1–10. IEEE, 2014. 47

[309] Christian Schaupp, L e Lemuria Carter: *E-voting: from apathy to adoption*. Journal of Enterprise Information Management, 18(5):586–601, 2005. 47

[310] Oostveen, Anne Marie e Peter Van Den Besselaar: *Trust, identity, and the effects of voting technologies on voting behavior*. Social Science Computer Review, 23(3):304–311, 2005. 47

[311] Tranoska Srbinoska, Elizabeta, Smilka Janeska Sarkanjac e Branislav Sarkanjac: *Voting technologies: from ostracon to e-voting*. 2022. 48, 52

[312] Fishbein, Martin e Icek Ajzen: *Belief, attitude, intention, and behavior: An introduction to theory and research*. 1977. 49

[313] Davis, Fred D, Richard P Bagozzi e Paul R Warshaw: *User acceptance of computer technology: A comparison of two theoretical models*. Management science, 35(8):982–1003, 1989. 49

[314] Vallerand, Robert J: *Toward a hierarchical model of intrinsic and extrinsic motivation*. Em *Advances in experimental social psychology*, volume 29, páginas 271–360. Elsevier, 1997. 49

[315] Ajzen, Icek: *The theory of planned behavior*. Organizational behavior and human decision processes, 50(2):179–211, 1991. 49

[316] Taylor, Shirley e Peter A Todd: *Understanding information technology usage: A test of competing models*. Information systems research, 6(2):144–176, 1995. 49

[317] Thompson, Ronald L, Christopher A Higgins e Jane M Howell: *Personal computing: Toward a conceptual model of utilization*. MIS quarterly, páginas 125–143, 1991. 49

[318] Moore, Gary C e Izak Benbasat: *Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users*. Em *Diffusion and Adoption of Information Technology: Proceedings of the first IFIP WG 8.6 working conference on the diffusion and adoption of information technology, Oslo, Norway, October 1995*, páginas 132–146. Springer, 1996. 49

[319] Compeau, Deborah R e Christopher A Higgins: *Application of social cognitive theory to training for computer skills*. Information systems research, 6(2):118–143, 1995. 49

[320] Rogers, Everett M: *Diffusion of innovations: modifications of a model for telecommunications*. Die diffusion von innovationen in der telekommunikation, páginas 25–38, 1995. 50

[321] Williams, Michael D, Nripendra P Rana e Yogesh K Dwivedi: *The unified theory of acceptance and use of technology (utaut): a literature review*. Journal of enterprise information management, 28(3):443–488, 2015. 50, 52, 111

[322] Venkatesh, Viswanath, James YL Thong e Xin Xu: *Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology*. MIS quarterly, páginas 157–178, 2012. 52

[323] Poddar, Varsha, Sayan Mondal, Neelava Dutta e Hrishab Dey: *Incorporating advancements in voting strategies: A survey*. Em *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, páginas 249–254. IEEE, 2018. 52, 53

[324] Europe, Concil of: *Recommendation cm/rec(2017)5 of the committee of ministers to member states on standards for e-voting*. `https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f`, acesso em 2023-08-05. 53, 62, 69, 74

[325] Popoveniuc, Stefan: *A framework for secure mixnet-based electronic voting*. Tese de Doutoramento, The George Washington University, 2009. 54

[326] Rosales, Sandra I Bautista, Chadwick Carreto Arellano, Eduardo Bustos Farías e Luis Enrique Hernández Olvera: *Model and architecture of mobile electronic voting*. 54

[327] Willemson, Jan: *Bits or paper: which should get to carry your vote?* Journal of information security and applications, 38:124–131, 2018. 55, 108

[328] Eleitoral, Tribunal Superior: *Cronologia da informatização do processo eleitoral*. `https://www.justicaeleitoral.jus.br/urna-eletronica/cronologia-da-informatizacao-do-processo-eleitoral.html`, acesso em 2023-07-23. 56, 57

[329] Fouard, Laure, Mathilde Duclos e Pascal Lafourcade: *Survey on electronic voting schemes*. supported by the ANR project AVOTÉ, 2007. 57

[330] Comission, United States Election Assitance: *Voluntary voting system guidelines*. `https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf`, acesso em 2023-08-05. 62, 69, 92

[331] Warkentin, Merrill, Shwadhin Sharma, David Gefen, Gregory M Rose e Paul Pavlou: *Social identity and trust in internet-based voting adoption*. Government Information Quarterly, 35(2):195–209, 2018. 74, 77

[332] Alvarez, R Michael, Gabriel Katz e Julia Pomares: *The impact of new technologies on voter confidence in latin america: Evidence from e-voting experiments in argentina and colombia*. Journal of Information Technology & Politics, 8(2):199–217, 2011. 74, 75, 82, 116, 145

[333] Mensah, Isaac Kofi e Samuel Adams: *A comparative analysis of the impact of political trust on the adoption of e-government services.* International Journal of Public Administration, 43(8):682–696, 2020. 74

[334] Sztompka, Piotr: *Trust: A sociological theory.* Cambridge university press, 1999. 74

[335] Paliszkiewicz, J: *Organizational trust–a critical review of the empirical research.* Em *Proceedings of 2010 international conference on technology innovation and industrial management*, volume 1618, 2010. 75

[336] Paliszkiewicz, Joanna Olga: *Trust management: literature review.* Management (18544223), 6(4), 2011. 75

[337] Wolf, Peter, Rushdi Nackerdien e Domenico Tuccinardi: *Introducing electronic voting: essential considerations.* International Institute for Democracy and Electoral Assistance . . . , 2011. 79

[338] GARNETT ANN, H. et al: *Electoral integrity global report. 2023.* `https://static1.squarespace.com/static/58533f31bebafbe99c85dc9b/t/649dee1ee6e6c50219e9fbd9/1688071716978/Electoral+Integrity+Global+Report+2023.pdf`, acesso em 2023-08-19. 83, 84, 85

[339] Santano, Ana Claudia: *As narrativas e as necessidades: o sistema eletrônico de votação brasileiro a partir de uma análise de política pública.* A&C-Revista de Direito Administrativo & Constitucional, 22(88):75–101, 2022. 88, 138, 140

[340] Graaf, Jeroen van de e Ricardo Felipe Custodio: *Tecnologia eleitoral e a urna eletrônica.* Relatório Técnico, Technical report, Universidade Federal de Minas Gerais, Universidade Federal de Santa Catarina, 2002. 88, 106, 137, 140

[341] Tolk, Andreas: *M&s body of knowledge: Progress report and look ahead.* SCS M&S Magazine, 4(4), 2010. 89, 90

[342] Tolk, Andreas, Saikou Y Diallo e Jose J Padilla: *Semiotics, entropy, and interoperability of simulation systems—mathematical foundations of m&s standardization.* Em *Proceedings of the 2012 Winter Simulation Conference (WSC)*, páginas 1–12. IEEE, 2012. 89

[343] Ogden, Charles Kay e Ivor Armstrong Richards: *The Meaning of Meaning: A Study of the Influence of Language upon Thought and of the Science of Symbolism.* Harcourt, Brace, 1927. 89, 90

[344] Gharajedaghi, Jamshid: *Systems thinking: Managing chaos and complexity: A platform for designing business architecture.* Elsevier, 2011. 91, 92

[345] Cybersecurity e Infrastructure Security Agency: *Election infrastructure cyber risk assessment. critical infrastructure security and resilience note.* `https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf`, acesso em 2024-02-25. 93

[346] Model, Electoral Maturity: *Terminology*. https://electoralmaturity.com/emm-initiative/terminology/, acesso em 2024-02-25. 94

[347] Brasil, Presidência da República do: *Constituição da república federativa do brasil de 1998*. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, acesso em 2024-03-03. 97, 98, 101

[348] Eleitoral, Tribunal Superior: *Normas e documentação – eleições 2022*. https://www.tse.jus.br/eleicoes/eleicoes-2022/normas-e-documentacoes/normas-e-documentacoes-eleicoes-2022, acesso em 2024-03-03. 98

[349] Brasil, Presidência da República do: *Lei nº 9.504 de 30 de setembro de 1997*. https://www.planalto.gov.br/ccivil_03/leis/l9504.htm, acesso em 2024-03-03. 98, 101, 102, 105

[350] Eleitoral, Tribunal Superior: *Resolução nº 23.669, de 14 de dezembro de 2021*. https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-669-de-14-de-dezembro-de-2021, acesso em 2024-03-03. 98, 101, 102, 103, 104, 105

[351] Eleitoral, Tribunal Superior: *Resolução nº 23.673, de 14 de dezembro de 2021*. https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021, acesso em 2024-03-03. 98, 99, 100, 101, 104, 105

[352] Eleitoral, Tribunal Superior: *Detalhes técnicos da urna eletrônica*. https://www.justicaeleitoral.jus.br/urna-eletronica/detalhes-tecnicos-da-urna.html, acesso em 2024-03-03. 99, 136

[353] Eleitoral, Tribunal Superior: *Universidades validam nova urna e códigos-fonte dos sistemas eleitorais*. https://www.tse.jus.br/comunicacao/noticias/2022/Agosto/universidades-validam-nova-urna-e-codigos-fonte-dos-sistemas-eleitorais-357621, acesso em 2024-03-03. 100

[354] Eleitoral, Tribunal Superior: *Resolução nº 23.444, de 30 de abril de 2015*. https://www.tse.jus.br/legislacao/codigo-eleitoral/normas-editadas-pelo-tse/resolucao-no-23-444-de-30-de-abril-de-2015-2013-brasilia-2013-df, acesso em 2024-03-03. 101

[355] Eleitoral, Tribunal Superior: *Resumos digitais (hashes) dos sistemas eleitorais*. https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/hash/resumos-digitais-hash-dos-sistemas-eleitorais, acesso em 2024-03-03. 103, 105

[356] Eleitoral, Tribunal Superior: *Portal de dados abertos*. https://dadosabertos.tse.jus.br, acesso em 2024-03-03. 104, 105

[357] Eleitoral, Tribunal Superior: *Estatísticas eleitorais*. https://www.tse.jus.br/eleicoes/estatisticas/estatisticas, acesso em 2024-03-03. 104, 105

[358] Rodrigues Filho, José: *E-voting and the creation of trust for the socially marginalized citizens in brazil*. JeDEM-eJournal of eDemocracy and Open Government, 2(2):184–193, 2010. 106

[359] Rivest, Ronald L: *On the notion of 'software independence'in voting systems*. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 366(1881):3759–3767, 2008. 107

[360] Eleitoral, Tribunal Superior: *Equipes do tse e da usp trabalham na inovação do sistema eletrônico de votação*. https://www.tse.jus.br/comunicacao/noticias/2022/Maio/equipes-do-tse-e-da-usp-trabalham-na-inovacao-do-sistema-eletronico-de-votacao, acesso em 2024-03-28. 107, 154

[361] Deputados, Câmara dos: *Proposta de emenda à constituição pec 135/2019*. https://www.camara.leg.br/propostas-legislativas/2220292, acesso em 2024-03-23. 107

[362] Eleitoral, Tribunal Superior: *Análise sobre a impressão do voto*. https://www.justicaeleitoral.jus.br/urna-eletronica/impressao-do-voto.html, acesso em 2024-03-23. 108

[363] Defesa, Ministério da: *Atuação das forças armadas em apoio ao tse no aprimoramento da segurança e transparência do processo eleitoral*. https://www.gov.br/defesa/pt-br/acesso-a-informacao/outros/atuacao-das-forcas-armadas-em-apoio-ao-tse-no-aprimoramento-da-seguranca-e-trans atuacao-das-forcas-armadas-em-apoio-ao-tse-no-aprimoramento-da-seguranca-e-trans acesso em 2024-03-23. 109

[364] Minas, Estado de: *Live de argentino sobre urnas causa furor nas redes bolsonaristas*. https://www.em.com.br/app/noticia/politica/2022/11/04/interna_politica,1417415/live-de-argentino-sobre-urnas-causa-furor-nas-redes-bolsonaristas.shtml#google_vignette, acesso em 2024-03-24. 109

[365] 360, Poder: *Partido de bolsonaro pede que tse invalide mais da metade dos votos*. https://www.poder360.com.br/justica/partido-de-bolsonaro-pede-que-tse-invalide-mais-da-metade-dos-votos, acesso em 2024-03-24. 109

[366] USP, Jornal da: *Relatório da usp atesta eleição absolutamente normal, apesar do clima beligerante no país*. https://jornal.usp.br/universidade/uma-eleicao-absolutamente-normal-apesar-do-clima-beligerante-no-pais, acesso em 2024-03-24. 109

[367] Atlas, Pesquisa: *Eleições brasil 2022*. https://bit.ly/3LIu8xn, acesso em 2024-03-24. 109

[368] Atlas, Pesquisa: *Eleições brasil 2022*. https://cdn.atlasintel.org/6a898327-1314-440c-be5a-aa1989554813.pdf, acesso em 2024-03-24. 109

[369] Transportes, Confederação Nacional dos: *Estudos e pesquisas. rodadas 149, 152 e 153*. https://www.cnt.org.br/pesquisas, acesso em 2024-03-24. 109, 139

[370] Folha, Data: *Cresce confiança nas urnas eletrônicas*. https://bit.ly/462UMdA, acesso em 2024-03-24. 109

[371] Jota: *Pesquisa aponta que 40urnas eletrônicas*. https://www.jota.info/eleicoes/pesquisa-aponta-que-40-dos-brasileiros-confiam-muito-nas-urnas-eletroni acesso em 2024-03-24. 109

[372] Uol, Política: *Quaest: crece confiança nas urnas, apesar de ataques de bolsonaro*. https://noticias.uol.com.br/politica/ultimas-noticias/2022/08/04/quaest-cresce-confianca-nas-urnas-apesar-de-ataques-de-bolsonaro.htm, acesso em 2024-03-24. 109

[373] Chalabi, Mohammed, Hazura Mohamed e Muriati Mukhtar: *The validation of an e-voting adoption model using focus group*. Em *2021 International Conference on Electrical Engineering and Informatics (ICEEI)*, páginas 1–6. IEEE, 2021. 111, 116

[374] Ruediger, Marco Aurelio, Amaro Grassi, Tatiana Dourado, Polyana Barboza, Victor Piaia e Dalby Hubert: *Desinformação on-line e contestação das eleições*. 2022. 116, 140, 146

[375] Gil, Antônio Carlos: *Como elaborar projetos de pesquisa*. Editora Atlas SA, 2002. 118

[376] Da Silva, Edna Lucia e Estera Muszkat Menezes: *Metodologia da pesquisa e elaboração de dissertação*. UFSC, Florianópolis, 4a. edição, 123(4):138, 2005. 118, 119

[377] Hair Jr, Joseph F, G Tomas M Hult, Christian M Ringle, Marko Sarstedt, Nicholas P Danks e Soumya Ray: *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer Nature, 2021. 122

[378] Hair Jr, Joe F, Marko Sarstedt, Lucas Hopkins e Volker G Kuppelwieser: *Partial least squares structural equation modeling (pls-sem): An emerging tool in business research*. European business review, 26(2):106–121, 2014. 123, 130, 131, 132, 133

[379] Hair, Joe F, Christian M Ringle e Marko Sarstedt: *Pls-sem: Indeed a silver bullet*. Journal of Marketing theory and Practice, 19(2):139–152, 2011. 123, 130, 131, 132, 133, 134

[380] Sarstedt, Marko, Joseph F Hair Jr, Jun Hwa Cheah, Jan Michael Becker e Christian M Ringle: *How to specify, estimate, and validate higher-order constructs in pls-sem*. Australasian marketing journal, 27(3):197–211, 2019. 123, 127, 129

[381] Ringle, Christian M, Sven Wende, Jan Michael Becker *et al.*: *Smartpls 4*, 2024. 124, 133

[382] Ramírez, Patricio E, Ari Melo Mariano e Evangelina A Salazar: *Propuesta metodológica para aplicar modelos de ecuaciones estructurales con pls: El caso del uso de las bases de datos científicas en estudiantes universitarios*. Revista ADMpg, 7(2), 2014. 124

[383] Ringle, Christian M e Marko Sarstedt: *Gain more insight from your pls-sem results: The importance-performance map analysis*. Industrial management & data systems, 116(9):1865–1886, 2016. 124, 148

[384] IBGE: *Panorama censo 2022*. `https://censo2022.ibge.gov.br/panorama/indicadores.html?localidade=BR`, acesso em 2024-04-21. 124, 125

[385] Educa, IBGE: *Conheça o brasil – população – educação*. `https://encurtador.com.br/h5ce6`, acesso em 2024-04-21. 126

[386] Federal, Senado: *Datasenado, pesquisa panorama político 2023*. `https://www12.senado.leg.br/institucional/datasenado/publicacaodatasenado?id=panorama-politico-2023`, acesso em 2024-04-21. 126

[387] Russo, Daniel e Klaas Jan Stol: *Pls-sem for software engineering research: An introduction and survey*. ACM Computing Surveys (CSUR), 54(4):1–38, 2021. 128, 133

[388] Hair, Joseph F, Jeffrey J Risher, Marko Sarstedt e Christian M Ringle: *When to use and how to report the results of pls-sem*. European business review, 31(1):2–24, 2019. 130

[389] Fornell, Claes e David F Larcker: *Evaluating structural equation models with unobservable variables and measurement error*. Journal of marketing research, 18(1):39–50, 1981. 131

[390] Chin, Wynne W *et al.*: *The partial least squares approach to structural equation modeling*. Modern methods for business research, 295(2):295–336, 1998. 133

[391] Catt, Helena, A Ellis, M Maley, A Wall e P Wolf: *Electoral management design. international idea*. Institute for Democracy and Electoral Assistance, 2014. 152, 153

[392] Denney, Ewen e Ganesh Pai: *Tool support for assurance case development*. Automated Software Engineering, 25(3):435–499, 2018. 153

[393] Zottmann, Carlos Eduardo Miranda, João José Costa Gondim, Thiago Melo Stuckert do Amaral, Edvan Gomes da Silva e Rafael Rabelo Nunes: *Comparação de abordagens de proteção à cadeia de suprimento de software*. Revista Ibérica de Sistemas e Tecnologias de Informação, (E70):657–675, 2024. 154